EMERSON WENDT

AS EXPECTATIVAS COGNITIVAS E NORMATIVAS DOS ATORES DE INVESTIGAÇÃO POLICIAL EM FACE DOS CRIMES CIBERNÉTICOS.

CANOAS, 2023

EMERSON WENDT

AS EXPECTATIVAS COGNITIVAS E NORMATIVAS DOS ATORES DE INVESTIGAÇÃO POLICIAL EM FACE DOS CRIMES CIBERNÉTICOS.

Tese de Doutorado apresentada e aprovada com Louvor no Programa de Pós-Graduação em Direito – Doutorado, Área de Concentração 'Direito e Sociedade', da Universidade La Salle Canoas.

Orientação: Prof.ª Dr.ª Renata Almeida da Costa

CANOAS, 2023

Dados Internacionais de Catalogação na Publicação (CIP)

W473e Wendt, Emerson.
As expectativas cognitivas e normativas dos atores de investigação policial em face dos crimes cibernéticos [manuscrito] / Emerson Wendt – 2023.
305 f.; 30 cm.

Tese (doutorado em Direito) – Universidade La Salle, Canoas, 2023.
"Orientação: Profa. Dra. Renata Almeida da Costa".

1.Direito. 2. Legislação penal e processual penal – Internet. 3. Teoria Geral dos Sistemas Sociais. I. Costa, Renata Almeida da. II. Título.

CDU: **343.451**

Bibliotecário responsável: Melissa Rodrigues Martins - CRB 10/1380

EMERSON WENDT

Tese aprovada como requisito parcial para obtenção do título de Doutor no Programa de Pós-Graduação em Direito – Doutorado, Área de Concentração ‘Direito e Sociedade’, da Universidade La Salle Canoas.

BANCA EXAMINADORA

Prof. Dr. Artur Stamford da Silva
Universidade Federal de Pernambuco

Prof. Dr. Matteo Finco
Università degli Sudi “La Sapienza” di Roma

Prof. Dr. Dani Rudnicki
Universidade La Salle

Prof. Dr. Diógenes Hassan Ribeiro
Universidade La Salle

Profª. Dra. Renata Almeida da Costa
Universidade La Salle

Área de concentração: Direito e Sociedade
Curso: Doutorado Acadêmico em Direito

Canoas, 28 de abril de 2023.

Documento com assinaturas digitais dos participantes da banca.

A Deus, por me permitir o autoconhecimento e por indicar o caminho a seguir, mesmo quando isso importe em angústia e sofrimento. Aos meus pais, Nilo e Neli, por me mostrarem que existem vários caminhos possíveis.

AGRADECIMENTOS

Agradeço às pessoas que sempre estiveram ao meu lado nesta caminhada em busca do doutoramento. Em especial, Valquiria, Luiz e Anna, com quem constituí um sistema chamado família. Ao meu pai, Nilo, um sistema psíquico formidável e amável, do qual tenho a honra de descender: ensinaste-me o essencial, ser simples e humilde.

Agradeço à Universidade La Salle, por meio de seu programa de bolsas institucionais, a me permitir os estudos neste Doutorado. Aos professores do PPPG da Universidade La Salle de Canoas/RS, por me propiciarem a autorreflexão, a autocrítica e o autoaprendizado. Em especial, à Coordenadora do PPGD e minha orientadora, Profª Drª Renata Almeida da Costa, que sempre me reconduziu ao caminho correto da pesquisa e da busca pela tese e sua proximidade da perfeição.

Aos professores Artur Stamford da Silva, Aldo Mascareño e Germano Schwartz, pelos ensinamentos e debates longínquos sobre a Teoria Geral dos Sistemas Sociais. Agradecimento, também, não pode deixar de ser feito às colegas do PPGD e entusiastas da TGSS, Karen Rubin e Juliana Bloise, pelos debates *off topic* e sempre interessantes da interpelação entre as percepções de Luhmann e a evolução da tecnologia digital, esta não vivenciada por ele.

Aos colegas policiais, agentes e delegados, de todas as unidades especializadas das Polícias Civis, responsáveis pela investigação cibernética. Em especial, aqueles que aceitaram participar das entrevistas programadas durante a pesquisa para o conteúdo da tese. Suas perspectivas são a base importante do contexto crítico deste trabalho.

Aos integrantes do Observatório de Segurança Pública de Canoas, pelos debates sobre metodologias e análises. Enfim, aos colegas e amigos, de vários guetos e tribos, que sempre me brindaram com seu carinho e amizade.

“É impossível não comunicar.”
[Teoria da Comunicação, Escola de Palo Alto, Paul Watzlawick e Gregory Bateson]

As verdades não são perenes ou imutáveis. Permitir à co
percepcionar e recepcionar novas informações é conser
evolução e administrar as complexidades.
[Emerson Wendt]

RESUMO

A presente tese aborda o tema da produção legislativa e normativa, nas áreas penal e processual penal, em relação à Internet e ao ciberespaço no Brasil, com análise a partir das expectativas cognitivas e expectativas normativas dos atores da investigação policial em face dos fatos e situações caracterizados como crimes cibernéticos, sob a perspectiva da Teoria Geral dos Sistemas Sociais, a partir de Niklas Luhmann (1983). A pesquisa procura, então, a partir do método de abordagem hipotético-dedutivo, responder quais são e como repercutem comunicativamente as expectativas cognitivas e normativas dos atores de investigação policial ante (a) a legislação brasileira [penal e processual penal] que absorveu formalmente no sistema do Direito aspectos atinentes da Internet e (b) em relação à estrutura de enfrentamento aos crimes cibernéticos. Parte-se da compreensão da Internet como um cibersistema, que propicia, a partir dos dados e informações, consubstanciados em uma programação binária 0/1 (zero e um) e com um código funcional conexão/desconexão, a interação, a ampliação e a transformação cultural na comunicação digital, e, por isso, ela é objeto de estudo da Sociologia do Direito, da cibersociologia, como prática de observação dessa relação no ciberespaço para além do Direito, incluindo a interação complexa e crítica dos aspectos tecnológicos, culturais e políticos (administrativos). A partir da observação empírica, com a utilização de entrevistas de integrantes das Polícias Civis no Brasil que atuam em órgãos especializados na investigação cibernética, busca-se conhecer quais são suas expectativas cognitivas e normativas, e as correspondentes frustrações e desapontamentos, sobre a estrutura normativa e procedimental de enfrentamento aos crimes no âmbito da rede de computadores, especialmente como e se comunicam essas circunstâncias aos demais sistemas sociais, especialmente o sistema político. Verifica-se que a expectativa desses atores de investigação criminal existe e é condicionada ao procedimento normativo, porém não impede a geração da reflexividade de expectativas, especificamente as cognitivas sobre as normativas, o que não significa, porém, que essas perspectivas sejam efetivamente e diretamente comunicadas aos demais sistemas, havendo um *gap* comunicacional entre o sistema psíquico e o sistema político. Também, utilizando-se de revisão documental, legislativa e normativa, conclui-se que a informação, eventualmente produzida pelo investigador cibernético, somente é recepcionada pelo legislador pela via indireta, ou seja, pelos veículos de comunicação social, os quais reproduzem, basicamente, as falas oficiais em suas notícias, mantenedoras de um sistema penal e processual focado em

criação e ampliação de novos tipos penais, além da ampliação das sanções penais já existentes, não dando a atenção expectável às regras procedimentais e/ou capazes de auxiliar na redução e mitigação de danos na Internet.

Palavras-chave: Expectativas cognitivas; Expectativas normativas; Internet; Legislação penal e processual penal; Teoria Geral dos Sistemas Sociais.

ABSTRACT

This thesis addresses the issue of legislative and normative production, in the criminal and criminal procedural areas, in relation to the Internet and cyberspace in Brazil, with an analysis based on the cognitive expectations and normative expectations of the actors of the police investigation in the face of facts and situations characterized as cybercrimes, from the perspective of the General Theory of Social Systems, from Niklas Luhmann (1983). The research seeks, then, from the hypothetical-deductive method of approach, to answer what they are and how they communicatively resonate the cognitive and normative expectations of the actors of police investigation before (a) the Brazilian legislation [criminal and criminal procedure] that formally absorbed in the system of Law concerning aspects of the Internet and (b) in relation to the structure for confronting cybercrimes. It starts from the understanding of the Internet as a cybersystem, which provides, from data and information, consubstantiated in a binary programming 0/1 (zero and one) and with a connection/disconnection functional code, the interaction, expansion and cultural transformation in digital communication, and, therefore, it is the object of study of the Sociology of Law, of cybersociology, as a practice of observing this relationship in cyberspace beyond Law, including the complex and critical interaction of technological, cultural and political aspects (administrative). From empirical observation, with the use of interviews with members of the Civil Police in Brazil who work in bodies specialized in cybernetic investigation, we seek to know what are their cognitive and normative expectations, and the corresponding frustrations and disappointments, about the normative structure and procedural aspects of coping with crimes within the computer network, especially how and if these circumstances are communicated to other social systems, especially the political system. It appears that the expectation of these criminal investigation actors exists and is conditioned to the normative procedure, but it does not prevent the generation of reflexivity of expectations, specifically the cognitive ones about the normative ones, which does not mean, however, that these perspectives are effectively and directly communicated to the other systems, with a communicational gap between the psychic system and the political system. Also, using a documentary, legislative and normative review, it is concluded that the information, eventually produced by the cybernetic investigator, is only received by the legislator indirectly, that is, by the media, which reproduce, basically, the official lines in their news, maintainers of a criminal and procedural system, focused on the

creation and expansion of new criminal types, in addition to the expansion of existing criminal sanctions, not giving the expected attention to procedural rules and/or capable of helping to reduce Internet harm mitigation.

Keywords: Cognitive expectations; Normative expectations; Internet; Criminal law and criminal procedure; General Theory of Social Systems.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

A presente tese tem como tema a produção legislativa e normativa em relação à Internet e ao ciberespaço no Brasil, especialmente quanto às áreas penal e processual penal, e as correspondentes expectativas cognitivas e expectativas normativas dos atores da investigação policial em face dos crimes cibernéticos, sob a perspectiva da Teoria Geral dos Sistemas Sociais, a partir de Niklas Luhmann (1983).

Objetivando delimitar o foco do tema, parte-se da circunstância de que a Internet, como um cibersistema, propicia, a partir dos dados consubstanciados em uma programação binária 0/1 (zeros e uns), a interação e a transformação cultural na comunicação digital, permitindo aos usuários com comportamentos divergentes a exploração de novas técnicas e condutas que causem danos [a usuários e sistemas] e a obtenção de dados e informações. Por isso, justifica-se a Internet também como um objeto de estudo da Sociologia do Direito, para fins desta tese a cibersociologia, mediante a análise do risco derivado dos comportamentos divergentes no ambiente cibernético, das transformações tecnoculturais da sociedade e das correspondentes e possíveis mutações normativas.

Para fins da presente observação, tem-se como divergente a conduta que, em determinado tempo e espaço[1], está convencionalmente em desacordo com o estipulado, seja por disposição de normas programáticas, seja por processos de autorregulação, autorregulamentação ou governança[2].

Assim, as circunstâncias relativas às condutas divergentes, concernentes a danos e a perigos abstratos, têm sido incorporadas na legislação brasileira, especialmente com a criação de novos tipos penais e/ou a ampliação dos já existentes. Por outro lado, percepciona-se que deixa o legislador de produzir normas que tenham relação com metodologias e práticas eficazes na prevenção e na redução de danos e riscos no ambiente cibernético, bem como em

---

[1] Castells (2013, p. 166), ao tratar, por exemplo, sobre a evolução dos movimentos sociais e a relação com o *tempo*, observou que eles *geraram sua própria forma de tempo, o tempo atemporal*, que combina dois tipos diferentes de experiência: (a) nos lugares ocupados, vivem um dia após o outro, livre de restrições cronológicas, e, (b) em seus debates e projetos, projetam um horizonte de possibilidades sem limites, onde novas formas de vida e comunidades emergem da prática do movimento. Então, vivem um "tempo emergente, alternativo, constituído de um híbrido do agora com o para sempre". Já sobre o *espaço*, Castells (2013, p. 164), pondera que o uso do espaço livre da internet, além de propiciar a conexão entre redes, formando uma rede das redes, estabelece a não identificação de um centro de comando, havendo um inter-relacionamento de múltiplos núcleos que garantem as funções de coordenação e deliberação, formando uma estrutura descentralizada que maximiza as chances de participação no movimento, além de reduzir as vulnerabilidades à ameaça de repressão.

[2] Também poder-se-ia analisar esse conceito sob a ótica de Becker (2008), considerando o autor de uma conduta divergente como um *outsider*.

relação à efetividade da investigação criminal, não se tendo, nesse compasso, conhecimento consolidado/científico sobre as expectativas cognitivas e normativas dos atores envolvidos na investigação policial quanto às medidas legais, procedimentais e mecanismos efetivos na redução desses danos/riscos cibernéticos.

A investigação criminal, por sua vez, é um dos pressupostos informacionais à persecução criminal. A falta e/ou insuficiência de órgãos [estaduais[3]] da polícia judiciária estruturados no Brasil, com setores e equipes especializadas no enfrentamento à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado, em suma, à criminalidade em âmbito cibernético, acaba por se tornar um entrave para a efetividade investigativa. Em face dessa premissa, estabelecem-se o problema e as hipóteses da presente pesquisa de doutoramento.

O primeiro organiza-se a partir do seguinte questionamento: quais são e como repercutem comunicativamente as expectativas cognitivas e normativas dos atores de investigação policial ante a legislação penal e processual penal existente relativamente à Internet no Brasil e em relação à estrutura de enfrentamento aos crimes cibernéticos?

Esse questionamento é, portanto, pautado na análise das expectativas cognitivas e expectativas normativas de alguém que detém o "papel" de realizar a investigação cibernética no Brasil, ou seja, tem a função constitucional de realizar as investigações policiais no âmbito dos Estados, e, por isso, delinearam-se as seguintes afirmações hipotéticas:

A primeira hipótese levantada é a de que as frustrações e os desapontamentos em relação às estruturas administrativas e normativas relacionadas aos crimes cibernéticos são mais latentes do que as expectativas cognitivas e/ou normativas, porém a comunicação delas não comunica, sendo apenas ruído.

A segunda afirmativa a pontuar é que o legislador brasileiro possui um foco direcionado à área penal, à produção de direito material penal, circunstância que é refletida sobre o sistema de persecução criminal, com medidas limitadas na área processual penal, capazes de reduzir ou mitigar os danos e riscos no ambiente cibernético.

A terceira proposição é a de que, com o quadro estrutural atual das Polícias Civis brasileiras, o estabelecimento de uma diretiva única no enfrentamento à criminalidade em rede de computadores, dispositivos de comunicação ou sistemas informatizados [criminalidade cibernética] torna-se difícil por depender de decisões não uniformizadas em

[3] Não se objetiva, nesta tese, fazer uma análise sobre a estrutura de investigação criminal cibernética no âmbito da competência e atribuição da Polícia Federal.

âmbito das unidades federativas, gerando frustrações e desapontamentos quanto à efetividade da resposta procedimental.

Relacionada com a hipótese anterior, aventa-se que os atores de investigação policial cibernética não possuem consenso quanto às necessidades de normatividade de medidas procedimentais e mecanismos efetivos na redução/mitigação dos danos cibernéticos.

Formuladas as hipóteses, torna-se fundamental delinear que o objetivo da presente pesquisa é examinar, a partir da perspectiva da Teoria Geral dos Sistemas Sociais, com base em Niklas Luhmann, especialmente sobre sua análise quanto à Sociologia do Direito (1983), as normas penais e processuais penais atinentes aos crimes cibernéticos no Brasil, as estruturas policiais e estaduais focadas neste tipo específico de investigação, explorando e categorizando as expectativas cognitivas e normativas por elas geradas nos atores de investigação policial. Assim, especificamente, objetiva-se:

1. Analisar quais são as expectativas cognitivas e as expectativas normativas dos atores da investigação criminal e que possam tornar efetivo o enfrentamento aos crimes cibernéticos;
2. Descrever, a partir da observação dos atores de investigação policial cibernética e de documentos normativos correspondentes, as estruturas e os meios atuais das Polícias Civis brasileiras no enfrentamento à criminalidade informática;
3. Examinar detalhadamente a linha do tempo da discussão e a produção legislativa no Brasil a respeito da Internet, especialmente a que tenha relação com as áreas penal e processual penal e, neste, os instrumentos legais e processuais aptos à persecução criminal cibernética;
4. Avaliar os meios existentes e aptos à criação, implementação e/ou incremento de procedimentos capazes de auxiliar no enfrentamento à criminalidade cibernética, reduzindo e/ou mitigando danos, como os mecanismos de retirada, exclusão e suspensão de conteúdo no âmbito da Internet;
5. Indagar a falta de efetividade [material] do Art. 4º da Lei nº 12.735/2012 em âmbitos nacional e estadual, que prevê a estruturação de equipes especializadas no combate à criminalidade tecnológica.

Justifica-se a construção desta tese, pois são insipientes as pesquisas, estudos e atenção aos assuntos relacionados ao ciberespaço, à Internet, e que possam gerar a transformação da cultura jurídica brasileira a partir da (a) produção normativa no Brasil e (b) da estruturação de setores administrativos cuja função é a investigação criminal cibernética. Por outro lado,

o processo legislativo se atém a momentos predominantemente emergenciais e/ou direcionados pela construção social produzida pelos meios de comunicação em massa, gerando a sensação de inexistência de regras do Direito quanto ao ambiente digital.

Além disso, é visível a tendência do legislador nacional à produção de normas de caráter penal, em detrimento de outras regras, capazes de melhorar os procedimentos investigativos e/ou de mitigar/reduzir danos em face das publicações e ações danosas no âmbito da Internet.

Por outro lado, faz-se necessário perquirir a existência de uma unicidade investigativa quando se trata de enfrentamento aos delitos cibernéticos, ou seja, aqueles praticados em rede de computadores, dispositivos de comunicação ou sistemas informatizados e interconectados, porquanto a atribuição compete às Polícias Civis dos Estados, as quais possuem políticas e estruturas próprias e dependem de decisão local [estadual] quanto ao direcionamento investigativo.

A exploração do tema busca revelar os meandros e aspectos críticos relativos à falta de política de segurança pública clara e adequada ao enfrentamento da criminalidade cibernética no Brasil, sob os seus principais aspectos: o penal e o processual penal. Por isso, revela-se fundamental conhecer o que os atores envolvidos na investigação criminal cibernética pensam e expectam sobre as normas, pensam e expectam sobre a estrutura investigativa, com o objetivo de que possa haver maior efetividade e retorno da atuação policial em relação à criminalidade cibernética: incremento na resolução dos casos, respostas adequadas às vítimas dos crimes e celeridade no envio de procedimentos ao Poder Judiciário.

A pesquisa tem aderência ao eixo temático Sociedade e Fragmentação do Direito, do Programa de Pós-Graduação em Direito e Sociedade da Universidade La Salle Canoas, uma vez que apresenta como objeto de pesquisa a necessidade de análise crítica da linha do tempo – *timeline* – da produção legislativa e normativa no Brasil em relação à Internet e quais as expectativas cognitivas e normativas que os atores da investigação policial no Brasil depositam sobre a estrutura das normas penais e processuais penais em questão e sobre as estruturas de investigação cibernética existentes no âmbito de sua atuação. Ainda, quais os motivos, aspectos e diretrizes que evidenciam o direcionamento para o campo penal, deixando em segundo plano os aspectos processuais penais (de investigação criminal) e procedimentais.

De outra parte, a pesquisa atual é uma continuação da pesquisa realizada no Mestrado[4], sobre a cultura do medo e o risco no ambiente cibernético e a percepção social deles, bem como o condicionamento dos pesquisados na intervenção do Direito como mecanismo de solução de problemas no ambiente cibernético e não somente como mecanismo de contingenciamento do risco, como ele é.

O método de abordagem para o desenvolvimento da presente pesquisa é o hipotético-dedutivo, com a técnica de análise de conteúdo, que se propõe, após entrevistas e categorização das respostas, (a) analisar quais as expectativas cognitivas e as expectativas normativas dos atores de investigação policial e dificuldades procedimentais (e estruturais) dos órgãos de polícia judiciária civis em relação à criminalidade cibernética em face da inexistência de política nacional de investigação da criminalidade cibernética, bem como (b) deduzir as premissas acerca da produção normativa no Brasil em relação à Internet, assim também em relação a (c) procedimentos e medidas preventivas, a partir da legislação, capazes de mitigar as ameaças e os riscos no ambiente cibernético.

Os métodos de procedimento utilizados são: o historiográfico e o monográfico. O método historiográfico é utilizado no estudo com análise documental de projetos de lei e normas vigentes, pois procura-se (a) indicar e analisar a linha do tempo da legislação penal, processual penal, de direitos e deveres e de políticas de redução de danos no ambiente cibernético, em relação à Internet no Brasil, e (b) delimitar, a partir do relato dos entrevistados, as dificuldades procedimentais (e estruturais) de polícia judiciária estaduais existentes no enfrentamento às ações delituosas em rede de computadores, dispositivos de comunicação ou sistemas informatizados, bem como (c) analisar as diretivas normativas (federais) direcionadas à prevenção e à redução de danos provocados pela criminalidade cibernética porventura existentes em âmbito nacional.

Por fim, é utilizado o método monográfico, uma vez que se objetiva dissertar sobre a sociologia do Direito e sua relação com a Internet, ou seja, a cibersociologia como prática de observação dessa relação no ciberespaço, e os estudos críticos que a envolvem e/ou necessitam que sejam envolvidos, inclusive além do Direito, ou seja, tecnológicos, culturais e políticos (administrativos). Também é utilizado o método para descrever os resultados havidos da pesquisa empírica, baseada em entrevista, consubstanciados na sua inserção em capítulo específico e, a partir daí, no decorrer da análise dos temas sequenciais.

---

[4] Dissertação de Mestrado sob o título "A INTERNET E A FRAGMENTAÇÃO DO DIREITO PENAL NO REFORÇO DA CULTURA DO MEDO NO BRASIL: percepção social e perspectiva legislativa", defendida em 26/02/2016, no PPGD da Universidade La Salle Canoas-RS. (WENDT, 2016).

As técnicas empregadas na elaboração do trabalho são a pesquisa bibliográfica e a pesquisa empírica. A pesquisa bibliográfica parte de fontes primárias e secundárias, com base em obras e textos que tratam da criminalidade cibernética, sua evolução a partir o uso massivo da Internet, a sua análise pela sociologia do Direito, especialmente sob (a) seus vários aspectos possíveis e que tenham repercussão no Direito e (b) a perspectiva da Teoria Geral dos Sistemas Sociais desenvolvida por Niklas Luhmann (1983). Além disso, são utilizados artigos de periódicos, legislação nacional e internacional e sites de notícias.

A segunda, a pesquisa empírica, resulta de uma de entrevista semiestruturada, em 5 tópicos principais e seus subtópicos (vide Anexos), direcionada aos integrantes dos órgãos especializados das Polícias Civis dos Estados que tratam da investigação de crimes cibernéticos, visando a percepcionar as expectativas cognitivas e as expectativas normativas dos atores de investigação policial quanto à efetividade da investigação e à redução de danos cibernéticos, pautando-se essa observação sobre as observações quanto às estruturas normativa e administrativa [procedimental] existentes para o enfrentamento dos crimes cibernéticos.

Quanto aos entrevistados, em face da técnica de análise de conteúdo proposta, bem como da abrangência nacional da pesquisa, o trabalho apresenta, proporcionalmente, representatividade nas cinco regiões do Brasil, embora nas regiões compostas por um número maior de Estados, há mais entrevistados. Objetivou-se entrevistar servidores policiais, delegados de polícia ou policiais integrantes do órgão especializado na investigação e atuação de enfrentamento aos crimes cibernéticos. Chegou-se aos entrevistados após comunicação da pesquisa ao Conselho Nacional de Chefes de Polícia Civil – CONCPC –, órgão colegiado que reúne os dirigentes máximos das Polícias Civis nos Estados e no Distrito Federal, ao qual foi enviado documento informando os detalhes da pesquisa, os objetivos, o foco e a necessidade de encaminhar, via Chefia de cada Polícia Civil, o documento, assinado pelo pesquisador e sua orientadora, informando da realização da pesquisa e que o pesquisador realizaria contato com os órgãos de investigação cibernética instituídos formalmente em cada Estado.

Assim, na fase de elaboração do projeto, partiu-se inicialmente da concepção de ter pelo menos um entrevistado em cada uma das regiões, porém podendo-se chegar ao número máximo de Estados e Distrito Federal (27) onde já existiam, naquele momento das entrevistas, órgãos específicos previstos e instalados (ou seja, a condição para a entrevista, além da voluntariedade, foi a existência de órgão formal criado com base na Lei nº 12.735/2012, e, assim, não existindo o órgão especializado o Estado, houve descarte da

participação na pesquisa e, portanto, sem entrevistado naquele Estado). Os possíveis entrevistados foram contatados, após formalização ao CONCPC e remessa da documentação às Polícias Civis, por meio de telefone e/ou WhatsApp e, *a posteriori*, por e-mail, quando foi enviado o TCLE para aceite e participação da entrevista, já com a agenda da entrevista e alerta de gravação dela.

O contato foi, então, realizado com os órgãos especializados na investigação cibernética e os respectivos entrevistados, que aceitaram ou não participar da entrevista, após o envio da documentação e informações sobre a pesquisa para a Instituição Coparticipante Conselho Nacional de Chefes de Polícia Civil – CONCPC – e a remessa por este às Polícias Civis dos Estados.

A partir de então, a etapa da entrevista teve como *fases prévias*:

1º) *contato com os integrantes dos órgãos especializados*, principalmente os titulares, por meio de telefone e/ou WhatsApp, explicando a pesquisa e o interesse em ter a participação de um integrante do referido órgão. Observação: os participantes foram contatados a partir da lista de participantes do 1º Cibercap, organizado pelo Ministério da Justiça e Segurança Pública (REPRESSÃO, 2021a; REPRESSÃO, 2021b), no qual o pesquisador foi palestrante e cujos nomes e telefones foram coletados durante o evento (pelo pesquisador) e de cujo grupo de WhatsApp o pesquisador faz parte.

2º) em caso de receber o sinal de que o contatado poderia participar da pesquisa, foi enviado um e-mail prévio com o seguinte conteúdo, e-mail este direto ao entrevistado e sem cópias a outros participantes:

> Prezado(a) Fulano(a)!
>
> Agradeço a disponibilidade em participar da pesquisa de doutorado, intitulada AS EXPECTATIVAS COGNITIVAS E NORMATIVAS DOS ATORES DE INVESTIGAÇÃO POLICIAL EM FACE DOS CRIMES CIBERNÉTICOS, e, conforme ajuste prévio, informo que a data xx/xx/xx, às xxhxxmin, foi colocada na agenda e um convite com o link do Google Meet foi enviado.
> No dia da entrevista, um novo e-mail será enviado com o Termo de Consentimento Livre e Esclarecido, o qual peço que possa responder dizendo que concorda com a participação na pesquisa e com a gravação da entrevista.
> Qualquer dúvida, responda este e-mail ou entre em contato comigo, pelo fone 519xxxxxxx.
> Emerson Wendt, Doutorando em Direito pela Universidade La Salle – Canoas-RS.

3º) agendamento, pela agenda do Google, de dia e horário, conforme previamente ajustado com o entrevistado, sendo acrescentado seu e-mail e o link da reunião.

4º) entrevista com o participante.

Em ambas as situações, de análise documental (*timeline* do direito normatizado e Projetos de Lei) e de entrevistas semiestruturadas, usou-se a técnica de análise de conteúdo (BARDIN, 1977), buscando-se categorizar os temas e respostas, respectivamente, propiciando a abordagem crítica sobre o enfrentamento da criminalidade cibernética, sua estrutura e procedimentos, suas peculiaridades e deficiências, suas perspectivas e desafios mais prementes.

Parte-se, contudo, de uma observação do cibersistema da Internet e da possibilidade de sua concepção como um subsistema social dentro da Teoria Geral dos Sistemas Sociais de Niklas Luhmann.

Para tanto, a pesquisa é dividida em três partes, adotando, necessariamente, uma análise de como é possível compreender a Internet como um cibersistema, destacando suas características, peculiaridades, sentido e função. A partir das observações sobre a autopoiese no cibersistema da Internet, busca-se analisar seu processo coevolutivo a partir da interação operacional, via comunicação, com o seu entorno, os sistemas psíquicos e sociais. Observa-se, assim, que a Internet é um sistema de sentido a partir de dados e informações capazes de comunicar e que sua diferenciação funcional está, então, na conexão e desconexão, capaz de absorver, armazenar e compartilhar informações aptas a comunicar.

No segundo capítulo, mediante a metodologia referida, abordam-se todos os aspectos inerentes à pesquisa empírica e seus resultados, especialmente voltados a observar quais são e como são delineadas as expectativas cognitivas e as expectativas normativas dos atores de investigação policial [criminal] cibernética, ou seja, aqueles especificamente designados para a função de persecução criminal em face dos crimes cibernéticos. Tais expectativas, reflexivas ou não, são observadas sobre o sistema do Direito, especialmente a estruturação normativa penal e processual penal, e sobre o sistema Político, notadamente (a) o processo legislativo em construção a partir da realidade social estabelecida, especialmente, pelos veículos de comunicação, os *mass media*, e (b) a estrutura organizacional de enfrentamento à criminalidade cibernética no Brasil e nos Estados.

Para finalizar, o último capítulo procura, a partir das expectativas cognitivas e normativas desses atores de investigação criminal cibernética, observar [e descrever] não só a estrutura normativa vigente, penal e processual, sobre os crimes cibernéticos, ou seja, as condutas divergentes no âmbito da Internet e sua investigação, mas também como o sistema legislativo brasileiro está procurando estruturar ou reestruturar socionormativamente o Direito em relação à temática.

Portanto, objetiva-se, em suma, compreender como são os processos comunicativos intersistêmicos da Internet, do Direito e da Política, a partir de expectativas cognitivas e normativas de um dos atores da persecução criminal, o/a policial que investiga os crimes praticados no âmbito do cibersistema da Internet, a fim de descrever a ausência e/ou ineficácia na comunicação dessas expectativas e frustrações aos sistemas que estão no seu entorno e como a não completude comunicacional afeta a construção das estruturas normativas no Brasil.

2 COMO É POSSÍVEL UM CIBERSISTEMA DA INTERNET?

> De esta forma el sociólogo se tiene que transformar en “cibersociólogo” en su afán por estudiar y comprenderla urdimbre social que se desarrolla en éste, otro espacio. (SORO, 2006).

A Internet tornou-se o principal meio de muitas atividades, de muitos processos, de muitos sistemas que se utilizam de dados, de informações e, com base nesses, de comunicação. Em 2020, esse atributo tornou-se ainda mais evidente em razão da pandemia da coronavírus. A economia mundial há muito se adaptou a esse processo tecnológico de interação, sob vários aspectos: o que comunica, como comunica, quando comunica. Os reflexos, com base em notícias advindas de todos os lugares espaciais, em bolsas de valores de diferentes países, que abrem e fecham de acordo com seu fuso horário, são sentidos já na abertura delas. As mobilizações sociais são refletidas instantaneamente em todos os países onde determinadas aplicações são mais ou menos utilizadas, são mais ou menos controladas, são mais ou menos reguladas.

A base da rede mundial de computadores, diga-se, de dispositivos interconectados, tornou-se, além de *bits* e *bytes*, “os” *bits* e *bytes*, representativos tecnológicos de *dados* e *informações*, com capacidade de produzir significados, de dar sentido ao conteúdo. Os significados diferentes são absorvidos ou não absorvidos pelos diferentes sistemas sociais de acordo com o código específico de seu sistema, de acordo com as suas funções.

Então, uma mobilização social que, por exemplo, inicia nos Estados Unidos da América com a morte de um homem preto por um policial branco, importa e exporta significados diversos, localmente e mundialmente, e que são percepcionados pelo sistema político, pelos sistemas organizacionais das polícias, pelo sistema da comunicação, pelo sistema do direito, pois essas diferentes percepções e significados, em face da comunicação daí advinda, podem vir a compor, a reordenar, a produzir e a reproduzir, a organizar e auto-organizar, a desenvolver e a autodesenvolver, circularmente, esses sistemas a que a comunicação irrita. Porém, nem toda comunicação advinda dessa informação – morte de um homem preto por um policial branco – vai ser absorvida pelos demais sistemas. Nesse exemplo, logicamente, a circunstância havida no contexto real-real é amplificada pelo real-virtual, mas também há outras circunstâncias em que os movimentos partem do virtual e chegam no real com bastante força, a exemplo dos movimentos sociais de 2013 no Brasil.

O que vai importar, então, para absorção de uma comunicação por um determinado sistema é a evolução do sistema social onde este sistema está inserido, o seu

desenvolvimento, a sua abertura cognitiva, pois que os sistemas político e do direito, por exemplo, são diferentes nos países do mundo, não só em relação à evolução do direito, à incorporação de direitos e garantias etc. O sistema de comunicação, que tem o objetivo principal de informar, pode estar regulado de maneira diversa e possuir um maior ou menor controle, advindo de regras normativas e/ou de interferência dos governos então dominantes.

A Internet, por sua vez e em razão de suas características, especialmente de não-tempo, de não-distância, permite, uma vez estabelecida a conexão, um não-freio à comunicação advinda desses dados e informações que são produzidos, reproduzidos e autoproduzidos em seu contexto. Formou, assim, um paradoxo onde redução de complexidade, pela facilidade e usabilidade de dados e informações, tornou-se mais complexidade, em razão da forma, da quantidade, da volatilidade, da agilidade, da transversalidade, dentre outras circunstâncias geradoras de complexidades oriundas dessa rede.

É nessa plêiade de complexidades que se pretende, nesta introspecção, abordar a Internet a partir da Teoria dos Sistemas desenvolvida por Niklas Luhmann, buscando compreender e caracterizar a diferenciação funcional desse cibersistema. O conceito de cibersistema também se forma a partir da teoria de Luhmann, unindo-se os termos "sistema" e "cibernético". Como método de pesquisa neste capítulo, adota-se o dedutivo, partindo do geral para circunstâncias específicas, facilitando a absorção das ideias. Como metodologia, busca-se uma revisão bibliográfica, partindo logicamente de Luhmann e suas influências, bem como de suas interpretações, especialmente as heterodoxas, as que permitem a (co)evolução da *superteoria*. Da mesma forma, sob a observação a partir da cibersociologia, interrelacionar a Internet e suas formas de acoplamento estrutural com os demais sistemas.

Assim, divide-se o capítulo em duas partes. A primeira parte do estudo é, por assim dizer, genérica, pautada no conhecimento de aspectos importantes da Teoria Geral dos Sistemas Sociais, da compreensão de *sistema* e de seu principal conceito, a autopoiésis, bem como a compreensão da função diferencial de um sistema social e/ou de um sistema psíquico. Associado a esses aspectos, parte-se também para observações quanto à (co)evolução dos sistemas para, a partir daí, poder observar o cibersistema da Internet. No segundo tópico, procura-se observar como é possível um cibersistema da Internet, abordando os principais pontos da teoria desenvolvida por Luhmann, porém aplicados ao cibersistema, composto por dados e informações, que é a Internet, o "seu" sistema e o "seu" entorno, os demais sistemas sociais (política, economia, saúde etc.) e psíquicos.

É um convite a uma releitura de como o sentido da Internet, os dados e informações, esse meio de comunicação simbolicamente generalizado, podem ser capazes de se comunicar

com os diferentes sistemas, a partir da diferenciação funcional deles. Não se procura dar respostas, mas um sentido à complexidade advinda da Internet.

2.1 Sistema, autopoiese, diferenciação funcional e coevolução

A Teoria Sistêmica desenvolvida por Niklas Luhmann tem ingresso no Brasil a partir do Direito e, em razão dos seus estudos sobre autopoiese (autopoiésis), dá uma guinada epistemológica em 1984 (LUHMANN, 1998, p. 37-76). Tem sua base a partir do conhecimento sobre *sistema* e, por isso, é importante compreender a base dos conceitos de *sistema*[5], que teve uma reformulação com o passar do tempo, especialmente a partir do início do século XX. Luhmann sofreu uma série de influências para desenvolver a sua *metateoria* ou *superteoria* (SILVA, 2018; HOMMERDING, 2020).

Quadro 1: Influências de Luhmann para o desenvolvimento da Teoria da Sociedade (Teoria Geral dos Sistemas Sociais)

Ideias da reflexividade cibernética, concepção e função de sistemas	Teoria da informação	Shannon e Weaver	Teoria da Sociedade de Niklas Luhmann
	Lógica bivalente, lógica policontextural	Gotthard Günther	
	Teoria dos sistemas que observam → autorreferência e da forma recursiva	Heinz von Foerster e Louis H. Kauffman	
	Teoria da forma de dois lados	George Spencer Brown	
	Cibernética como teoria da comunicação	Norbert Wiener	
	Teoria da evolução da *Autopoiesis*: construtivismo epistêmico	Maturana e Varela	
	Teoria crítica	Escola de Frankfurt	
	Cunho sistêmico à sociologia e ênfase à função	Talcott Parsons	
	Teoria Geral dos Sistemas	Ludwig von Bertalanffy, William Ross Ashby e George Klir	

Fonte: Produzido pelo autor[6] (2022).

[5] O uso reiterado da palavra "sistema" se justifica nos parágrafos desta tese para que haja uma compreensão correta a respeito do tema. Para outras compreensões, relacionadas ao jurídico, ver Soares (2015) e Vieira (2000), especialmente quanto às abordagens sobre "sistema" por Tércio Sampaio Ferraz Júnior.

[6] Quadro das influências de Niklas Luhmann, desenvolvidas a partir de Silva (2018) e Hommerding (2020). Hommerding (2020) tem uma visão diferente das influências de Luhmann, mas acredita-se que apenas do ponto de vista metodológico e referencial, apoiado nos estudos de Eduardo Ángel Russo: 1ª influência: Escola

E, como adverte Rodrigues (2020)[7], quando se fala em *sistema* é bom dizer em que dimensão, em que abordagem, está se referindo. Essa abordagem sobre *sistema* iniciou com Pareto (1916)[8] e é alterada em 1951, com Parsons (1974)[9]. Porém, essa concepção de sistema sofre um novo enfoque com a Teoria de Santiago, a teoria autopoiética, em 1968, com dois biólogos, Maturana e Varella[10], cuja publicação reflete em Luhmann a partir de 1984.

Para diferenciar da ideia de estrutura, surge a concepção de *sistema* como algo mais dinâmico, com movimento e não estático, não coagulado (RODRIGUES, 2020). Ludwig von Bertalanffy (2009), na primeira metade do século XX, debruçou-se sobre a ideia de *sistema* desde a visão de sistema da termodinâmica (que vem de 1850) e informa, então, que os sistemas vivos orgânicos são diferentes dos sistemas trazidos pela termodinâmica, porque estes eram fechados. Por isso, Bertalanffy (2009) traz a ideia de sistemas abertos, dizendo que organismos vivos são sistemas abertos[11]. Então, a concepção de *sistema* se consubstanciava na ideia de movimento, a ideia da cibernética do século XIX, e, pela análise de Bertalanffy (2009, p. 195-196), os sistemas dos organismos vivos são diferentes dos sistemas entrópicos, dos sistemas trazidos pela cibernética, ou seja, os sistemas biológicos são abertos.

Esse conceito de *sistema* aberto perdura por poucos anos, pois a partir dos estudos de Maturana e Varela (1995) sobre os organismos vivos é construída uma nova teoria, uma nova perspectiva sistêmica, porque para eles o sistema é fechado, mas um fechamento não significa um fechamento que exclui todas as possibilidades de recebimento, por exemplo, de matéria

---

de Frankfurt, da Teoria Crítica, em razão da capacidade crítica relacionada como elemento essencial da teoria científica (HOMMERDING, 2020, p. 53); 2ª influência: Talcott Parsons, que fez uma releitura da sociologia weberiana, inspirada na teoria dos sistemas da Cibernética e da Biologia, dando o cunho sistêmico à sociologia, com o seu estrutural-funcionalismo dando ênfase à função como forma de manutenção do sistema (HOMMERDING, 2020, p. 53-57). A partir de Parsons, Luhmann analisa criticamente a sua teoria e se apoia na análise dos processos sistêmicos autopoiéticos estudados, analisados e desenvolvidos por Maturana e Varela; 3ª influência: a Teoria Geral de Sistemas, desenvolvida especialmente por Ludwig von Bertalanffy (também por William Ross Ashby, em 1956, e George Klir, em 1967).

[7] Aula proferida na disciplina Sociedade, Sistemas e Direito do Doutorado em Direito do PPPG da Universidade La Salle – Canoas/RS, em 27 mai. 2020.

[8] No Brasil, Vilfredo Pareto possui mais obras traduzidas da área econômica. A mais recente, traduzida ao português, é **A Transformação da Democracia**, pela Editora Leya, em 2019 (PARETO, 2019). Sua obra **Trattato di sociologia** é de 1916.

[9] Talcott Parsons lança, em 1951, sua obra **O sistema social**. No Brasil, em 1974, chega o livro "O sistema das sociedades modernas", pela editora Pioneira.

[10] Humberto Maturana e Francisco Varela lançaram sua obra central, sobre a qual Luhmann desenvolveu a Teoria dos Sistemas Sociais.

[11] Bertalanffy lança essa ideia em seu livro Teoria Geral dos Sistemas, em 1960. No Brasil, esse livro foi lançado em 1975. A edição citada é a 4ª, lançada em 2009.

e energia em formação; mas, o *sistema* é fechado na sua sistematicidade. Em outras palavras, o sistema é fechado operativamente, porém aberto cognitivamente (SILVA, 2016).

Com base nessa nova concepção de *sistema*s fechados e autopoiéticos, desenvolvida no contexto da biologia[12], Luhmann concebe a de fechamento operativo dos sistemas[13], pois tem-se de mentalizar a ideia de *sistemas* como sistemas fechados do ponto de vista operacional, porque "sistemas não podem operar além do seu limite" (RODRIGUES, 2020; RODRIGUES; NEVES, 2017, p. 32; LUHMANN, 1998, p. 51-53), onde forma sua unidade de sentido. Incorpora-se, então, à concepção de sistemas a autopoiese, idealizando o *sistema* como uma unidade, sistema que, necessariamente, tem de ser fechado em termos de sua identidade sistêmica, da sua autonomia sistêmica, um fechamento então operacional, de circulação de informação ou de comunicação, em acepção mais ampla.

A ideia de autopoiese é fundamental para a compreensão de um sistema como sistema fechado, pois se os sistemas são autopoiéticos, ou seja, sistemas fechados, são sistemas que se auto-organizam, se retroalimentam, se autorreferenciam e, por isso, são autopoiéticos (RODRIGUES; NEVES, 2017). Autopoiésis também se reforça em razão dos sistemas reagirem [sua forma de interação] às mudanças do meio ambiente [entorno] em que estão acoplados, reação que se dá através de processos que garantem o fechamento operativo do sistema.

Luhmann (1998), por homologia, estende epistemologicamente a concepção sistêmica orgânica, ou seja, concebe o mesmo *logus* entre sistemas orgânicos e outras categorias de sistemas, que ele chamou de sistema psíquico e sistema social. Por isso, autopoiese tem significado perante os sistemas, pois eles produzem seus elementos e devem se referir a si mesmos tanto na constituição quanto nas suas operações elementares.

Quanto ao sistema psíquico[14], de cada ser humano, também é operacionalmente fechado, pois se tende a manter a identidade própria e todo o conhecimento, pois não se tem como saber (exatamente) qual o conhecimento/sentimento outro indivíduo possui, porém, toda a irritação externa vai produzir uma emergência interna do sistema, ou seja, o sistema sempre vai produzir mudanças a partir do seu interior próprio tendo sido irritado pelo

---

[12] Segundo Rodrigues (2020), do ponto de vista epistemológico, Luhmann não constrói analogias, mas identifica classes diferentes de sistemas que apresentam um comportamento idêntico ao comportamento dos sistemas orgânicos descritos pela biologia, ou seja, que existem sistemas que operam exatamente como o sistema descrito pela biologia.

[13] Vide quadro de influências de Luhmann.

[14] Vide Luhmann (1998, p. 77-112 e p. 236-254), quando o autor faz análises quanto ao sentido e quanto à individualidade do sistema psíquico.

exterior. Por isso, a partir de Luhmann também se afirma que “conhecer é sempre um autoconhecimento” (RODRIGUES, 2020).

O acoplamento estrutural do sistema psíquico com os sistemas e subsistemas do seu entorno se dá por meio da linguagem, um dos três meios de sentido que foram se estabelecendo (SILVA, 2016, p. 55). Portanto, a linguagem é um dos médium [de sentido] da comunicação[15], sendo esta o principal elemento constitutivo dos sistemas sociais, partindo e sendo definida a partir de três relações elementais (MANSILLA, 2007, p. X): (a) seleção da informação [informar], (b) modo de dar a conhecer [ou seja, o compartilhar], e (c) o modo de compreender [entender]. Os dois primeiros ficam a cargo do sistema emissor [o Alter]; o último, a cargo do sistema receptor [o Ego], sendo resumido no processo de ‘entender’ a informação anteriormente selecionada e dada a conhecer. A partir daí, pode-se autoproduzir, no sistema receptor, com base na sua memória e em seus conhecimentos prévios, o conhecimento.

O conhecimento, por sua vez, como produto de uma comunicação bem-sucedida, sozinho não tem nenhuma mobilidade, ou seja, ‘não vem’ de fora do sistema, isso porque o conhecimento não consegue atravessar o fechamento operativo do sistema. O conhecimento autoproduzido ou autoabsorvido a partir dessa comunicação realizada com sucesso é precedido de uma irritação no meio em que o sistema está acoplado e [o autoconhecimento] faz emergir sentido a partir de dentro desse sistema próprio. E por isto que se tem a clara noção de que não se consegue pensar com o pensamento do outro, ou seja, Alter não consegue pensar com o pensamento de Ego e vice-versa. Essa é a noção de fechamento operativo:

> eu não consigo pensar com os teus pensamentos e eu não tenho certeza que tudo o que estou dizendo agora é exatamente aquilo que eu gostaria que cada um de vocês entendesse na plenitude com que eu acho que deveriam entender, porque eu não consigo acessar os conhecimentos de vocês e não consigo acessar os pensamentos (de vocês). (RODRIGUES, 2020).

Luhmann (2006) afirma que a comunicação é possível, mas é improvável, ou seja, nunca se comunica exatamente aquilo que acha que comunica, porque toda a produção de sentido, de nexo, é sempre uma emergência a partir das próprias estruturas cognitivas ou das estruturas internas do sistema cognitivo. A concepção de autopoiésis reforça, então, a ideia

[15] Também são meios de sentido da comunicação, segundo Silva (2016, p. 55), os meios de difusão, representados pela imprensa, rádio, televisão e a Internet, e, também, os meios de comunicação simbolicamente generalizados, que são meios autônomos de comunicação.

de que os sistemas psíquicos são sistemas autorreferentes e não são abertos, do ponto de vista operativo, para o exterior.

Os sistemas psíquicos são sistemas que quando se diz, por exemplo, que cognitivamente alguém aprendeu ou se desenvolveu, ou evolui, isso tudo vai ser um autodesenvolvimento, uma autoevolução, uma autoaprendizagem. Isso está ligado, por sua vez, à concepção de auto-organização, conceito que vem da cibernética, porém não num significado dicotômico, de causa e efeito, mas numa orientação reflexiva, circular e reflexiva, de circularidade reflexiva (RODRIGUES, 2020). O mecanismo de acoplamento estrutural entre consciências e comunicação ocorre por meio dos sistemas psíquicos e, no caso da Internet, a relação da consciência ocorre com a comunicação dos dados e informações disponíveis, cuja linguagem é escolhida/selecionada conforme for a aplicação utilizada.

Por ser o conhecimento sempre um autoconhecimento, as irritações que vêm de fora do sistema, que vêm do ambiente, do entorno do sistema, geram reacomodações, readaptações internas do próprio sistema a este ambiente. Se o ambiente, se o entorno, se a periferia muda, o sistema necessariamente vai mudar. Nesse contexto dá-se a lógica do processo coevolutivo dos sistemas, psíquicos e sociais, porém dentro de padrões de suas diferenciações funcionais, ou seja, percepciona-se, a partir da análise da sociedade moderna, que ela vem se diferenciando, autodiferenciando com os sistemas funcionais, aumentando sua complexidade num processo de diferenciação funcional.

Luhmann (1998) analisa que os sistemas sociais são sistemas que se autonimizaram e se diferenciam (funcionalmente). Por exemplo, o sistema da ciência, o sistema da economia, o sistema da arte, o sistema da política, o sistema da comunicação. Estes sistemas são diferenciações funcionais num processo sistêmico coevolutivo e num permanente aumento de complexidade da sociedade contemporânea.

Nesta esteira, segundo Guibentif (2012), Luhmann aborda os direitos subjetivos, até o momento em que (a) forma a teoria da relação entre sistemas psíquicos e sistemas sociais e (b) a evolução dessa teoria é a base dos direitos subjetivos, que introduz importantes elementos novos e incorpora num modelo complexo os vários elementos formulados[16].

---

[16] Por isso, segundo Guibentif (2012), tem-se a relação entre os direitos subjetivos com o fenômeno da diferenciação funcional, possibilitando-se (i) o estudo dos direitos subjetivos a partir da função que desempenham na sociedade, (ii) apreciar as consequências da diferenciação funcional, enquanto (iii) o conceito de direito subjetivo valoriza o ser humano. Por isso, (iv) os paradoxos surgem a partir da questão de definir o direito a partir de si próprio e da necessidade de se aplicar a violência para restabelecer a conformidade ao direito, e (v) o caráter autológico da subjetividade obriga o sujeito a confrontar-se com o que o distingue do resto do mundo. Para ele, os direitos subjetivos são mecanismo de acoplamento estrutural

Luhmann afirma que que os sistemas sociais são sistemas de comunicação e que cada qual apresenta um código (RODRIGUES; NEVES, 2017, p. 83-107). Assim, o Direito é um sistema de comunicação que apresenta um código (binário) legal/ilegal (*recht*/*unrecht*); a Ciência é um sistema em que o código é verdade/não verdade; a Comunicação é um sistema em que o código é informação/não informação (LUHMANN, 2005, p. 39). No caso do direito, a sua função é, ao reduzir complexidades, de estabilizar determinadas expectativas normativas, permitindo às consciências individuais presumir que outras consciências funcionarão na base dessas expectativas (GUIBENTIF, 2012).

Luhmann mostra que a sociedade, na medida em que vai se tornando mais complexa, vai produzindo sistemas que vão se diferenciando e se fechando sobre si com o seu próprio código binário, em que (através do que) ele vai aceitar ou rechaçar comunicações (RODRIGUES; NEVES, 2017, p. 89).

Mas o que são estas comunicações? Essas comunicações não são falas, retóricas ou ruídos, necessariamente[17]. Assim, na construção dos sistemas sociais importa não a retórica comunicativa, mas o que importa são as comunicações que o sistema toma como comunicações que vêm do entorno e servem para sua dimensão autopoiética, como um sistema de comunicação. Então, todos os sistemas sociais são sistemas de comunicação e são formados somente por comunicação. Os seres humanos, neste plexo dos sistemas sociais, estão fora do sistema. Eles são entorno, são a periferia dos sistemas. Os sistemas não precisam dos humanos para ser considerados autonomizados como sistemas comunicativos (LUHMANN, 1998, p. 77).

Luhmann (1998, p. 140-171) sustenta que os homens agem, se comunicam. Esse agir, esse comunicar, esse fazer, esse não fazer, é comunicação. E essas dimensões comunicativas são dimensões que vão fazendo com que os sistemas vão, ao longo deste aumento de complexidade, se diferenciando. Então, segundo Rodrigues (2020), Luhmann fornece uma dimensão de complexidade um tanto paradoxal e interessante: ele afirma que os sistemas sociais existem para reduzir complexidade. À medida que os sistemas sociais se diferenciam eles estão buscando a redução de complexidade do sistema mundo (sistema ao qual pertencem).

---

do direito com outros sistemas sociais e, ainda, tem-se a discussão dos direitos humanos como componente da sociedade mundo.

[17] Segundo Luhmann (2005, p. 158), "as ambivalências e os mal-entendidos são transmitidos juntos com a comunicação à medida que não a bloqueiam; entender é praticamente um mal-entender sem entendimento desse mal".

Então, o sistema vai se diferenciando em subsistemas – do Direito, da Educação, da Economia, da Política, (por sua vez) em subsistemas, que vão se diferenciando cada vez mais na direção de reduzir a complexidade. Mas, paradoxalmente, à medida que ele reduz complexidade, ele aumenta complexidade. Para Luhmann (RODRIGUES, 2020) existe uma redução de complexidade mediante complexidade e a complexidade só pode ser reduzida mediante aumento de complexidade, o que é de fato uma dimensão paradoxal.

Em um momento posterior desta tese aborda-se outro aspecto importante relacionado à comunicação e sua relação com a consciência e a formação da memória e do saber, que conduzem o sistema psíquico para a formação das expectativas e, a partir daí, como os sistemas sociais formam suas estruturas de generalização das expectativas, reduzindo as possibilidades seletivas.

2.2 Internet, cibersistema, informação e comunicação

Quando se questiona "como é possível um cibersistema da Internet?", não é simplesmente apresentar uma parcela de um problema de pesquisa em sua forma mais genuína. Também pode não representar ou dar o contexto ideal e total do que se propõe. Parte-se, naturalmente, de uma inquietação constante e um autoaprendizado coevolutivo (de um sistema psíquico específico, enquanto observador) sobre os sistemas sociais e os conceitos que interagem e reagem entre esses sistemas sociais e a tecnologia contemporânea da Internet. Parte-se, também, da junção entre os termos "sistema" e "cibernético", pois que os dados e informações estão nesse contexto digital e atual de *bits* e *bytes*.

O estudo da cibernética não é novo. Atualmente a nomenclatura está associada à Internet, mas seus primeiros ensaios datam do século XIX, com Ampère (1775-1836), e remontam à Platão, partindo de sua categorização conceitual como a arte de governar o Estado e sendo direcionada à arte de governar em geral, de condução ao aperfeiçoamento social, conforme Epstein (2000).

Os estudos essenciais e destacados sobre a cibernética foram realizados por Wiener (1970) e publicados inicialmente em 1948 e 1950, logo após a 2ª Guerra Mundial, relacionados à comunicação e ao controle, ou seja, tudo que for campo do controle e da teoria da comunicação, seja na máquina ou animal, é cibernética para ele. Nesse contexto, importante observar que a sistemática da cibernética sempre foi a de se relacionar a sistemas

que se autorregulam, se autorreproduzem, evoluem e aprendem. Luhmann pautou-se também nestes estudos de Wiener para formular sua superteoria[18].

Aliás, para compreender o sistema cibernético é necessário compreendê-lo no sentido de processo, ou seja, como um conjunto coordenado e concatenado de passos destinados a um fim.

> Os modelos abstratos, surgidos da generalização de determinado processo empírico, podem ser estendidos a outros processos, revelando suas características e explicando seus comportamentos anteriormente desconhecidos. O 'sistema cibernético' nasce, portanto, da formalização de vários fenômenos empíricos que apresentam algumas características comuns. (LOSANO, 2019, p. 10).

Losano (2019) resume os conceitos inerentes à cibernética e que são aplicados, interdisciplinariamente, às ciências sociais e ao Direito: controle (guia), regulação, adaptação e *black box* (caixa preta)[19]. O mesmo autor destaca que os estudos da cibernética foram substituídos pela informática jurídica e pelo direito informático a partir dos anos 1980[20]. Porém, Niklas Luhmann manteve vários conceitos da cibernética em sua teoria, incluindo os

---

[18] Vide quadro de influências de Luhmann.

[19] O *controle* nos sistemas existe para que a entrada de uma nova informação no desenrolar do processo seja guiada pela informação originária, não havendo modificações na cadeia de consequências. Já a *regulação* é "quando a informação de entrada serve para restabelecer o equilíbrio de um sistema" (LOSANO, 2019, p. 11). No caso de haver um erro ou defeito no sistema, esse 'sinal' no processo provoca uma série de reações que corrigem o erro/defeito e o levam às condições necessárias para alcançar o fim previsto. Isso se chama "retroação negativa" (*feedback*), que elimina um distúrbio. Já o processo de *adaptação* é em parte similar ao processo de regulação. Neste, o fim a ser alcançado é atribuído por uma entidade externa ao sistema, que o guia para sua realização, ou seja, "é o próprio sistema que se corrige" (LOSANO, 2019, p. 12). Já, complementar, "Um caso especial e importante de adaptação é a aprendizagem. Um sistema dotado de memória pode conservar as informações reunidas no passado e usá-las para determinar o próprio comportamento futuro. [...] A cibernética constrói também desde máquinas capazes de aprender, portanto, de se autorregular com base na experiência memorizada, até o caso-limite da autorreprodução". Por fim, o conceito de *black box* ou caixa-preta: uma situação difusa, pois "a um impulso corresponde a uma determinada reação, sem que se saiba quais os processos levaram da primeira à segunda", ou seja, um modo típico de proceder do conhecimento humano (LOSANO, 2019, p. 12): "a cibernética o retomou de modo sistemático e formalizado, construindo uma teoria que tem por objeto os sistemas abertos dos quais se conhecem o *input* e o *output*, ao passo que sua estrutura é desconhecida (ou deliberadamente ignorada) no todo ou em parte". Ainda, "por passos sucessivos, usando o método da caixa preta, o cientista social pode formular conjecturas cada vez menos imprecisas sobre a estrutura e sobre o funcionamento do sistema social que está estudando. O método da caixa-preta é, portanto, um processo para conhecer a estrutura de um sistema, sua complexidade e a relação entre sua estrutura e sua função. Ele permite passar de um conhecimento relativo de nível inferior parar um conhecimento relativo de nível superior. Antes de tudo, o objeto de estudo é concebido como caixa-preta de primeiro nível, e uma primeira análise das relações entre *input* e *output* permite estabelecer uma hipótese de sua estrutura interna. Na fase seguinte, as partes do sistema não esclarecidas são, por sua vez, estudadas como caixas-pretas de segundo nível, e assim por diante até atingir um conhecimento do sistema considerado suficiente" (LOSANO, 2019, p. 13).

[20] *Direito da informática*: se ocupa da aplicação das normas jurídicas à informática e é prerrogativa dos juristas; *Informática jurídica*: se ocupa de aplicar a informática ao direito, automatizando a administração pública, a justiça (LOSANO, 2019, p. 140-1).

de *input* e *output*, aplicáveis igualmente à linguagem binária dos computadores e da Internet e ao Direito.

Como a Internet é uma rede que se auto-organizou, autorregulou-se e evoluiu nas últimas décadas, também ela é observável a partir de diversos sistemas funcionalmente diferenciados. Definir ou pontuar a Internet como um subsistema social não é necessariamente novo, pois Stockinger (2001, 2003) procurou fazê-lo no decorrer de suas pesquisas, baseado, logicamente, na teoria sistêmica de Niklas Luhmann, circunstância já relatada em pesquisa anterior:

> Gottfried Stockinger (2003), apoiado na teoria dos sistemas de Niklas Luhmann (1983; 1985), vê o ciberespaço como um sistema autônomo (*sui generis*) e não apenas como um novo *medium* (meio pelo qual passam as comunicações), no dizer do referido autor "é – funcionalmente falando – um mensageiro" (STOCKINGER, 2003, p. 162) que amplia a comunicação social. É autopoiético, pois produz elementos para continuar produzindo mais elementos estando, como referido, auto-organizado, a exemplo da larga teia mundial (rede "www") lançada em 1992 e com estruturas e elementos definidos quanto à distribuição de domínios e conjuntos de protocolos de internet (IP) por todo o mundo. De outra parte, do ponto de vista de ser um processo de comunicação, entre os (sub)sistemas, pode ser tido como um ***super* mecanismo de acoplamento estrutural** entre eles (os sistemas), não só pela agilidade de transmissão de dados, mas pela instantaneidade e pelo transpasse de barreiras físicas, antes intransponíveis ou difíceis de serem derrubadas. (WENDT, 2017b, p. 43-44, grifos nossos).

Stockinger (2001, p. 5) dá então a compreender a Internet como um subsistema de comunicação *sui generis*, correlacionando-o com o sistema de comunicação tradicional, porém como um sistema "desordenado, caótico, estranho". Pode se observar, a partir desse referencial, que a Internet, por ser um subsistema "construído [por] suas próprias estruturas de funcionamento e funcionalidade" (WENDT, 2017b, p. 43), é, portanto, auto-organizada, cuja principal característica é a comunicação, advinda de dados e informações. Seria "*sui generis* no referencial de Stockinger (2003)", possuindo suas próprias regras e sendo fechada operativamente, porém tendo em seu entorno os sistemas psíquicos (usuários) e utilizando, também, a comunicação para interagir com os demais sistemas sociais (direito, moral, economia etc.), irritando-os ou sendo irritada (WENDT, 2017b, p. 43).

Ao problematizar novamente a questão, parte-se de uma perspectiva questionadora e com intuito de ampliar o espectro de respostas, porém numa abordagem não filosófica e sim social-tecnológica, contemplando o espectro tecnológico-digital surgido nos últimos 50 anos e, mais especificamente, a interação social, cultural, econômica, política etc., gerada a partir do alcance comercial da Internet e dos computadores nas últimas três décadas (no Brasil, especialmente após 1995).

Contempla-se, então, um sistema em que dados e informações são sua base principal, e mesmo informações são representações codificadas em razão do processamento digital/eletrônico (LE COADIC, 1996, p. 6), ou seja, são dados. Dados e informações são, na compreensão digital/eletrônica, compreensíveis ou não de acordo com a aplicação que os conecta/mostra aos demais sistemas. São, também, possibilidades de comunicação, porém esta será possível se compreensível ou adaptada ao sistema receptor. Conexão, acesso, permissão, disponibilidade, acessibilidade, confidencialidade, dentre outros, são propriedades atribuídas aos dados e informações para que possam ou não estar visíveis, pois, segundo Le Coadic (1996, p. 6), existe um sistema de gerencialmente desses conjuntos "de dados e suas relações".

Então, a partir da hipótese afirmadora da condição sistêmica da Internet, ou seja, de ser um subsistema do sistema da sociedade, parte-se da análise, mesmo que prévia, das características de um sistema/subsistema, enfocando-se a sistematicidade autopoiética da rede mundial de computadores, correspondendo, ao mesmo tempo, a um sistema autopoiético basal, derivado e estaminal[21], cujo fechamento operativo é singular e sua diferenciação funcional caracteriza-se, internamente, pela existência de múltiplos e específicos códigos binários, pois dependentes de sua especificidade digital, bem como pelo sentido, o limite da Internet, dado pela construção cultural dos observadores, porém, baseado totalmente em informação, ou seja, o sentido-informação ou a informação-sentido. Se podem, internamente, existir múltiplos códigos, a programação é uma só, a programação binária da rede, em "0s" (zeros) e "1s" (uns) (0/1 – binariedade).

Melhor dizendo: o sentido da Internet é informação em seu sentido mais puro, com possibilidade de conexão entre dados, não necessariamente interpretados, reinterpretados, readaptados, percepcionados ou não, mas é só informação, a partir da qual o sistema se

[21] Tonet (2019, p. 79-80) faz uma análise crítica à limitação sistêmica do problema autopoiético na teoria dos sistemas, observando que as teorias biológicas têm em vista a autopoiese de primeira e segunda ordem, onde aquela é encerrada em si mesma e esta é multicelular. Porém, em um processo de reobservação da teoria dos sistemas sociais, segundo o autor, "existem comunicações especializadas mesmo fora do sistema, e que apenas não são observadas no momento" (TONET, 2019, p. 79), sendo que a observação da introdução das células estaminais originou um "verdadeiro paradoxo nos estudos autopoiéticos, pois alteram sua densidade, demonstrando em um quadro autopoiético as relações entre seus componentes, e não os componentes em si" (TONET, 2019, p. 79). Por esse raciocínio, as células estaminais, as células-tronco, "têm a capacidade de autorrenovar e dar origem a novas células especializadas" (TONET, 2019, p. 80), o que diz que, transportado o conceito para a teoria dos sistemas sociais, "a autopoiese estaminal estaria presente em tudo, podendo adentrar em qualquer sistema, independente da sua identidade binária, pois o que importaria seria a comunicação, onde quer que fosse produzida", também "abrindo o espaço de aprendizagem intrassistêmico/extrassistêmico, aumentando sua complexidade, bem como possibilitando novas observações" (TONET, 2019, p. 80).

comunica. Então, é o sentido da Internet a informação capaz de comunicar[22], de reduzir complexidade, e para que essa comunicação tenha possibilidade, especialmente atuando sob a forma de obrigar a seleção de uma possibilidade em relação a outras possibilidades. Então, sentido a partir da informação na Internet também reduz e mantém a complexidade, notadamente se escolhermos uma aplicação em detrimento de outra para comunicar [o mesmo dado ou a mesma informação].

É, por isso, funcionalmente diferente do *sistema* da comunicação, também baseado em informação, pois este possui no seu código os polos positivo e negativo, respectivamente, de informar e não informar (LUHMANN, 2005, 39), ou seja, já com processos de interpretação, reinterpretação, readaptação etc. A informação é, portanto, o sentido da Internet, sua essência, porém (a) nem todos os dados e informações são capazes de comunicar com os demais sistemas ou subsistemas, e (b) mesmo as informações, e seus respectivos dados, que não comunicam fazem parte do cibersistema e de seus microssistemas/subsistemas.

Por consequência, são necessárias a análise e a abordagem dos aspectos atinentes ao acoplamento estrutural aos demais sistemas/subsistemas e à sociedade, como *matter system*, procurando compreender os processos de irritação gerados no entorno e dentro do sistema do direito e do sistema político, com produção de novos atos normativos, reguladores de direitos e demais tipos penais e normas de conduta no contexto da Internet, porém, sem o intento de exaurir as possibilidades, mas, sim, de dar um norte para análises que se seguirão.

Também é necessária a observação sobre como os sistemas psíquicos percepcionam a comunicação advinda desses dados informacionais e, especificamente, como geram expectativas cognitivas e/ou normativas sobre a estruturação relacional da Internet com o Direito, da Internet com a Política (legislativa) e da Internet com o sistema organizacional da persecução criminal no âmbito cibernético. Porém, antes é necessário continuar as observações cibersistêmicas.

E qual é o código do cibersistema baseado na Internet? Qual é o código binário da Internet?[23] Pode-se inferir, como já referido (WENDT, 2017b, p. 49), a existência de vários códigos. Porém, dentre todos os códigos possíveis, um principal, um código que é responsável pela abertura e pelo fechamento operativo: conexão/não conexão ou desconexão (*connection*/*disconnection*).

---

[22] Le Coadic (1996, p. 5) já afirmava que "A informação comporta um elemento de sentido".

[23] Em Wendt (2017b, p. 49), observou-se que "Tal qual os espaços urbanos, a Internet também é segregativa, não apenas socialmente, mas culturalmente, onde os códigos binários belo/feio, legal/chato (*cool/not cool*), certo/errado, acesso/não acesso, funcional/não funcional, por exemplo, são constantes de autosseletividade dos seus usuários (sistemas psíquicos), cada qual com seus critérios de valoração e concepção de verdade".

Conexão ou não conexão a dados e informações capazes de gerar observação pela consciência e, a partir da memória, conhecimento/autoconhecimento, de reduzir complexidades e de produzir complexidades. Conexão ou não conexão a dados e informações capazes de comunicar os sistemas sociais já formados, os quais, de acordo com cada um dos seus códigos, absorverão ou rechaçarão essa comunicação.

Um polo positivo – *connect* – e outro negativo – *disconnect* –, o *input* e o *outupt*, possibilitam a relação do *sistema* da Internet com seu entorno. Por outro lado, sob a ótica dos usuários da Internet, estar *on-line*/*off-line* é um código relativo ao entorno do sistema psíquico, do indivíduo em relação à Internet. Estar *on-line* é estar conectado; estar *off-line* é estar não conectado: não representa, no entanto, que o cibersistema não continue operando, coevoluindo e desenvolvendo-se.

Assim, sob a ótica dos direitos humanos, o código comum em relação à Internet poderia ser construído sob a dualidade, o polo positivo/negativo, respectivamente, de acesso/não acesso, possuir ou não (o direito, a disponibilidade de) acesso à rede mundial de computadores[24]. Esse acesso ou não acesso à rede mundial de computadores, por sua vez, correlaciona-se com o metacódigo da teoria dos sistemas sociais *exclusão*/*inclusão*.

No interior do cibersistema da Internet formaram-se/formam-se/agregam-se vários outros subsistemas, a exemplificar[25]:

(a) mídias sociais (blogs[26], microblogs[27], redes sociais[28] e comunicadores instantâneos[29]);

(b) jogos eletrônicos;

(c) *Deep Web*;

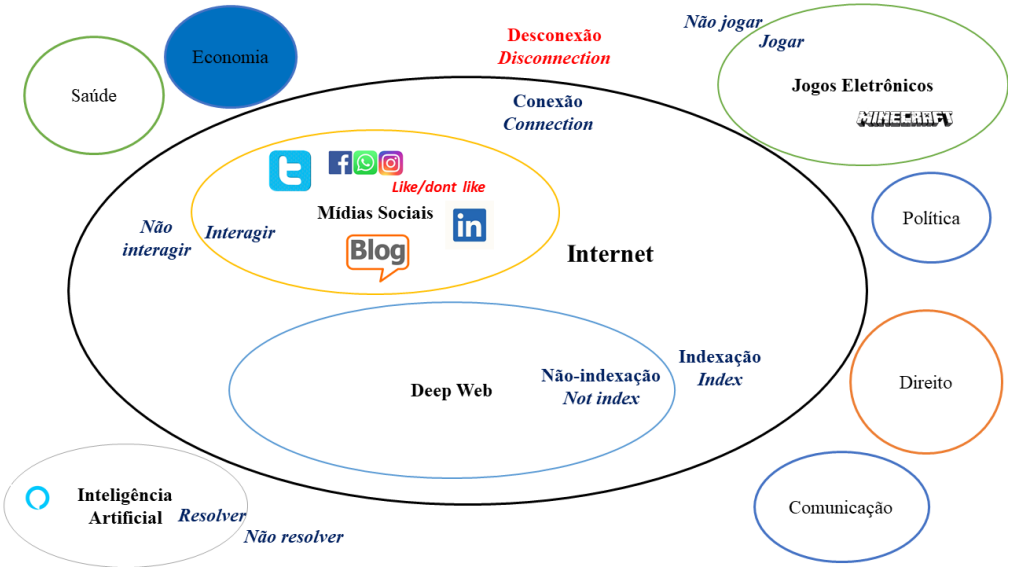
(d) Inteligência Artificial.

Cada subsistema formado através de processos de fragmentação digital, de fragmentação [da linguagem] dos computadores e da Internet, como forma de redução de complexidade, também produziu complexidades e pode, também, ser diferenciado funcionalmente através de seus principais códigos específicos, porém, baseados no principal, ou seja, *connection*/*disconnection*, sem o qual não ocorrem os subcódigos.

---

[24] O site *Internet World Stats* acompanha um índice mundial de acessibilidade à Internet no mundo, nos continentes, regiões e países. Disponível em: https://www.internetworldstats.com/. Acesso em: 27 jul. 2022.
[25] Os exemplos não esgotam, logicamente, as possibilidades infinitas de subsistemas existentes no interior do cibersistema da Internet.
[26] Exemplos: Blogspot e Wordpress.
[27] Exemplo: Twitter.
[28] Exemplos: Facebook, Instagram e LinkedIn.
[29] Exemplos: WhatsApp e Telegram.

Figura 1: Cibersistemas da Internet, seu código, subsistemas e subcódigos



Fonte: Produzido pelo autor (2022).

A *Deep Web*, por sua vez, que é a camada invisível da Internet, por exemplo, possui como código *index*/*not index* (BLOISE; RUBIM; WENDT; COSTA, 2021) pois o que a diferencia da Internet visível, da camada de aplicação e interação usual da rede mundial de computadores, é a indexação pelos buscadores (CALDERON, 2017, p. 216-2019)[30].

Os códigos dos subsistemas da Internet são, portanto, diferentes e dependentes da sua função diferencial em relação aos demais: mídias (redes) sociais: interagir/não interagir; blogs: opinar/não opinar (uma das formas do sistema da comunicação, cujo código é informar/não informar); jogos eletrônicos: jogar/não jogar (por exemplo, no jogo Minecraft, o código é criar/destruir[31]); Inteligência Artificial: resolver/não resolver. Outros códigos, como, por exemplo, gostar/não gostar (*like*/*dont like*), são características dos subsistemas de mídias sociais.

---

[30] Os engenhos de busca – buscadores – mais conhecidos da *surface web* são Google e Bing.

[31] O jogo Minecraft é um jogo em mundo virtual, em que o jogador pode estar *on-line* ou *off-line* (SOUZA; CANIELLO, 2015, p. 39-40). Segundo Cagnini *et al*. (2015, np) "Minecraft é um jogo produzido pelo estúdio sueco Mojang e lançado em 2009. O jogo segue o estilo *sandbox* – isto é, o jogador não é impelido a perseguir um objetivo principal, ficando livre para realizar quaisquer atividades dentro do jogo. Minecraft divide-se em dois modos de jogo principais: *creative* e *survival*. No modo *creative*, não existe limite de recursos que podem ser utilizados pelo jogador. Já o modo *survival* impõe restricões, tais como a necessidade de se alimentar e construir abrigo para se proteger de inimigos" Segundo Souza e Caniello (2015), "Com o seu avatar, o jogador pode criar de pequenas casas a grandes castelos e cidades inteiras. Para tanto, utilizam-se de blocos minerados, daí o nome do jogo". Esse jogo, assim como outros, também é estudado e usado em outros sistemas sociais, como a educação, por exemplo, em razão do seu código (criar/destruir), possuindo uma versão *MinecraftEdu*, específica para a educação, conforme Cagnini *et al.* (2015), Dias e Rosalen (2014) e Souza e Caniello (2015, p. 40).

Percebe-se, também, que há interação e coevolução entre os subsistemas de Internet. Segundo Stockinger (2001, p. 5), os "sistemas sociais virtuais [...] vivem e sobrevivem da contínua criação/diferenciação de informação (novidades)"[32]. Por exemplo, os processos de Inteligência Artificial podem ser readaptados de acordo com sua utilização dentro de jogos eletrônicos (*Game AI*[33]), pois sua finalidade principal é ampliada e, também, readaptada não necessariamente para resolver problemas, para encontrar soluções, mas para propiciar o jogar (polo positivo) com diversão (KISHIMOTO, 2004).

A coevolução também é totalmente presente, pois que, conforme Kishimoto (2004, n.p), a partir do mesmo exemplo dos jogos eletrônicos, verifica-se sua disseminação no meio tecnológico após a década de 1960, com jogos como *Spacewar* (1961) e seu evolutivo seguinte, o *Computer Space* (1970).

A Inteligência Artificial (IA) começa a ser usada nos jogos eletrônicos em 1974 e, a partir dos anos 1990, os jogos eletrônicos também começam a ter uma interação *on-line* através da Internet (KISHIMOTO, 2004)[34]. As interações são, então, mais intensificadas e significam um processo coevolutivo de maior intensidade a partir da Internet e sua disseminação, especialmente das mídias e redes sociais. O cibersistema da Internet, nesta evolução célere e constante[35], correlaciona-se, então, com outros subsistemas, por exemplo, a IA, aprendizado de máquinas, os jogos eletrônicos, e absorveu [nov]as formas de estabelecer redes sociais, as formas de comunicação [agora, por aplicativos de mensageria].

Repete-se, cada subsistema do cibersistema da Internet possui sua diferenciação funcional. Por outro lado, cada um também possui o seu próprio *direito*, e este, funcionalmente reativo dentro do sistema/subsistema da Internet, também mantém seu fechamento operativo baseado na sua diferenciação funcional legal/ilegal. Aqui, verifica-se talvez o principal campo de interação entre subsistemas da Internet e subsistema do Direito, porquanto suas autopoiésis estaminais reafirmam seus códigos independentemente do campo onde estão sendo executados: *on-line* ou *off-line*. No jogo Minecraft, antes referido, os

---

[32] Stockinger, em seu texto de 2001, por considerar a Internet um subsistema de comunicação, parece usar os conceitos de *informação* e *comunicação* como sinônimos. A premissa de que ele parte é diferente da apresentada neste texto, porém, seu raciocínio quanto à lógica da rede de computadores não é incorreto quando se refere às características da *informação*.

[33] *Game Artificial Inteligence*.

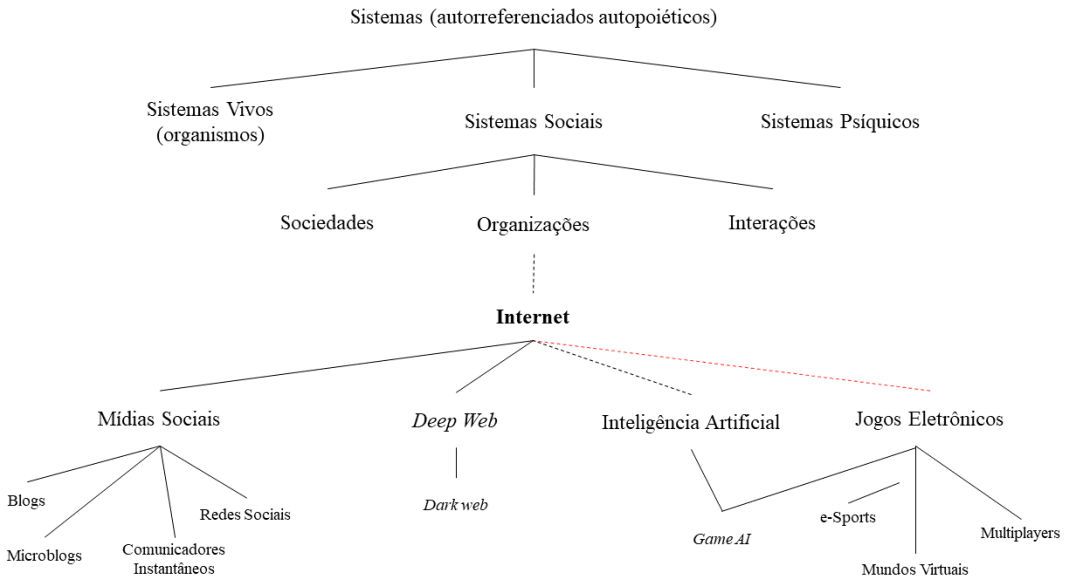
[34] Também fazem parte do subsistema dos jogos eletrônicos os *e-Sports*, com ampla relação com os sistemas de comunicação, da economia, da cultura e psíquicos (WENDT; WENDT, 2015).

[35] Vasconcelos e Brandão (2013, p. 127) destacam a Internet como uma ferramenta que ocasionou uma verdadeira ruptura com o passado, "caracterizando o que alguns economistas denominaram de 'destruição criadora'". Os autores também focam sua análise sobre os reflexos da utilização massiva das mídias e redes sociais a partir do início do século XXI, especialmente no Direito. Sobre a evolução da Internet no Brasil, ver também Lins (2013).

códigos específicos do subsistema do jogo em questão (criar/destruir) e o do Direito (legal/ilegal) subsistem mesmo quando o jogo é realizado *off-line*. Pelo Direito e sua autopoiese estaminal, o acoplamento se dá perante a recepção da informação e comunicação a partir de cada espaço [digital] dentro do cibersistema da Internet. Por outro lado, para que se proceda a autopoiese nos cibersistemas, há necessidade de ocorrer o acoplamento estrutural pela conexão, ou seja, sem conectar-se ao jogo não há possibilidade de provocar a reação do subsistema do jogo eletrônico, seja qual ele for.

Também, complementando-se, a informação (dados) contida em um *pen-drive* ou *Hard Disk* se mantém e somente o seu acoplamento estrutural (conexão) com um receptor (computador, *smartphone* etc.) é produtor da reação/interação. Não conectado, o *pen-drive* ou *Hard Disk* permanece estático e fechado operativamente; conectado, permite-se à coevolução pela sua interação/reação com o sistema cibernético da rede de computadores e com o sistema psíquico, este que percepciona a comunicação dali advinda pela programação binária 0/1, porém traduzida – e apta a dar sentido – por meio das aplicações (navegadores, e-mails, *apps* etc.). A conexão, portanto, permite o espaço criativo e, a partir das comunicações absorvidas e geradas, inclusive e especialmente pelos algoritmos, também permite a evolução.

Figura 2: Sistemas autorreferenciados autopoiéticos



Fonte: Produzido pelo autor[36].

[36] Luhmann (1998, p. 27) e Rodrigues e Neves (2017, p. 37).

Reforça-se, por essa figura representativa dos sistemas autorreferenciais autopoiéticos, onde inseriu-se a Internet como um subsistema, o cibersistema, que a diferenciação funcional da Internet permitiu seu processo evolutivo (coevolutivo quando associado aos demais sistemas), abarcando inúmeras novas subfunções, subcódigos, de acordo com cada subsistema analisado. Observa-se o cibersistema da Internet como um conjunto de organizações, com função de ligações mais estreitas/específicas entre categorias de comunicação e categorias de pessoas (distinção 'membro/não membro')[37], tal qual ocorre nas organizações sociais, a distinção entre papéis, no caso dos sistemas psíquicos que fazem parte da estrutura específica (LUHMANN, 1983).

Complementando-se, de outro modo, o raciocínio quanto aos jogos eletrônicos, por exemplo, estes já existiam antes mesmo da Internet, porém, com ela, acabaram por ser basicamente digitais e *on-line*, não perdendo, assim, sua essência: jogar/não jogar, independentemente da conexão/desconexão em rede.

Embora possa se ter, como observador-usuário, a noção de que a Internet é basicamente um médium, um meio de comunicação, conforme busca-se observar, ela vai além disso, em razão do seu ambiente estrutural, da sua organização e composição, e da sua formação de autorregras (seja dentro das aplicações de Internet, seja no contexto geral, como, por exemplo, as regras sobre configuração de e-mails e as recomendações internacionais aos referidos serviços ou a distribuição e recomendações sobre as configurações do Protocolo de Internet – IP[38]). Seus algoritmos, compostos por dados e informações, carregados de memória sobre o que já foi realizado, por exemplo, por um outro sistema [usuário], conformam o próprio sentido do cibersistema: a partir da conexão, facilitar e ampliar evolutivamente também o espectro de outros sistemas.

2.2.1 Autopoiese no cibersistema da Internet

A autopoiese [ou autopoiésis] é caracterizada por corresponder a sistemas autorreferentes, autodesenvolvidos, auto-organizados, autorregulados, autorreprodutivos de uma unidade sistêmica, fechada. No dizer de Tonet (2019, p. 79), "a autopoiese se caracteriza pelo fechamento de produção e reprodução de seus elementos e, naquela, os sistemas geram

[37] Poder-se-ia desenvolver que essa distinção seria uma autodistinção, provocada pelos algoritmos, que ofertam a conexão (a amizade numa rede social, por exemplo), que ofertam uma facilidade (uma evolução do avatar no jogo, por exemplo), mas também é uma distinção a partir do sistema utilizador, no caso, especialmente, o psíquico.

[38] Vide https://www.iana.org/numbers (*Internet Assigned Numbers Authority*).

sentidos, observam as comunicações sistêmicas, se referindo para si mesmo (dentro) e para seu ambiente (fora)".

A autorreferência é correspondente ao sistema operando a diferenciação funcional com seu entorno (centro/periferia; sistema/entorno), pois o que o caracteriza é essa diferença entre o sistema e seu entorno. Essa perspectiva de sistema/entorno ou de centro/periferia, que caracteriza os processos autorreferentes, tem a possibilidade de auxiliar no enfrentamento da complexidade gerada, no caso, a partir da Internet, especialmente porque, paradoxalmente, quanto mais fechado o sistema for em suas operações – o que é o caso da Internet, com sua *programação 0/1* – mais aberto ele será em suas observações, ou seja, fechamento operativo e abertura cognitiva.

A autorregulação na Internet se correlaciona ao processo de estabilidade do sistema, mesmo quando há interações e alterações causadas por perturbações externas, advindas de outros sistemas, possibilitando o retorno da estabilidade[39]. Em face da autopoiese basal (CLAM, 2013[40]), que ocorre dentro do sistema, possibilita-se sua estabilidade, gerada pela sua auto-organização e pelo padrão de organização específico da Internet, com padrão e protocolo de interação único, algorítmico, por *bit* e *bytes*, por pacote de dados, por meio do Protocolo de Internet (o protocolo TCP/IP).

Como o cibersistema da Internet possui os seus próprios elementos, produtos de sua diferenciação funcional, ele (o cibersistema) se autoproduz e autorreproduz e tem a capacidade de se autorreparar, de se autoreestruturar, de se autotransformar e de se adaptar, por isso ele é autopoiético.

Porém, a autopoiese do cibersistema não é só basal, no interior do sistema. Ela é uma autopoiese derivada, ocorrendo também na membrana do sistema, possibilitando a sua lógica coevolutiva, mesmo porque é um sistema novo e não se encontra totalmente completo e, dada a sua característica, talvez nunca o seja. Ainda, pode-se dizer que é um dos poucos sistemas em que a diferenciação funcional também possibilita uma autopoiese estaminal (TONET, 2019, p. 26, 50-51 e 79-80), porquanto *bit* e *bytes* subsistem fora do cibersistema multi ou

---

[39] Essa autorregulação ocorre em um processo anterior ao sistema do Direito, com a estipulação de regras próprias dentro dos subsistemas (mídias sociais, por exemplo, onde Facebook tem, independentemente das regras de Direito dos países onde existem usuários cadastrados, regras específicas de remoção de conteúdo e de verificação de contas inautênticas), bem como outras regras adaptadas aos sistemas do Direito. Maranhão e Campos (2018) chamam isso de "autorregulação regulada".

[40] Livro elaborado em conjunto com Leonel Severo Rocha e Germano Schwartz.

pluriconectado e são os grandes responsáveis pelo processo de informação, com base em dados e produção de sentido, capaz de possibilitar comunicação com os demais sistemas[41].

Clam (2013, p. 81), ao abordar a autopoiese e as fases de Luhmann, pondera que a teorização realizada por este "se articula em torno de 'lugares' primordiais, tais como a complexidade, o sistema e seu ambiente, a dupla contingência, o sentido, o 'fazer experimentar' (*Erleben*) e o agir, a comunicação, o tempo, a autorreferência...", sem que estes tópicos sejam colocados em um esquema fictício ou hierárquico e que a leitura/compreensão de um não dependa da leitura anterior de outro (CLAM, 2013, p. 81; RODRIGUES, 2020).

Poder-se-á, então, questionar: ao que exatamente Clam (2013) se refere quando fala em "fazer experimentar" e "agir"? Os campos de relações, no sistemismo, são inter-relacionais, circulares e possuem uma "estrutura reticular de interdependência", sendo ao mesmo tempo difusos e nodosos e "não se permitem organizar de uma maneira transitiva ou hierárquica" (CLAM, 2013, p. 81) e, por serem inter-relacionais, também são interdisciplinares [uma das características primordiais da cibernética], o que permite à teoria ter seu próprio movimento e acessar todos os saberes possíveis.

A aplicação da teoria sistêmica, portanto, à Internet torna-se não só possível como necessária, dado o fluxo cognitivo atinente aos sistemas que são sensíveis e "incidentes de estipulações e de irritações provenientes de todos os tipos de pesquisa em ciências humanas" (CLAM, 2013, p. 83). A Internet, por sua estrutura organizacional, sua auto-organização, autorreferencialidade, autodesenvolvimento, tendo por sentido principal a informação capaz de gerar comunicação, possui campo de relações em todos os sistemas e subsistemas da sociedade contemporânea e possui, também, uma inter-relação e uma interdisciplinaridade inigualável à dos demais sistemas/subsistemas[42].

2.2.2 Informação, comunicação e diferenciação funcional com outros sistemas

Por ser o sentido da Internet [o dado e] a informação capaz de gerar comunicação, a aproximação estrutural, que ocorre no seu entorno, com os demais sistemas é percepcionada de diversas formas. A exemplo do sistema de saúde, cujo código binário é saúde/enfermidade (LUHMANN, 1998, p. 393), nada impede que uma dada informação/comunicação seja

---

[41] Tonet (2019, p. 51) refere que a "autopoiese estaminal não obedece aos limites temporais próprios de cada sistema, pois se produz fora dos seus ritmos, se produz pela comunicação. Dessa forma, a capacidade de observar as novas produções normativas descentralizadas caracteriza a nova forma de pensar autopoiético".

[42] Sobre as interpretações da Teoria Sistêmica de Niklas Luhmann e as relações com o sistema do Direito, vide Rocha, King e Schwartz (2009), Rocha, Schwartz e Clam (2013) e Schwartz, Pribán e Rocha (2015).

considerada própria deste sistema, porém também ser parte, por exemplo, do cibersistema da Internet, do sistema da Economia, do sistema do Direito, além de outros.

Nesse caso, por exemplo, pode-se referir que os dados pessoais relativos à saúde[43], porquanto armazenados no cibersistema[44], comunicam enfermidade ou saúde, importante para a definição e resposta do sistema da Saúde; e, no sistema Econômico, os mesmos dados pessoais, pelo código pago/não pago, comunicam a possibilidade ou impossibilidade de cura, respectivamente, pela existência ou não de condições financeiras do titular do dado; ainda, esses mesmos dados, indicando enfermidade ou saúde, podem ser analisados sob o prisma sistema do Direito, porém pelo seu código específico legal/ilegal, pois em razão da negação de um atendimento ao plano de saúde, em face da análise dos dados armazenados, essa comunicação específica pode irritar o sistema do Direito, podendo o detentor dos dados movimentá-lo para que seus direitos subjetivos sejam atendidos.

Tal comunicação, então específica do campo da Internet, conectada e enraizada no cibersistema, dos dados pessoais relativos à saúde, produz diferentes comunicações e irritações nos demais sistemas/subsistemas. Pode [essa comunicação, então] produzir essas irritações sistêmicas e, pela ótica do direito, como forma de reduzir complexidade, provocar o contingenciamento e a estabilização das expectativas normativas por um regramento normativo, como o instituído pela Lei Geral de Proteção de Dados (Lei nº 13.709/2018), visando à proteção, ao resguardo e à anonimização dos dados pessoais dos usuários da Internet no Brasil.

Em outra observação sistêmica, uma Constituição Federal comunica [sistemas, valores, diretrizes] para o sistema Político e para o sistema do Direito (SCHWARTZ, 2020), porém também comunica para o cibersistema, protegendo direta ou indiretamente os dados e informações e a comunicação quando relativos à privacidade, à intimidade, à liberdade de expressão, ou seja, à proteção de dados coletados pelas aplicações e relativos a todos os indivíduos que usam a Internet.

Da mesma forma, comunica-se, e é recepcionada pelo código do Direito, a necessidade de não discriminação, de igualdade formal e material, entre os usuários da Internet no caso, por exemplo, de um processo seletivo a uma vaga de emprego feita por um sistema de

---

[43] No Brasil, a regulação da proteção de dados pessoais foi prevista inicialmente na Lei nº 12.964/2015 (Marco Civil da Internet) e ampliada em normativa específica, a Lei nº 13.709/2018, com vigência a partir de agosto de 2020, a Lei Geral de Proteção de Dados (LGPD).

[44] Um relógio inteligente (*smartwatch*) conectado ao *smartphone*, por sua vez conectado à nuvem, coleta informações constantes de batimentos cardíacos, de deslocamentos, de utilização de aplicações várias, em regra algumas já sugeridas pelo próprio desenvolvedor e, também, outras aplicações instaladas pelo usuário.

inteligência artificial orientado para esse fim (resolver/não resolver), não se podendo, como dito, discriminar por sexo, cor, raça ou religião, dentre outros direitos protegidos constitucionalmente. Tal comunicação, por conter não apenas dados designativos da vida humana, porquanto também conter dados [e informações] que deveriam ser protegidos constitucionalmente, restou por irritar o sistema político brasileiro, pois que se discutiu a fundamentalização do "direito à proteção de dados" na Constituição Federal, por meio de um Projeto de Emenda Constitucional, nº 17/2019 (SCHREIBER, 2019), erigido à Emenda Constitucional nº 115/2022.

Por isso, a Internet, 'ofertando' as suas características supra e intersistêmicas, vai além de propiciar uma circularidade reflexiva, própria do seu sistema, permitindo uma polireflexividade entre os sistemas, da Política, do Direito, da Educação, da Economia, da Ciência, da Saúde etc. O que parece desconectado não o é: há interrelação sistêmica e polireflexividade.

Dado, então, a sua diferenciação funcional, o cibersistema da Internet também permitiria a análise sob a ótica de metacódigos, que podem vir a ser discutidos em razão da pós-conexão, da interação digital, como o da privacidade/não privacidade e o da anonimicidade/publicidade[45]. Por isso, o controle pelo Estado dos processos de comunicação e interação digital, com ordem/contraordem para taxação de conteúdo como desinformação, conforme o Projeto de Lei nº 2630/2020[46], iniciado no Senado Federal, tratando sobre "Fake News", pode ser tido como operação de coevolução de, ao menos, tripla reflexividade: Internet, Política e Direito (ver 4.3.2). Porém, é um processo complexo de circularidade reflexiva da comunicação, cognitivamente aberta e interagindo em diversos sistemas organizacionais e sociais, desde o Poder Judiciário, com o Inquérito Policial determinado pelo STF (FAKE, 2020), até o sistema político, que desconsidera outra comunicação advinda dos sistemas psíquicos (cidadãos brasileiros), contrários ao referido PL[47], e mesmo assim, aprovou e encaminhou à Câmara dos Deputados (CRUZ, 2020).

---

[45] O código da anomicidade é um código comum na Internet, seja ele visível ou invisível, porém, essa mesma comunicação da anomicidade, uma vez analisada sob a ótica do sistema do Direito no Brasil, é, também, avaliada pelo seu código específico, valorada na direção negativa, ou seja, ilegal, isso porque a Constituição Federal estabelece no art. 5º, IV, que é vedado o anonimato.

[46] O tema das *fake news* é retomado na pesquisa empírica e na análise da estrutura normativa brasileira, no terceiro e quarto capítulos, respectivamente.

[47] A pesquisa de opinião realizada pelo Senado Federal aponta que 424.819 brasileiros votaram contra a proposta do PL nº 2630/2020, enquanto 353.205 votaram a favor. Os dados constam na página do Senado Federal relativamente ao PL citado (vide https://www25.senado.leg.br/web/atividade/materias/-/materia/141944, acesso em 13 jan. 2023).

Autorreferência e heterorreferência do sistema político se tornam evidentes, especialmente esta quando contrastada com a comunicação das expectativas cognitivas advindas dos sistemas psíquicos enquanto entorno daquele sistema. O sistema político, então, por autorreferência, por autoproteção, dentro do seu fechamento operacional e autodesenvolvimento, tende(rá) a criar uma norma que vise justamente um interesse seu, do sistema político, e não dos cidadãos brasileiros, sendo, portanto, diferente sua retórica (de atender ao povo brasileiro) da prática discursiva (atender aos interesses do sistema político): a redução da complexidade tenderá então a selecionar expectativas e realizar seletivamente a congruência, generalizando expectativas normativas.

Aliás, a comunicação sobre as chamadas *fake news*, os processos de desinformação, tem irritado sobremaneira o sistema político brasileiro, já contemplando mais de 80 projetos de lei nas duas casas legislativas (CÂMARA, 2022), sendo parte considerável das propostas encaminhadas após 2020, ou seja, 2021 e 2022, pós início da pandemia do coronavírus, algumas delas com propostas de criminalização da conduta. O sistema político, então, tende(rá) a contingenciar duplamente sua escolha por atender ao seu código e, também, por receber a comunicação advinda da Constituição Federal quanto ao necessário encaixe de eventual norma penal às regras constitucionais.

2.3 Observações sobre observações cibersistêmicas

A leitura de Niklas Luhmann, base teórica referencial desta tese pautada na Teoria Geral dos Sistemas Sociais, não pode ser usada como um processo automático de solução e compreensão de problemas: "Quem busca fórmulas, conselhos, soluções prévias ou doutrinação, Luhmann não é autor para leitura nem pesquisa" (SILVA, 2018, p. 28). Porém, a partir do constructo de sua metateoria é possível compreender os sistemas sociais, organizacionais e psíquicos, onde e como se relacionam, como reagem e interagem, como expectam e, especialmente, como utilizam a comunicação nos processos de irritação e seleção da informação de acordo com cada diferenciação funcional, ou seja, conforme cada função específica.

Observar é constituir uma determinada realidade e, segundo Bôas Filho e Gonçalves (2013, p. 36), essa "realidade é uma construção do observador, faz parte do seu campo experimental", onde o "observador é entendido como parte do mundo que observa". Por isso, o que se apresenta nesta pesquisa é uma observação que procura constituir uma determinada realidade, a da investigação dos crimes cibernéticos no Brasil, porquanto, como parte do que

se observa, descreve-se o mundo que está frente aos olhos. Porém, não são só observações do que está em frente aos olhos, mas também observações sobre observações de outros sistemas, no caso, sistemas psíquicos que desenvolvem funções específicas na sociedade, nas organizações.

Nessa lógica luhmaniana, buscou-se inicialmente não necessariamente trazer solução a algum problema, mas sim tecer observações sobre como é possível compreender o cibersistema da Internet, ou seja, a Internet como um dos subsistemas do sistema social, desenvolvido a partir da evolução tecnológica e baseado em dados e informações, correspondentes a algoritmos.

Assim, nesta parte basal da tese, procurou-se, em um primeiro momento, analisar o conceito evolutivo de *sistema*, especialmente a partir do início do século XX até chegar à teoria desenvolvida por Niklas Luhmann, enfocando-se na principal característica sistêmica, ou seja, a autopoiese, a partir do que se pode idealizar o *sistema* como uma unidade, sistema necessariamente fechado em termos de sua identidade sistêmica, de sua autonomia sistêmica, um fechamento então operacional, de circulação de informação ou de comunicação, em acepção mais ampla. Essa ideia de autopoiese é fundamental, a partir de Maturana e Varela, para Luhmann delimitar um sistema como sistema fechado, pois se os sistemas são autopoiéticos, ou seja, sistemas fechados, são sistemas que se auto-organizam, se retroalimentam, se autorreferenciam e, por isso, são autopoiéticos.

Também, a partir da concepção de sistemas sociais e psíquicos, formatados por Luhmann homologamente a partir dos sistemas orgânicos (também fechados operativamente), ele também afirma que que os sistemas sociais são sistemas de comunicação e que cada qual apresenta um código binário, um polo positivo e outro negativo, que se caracterizam e são definidos a partir da sua função, ou seja, forma a sua diferenciação funcional.

Já num segundo ponto, partindo dos conceitos então analisados e da cibersociologia, afirma-se a Internet como um sistema, um cibersistema, cujo fechamento operativo é singular e sua diferenciação funcional caracteriza-se, internamente, pela existência de múltiplos e específicos códigos binários, pois dependentes de sua geolocalização digital (*digital space*), bem como pelo sentido, o limite da Internet, dado pela construção cultural dos observadores, porém, baseado totalmente em [dados e] informação, ou seja, o sentido-informação ou a informação-sentido, informação capaz de gerar comunicação.

Porém, alertou-se e alerta-se que, dentre todos os códigos possíveis, há um principal, um código que é responsável pela abertura e pelo fechamento operativo: *connect*/*disconnect*

(conexão/desconexão). Conexão ou não conexão a dados e informações capazes de gerar conhecimento/autoconhecimento, de reduzir complexidades e de produzir complexidades. Um positivo – *connection* – e outro negativo – *disconnection* –, possibilitando a relação do *sistema* da Internet com seu entorno.

Também, afiança-se que o processo (co)evolutivo da Internet possibilitou o desenvolvimento de subsistemas internos, como as mídias sociais, os jogos eletrônicos, a Inteligência Artificial, dentre outros, cada qual com sua diferenciação funcional e código específico.

Esses dados e informações, base da Internet, algoritmizados e capazes de gerar comunicação, permitem que uma dada informação/comunicação seja considerada própria deste sistema, porém também ser parte, por exemplo, do cibersistema da Internet, do sistema da Economia, do sistema do Direito, além de outros, tendo-se usado o exemplo dos dados pessoais relativamente à saúde e seu potencial discriminador e irritador nos sistemas envolvidos. Aliás, são os *dados pessoais* um meio de comunicação simbolicamente generalizado, tal qual o amor, a verdade etc., já que sua referência, em qualquer contexto, é compreensível no contexto hodierno.

A demonstração mais simplificada de que o sentido da Internet e dos computadores são os dados e informações que podem comunicar é visualizar essa informação e tentar compreendê-la:

01010110 01101111 01100011 11101010 00100000 01110011 01100001
01100010 01100101 00100000 01101111 00100000 01110001 01110101
01100101 00100000 01100101 01110011 01110100 01101111 01110101
00100000 01110100 01100101 01101110 01110100 01100001 01101110
01100100 01101111 00100000 01100100 01101001 01111010 01100101
01110010 00111111

Pode-se imaginar que, num simples olhar de qualquer sistema psíquico, essa informação, constante do cibersistema da Internet, não restou compreensível, mas encontra-se, de alguma maneira, registrada e armazenada em algum ambiente do ciberespaço, necessitando, pois, de elementos que ajudem a transformá-la em comunicação. Por isso, esse conjunto de ‘zeros e uns’ corresponde, tão-somente, à seguinte pergunta[48]: “Você sabe o que estou tentando dizer?”

[48] Para a codificação e decodificação foi usado o site https://www.invertexto.com/codigo-binario (acesso em 26 fev. 2023).

Reforça-se, por esses argumentos, que a Internet, dadas as suas características supra e intersistêmicas, com uma estrutura mundial e com uma rede de interação própria e com linguagem e programação específicas, vai além de propiciar uma circularidade reflexiva, própria do seu sistema, permitindo uma polireflexividade entre os sistemas, da Política, do Direito, da Educação, da Economia, da Ciência, da Saúde etc. Isso permite a discussão e análise do cibersistema da Internet sob a direção dos metacódigos, especialmente o da inclusão/exclusão, um código comum e suprasistêmico[49].

As expectativas cognitivas e normativas relativas a esta estrutura cibersistêmica precisam ser compreendidas, estruturadas, generalizadas e estabilizadas, e, por isso, a sua análise reflexiva com o sistema do Direito é fundamental. Mas não é menos importante a análise dessas expectativas frente ao sistema estrutural, por exemplo, da persecução criminal [no Brasil]. Porém, antes, é preciso compreender a logicidade envolvida nos papéis frente a esta estrutura, objetivo que se pretende alcançar já no próximo capítulo.

Há que se ir além? Sim, aqui o primeiro alerta: este princípio de análise da Internet como cibersistema não caracteriza o fechamento operativo do raciocínio quanto ao tema, pois a atemporalidade, perda de noção de espaço e não-freio da proliferação da informação, características da Internet, tal qual seu desenvolvimento e envolvimento social e espacial mundial do sistema mundo, geram, naturalmente, a sua (co)evolução, e, sob a ótica do sistema do Direito, a irritação que surge é quanto à estruturação de regras de controle e à necessidade de contingenciamentos, de generalizar congruentemente expectativas normativas[50].

Se o próprio Direito estrutura os conceitos do ambiente cibersistêmico, como a definição do art. 5º, I, do Marco Civil da Internet (Lei nº 12.965/2014), quanto à 'internet', como "o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes", não se pode absorver essa definição como aplicável para fora do sistema do Direito, porquanto esta estruturação normativa, gize-se, procurou compreender as comunicações do entorno num determinado momento e espaço.

---

[49] Sobre inclusão e exclusão, vide Ribeiro e Ribeiro (2015): "A inclusão há de ser compreendida como possibilidade de consideração social das pessoas; melhor dito, a inclusão é a forma cujo lado interior (inclusão) assinala a oportunidade de que as pessoas sejam reconhecidas socialmente e cujo lado exterior se mantém sem assinalar (LUHMANN, 2007, p. 492)".

[50] E, reforça-se, sequer se ponderou sobre os impactos no sistema do Direito relativos aos avanços tecnológicos e os implantes em humanos que estão sendo utilizados de maneira voluntária ou como tratamento médico, bem como aqueles que ainda serão desenvolvidos, como as interfaces mentais, mesclando o orgânico e o tecnológico-digital, a mente binária.

Há que se dizer, em outros termos, que essa definição não determina a Internet, pois ela só pode ser definida a partir de seu interior, de sua estrutura e organização evolutivas.

3 OBSERVAÇÕES SISTÊMICAS: EXPECTATIVAS COGNITIVAS E NORMATIVAS, INTERNET E DIREITO.

> "[...] a relação do homem com o mundo é constituída de *forma sensitiva*." (LUHMANN, 1983, p. 44).

Onde se encaixa o ser humano, o indivíduo, ou melhor, como compreender sua função nessas estruturas sociais que se formaram ao longo do tempo? Qual teoria melhor se adequa a essa finalidade de observar o indivíduo frente a situações em que suas expectativas e frustrações são constantes? Assim, antes de adentrar nas observações sobre os resultados da pesquisa empírica realizada nesta tese, objetiva-se situar e explicar essa correlação entre o indivíduo e seu papel frente a estrutura, claro que focando especificamente em um aspecto do sistema de persecução criminal: a investigação criminal cibernética e o responsável por essa investigação.

Niklas Luhmann (1983), ao observar sobre a sociologia do direito e a função do direito, analisou as teorias até então desenvolvidas e as classificou, em sua grande maioria, como unilaterais, por não vislumbrarem o contexto complexo da relação dos sistemas social e do direito, seja pela observação do aspecto da economia/propriedade (Karl Marx), seja pelo contrato como relação entre estrutura social e direito (Henry Summer Maine), seja pela concepção da solidariedade social e restitutividade sancionatória do direito (Émile Durkheim). Cada uma dessas teorias apresentou apenas um dos aspectos que o direito tem de apresentar nas sociedades modernas.

Mesmo Max Weber, com sua análise da ação social e tipos ideais, composta por uma subjetividade de sentido, acaba por não absorver todo o contexto social, e sua unilateralidade é apontada por Luhmnann (1983, p. 29) como sendo pautada em determinados interesses então dominantes. Já sobre a teoria desenvolvida por Talcott Parsons, Luhmann (1983) a afirma convincente como fundamentação funcional da imprescindibilidade de normas em sistemas sociais, porém ela é 'forçadamente dilatada' com a afirmação parsoniana de que a "estrutura dos sistemas sociais *constitui-se* de expectativas normativas, com o que ele exclui do sistema social as estruturas de outros tipos" (LUHMANN, 1983, p. 31).

Ao observar sobre as ideias de Eugen Ehrlich, reconhece que seu trabalho foi voltado ao desenvolvimento da dogmática jurídica comparativa, "evidenciando o papel dos institutos do direito, dos princípios jurídicos, das normas, das regras de argumentação etc., em sua função como se fossem sistêmicas de encaminhamento dos problemas" (LUHMANN, 1983, p. 33), ou seja, o direito é [tão-somente] a organização fática do comportamento em

corporações sociais, deixando de lado as diferentes funções dos sistemas parciais que surgem com o processo evolutivo da sociedade.

Ao abordar sobre as teorias e considerar suas contribuições para a sociologia do direito, Luhmann (1983, p. 33-4) alerta que o "direito não é determinado por si próprio ou a partir de normas ou princípios superiores, mas por sua referência à sociedade. [...] O direito surge então como elemento codeterminante e codeterminado desse processo de desenvolvimento". Então, faltava aos autores anteriores delimitarem qual a função do direito "como componente da estrutura dos sistemas sociais" (LUHMANN, 1983, p. 35).

Nem *hábito* (usos e costumes), nem *regras morais*, nem o *direito*, que formavam tipos de relações sociais abordadas historicamente, ou seja, formavam, segundo Luhmann (1983, p. 42), uma tipologia das normas e suas classificações, não eram e não são suficientes para desvendar a "independência funcional e a relação [...] entre os diferentes tipos" e "muito menos sua relação com outras estruturas cognitivas", pois é uma tipologia baseada em suposições de condições de "ilegalidade". Ao considerar um comportamento divergente, estas classificações o jogavam para fora da sociedade, quando, em verdade, continuam a ser uma condição inerente a ela.

Para Luhmann, essas teorias deixaram de questionar qual o *sentido* e a *função* do *dever ser*, devendo haver a necessária separação de personalidades e sistemas sociais, que são estruturas distintas de assimilação de experiência, embora o "material" da psicologia e da sociologia sejam os mesmos, devendo mudar-se a indagação quando se trate de uma ou outra, respectivamente, quanto à função de determinadas experiências ou ações estarem relacionadas à personalidade ou tematizadas no contexto funcional e estrutural dos sistemas sociais (LUHMANN, 1983, p. 44).

A necessidade de se ir além nas observações da real função do direito tem a ver com a complexidade e contingência das sociedades modernas, compreendendo-se como *complexa* a situação em que sempre existem mais possibilidades do que se pode realizar, levando a uma seleção forçada, e, como *contingente*, quando as possibilidades apontadas para as demais experiências poderiam ser diferentes das esperadas, o que leva ao perigo de desapontamento e necessidade de se assumirem riscos (LUHMANN, 1983, p. 46).

Nessa análise se concentram as expectativas e os desapontamentos, que precisam/podem ser estabilizados. Essa estabilização frente a desapontamentos ocorre, segundo Luhmann (1983), em razão de que as premissas de *experimentação* e do *comportamento* são enfeixadas [estruturadas], constituindo sistemas que evoluem quando reafirmam sua codificação funcional em relação ao seu entorno (FARÍAS, 2023).

> As comprovações e as satisfações imediatas são em parte substituídas por técnicas de abstração de regras confirmadamente úteis, e de seleção de formas adequadas de experimentação e de auto certificação. A esse nível de comportamento seletivo podem ser formadas e estabilizadas expectativas com relação ao mundo circundante. (LUHMANN, 1983, p. 46).

As expectativas se fundam nas formas comprovadas de seleção relativamente imunes a desapontamentos que aparecem como sentido, cuja identidade pode ser apreendida (coisas, homens, eventos, símbolos, palavras, conceitos, normas etc.). As expectativas estão, então, relacionadas à contingência e à dupla contingência, pois

> Reconhecer e absorver as perspectivas de um outro como minhas próprias só é possível se reconheço o outro como um outro eu. [...] Frente à contingência simples erigem-se estruturas estabilizadas de expectativas, mais ou menos imunes a desapontamentos [...] Frente à dupla contingência necessita-se outras estruturas de expectativas, de construção muito mais complicada e condicionada: as expectativas. (LUHMANN, 1983, p. 47).

A dupla contingência está, portanto, vinculada à expectativa de quem informa, ou seja, de compreensão da informação repassada, e, também, à expectativa de quem recebe a informação em relação a quem a informa, pois um depende do outro. "É duplamente contingente porque tanto quem informa depende de quem compreende, como quem compreende depende de quem informa" (SILVA, 2016, p. 57).

Para Silva (2016, p. 56), por serem meios autônomos em relação direta com o problema da improbabilidade da comunicação,

> os meios de comunicação simbolicamente generalizados (MCSG) – [...], ainda que pressuponham a codificação sim/não da linguagem e que respondam pela função de fazer esperável a aceitação de uma comunicação nos casos em que a negação é o provável – permitem-nos ter expectativas (cognitivas ou normativas). (SILVA, 2016, p. 56).

Assim, devido aos MCSG, destacados por Luhmann (2007) e referidos por Silva (2016), podemos nos comunicar sobre determinados temas independentemente de saber o que são, pois eles "viabilizam que ocorra uma perspectiva de aceitação da informação partilhada" (SILVA, 2016, p. 56). Então, podemos nos comunicar sobre Internet, mesmo não sabendo e compreendendo como está estruturada e organizada.

Segundo Luhmann (1983, p. 47), as estruturas de expectativas têm que ser construídas de forma mais complexa e variável, pois o comportamento do outro não pode ser tomado como fato determinado, ou seja, o comportamento do outro tem de ser expectável em sua

seletividade, como seleção entre outras possibilidades do outro, sendo que, porém, essa seletividade [do outro] é comandada pelas estruturas de expectativas do outro: "Para encontrar soluções bem integráveis, confiáveis, é necessário que se possa ter expectativas não só sobre o comportamento, mas sobre as próprias expectativas do outro".

Assim, quando se seleciona uma regra a ser seguida em detrimento de outra, abstratamente se molda uma estrutura normativa e se cria a expectativa de comportamento [do outro] de acordo com essa moldura, expectando-se também sobre a estrutura quanto à resposta pelo comportamento divergente.

Ou seja, o controle de uma complexão de interações sociais exige que cada um tenha uma expectativa sobre a expectativa que o outro tem dele, o que leva Luhmann (1983, p. 48) a dizer que na dupla contingência todo agir social tem uma dupla relevância:

> uma ao nível das expectativas imediatas de comportamento, na satisfação ou no desapontamento daquilo que se espera do outro; a outra em termos de avaliação do significado do comportamento próprio em relação à expectativa do outro. Na área de integração desses dois planos é que deve ser localizada a função do normativo – e assim também do direito. (LUHMANN, 1983, p. 48).

Essa estrutura de expectativas se torna fundamental nas contradições, ou seja, na expectativa sobre expectativas [A tem a expectativa de que B cumpra sua parte no acordo e B tem a expectativa de que A cumpra a sua parte], ou também na reflexividade das expectativas em vários planos, ou seja, expectativas sobre expectativas de expectativas [C tem a expectativa de que A e B cumpram o acordado; expectadores de um jogo *on-line* esperam que a equipe A e a equipe B joguem de acordo com as regras, o mesmo esperado por integrantes da A em relação a integrantes da B e integrantes da B em relação a integrantes da A]. É nessa reflexividade de expectativas que surgem os conflitos e que eles podem ser resolvidos:

> A adaptação social da reflexividade das expectativas [expectativas que se referem a outras expectativas] ainda pode ser possível em sistemas sociais pequenos e constantes, em famílias e grupos de amigos, nas faculdades tradicionais ou em pequenas unidades militares (e isso pelo menos no contexto de situações-problema), mas no caso de crescente complexidade dos sistemas sociais, ou no acúmulo de situações-problema em sistemas sociais simples, é necessária a criação de reduções, simplificações, abrandamentos, que poderão ter a forma física ou social. (LUHMANN, 1983, p. 50).

Luhmann faz a advertência anterior em razão do incremento da complexidade e da referência mútua das expectativas, o que gera um aumento da complexidade e o risco dos

erros. “Portanto, as simplificações, inevitáveis na busca de orientação, precisam estar, ao mesmo tempo, imunizadas contra o risco do erro” (LUHMANN, 1983, p. 50-1), ou seja, elas precisam poder preencher sua função estruturalizante em todos os aspectos, inclusive quando interpretam erroneamente a realidade ou as expectativas sobre a realidade.

Silva (2016), tratando do tema, observa que a comunicação é contingente em relação às suas três partes, ou seja, existe contingência tanto na seleção da informação quanto no modo de partilhá-la e, ainda, na sua compreensão, o que não se confunde com não ter expectativas quanto a estas três seleções. A escolha da informação, dentre as várias possíveis, assim como a escolha do modo de dar a conhecer, dentre os vários possíveis, é um processo contingente para *Alter*, que tem expectativas de ser compreendido e de sua comunicação ser efetiva, porém, ainda lhe é contingente o processo de compreensão de *Ego*.

Para Luhmann (1983, p. 51-2), os sistemas psíquicos e os sistemas sociais observam as expectativas de maneiras diversas.

> Os sistemas psíquicos parecem apoiar suas simplificações principalmente na circunstâncias [sic] de que a expectativa sobre expectativas alheias pode ser conduzida como questão interna ao próprio sujeito. [...] Tais expectativas sobre expectativas podem, com o auxílio de esquematizações interpretativas altamente flexíveis, ser praticamente imunizadas contra a refutação através da expectativa fática e do comportamento do outro. (LUHMANN, 1983, p. 51).

Já os sistemas sociais, segundo Luhmann (1983, p. 52), “utilizam um outro estilo de redução [generalizante]. Eles estabilizam expectativas objetivas, vigentes, pelas quais ‘as’ pessoas se orientam. [...] O importante é que se consiga uma simplificação através de uma redução generalizante”. Ou seja, essa redução é o resultado de uma abstração, de uma generalização.

Nos sistemas sociais, as expectativas podem estar verbalizadas por normas do dever ser [abstração], por determinações qualitativas, delimitações da ação, regras de cuidado etc., ou seja, não servindo apenas para tornar comportamentos previsíveis, mas também servindo para regular a expectativa sobre expectativas. Então, as sínteses regulativas não são captadas apenas da visão da expectativa comportamental, mas também em decorrência da garantia do cumprimento conforme as expectativas:

> Essa função tem seu centro de gravidade no plano reflexivo da expectativa sobre expectativas, criando aqui segurança em termos de expectativas, à qual se segue, apenas secundariamente, a segurança sobre o comportamento próprio e a previsibilidade do comportamento alheio. [...] Isso porque a segurança na expectativa sobre expectativas, seja ela alcançada por meio de estratégias puramente psíquicas ou por normas sociais, é uma base imprescindível de todas as

> interações, e muito mais importante que a segurança na satisfação de expectativas. (LUHMANN, 1983, p. 52-3).

Há que se dizer, então, que a estruturação de normas exerce sua função de redução congruentemente generalizada, ou seja, de seletividade comportamental, sobre a qual são formadas expectativas normativas, e eventual comportamento divergente é visto como um desapontamento.

Buscando colocar em prática as observações de Luhmann em razão do contexto da Internet, expectativas cognitivas e expectativas normativas, comportamentos convergentes e comportamentos divergentes, utiliza-se o seguinte exemplo:

No caso de A esperar que surja uma oferta de um produto na Internet e B faça-lhe a oferta de um produto com desconto, A, portanto, espera que B lhe entregue o produto e B espera que A lhe repasse o valor pelo produto. C, por sua vez, também sabendo que A quer um produto abaixo do valor de mercado, oferta-lhe uma promoção. A deve escolher entre as ofertas, repassar o valor e tem a expectativa de receber o produto. Tem de escolher qual risco assumir. A observa que B oferta o produto, um pouco mais caro que C, em um site [aplicação] que garante a entrega do produto ou a devolução do dinheiro, e que também cumpre a previsão do Código de Defesa do Consumidor. A também observa que C está ofertando seu produto nas redes sociais e tem boas avaliações quanto à entrega. A observa ainda os meios de pagamento em relação a B e a C, respectivamente, com cartão de crédito e transferência financeira via PIX. A observa então que C, mesmo tendo um produto mais barato, não lhe apresenta a mesma garantia de entrega do produto, embora afirme que sim.

Em ambos os casos, A tem expectativas cognitivas sobre a compra e o produto e expectativas normativas quanto à entrega do produto, mais ou menos estruturadas. A ainda tem a expectativa de, frente às regras normativas, buscar a reparação do dano ou, no caso de um comportamento divergente doloso de não entrega do produto, acionar a estrutura policial e o sistema e persecução penal. Ainda, além da estrutura normativa de proteção ao consumidor, A tem, especialmente em relação a B, a expectativa de um risco menor, pois o site em que este [B] oferta o produto contempla uma autorregra de garantia da entrega do produto ou devolução do valor.

Essas normas, estruturadas funcionalmente pelo Direito ou por autorregras, podem gerar a segurança, mas não vão impedir que B e C tenham comportamentos divergentes e frustrem as expectativas de A, do sistema do direito ou das regras do site, não entregando o produto e/ou induzindo A a uma compra fraudulenta. Aliás, no caso do sistema do Direito no Brasil, há o contingenciamento de expectativas tanto por regras normativas do consumidor

quanto por regras de direito penal, circunstância em que, uma vez frustrada a expectativa de A em relação à entrega do produto, num ou noutro caso, a comunicação gerada poderá acionar a avalição de aplicação das respectivas sanções, quando cabíveis.

Assim, ao tratar das expectativas concretas – e das abstrações que as regulam e a integram –, Luhmann (1983, p. 53) destaca que a referência à complexidade e à contingência no âmbito da experimentação, acrescentando a elas – as expectativas – a função de uma *estrutura*, esta, em geral, é definida "por uma propriedade, isto é, por uma constância relativa", porém, na verdade, o que se deve questionar é o porquê dessas constâncias relativas serem necessárias. Luhmann (1983, p. 54) então define a *estrutura* através da sua função de fortalecimento da seletividade, na medida em que ela possibilita a *dupla seletividade*, pois existem diversos passos da seleção.

Segundo Luhmann (1983), a estrutura de seleção continua sendo seletiva mesmo quando ela não é realizada conscientemente, ou seja, quando é simplesmente vivenciada, pois existem outras possibilidades e elas se apresentam ao ocorrerem desapontamentos de expectativas, sendo que é "nessa possibilidade de desapontamento e não na regularidade de satisfação que se evidencia a referência de uma expectativa à realidade". Como as estruturas sedimentam como expectáveis um número mais delimitado de possibilidades, "elas são enganosas com respeito à complexidade do mundo" e permanecem, por isso, expostas aos desapontamentos. "Do ângulo do sistema psíquico, portanto, podemos dizer: elas regulam o medo" (LUHMANN, 1983, p. 55).

O que importa dizer é que toda estrutura tem em si, imanente, o problema do desapontamento, ao passo que a avaliação da adequação de estruturas, segundo Luhmann (1983, p. 55), deve sempre considerar o problema do desapontamento. Racionalizar uma estrutura significa dosar entre complexidade sustentável e carga suportável de desapontamentos. Para a estabilização de uma estrutura, ela não contém apenas o esboço "coerente do seu perfil" (leis naturais, normas etc.), mas igualmente a disponibilidade de mecanismos para o encaminhamento de desapontamentos (manutenção ou reparo da estrutura).

Essa relação de dependência entre estrutura e desapontamentos é que força a aceitação de riscos. Existem duas possibilidades contrárias de reação a desapontamentos de expectativas: a) existe a alternativa de modificação da expectativa desapontada, adaptando-a à realidade decepcionante; b) existe a alternativa de sustentar a expectativa e seguir a vida protestando contra a realidade decepcionante. Ou seja, trata-se de expectativas cognitivas ou expectativas normativas, cuja diferenciação se dá em termos funcionais, tendo em vista a

solução de um determinado problema: “Ao nível cognitivo são experimentadas e tratadas as expectativas que, no caso de desapontamentos, são adaptadas à realidade. Nas expectativas normativas ocorre o contrário: elas não são abandonadas se alguém as transgride” (LUHMANN, 1983, p. 56).

> Dessa forma as expectativas cognitivas são caracterizadas por uma nem sempre consciente disposição de assimilação em termos de aprendizado, e as expectativas normativas, ao contrário, caracterizam-se pela determinação em não assimilar os desapontamentos. [...] as normas são *expectativas de comportamento estabilizadas em termos contrafáticos*[51]. Seu sentido implica na incondicionalidade de sua vigência na medida em que a vigência é experimentada, e portanto também institucionalizada independente da satisfação fática ou não da norma. (LUHMANN, 1983, p. 57).

Em outros termos, Silva (2016, p. 56-7) procura diferenciar as expectativas cognitivas [“aquelas passíveis de serem alteradas a cada conhecimento novo”] das expectativas normativas [“as contrafáticas, que persistem ao invés de mudarem ou se amoldarem e adaptarem diante de desenganos”], porém, alerta que a “expectativa não é um estado atual da consciência de um indivíduo em particular, mas a temporalidade do sentido nas comunicações”.

No exemplo anterior, da busca de A por adquirir um produto ou de B ou de C, o desapontamento com a não entrega do bem pago pode ocasionar em A uma assimilação, modificação ou abandono da expectativa e, pelo menos, um aprendizado, permanecendo a expectativa normativa das regras do Direito (de consumo, cíveis e penais) e das autorregras do site (no caso do vendedor B), ou seja, elas não são abandonadas.

Para Luhmann (1983, p. 61), a ausência de uma classificação de uma situação de desapontamento, especialmente nas situações pré-jurídicas, e de uma denominação para ela, traz consigo uma impossibilidade de estereotipagem, “dificultando a percepção da possível homogeneidade de uma multiplicidade de singularidades, fazendo com que elas não sejam facilmente sentidas como ameaçadoras”. Ou seja, os desapontamentos são tratados caso a caso e essa concreção do processamento da experimentação dá origem à construção de alternativas.

> A separação entre expectativas cognitivas e normativas exige que o risco seja deslocado para o interior da estrutura de expectativas, onde ele emerge à consciência e é controlado. Trata-se [...] de deslocar o duplo problema de

[51] A expectativa da vigência contrafática é expressada no símbolo do “dever ser”, expressando o sentido e a função dele, onde o dever ser não é menos fático que o de ser.

> complexidade e da contingência para o interior da própria estrutura de expectativas, que a partir daí é obrigada a sustentá-lo na forma de uma contradição. (LUHMANN, 1983, p. 62).
> [...]
> Além disso formam-se, tanto na esfera das expectativas cognitivas quanto na das normativas, estratégias de minimização de riscos. No âmbito das expectativas cognitivas persiste a possibilidade de que desapontamentos não sejam assimilados. Com relação às expectativas normativas existem possibilidades de assimilação. A minimização do risco, portanto, é obtida através de um momento estranho ao estilo da expectativa, através da introdução encoberta da possibilidade do comportamento oposto. (LUHMANN, 1983, p. 63).

Buscando condensar o contexto das expectativas cognitivas, segundo Luhmann (1983, p. 63), elas correspondem às situações em que: (a) há disposição à assimilação; (b) mantém-se a expectativa; e (c) o desapontamento é tido como exceção. Por isso, reforça Luhmann que:

> O esquema regra/exceção, a concepção de desdobramentos normais e irregulares, e ainda a construção de uma complicada visão de mundo, sustentada por hipóteses básicas e abstratas e quase irrefutável, garantem um alto grau de imunização perante desapontamentos também no caso de expectativas cognitivas. (LUHMANN, 1983, p. 63).

Já quanto às expectativas normativas (LUHMANN, 1983, p. 63-4), tem-se que: (a) expectativas repetidamente desapontadas têm seus limites; (b) a inserção de possibilidades contrárias não anula o direcionamento original [regras, exceções, desapontamentos], que continua constituindo a base do comportamento regular; e (c) ninguém se ridiculariza ao sustentar suas expectativas no âmbito normativo, professando-as apesar das decepções.

As observações de Luhmann (1983) sobre as expectativas [dos sistemas psíquicos e sistemas sociais] o fizeram apontar um *terceiro modo de combinação das expectativas cognitivas e normativas*: possibilidade de ter expectativas sobre expectativas [dupla reflexividade], ou seja, formação de cadeia de expectativas, com possibilidades de assimilação e possibilidades de não assimilação: “No caso da dupla reflexividade, portanto, temos quatro possibilidades de combinação: cognitivo-cognitivo, cognitivo-normativo, normativo-cognitivo, normativo-normativo – e esse número de possibilidades cresce proporcionalmente à frequência da reflexividade” (LUHMANN, 1983, p. 64).

Nessa plêiade de possibilidades combinatórias de reflexividade das expectativas, baseadas na sua frequência, destaca-se que somente através “da expectativa normativa de expectativas, o estilo dessas expectativas pode ser submetido a regras normativas”, e os aspectos “de assimilação ou não, no caso de desapontamentos, é tão importante ao ponto dela

[sic] não poder ser relegada ao arbítrio privado. A escolha de um ou outro tipo tem que ser institucionalizada" (LUHMANN, 1983, p. 64).

> Uma diferenciação entre os estilos cognitivo e normativo das expectativas só se estabelece se a própria opção por um desses estilos é expectável; só assim ela torna-se socialmente regulada, só assim ela pode ser prevista. A expectabilidade das expectativas dos outros é, assim, uma sólida conquista no convívio humano. É só a partir dessa base que podem formar-se expectativas especializadas no sentido normativo e na sua manutenção, mesmo no caso de desapontamentos.
> O caso contrário, ou seja, o da expectativa cognitiva de uma expectativa normativa ou cognitiva, privilegia a assimilação individual e não a regulamentação social. Aqui o indivíduo está orientado no sentido da assimilação das expectativas dos outros, sejam elas normativas ou cognitivas. Ele não estabelece normas, mas toma conhecimento de eventuais surpresas e está em condições de adaptar-se se outros reformulam suas expectativas normativas ou cognitivas. (LUHMANN, 1983, p. 65).

Exemplos dessa última afirmação de Luhmann estão na aprovação e no sancionamento de uma nova lei, decisão jurídica inesperada etc. Tanto num caso quanto no outro, expectativas foram selecionadas e normatizadas, porém isso não impede a sua manutenção em face dos desapontamentos, respectivamente, à nova lei ou à decisão jurídica dada. Porém, "estruturas seletivas de expectativas, que reduzam a complexidade e a contingência, são uma necessidade vital. É por isso que a não satisfação de expectativas se torna um problema", afirma Luhmann (1983, p. 66).

Alertam Schwartz, Ribeiro e Ribeiro (2020, p. 467) que a seleção realizada pelos/nos sistemas sociais é sempre contingente, "no sentido de que haveria outras possibilidades de escolha", significando que as "não escolhas" geram frustrações/desapontamentos, podendo haver, por outro lado, a partir de uma escolha forçada "de uma alternativa de solução", um resultado de escolha equivocada, o que não é diferente no processo de construção da legislação pelo poder político.

Assim, o processo de estruturação seletiva das expectativas do Poder Legislativo é realizado com base em projetos de lei (PLs), tanto na Câmara dos Deputados quanto no Senado Federal. Essas expectativas são estruturadas por ação dos deputados ou senadores que as recebem de outras organizações, movimentos sociais, movimentos organizados, grupos de ativistas, pesquisadores, setores do comércio, indústria etc., cada qual com uma série de expectativas. A existência de um projeto sobre determinado tema não obsta a manutenção de expectativas e o encaminhamento de outras propostas sobre o mesmo tema, que passam a ter, segundo o sistema legislativo, uma atenção protocolar.

Mesmo durante o processo de análise e encaminhamentos, as expectativas [cognitivas/normativas] dos atores e sistemas sociais e organizacionais envolvidos são postas em análise, frente também às expectativas [normativas] do próprio sistema legislativo, num contexto de complexidade e dupla contingência face à reflexividade das expectativas e, por que não dizer, polireflexividade das expectativas. Vide, por exemplo, o conjunto de propostas normativas sobre o tema das *fake news* [item 4.3.2].

Há que se observar, também, que o poder político central, o Poder Executivo, também tem a tarefa e a incumbência de irritar o sistema legislativo com suas propostas normativas, que, por sua vez, podem colidir com os interesses e as expectativas dos sistemas psíquicos e dos sistemas sociais. Por outro lado, também pode o Poder Executivo absorver, organizar e selecionar as mais variadas expectativas sobre um determinado tema e encaminhar uma proposta normativa, provocando o sistema legislativo a um debate complementar e necessário para a formatação da norma, já com as expectativas manifestadas pelo conjunto de sistemas interessados, não se afastando, por lógico, a geração de novas expectativas sobre as expectativas já estruturadas, já normatizadas.

Esses caminhos de análise de expectativas sobre expectativas pode ser observado na discussão e nos encaminhamentos tanto da Lei nº 12.965/2014 (Marco Civil da Internet) quanto da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados), cujos procedimentos iniciais foram pautados pelo Governo Federal, coletando as expectativas dos mais variados sistemas psíquicos, sociais e organizacionais, formatando, inicialmente, anteprojetos de lei e, posteriormente, em nova rodada de análise e observações sobre as expectativas geradas sobre as expectativas já condensadas e registradas, Projetos de Lei para análise do sistema legislativo[52].

Neste ‘âmbito de discussão’, velhas e novas expectativas foram analisadas e, em razão da complexidade inerente aos temas, operando-se a seletividade e a redução de complexidade, o que não afastou a geração de novas complexidades, especialmente, por exemplo, em face da constitucionalização do direito fundamental dos dados pessoais (EC nº 115/2022) e do projeto de LGPD Penal (do Anteprojeto, criado por uma comissão, e o PL nº 1515/2022)[53]. Essas circunstâncias também fazem parte da estruturação necessária das

---

[52] Sobre o Marco Civil da Internet, ver todo o processo de discussão pré-legislativo em http://pensando.mj.gov.br/marcocivil2009/ (acesso em 21 fev. 2023). Também ver Cruz (2015), Murilo (2015) e Foletto (2010).

[53] Ver 4.4.1.

expectativas, pois que algumas expectativas [não estruturadas] continuam sendo apenas expectativas.

Para Luhmann (1983, p. 66), "desapontamentos levam ao incerto" e, por isso, não podem ser deixados ao alvedrio de decisões individuais:

> A repercussão do desapontamento de expectativas normativas, extravasando os casos individuais, demonstra-se através da força da reação. [...] Seu acionamento [dos mecanismos psíquicos], por outro lado, não pode ser ignorado pelo sistema social. **O tratamento do desapontamento não pode ser deixado a cargo apenas dos mecanismos individuais de excitação e tranquilização**. Existe o duplo perigo de que o desapontado, devido à excitação, aja de forma imprevisível, que ele, para salvar uma expectativa, desaponte muitas outras expectativas, ou seja, crie mais problema que soluciona; [...] É por isso que o sistema social tem que orientar e canalizar o processamento de desapontamentos de expectativas – e isso não só para impor eficazmente expectativas corretas (p. ex. normas jurídicas), mas sim para criar a possibilidade de **expectativas contrafáticas, que se antecipem a desapontamentos, ou seja: normativas**. [...] A canalização e o arrefecimento de desapontamentos fazem parte da estabilização de estruturas. (LUHMANN, 1983, p. 67, grifos nossos).
>
> Mesmo no caso de desapontamentos a expectativa deve poder ser manifestada. [...] Ela tem que encontrar, apesar de tudo, um lugar e um sentido no mundo; precisa poder persistir. E isso só é possível com determinados sustentáculos sociais.
>
> Muitas transgressões às normas são superadas, ou despidas de suas implicações simbólicas, apenas por serem ignoradas. [...] Esse ignorar tem em vista não os fatos, mas a norma; ele a protege contra informações discrepantes que a questionam, e protege aquele que se desaponta da obrigação de reagir. Essa proteção está baseada na circunstância de que as normas se enraízam em comunicação, e não em fatos. (LUHMANN, 1983, p. 68).

Assim o é [ao menos era] com relação à primeira redação do art. 154-A do Código Penal, dada pela Lei nº 12.737/2012, porquanto as expectativas geradas sobre a estruturação normativa e sobre os desapontamentos a ela estabeleceram, via comunicação, uma proteção simbólica nos casos de invasão de dispositivos informáticos. Os desapontamentos continuaram acontecendo, mas a expectativa normativa continuou ativa e manifesta. Porém, novas expectativas foram geradas sobre essa expectativa normativa em face dos casos de desapontamento e da linguagem [penal] complexa consubstanciada na estruturação do tipo penal, cuja comunicação irritou o sistema legislativo e nova seletividade de expectativas foi observada e realizada, modificando-se a expectativa normativa anteriormente posta, pela Lei nº 14.155/2021 [que deu nova redação ao art. 154-A], para que os comportamentos desapontadores, divergentes à norma, pudessem ser questionados.

Portanto, com base em Luhmann (1983, p. 68), expectativas normativas novas são geradas com a reestruturação desse documento normativo, ampliando a seletividade de condutas divergentes, desapontadoras da seletividade normativa realizada e expectável pelos demais sistemas.

> A norma permanece norma, e a 'causa' do desapontamento reside no comportamento divergente.
> Dessa forma não apenas isola-se, individualiza-se, personaliza-se o acontecimento, mas ao mesmo tempo é fornecido um ponto de referência para uma *explicação* do *desapontamento*. As explicações de desapontamentos têm a função de acomodar no mundo o desapontamento que se tornou inegável enquanto fato. [...] A expectativa e o acontecimento têm que ser simbolicamente isolados de tal forma que o acontecimento não possa afetar a expectativa, não colocando em questão a continuidade. (LUHMANN, 1983, p. 69).

Alerta Luhmann (1983, p. 71) que "é preciso considerar que nem todo tipo de explicação é compatível com o estilo normativo de expectativas". Luhmann quer dizer que algumas explicações precisam ficar reservadas à esfera cognitiva e não abranger o estilo normativo.

> Seja qual for a explicação escolhida para o desapontamento, sua função consiste em possibilitar a manutenção da expectativa apesar de acontecimentos discrepantes. Esta não é só uma questão de interpretação. [...] **Uma expectativa constantemente desapontada, sem poder manifestar-se, esvai-se. Ela é imperceptivelmente desaprendida e, finalmente, seu próprio sujeito não mais acredita nela**. Ele acostuma-se ao desapontamento e lembra-se eventualmente da sua expectativa 'propriamente dita'. (LUHMANN, 1983, p. 71, grifos nossos).

Pelas observações feitas, há que se afirmar, com base luhmaniana, que

> A contribuição da expectativa normativa para o desenvolvimento de sistemas complexos está relacionada a sua tendência a dilatar as possibilidades de expectativas, juntamente com sua interação contrafática. [Esse mecanismo] gera as possibilidades do esperar-se normativamente, com relação ao qual o direito pode ser uma estrutura seletiva. (LUHMANN, 1983, p. 76).

No entanto, essas ponderações feitas têm uma base temporal, uma dimensão temporal, havendo necessidade de se explorar também outras dimensões, quais sejam, a social e a material/objetiva. Esse grupo de mecanismos é, portanto, especializado "para a estabilização *temporal* e para a imunização das expectativas frente ao desapontamento, apenas preenche aquela primeira necessidade de alta variabilidade do sistema" (LUHMANN, 1983, p. 76).

Observa Luhmann (1983, p. 76) que a institucionalização produz uma 'seleção evolutiva' na medida em que se escolhe 'consensualmente' quais projeções normativas são úteis em uma [determinada] sociedade. Projeta-se, então, na dimensão social, "uma extensificação e intensificação das vinculações temporais normativas" (LUHMANN, 2016, p. 173), o que produz novas oportunidades de consenso/dissenso, produz situações de decisão

e esta, por sua vez, é "definida de tal modo que se tem de decidir a favor ou contra a expectativa" (LUHMANN, 2016, p. 173).

Assim, para Luhmann (1983), são normais as contradições entre expectativas, e os conflitos são uma condição para a manutenção do sistema social num ambiente de grande complexidade. Pelo fato de as expectativas não poderem estar constantemente ou continuamente expostas a desapontamentos/serem desapontadas, é que elas, as expectativas normativas, têm que ser direcionadas de forma a poderem ser bem-sucedidas. Por tal motivo é que Luhmann faz a abordagem do tema da *institucionalização de expectativas comportamentais*, pretendendo com ele delinear "*o grau em que as expectativas podem estar apoiadas sobre expectativas de expectativas supostas em terceiros*" (LUHMANN, 1983, p. 77, destaque no original).

Podemos descrever tal reflexividade de expectativas, por exemplo, entre os atores de investigação criminal e as organizações/empresas responsáveis pelas aplicações de Internet, pois aqueles esperam que estas atuem de acordo com a Lei e repassem os dados [cadastrais ou de *logs* de criação e/ou de acesso], enquanto que as organizações/empresas responsáveis pelas aplicações de Internet também são as que esperam que a interpretação dada por eles sobre a Lei e sua obediência a regras normativas de outros países [ou a obediência a regras e procedimentos de cooperação internacional] sejam compreendidas pelos investigadores e que determinados pedidos não sejam formalizados. "Nem todos podem esperar tudo concretamente, e tampouco todos podem realizar todas as ações esperadas" (LUHMANN, 1983, p. 78).

E como se resolve esse conflito entre *atores*? Institucionalizando as expectativas, através de um terceiro não interessado, neutro, 'anônimo':

> É exatamente a indeterminação, o anonimato, a imprevisibilidade e a incógnita de terceiros relevantes que garante a confiabilidade e a homogeneidade das instituições. Ela se baseia na neutralização de todas as referências que levam a que determinados terceiros possam ter outras expectativas que as esperadas. (LUHMANN, 1983, p. 84).

Para Luhmann (1983, p. 92-3, destaque no original), o desenvolvimento de instituições especificamente jurídicas consistiu "na *diferenciação de papéis especiais e de sistemas parciais com poder decisório sobre o direito, de efeito vinculativo em termos sociais globais*", o que possui forma básica da institucionalização do institucionalizar expectativas comportamentais, realizando uma maior abstração, uma maior precisão, uma maior

segurança motivacional em um único ponto (o papel do juiz) e "a partir daí transferindo-as a toda a estrutura de expectativas".

Assim, além de uma abordagem das expectativas cognitivas e normativas a partir de uma dimensão temporal, passa-se por uma necessária abordagem da dimensão social e a absorção dessas expectativas por meio da institucionalização das expectativas comportamentais e, como complementação, uma abordagem sobre os planos de abstração em um nível, em uma dimensão prática/objetiva.

Por que isso? Quanto mais complexa for a sociedade, maior tenderá a ser o nível de abstração e, por isso, o processo de generalização congruente do direito tende a agir estabilizando expectativas e comportamentos: "Aparentemente o que ocorre é que com a crescente complexidade da sociedade *todos* os planos da generalização são *mais fortemente* exigidos, tendo então que ser mais nitidamente diferenciados" (LUHMANN, 1983, p. 104), diga-se, esses planos de abstração precisam ser compreendidos de acordo com as expectativas comportamentais, o que é considerado, o que é valorizado, o que é avaliado etc.

Para promover a abstração necessária, existem as estruturas ou o processo de estruturação das expectativas, ao passo que Luhmann (1983, p. 99-104) questiona: "de quais estruturas sociais depende o grau de abstração necessário ao ordenamento menos atritivo possível das expectativas?"

Responde Luhmann ao seu próprio questionamento, pois há necessidade de diferenciar os diversos *planos de abstração*. Aborda-se este tema justamente para compreender onde estão [inseridos] os atores de investigação policial nessa análise sobre as expectativas cognitivas e normativas.

Quadro 2: Estruturação de expectativas comportamentais de acordo com Luhmann (1983)

Expectativas comportamentais Sobre →	*Pessoas* concretas	[Valoriza] Características (pessoais)
		[Considera] Experiências
		[Considera] Ações
		[Avalia] Interação (pessoal/intimidade)
		[Avalia] Possibilidades de autoexposição
		Qualquer deslize comportamental é assumido moralmente
	Determinados *papéis* [atores sociais]	[Desconsidera] características pessoais e individuais
		Podem ser assumidos por diferentes atores
		As expectativas tornam-se transferíveis de uma pessoa a outra

		Avança-se em termos de abstração
		Avança-se em termos de riscos
		Pode predominar uma determinada *intenção* ou determinada *atitude* ou *convicção mais íntima*
		Podem ser definidos por *relação hierárquica* ou *critérios de companheirismo*
		Podem agregar elementos intencionais e de convicção
		Estabiliza-se a expectativa pela indiferença
		Em caso de desapontamentos, poucas frustrações são relevantes
	Determinados *programas* [fins, normas]	[possuem] grau de abstração muito mais alto e fortemente variável
		Regra decisória pode valer para uma multiplicidade de *pessoas* e *papéis*
		As regras podem ser modificadas nos casos em que pessoas ou papéis percam sua identidade
		A vigência da regra não é afetada pela morte da pessoa concreta ou pelo fato de determinados papéis desaparecerem
		As condições de aplicabilidade [dos programas] são especificadas
		[Dupla função] de servir de apoio às decisões e às expectativas
	Determinados *valores*	Nível mais abstrato da generalização
		[São] julgamentos sobre a preferibilidade de ações
		Fornecem referências muito indeterminadas para a formação e a integração de expectativas
		[Apresentam] complexidade muito indeterminada com referência às ações permitidas
		Oferecem grandes possibilidades de consenso
		[Baseados no consenso] são dificilmente modificáveis
		Não existe ‘sistema de valores’
		Não existe ‘hierarquia de valores’
		Sua urgência depende do grau em que outros valores também estejam sendo afetados e do próprio grau de cumprimento

Fonte: Produzido pelo autor (2023).

As *pessoas*, os *papéis*, os *programas* e os *valores* representam, assim, diferentes momentos da generalização, planos "através dos quais expectativas comportamentais podem ser enfeixadas por meio de um princípio objetivo de identificação, e assim ancoradas no mundo exterior" (LUHMANN, 1983, p. 104). Essa classificação não significa, segundo Luhmann (1983), que essa separação no plano do sentido leve ao isolamento de cada um dos momentos de generalização; pelo contrário, eles se pressupõem e se condicionam mutuamente.

O que Luhmann quer dizer é que, mesmo se trocarmos valores ou que eles sejam atacados, não há necessidade de tocar ou trocar os papéis ou a identidade de pessoas. Porém, em nome de valores é que podem ser reestruturados programas e papéis. O importante é reconhecer que todos os planos de sentido, segundo Luhmann (1983, p. 105), sempre participam da formação de expectativas e, nas sociedades mais modernas, o centro de gravidade desloca-se principalmente para os *papéis* e *programas*, pois é somente nesses planos que "a complexidade da sociedade pode ser reproduzida adequadamente" (LUHMANN, 1983, p. 107).

Aliás, é por meio dos papéis e dos programas que se legitimam, dentro dos sistemas sociais, atuações e decisões, em que os comportamentos dos atores envolvidos seguem um comportamento interrelacional, exercendo interações contínuas com outros atores dentro de um programa (LUHMANN, 1980, p. 71-77). O direito, então, deslocou-se, na contemporaneidade, para os planos dos papéis e programas, porquanto a mutabilidade das complexões de expectativas no direito não está mais vinculada a pessoas ou a valores.

Assim, embora não se desconsiderem, nesta pesquisa, as 'pessoas' vinculadas aos papéis de *atores de investigação policial*, parte-se destes para observar e compreender suas expectativas sobre, especialmente, a estrutura normativa consolidada/em consolidação sobre os crimes cibernéticos no Brasil, observando-se, também, suas expectativas sobre seu próprio papel como terceiro institucionalizado frente aos danos cibernéticos e, ainda, sobre suas expectativas em relação à estrutura organizacional construída/em construção para o enfrentamento da criminalidade cibernética.

Ademais, os outros atores da persecução criminal não são desconsiderados nesta pesquisa, porém não são os promotores e juízes os observados, nem quanto às suas expectativas, nem quanto aos seus papéis, embora possam os atores de investigação cibernética também sobre eles ou sobre a estrutura a que pertencem lançar suas expectativas e seus desapontamentos.

3.1 Pesquisa empírica: da perspectiva teórica de Luhmann à observação das expectativas de um papel institucional, de investigador policial

> Toda sociedade, conforme sua própria complexidade, precisa prever um volume suficiente de diversidade de expectativas normativas, e possibilitá-la estruturalmente, por exemplo por meio da diferenciação de papéis. (LUHMANN, 1983, p. 77).

A pesquisa empírica, conforme planejada e autorizada pelo Comitê de Ética e Pesquisa[54], pautou-se em entrevistar policiais, agentes ou delegados com experiência e atuação na área de investigação criminal cibernética. Ou seja, observar as observações de terceiros, integrantes do mundo a observar, do mundo que está frente aos olhos (BÔAS FILHO; GONÇALVES, 2013).

Assim, após trâmites de autorização, os documentos (Requerimento de Encaminhamento, Carta de Apresentação e Projeto de Pesquisa) foram encaminhados, via e-mail, à Presidência do Conselho Nacional de Chefes de Polícia (CONCPC)[55], que os remeteu, também por e-mail, às Polícias Civis dos Estados e Distrito Federal[56].

Ciente desse envio, pela programação projetada, especialmente de realização das entrevistas, de posse da lista de contatos dos participantes do *I Seminário sobre a Capacitação das Unidades de Repressão aos Crimes Cibernéticos – Ciber Cap* (REPRESSÃO, 2021a; REPRESSÃO, 2021b), no qual o pesquisador foi palestrante, iniciou-

---

[54] Submissão nº 56881422.3.0000.5307 (Plataforma Brasil), autorizada pelo Comitê de Ética e Pesquisa da Universidade La Salle – Canoas-RS. Parecer com aprovação emitido em 27/04/2022.

[55] O Estatuto do CONCPC, disponibilizado pela entidade neste link http://www.concpc.com.br/res-019-2018-concpc/, prevê, segundo o Art. 2º, que a entidade é constituída pelos Delegados de Polícia, chefes de Polícia Civil dos Estados e do Distrito Federal, sendo constituído de uma diretoria, com Presidente, Vice-Presidente Executivo e Vice-Presidentes Regionais, além de órgãos de assessoria. O art. 1º do Estatuto contempla as competências do CONCPC, destacando-se os itens II, III e IV, ou seja, a proposição de diretrizes e normas relativas à uniformização de procedimentos das Polícias Judiciárias, a elaboração de estudos relacionados à promoção da modernização das estruturas organizacionais nos Estados e a promoção dos estudos visando ao aperfeiçoamento e ao intercâmbio técnico-profissional e científico do pessoal que integra as carreiras dos quadros da Polícia Civil. Além disso, os demais pontos também são delineadores de atribuições tencionadas a ampliar a troca de informações, de experiências e melhoria da gestão nas Polícias Civis dos Estados e do Distrito Federal.

[56] Tópicos do requerimento, assinado em 28 maio 2022: "1 – Seja remetido um comunicado às Polícias Civis de que o signatário realiza pesquisa de doutoramento na Universidade La Salle, na cidade de Canoas, Rio Grande do Sul, sob o título informado e que uma das fases da pesquisa compreende a realização de entrevistas com agentes/delegados integrantes de órgãos de polícia judiciária que atuam especificamente na investigação/inteligência sobre crimes cibernéticos, de acordo com a Lei nº 12.735/2012;

2 – Assim, que entrarei em contato com os referidos órgãos via telefone, WhatsApp e/ou e-mail, explicando a pesquisa e verificando voluntários para participar da entrevista, que, dada a exigência do CEP, terá um Termo de Consentimento Livre e Esclarecido que será enviado por e-mail ao entrevistado e que este, em resposta, dará o de acordo para participação, quando então haverá o agendamento da entrevista;

3 – A entrevista terá duração de 45 a 60 minutos e poderá ser gravada, para fins de degravação e elaboração da tese, sendo preservadas as informações dos participantes caso assim o queiram".

se a interlocução por serviço de mensageria (WhatsApp), telefone ou por e-mail, agendando-se as entrevistas. Nos Estados com dificuldades de contato, foram realizados novos contatos locais e interação com policiais do setor cibernético, quando existente.

Por essa interação inicial, quando foram buscados dados e contatos, verificou-se que quatro Estados não possuíam órgão de atuação especializada na inteligência ou investigação cibernética devidamente instalado e com atuação efetiva, quais sejam: Ceará, Mato Grosso do Sul, Acre e Rio Grande do Norte. Porém, Acre, Ceará e Rio Grande do Norte já possuem atos normativos com previsão sobre o órgão, contudo sem a instalação efetiva dele, ou seja, sem instalações físicas, recursos humanos e/ou materiais. Mesmo assim, dada a voluntariedade dos contatados em participar da entrevista, bem como de conhecer uma perspectiva diferenciada desses atores, realizou-se a entrevista com os integrantes das polícias civis do Acre e Rio Grande do Norte, deixando-se de realizar a entrevista de policiais do Ceará e Mato Grosso do Sul, embora os contatos tenham sido realizados. Por outro lado, tendo Rondônia um órgão de inteligência cibernética (laboratório) e uma delegacia focada na repressão às fraudes, a entrevista foi realizada com integrante deste último órgão, pois o órgão especializado tem apenas um servidor e não foi autorizado contato.

Por outro lado, embora a documentação do CONCPC tenha chegado à Polícia Civil do Rio de Janeiro e tenha sido feito o contato com o titular da especializada no Estado, havendo a indicação de um possível participante da pesquisa, este declinou da participação, não havendo indicação de substituto. Assim, ao todo, foram destacados 24 policiais para a entrevista.

Agendadas as entrevistas, seguiu-se o roteiro semiestruturado das perguntas, iniciando-as com o alerta quanto ao conteúdo do Termo de Consentimento Livre e Esclarecido, os riscos e benefícios da pesquisa, e, somente após a concordância do entrevistado, seguia-se para os questionamentos. Todas as entrevistas foram gravadas.

O primeiro tópico consistia em buscar conhecer aspectos básicos sobre o entrevistado, especialmente quanto ao seu papel como policial e, especificamente, como investigador e atuante na área de investigação policial cibernética. Optou-se, também, por nunca interromper a fala do entrevistado enquanto este respondia às perguntas e somente passar para a próxima questão após a conclusão da resposta anterior.

Embora conste no anexo desta tese o roteiro da entrevista, cumpre observar que ela foi dividida em cinco momentos principais, cujos destaques são os seguintes:

Primeiro momento: pautado nas expectativas cognitivas e normativas, objetivou-se conhecer quais normativas (legislação brasileira vigente) os entrevistados conheciam sobre

crimes cibernéticos, sobre proteção de dados (LGPD), sobre o Marco Civil da Internet (Lei 12.965/2014) e, especialmente, sobre a Lei nº 12.735/2012, fazendo-se, neste caso, a leitura do art. 4º da referida norma[57].

Também, nesse momento da entrevista, buscou-se o entendimento, a perspectiva do entrevistado, quanto às normas de caráter penal (direito material penal), seja sobre as tipificações de crimes (existentes), seja sobre as penas. Na sequência, questionou-se sobre as normas de caráter procedimental, normas processuais penais vigentes, quanto às práticas envolvidas e cotidianas, de interação tanto com provedores de conexão quanto de aplicação e as experiências de atuação com as forças de Lei, nacionais e internacionais, policiais e judiciais.

Segundo momento: pautou-se em conhecer as expectativas cognitivas e normativas em relação à estrutura administrativa, os aspectos procedimentais dos órgãos especializados já existentes, abordando-se tópicos sobre o tempo de existência do órgão, estrutura, instalações, equipamentos, softwares, verbas e investimentos feitos pelo Estado, pela União e/ou iniciativa privada.

Terceiro momento: direcionado ao foco de atuação do órgão policial, com suas atividades principais e acessórias, delimitadas ou não por normativas estaduais, adequadas ou não às realidades locais/regionais, bem como a relação efetiva com os demais órgãos da persecução criminal dos crimes cibernéticos: Polícia Federal, Ministério Público e Poder Judiciário. Questionou-se, também, sobre como dar efetividade à Lei nº 12.735/2012.

Quarto momento: foi delimitado sobre a qualificação e o treinamento dos policiais envolvidos na investigação cibernética, se local, nacional, estadual ou com custeio privado/próprio.

Último momento: foi direcionado à reflexão dos entrevistados quanto à experiência com mecanismos de redução e mitigação de danos na Internet e sobre a aplicabilidade dessa prática na investigação criminal, como atividade supletiva a ela. Este momento também consistiu em formular questionamento genérico sobre o 'caminho ideal' para melhorar a persecução da criminalidade no âmbito da Internet. O fato de ela ter sido feita por último permitiu ao entrevistado não só fazer uma síntese de sua reflexão, mas, ao fazê-lo, expressar aquilo que possivelmente mais se destaca em relação às suas expectativas e frustrações. Ou seja, ele já havia refletido e falado sobre várias coisas; observa-se que, neste momento, ele

---

[57] Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

trouxe aquilo que lhe é mais caro, lhe é mais importante, enquanto ator de um papel importante na persecução da criminalidade cibernética.

Foram, assim, realizadas 24 entrevistas, totalizando 25 horas, 15 minutos e 13 segundos de gravações, entre os dias 02 e 24/06/2022. Conhecer e observar a perspectiva das expectativas a partir dos próprios atores e buscar confirmar ou negar as hipóteses da tese é, assim, o objeto desta tese.

3.1.1 Estruturação de órgãos especializados na investigação cibernética

As Polícias Civis são estruturadas no âmbito dos Estados e dirigidas por Delegados de Polícia de Carreira (art. 144, IV e §§ 4º e 6º, da Constituição Federal), ou seja, são subordinadas aos Governadores dos Estados e do Distrito Federal e dos Territórios. Assim, a estruturação, administrativa e financeira, e os recursos materiais e humanos são temas delineados e administrados nesse âmbito, ou seja, das próprias unidades federativas.

No entanto, as Polícias Civis também fazem parte do Sistema Único de Segurança Pública, previsto na Lei nº 13.675/2018 (art. 9º, IV), e, por serem dirigidas por delegados de polícia de carreira, fazem parte do Conselho Nacional de Chefes de Polícia – CONCPC, entidade que congrega os dirigentes institucionais das Polícias Civis e emite recomendações através de resoluções[58].

No âmbito de cada Estado e do Distrito Federal, cada Polícia Civil promove sua estruturação orgânica baseada nos critérios de conveniência e oportunidade administrativa[59], institucionalizando ou não determinados órgãos especializados – também tendo em vista o incremento ou não do registro de determinados crimes –, como grupos operacionais, setores de inteligência, de enfrentamento ao crime organizado, lavagem de dinheiro e enfrentamento à corrupção, dentre outros, inclusive o de enfrentamento aos crimes praticados com o uso da rede mundial de computadores, a Internet (art. 4º da Lei nº 12.735/2012)[60].

Estes órgãos, especializados no enfrentamento à criminalidade cibernética, são bastante novos, incorporados aos poucos nas estruturas administrativas das polícias judiciárias dos

---

[58] Vide nota anterior sobre as funções do CONCPC. Sobre as resoluções já emitidas, vide sítio da entidade: http://www.concpc.com.br/.

[59] Essa observação se tornará mais clara na análise posterior do conteúdo das entrevistas, porquanto entrevistados afirmam que para a criação, instalação e exercício efetivo da delegacia ou órgão especializado, há necessidade de um convencimento político-administrativo.

[60] Há que se observar que alguns tipos penais se referem não à *rede mundial de computadores*, mas, simplesmente, à *rede de computadores*, como referido, por exemplo, pelos artigos 122, § 4º, e 154-A, ambos do Código Penal.

Estados. A Lei nº 12.735/2012, mesmo com a existência de setores no âmbito de alguns Estados, previu a criação destes órgãos, não impondo prazos, condições ou sanções pelo não cumprimento. Para delinear a estruturação existente no Brasil, nesta pesquisa optou-se por, durante as entrevistas, coletar informações da estruturação existente em cada Estado e condensar os documentos normativos repassados pelos entrevistados, complementando-se as informações com pesquisas na Internet. Ou seja, três metodologias diferentes nesta parte da pesquisa: entrevista, análise documental e pesquisas na Internet.

Então, conforme dados coletados[61], a estruturação fática desses órgãos no Brasil começou em 2000 (Rio de Janeiro), 2001 (São Paulo), 2005 (Pará) e 2006 (Minas Gerais). A evolução destes dois últimos órgãos é, porém, recente, sendo estabelecidos, respectivamente, uma divisão (com delegacias) e um departamento (com divisões e delegacias). Também incluem setores de inteligência cibernética, um avanço evolutivo necessário detectado a partir das entrevistas, pois buscam compreender as ameaças e vulnerabilidades no contexto da Internet e estabelecer procedimentos hábeis a conhecer o *iter criminis* e onde e em qual momento buscar evidências e provas. Voltar-se-á a esse ponto quando das análises das entrevistas quanto à estrutura existente nos Estados.

3.1.2 Análise do perfil dos entrevistados

Dos 24 entrevistados, os quais são identificados pelo número de ordem da entrevista seguido pela sigla do Estado a que pertence (ex.: entrevistado número sete, do Estado da Paraíba = 07PB), a maioria tem mais de dez anos de atividade policial (=54,16%) e apenas dois têm menos de cinco anos na profissão (=8,33%). Os outros nove (=37,5%), possuem entre cinco e dez anos de atividade na Polícia Civil.

Quadro 3: Tempo de atividade policial dos entrevistados

Tempo de atividade	Quantidade	Percentual	Agregação de fatores
Menos de 5 anos	2	8,33%	45,83%
Entre 5 e menos de 10 anos	9	37,5%	
Entre 10 e menos de 20 anos	11	45,83%	54,17%
Mais de 20 anos	2	8,33%	

Fonte: Produzido pelo autor (2023).

[61] Vide Quadro no Anexo III.

Esse tempo de atividade policial não corresponde, no entanto, ao tempo de atividade de investigação na área cibernética especializada – ao que poderíamos chamar de ‘tempo de atividade ciber’ –, uma vez que nenhum deles possui mais de sete anos nesta seara de atuação. 58,33% (=14) dos entrevistados possuem menos de três anos na atividade de investigação cibernética, enquanto 33,32% (=8) possuem mais três anos ou mais exercendo a atividade na área.

Conforme quadro a seguir, percebe-se uma inserção ainda recente dos policiais no âmbito da investigação cibernética. Não há dados, no entanto, para estender esse parâmetro de dados coletados, ou seja, o mesmo percentual alcançado nesta pesquisa para todos os policiais que atuam na área no Brasil, pois a observação não objetivou este dado, nem se projetou eventual margem de erro.

Quadro 4: Tempo de atividade policial dos entrevistados na área cibernética

Tempo de atividade na área cibernética	**Quantidade**	**Percentual**	**Agregação de fatores**
Menos de 1 ano	5	20,83%	58,33%
1 ano até 2 anos	5	20,83%	
2 anos até 3 anos	4	16,67%	
3 anos até 4 anos	4	16,67%	33,34%
4 anos até 5 anos	3	12,5%	
Até 7 anos	1	4,17%	
Prejudicado ou não verificado	2	8,33%	8,33%

Fonte: Produzido pelo autor (2023).

Quando os entrevistados foram questionados sobre o que os conduziu à posição do papel de investigador dos crimes cometidos no meio cibernético, destacam-se (a) a busca por novos desafios, curiosidade e interesse na área (02SE, 07PB, 10SC, 16ES, 22MG, 17MT), (b) convite superior (04RS, 19DF, 24PA), (c) atuação anterior em casos da área (05AL, 12PI, 14PR, 18RO, 20RR, 21RN, 23SP), (d) inspiração em colegas (03BA, 12PI), e (e) formação ou especialização na área (06AP, 07PB, 08PE, 09MA, 13AL).

Percebe-se, assim, que, apesar dos motivos e circunstâncias serem os mais variados, a grande maioria, destaca-se, acabou se aproximando da área investigativa cibernética por interesse e pelas circunstâncias da atividade diária policial. O desafio relatado por alguns dos entrevistados refere-se ao tema específico da investigação cibernética, baseado em [busca de] novos conhecimentos, ainda mais especializados: "seria uma melhoria para a instituição, melhoria para a sociedade" (02SE), "não tinha formação na área de tecnologia da informação, mas é uma área que me fascinava, que eu gosto" (17MT), "percebi que a matéria assustava" (19DF), "aceitei o desafio" (19DF), "a missão de desenhar uma forma de atendimento, selecionar e treinar policiais" (19DF), "eu não quis aceitar porque não tinha conhecimento na área e era muito complicado" (24PE), "inicialmente foi muito dificultoso" (24PE).

As expectativas sobre as estruturas administrativas, consolidadas ou em consolidação, sobre as expectativas normativas e as expectativas sobre a evolução normativa partem desse perfil de atores, desse perfil de papéis, aspectos sobre os quais esta tese passará a aprofundar as observações nos próximos tópicos.

3.2 Expectativas dos atores de investigação policial sobre o contexto normativo penal e processual penal: as frustrações e os desapontamentos

> Os papéis e os programas, ao contrário, através do alto grau de complexidade, franqueza, interdependência e contradição das expectativas comportamentais com eles identificados, produzem eles mesmos, constantemente, aspirações de mudanças. Quanto maior for sua independência, mais dinâmica será a sociedade, mais imprescindível será encontrar novas soluções para a estabilização social e institucional de expectativas comportamentais. (LUHMANN, 1983, p. 108).

O *primeiro momento* da entrevista, como planejado, buscou correlacionar a perspectiva teórica de Luhmann (1983) à realidade fática das normas penais e processuais vigentes no Brasil relativas aos crimes cibernéticos, porém sob a perspectiva [única] dos atores de investigação criminal, analisando-se suas observações, repassadas durante a entrevista, a partir de suas memórias individuais, fruto de suas experiências de suas operações.

3.2.1 Expectativas sobre expectativas: (auto)conhecer ou não (auto)conhecer o contexto normativo

A perspectiva de autoconhecimento de uma pessoa, do sistema psíquico, leva à ampliação ou redução de expectativas sobre expectativas normativas? Luhmann (1983, 2007)

afirma que a formação da memória dos sistemas os ajuda a absorver comunicações, a permitir ou não permitir que elas se acoplem no sistema em face da sua função. Não há, no entanto, uma resposta prévia quando se trata dos atores em papéis de investigadores policiais no âmbito cibernético, especialmente em razão do tempo de atividade na área e de formação de experiências e memórias acumuladas.

Objetivou-se, assim, com as entrevistas, observar as observações dos entrevistados sobre o contexto normativo brasileiro no que diz respeito à legislação existente sobre crimes cibernéticos, tanto do ponto de vista do/sobre o direito material (penal) quanto do direito processual/adjetivo (processual penal).

Conforme já descrito, o procedimento da entrevista, semiestruturada em cinco conjuntos, partes/*momentos* sequenciais, teve como objetivo de compreender/observar o autoconhecimento dos entrevistados, suas expectativas cognitivas e normativas sobre a estrutura normativo-penal brasileira. Partiu-se de perguntas prévias, sobre o domínio – autoconhecimento – de normas citadas voluntariamente e que têm relação com a investigação dos crimes cibernéticos. Após, as perguntas foram direcionadas à área penal, especialmente sobre as possibilidades fáticas de enquadramento de determinadas condutas 'divergentes' na Internet nas normas penais brasileiras (Código Penal e legislação complementar), tanto no seu aspecto mais genérico (âmbito do Estado), ou seja, expectativas e frustrações quanto à legislação penal em si e a relação com os fatos que ocorrem na rede mundial de computadores, quanto no seu aspecto mais específico, âmbito local, abrangendo a atuação da delegacia ou o órgão onde o ator exerce a sua atividade.

Finalizando a primeira parte da entrevista, questionava-se sobre os aspectos do direito processual penal aplicável à realidade das investigações dos crimes praticados com o uso e por meio da Internet, se há ou não um condicionamento do órgão à legislação processual, como é a coleta e busca de evidências, a relação com provedores de conexão e de aplicação, o uso ou não dos procedimentos de cooperação penal policial e a cooperação penal internacional, o tempo de atividade sobre cada procedimento policial e as expectativas de mudanças normativas sobre os procedimentos.

3.2.2 Observações sobre as expectativas normativas gerais dos atores de investigação criminal cibernética

Nessa fase inicial da entrevista, foram quatro perguntas, consideradas 'prévias' à sequência de questionamentos. A primeira visou observar o autoconhecimento dos

entrevistados sobre o domínio (e qual o domínio) que têm sobre os crimes cibernéticos num sentido amplo: "Quais as normativas que você mais domina sobre os crimes cibernéticos?". Ou seja, quais observações poderiam contribuir a partir do "mundo que está em seus olhos" (BÔAS FILHO; GONÇALVES, 2013, p. 38).

As respostas principais, que foram múltiplas, foram direcionadas à autodeclaração de autoconhecimentos/domínio sobre a parte penal (18 = 75%), especialmente sobre o crime de estelionato (8 = 33,33%), sendo citados, ao menos uma vez, as fraudes bancárias, as fraudes eletrônicas, o crime organizado, a lavagem de dinheiro, a invasão de dispositivo informático, a pedofilia, os crimes contra a honra e a violação aos direitos autorais.

A autodeclaração de conhecimento sobre o processo penal foi referida por oito entrevistados (=33,33%). Destacou-se, também, a citação de autoconhecimento sobre o Marco Civil da Internet (10 = 41,66%), interceptação telefônica/telemática (2 = 8,33%) e normas ISO[62] (2 = 8,33%). Citados, ao menos uma vez, foram a LGPD, as normas de inteligência, os tratados internacionais, a gestão administrativa e operacional e a Lei do Delegado de Polícia (Lei nº 12.830/2013[63]).

As citações sobre a parte penal, processual penal e Marco Civil da Internet, por fazerem parte do dia a dia da investigação cibernética, eram expectáveis na observação das entrevistas. Não o eram [expectáveis] as referências sobre, por exemplo, as normas ISO e a gestão administrativa e operacional, pois são temas importantes no contexto da gestão da investigação cibernética, especialmente qualificando o resultado dela, com cuidados e resguardos sobre evidências e provas, como no caso da ABNT NBR ISO/IEC 27.037, aplicável aos casos sob investigação tendo em vista a Lei nº 13.964/2019 (FURNALETO

---

[62] As chamadas normas ISO são publicadas pela ISO (*International Organization for Standardization*), que é uma federação mundial dos organismos nacionais de normalização (https://www.iso.org/), do qual o Brasil faz parte, com a participação da ABNT (Associação Brasileira de Normas Técnicas). A ABNT (https://www.abnt.org.br/) e seus diversos comitês têm a responsabilidade de internalizar as normas ISO, que passam a ter a mesma numeração internacional, porém a menção à norma 'ISO-NBR'. "Tipicamente, as normas são de uso voluntário, isto é, não são obrigatórias por lei, e então é possível fornecer um produto ou serviço que não siga a norma aplicável no mercado determinado. Em diversos países há obrigatoriedade de segui-las, pelo menos em algumas áreas (para o caso brasileiro, é o Código de Defesa do Consumidor)" (ABNT, 2022).

[63] Diz o art. 2º da Lei nº 12.830/2013: "As funções de polícia judiciária e a apuração de infrações penais exercidas pelo delegado de polícia são de natureza jurídica, essenciais e exclusivas de Estado.

§ 1º Ao delegado de polícia, na qualidade de autoridade policial, cabe a condução da investigação criminal por meio de inquérito policial ou outro procedimento previsto em lei, que tem como objetivo a apuração das circunstâncias, da materialidade e da autoria das infrações penais.

§ 2º **Durante a investigação criminal, cabe ao delegado de polícia a requisição** de perícia, **informações, documentos e dados que interessem à apuração dos fatos**. [...]" (grifos nossos)

NETO; SANTOS, 2020), que inseriu na legislação processual penal a preservação da cadeia de custódia, embora não tenha previsto literalmente a evidência digital.

Essas observações dos entrevistados ganham sentido quando analisadas em conjunto com a mencionada falta de padronização de procedimentos na investigação e cadeia de custódia, especialmente considerando a possibilidade de nulidade do processo. Essas notas, mesmo que realizadas por um ou outro entrevistado, demonstram, por outro lado, a importância [e carência] desses protocolos, mais delineados e direcionados à atividade diária.

Na parte penal, o destaque ao estelionato é 'resultado' do então momento vivido pelo Brasil pós-pandemia da Covid-19, porquanto houve migração da prática de crimes ao ambiente cibernético, com o aumento dos casos das chamadas fraudes eletrônicas.

Dados do Fórum Brasileiro de Segurança Pública informam um aumento de 497,5%, na variação de 2018 para 2021, no estelionato por meio eletrônico e no caso do estelionato sem especificação do meio, um aumento de 179,8%, no mesmo período, com a observação de que nem todos os Estados fazem esta diferenciação, ou seja, a categorização do meio pelo qual o crime foi cometido, na hora do registro de ocorrência (BUENO; LIMA, 2022, p. 110-1, 120-1)[64].

A segunda pergunta prévia feita se relacionava a conhecer ou não conhecer a Lei Geral de Proteção de Dados (LGPD) brasileira (Lei nº 13.709/2018), onde é possível perceber que o ator de investigação criminal cibernética dá atenção ao tema da proteção de dados, uma vez que nenhum informou desconhecer a normativa. Destaca-se, entretanto, que nove (=37,5%) comentaram ter conhecimento apenas básico ou razoável sobre a norma. Já os demais, todos conhecem as regras sobre proteção de dados no Brasil.

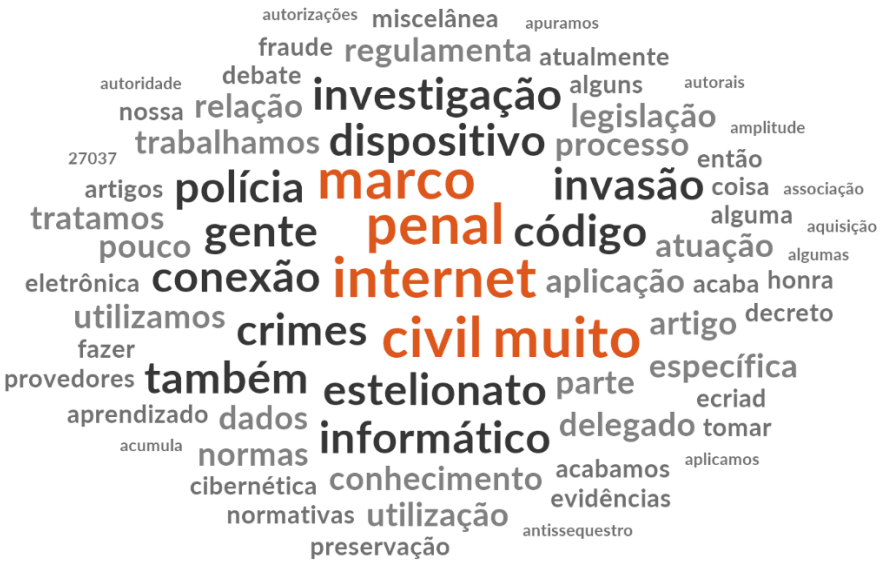
Já a terceira pergunta, sobre o autoconhecimento do Marco Civil da Internet (Lei nº 12.965/2014), revelou que 21 (=87,5%) dos entrevistados afirmam conhecê-lo e aplicá-lo, e apenas 3 (=12,5%) referiram ter um conhecimento básico ou razoável sobre a norma. Neste sentido, cabe lembrar que esta normativa foi citada, de forma voluntária, por vários entrevistados no primeiro questionamento.

A incidência do Marco Civil da Internet pode ser verificada na nuvem de palavras gerada a partir das entrevistas:

---

[64] Há uma grande incompletude sobre os dados dos crimes cibernéticos no Brasil, porquanto os sistemas dos Estados não são padronizados e direcionados à categorização desses crimes, de maneira a se ter a noção exata de quantos casos são registrados no Brasil e que são cometidos com uso da Internet.

Figura 3: Declaração de autoconhecimento do contexto normativo brasileiro pelos entrevistados



Fonte: Produzido pelo autor (2023), com base no programa nVivo[65]

Finalizando as perguntas prévias, de autoconhecimento geral sobre as normas aplicáveis no contexto da investigação dos crimes cibernéticos, questionou-se sobre o autoconhecimento da Lei nº 12.735/2012, ao que era referido e lido o teor do art. 4º. A maioria dos entrevistados afirmou desconhecer a norma (14= 58,33%), enquanto uma parcela deles afirmou conhecer razoavelmente (2 = 8,33%) ou totalmente (8 = 33,33%) a norma que previu a estruturação dos órgãos para o enfrentamento à criminalidade no âmbito da Internet. Esta norma é, portanto, mais desconhecida dentre os atores de investigação criminal cibernética.

3.2.3 Expectativas sobre expectativas e frustrações: as normas penais em observação

Ainda dentro do primeiro momento da entrevista, foram feitas aos entrevistados quatro perguntas sobre o seu autoconhecimento, seu entendimento, quanto ao direito penal, especificamente das normas penais brasileiras, aplicáveis às condutas no âmbito cibernético.

Primeiro, questionou-se aos entrevistados, a partir de sua experiência profissional, se os tipos penais existentes são suficientes para o enquadramento das situações fáticas que ocorrem na Internet, em especial referência aos fatos registrados no âmbito do Estado (âmbito

[65] O programa nVivo (https://support.qsrinternational.com/s/) foi utilizado como complemento à análise de conteúdo das entrevistas, especialmente para a geração de nuvem de palavras.

geral) e, a seguir, o mesmo questionamento era feito, porém relacionado à incidência no âmbito da sua delegacia/órgão de lotação (âmbito local).

A partir do âmbito geral, a maioria dos entrevistados (13 = 53,16%) afirmou que a legislação penal vigente no Brasil não abarca todas as situações fáticas acontecidas no âmbito do Estado. Porém, dentre estes, seis (=46,15%) também afirmaram que no âmbito local, da delegacia, as normas penais atendem às necessidades e podem ser plenamente aplicadas aos fatos registrados, ou seja, dos 13 entrevistados, seis observaram essa aplicabilidade normativo-penal sobre os casos que chegam/chegaram ao seu conhecimento formal por um registro de ocorrência.

Observa-se, ainda, a partir dessas respostas, que pelo menos oito deles, independentemente de afirmar pela suficiência ou insuficiência das normas penais, fazem referência às penas brandas quando tratam do enquadramento das condutas. Observa-se que a pergunta estimulada era sobre a suficiência dos tipos penais para enquadramento, tendo a expectativa pelo aumento de penas aparecido espontaneamente nas respostas, indicando, assim, uma expectativa latente. Isso acaba se reafirmando posteriormente, na pergunta específica sobre o aumento de penas.

Afirmações sobre expectativas e frustrações, portanto, das mais variadas:

> [...] as normas penais brasileiras, no meu entendimento, [...], não são funções normativas eficazes. (02SE).
> [...] legislação bem fraca. (10SC)

Além de variadas, observa-se que elas foram também em sentido oposto, a depender da esfera: geral x local e/ou [direito penal] abstrato x aplicado. Explica-se: quando o *locus* é abstrato e está distante, avaliam [a maioria] os entrevistados pela não suficiência; já quando o *locus* é a prática aplicada e cotidiana, avalia-se a legislação penal como suficiente. Ou seja, no dia a dia da análise dos fatos e do enquadramento deles às situações abstratamente previstas, há consideração pela suficiência da norma, embora o reclame voluntário e acentuado quanto à pena.

Denota-se, a partir da observação sobre as perspectivas dos entrevistados, não só a frustração deles, mas também o caráter de manutenção da expectativa normativa, generalizada pelo direito penal posto em razão de sua adoção como norma, legislada, sancionada e vigente. Isso também não impede que os atores de investigação criminal permaneçam com suas expectativas cognitivas sobre as expectativas normativas, ou seja, pela adoção de novos tipos penais e/ou incidência de pena mais severa do que a existente.

Assim, para melhor compreender essas expectativas sobre expectativas normativas e as frustrações ou desapontamentos dos atores de investigação criminal cibernética, há que se fazer a análise das respostas às duas outras perguntas sobre a parte penal: se haveria necessidade de outras tipificações e se há necessidade de incremento das penas (sanções penais) existentes.

A grande maioria dos entrevistados entende pela ampliação dos tipos penais (16 = 66,66%) e, principalmente, pela ampliação das penas em alguns delitos (19 = 79,16%). Dentre as novas condutas a serem tipificadas pelo legislador, pela expectativa dos entrevistados, estão as *fake news*, o *bullying*, a desconfiguração de páginas da Internet (*defacement*), o uso de *ransomwere* (encriptação de arquivos com uso de código malicioso e solicitação de resgate em criptoativos), perfil falso no âmbito da Internet (perfis de pessoas físicas ou jurídicas), estupro pela Internet, invasão e sequestro de contas de redes sociais e, também, lavagem de dinheiro com criptoativos [vide 4.3]. Houve, também, menção a necessidade de controle e criminalização dos atos preparatórios, publicados ou como vídeo ou como *e-commerce*, por exemplo, ensinando a montagem de explosivos ou demonstrando como aplicar um golpe ou uma fraude com sucesso.

Dentre as observações sobre os 'novos tipos', também eram citados tipos penais existentes, porém ou com sugestão de ampliação da pena ou modificação da redação da norma, como nos casos de invasão de dispositivo informático, onde sugerem uma modificação do conceito que abranja o "sistema informático" ou ampliação do rol de condutas e melhor diferenciação dentre elas. A frustração pelo enquadramento é referenciada pelos entrevistados:

> o site de determinada pessoa é invadido e alteram a configuração, se esse site tiver uma função pública, como o site do Detran, conseguimos tipificar ele no artigo 265 do código penal, mas caso seja um site privado, sem função pública, caímos num abismo tentando enquadrar ele num dano, é algo que fica nebuloso. (10SC)
> Tem, também, o artigo 154A, invasão de dispositivos informáticos, que tem redação muito complexa, mesmo com a redação nova, não nos ajuda, é um crime que raramente vemos condenação. (19DF)

Isso porque, conforme analisado nas considerações iniciais deste capítulo, a primeira redação do art. 154-A do Código Penal, dada pela Lei nº 12.737/2012, gerou expectativas normativas sobre sua aplicação efetiva, porém frustrada e desapontada socialmente, formando-se novas expectativas cognitivas sobre essa expectativa normativa em face, especialmente, da linguagem [penal] complexa e de difícil enquadramento fático, consubstanciados na estruturação do tipo penal. Gerou-se, a partir de um processo legislativo

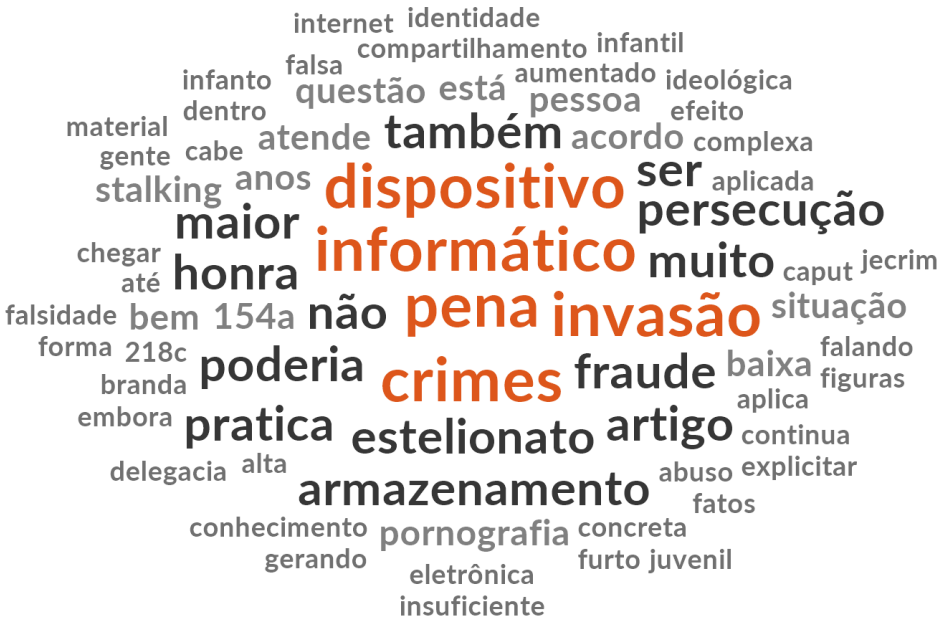
complementar, uma reestruturação do tipo penal, com base na Lei nº 14.155/2021 [que deu nova redação ao art. 154-A], para que os comportamentos desapontadores, divergentes à norma, pudessem ser questionados com maior efetividade. Porém, conforme demonstram as entrevistas, as expectativas cognitivas ainda pairam sobre uma modificação normativa capaz de gerar uma reestruturação penal que possibilite o enquadramento de condutas ainda não possíveis de tipificação ou de compreensão comunicativa diversa, a depender do ator envolvido, acusação ou defesa do investigado/réu, a exemplo do conceito de 'dispositivo informático'.

A referência à adequação necessária dos crimes às condutas no contexto virtual é reforçada pelos entrevistados, em vista de suas afirmações:

> A legislação está muito rasa em relação aos crimes cibernéticos. Infelizmente, temos visto situações midiáticas legislativas. (10SC).
> Algumas situações de prática, no meio virtual, que se inserem em vácuos legislativos, […] invasão e sequestro de contas, em redes sociais, que os criminosos utilizam de engenharia social para apropriação das contas de vítimas. (15TO).
> Tiveram avanços significativos nos últimos anos, mas percebo, em muitas situações, que podemos enrijecer a aplicação da pena ou normatizar com tipos penais mais específicos para auxiliar no combate. (18RO).

Esses parâmetros de observações podem ser vislumbrados com a nuvem de palavras correspondente:

Figura 4: Expectativas cognitivas dos entrevistados frente à estrutura dos tipos penais relacionados à Internet



Fonte: Produzido pelo autor (2023).

"O ideal seria um estudo para sabermos o que realmente precisamos" (02SE), afirma o entrevistado sobre os 'novos tipos', sobre os quais as expectativas estão postas. Outra expectativa foi realçada por um dos entrevistados (18RO): "Tem um limbo em relação a duas situações: a questão de subtração de valores de contas *fintechs*, pois não sabe se entra no furto qualificado mediante fraude ou se entra na invasão de dispositivo".

Na expectativa sobre o aumento de pena, destacam-se as afirmações sobre uma ampliação das sanções dos delitos de invasão de dispositivo informático e de estelionato, mesmo considerando a ampliação do tipo e da pena e a criação do tipo penal, respectivamente, gerado pela Lei nº 14.155/2021:

> O estelionato no Brasil é a maior vergonha que existe, porque ninguém fica preso, nenhum juiz dá prisão, a gente vê roubalheiras dentro de inquéritos que estamos fazendo, pedindo prisão preventiva, temporária, e tudo é negado, porque não há risco à vida. (04RS).
> A lei material tem que melhorar muito ainda, porque os crimes proliferam todo o dia, com golpe novo. (09MA).
> Realizamos vários procedimentos, sigilo de quebra, chegamos no autor, mas não tem, quase nenhuma, penalização. (11AM).

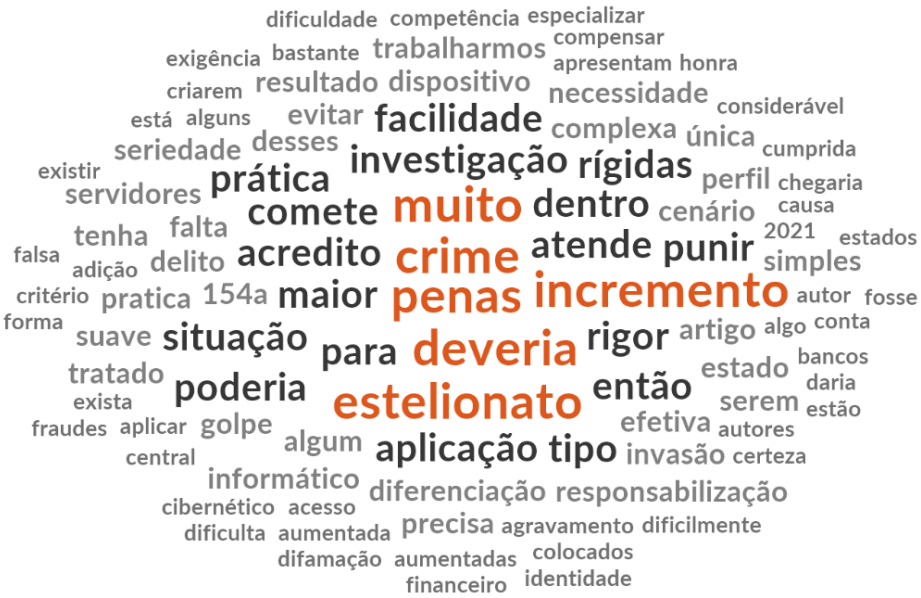
A expectativa (cognitiva) fática, da prisão do autor ou autores identificados na investigação cibernética como resultado dela, leva à frustração pela inocorrência processual, seja pela pena estipulada no tipo penal, seja pelo não reconhecimento do Judiciário quanto ao pedido da ordem de prisão. Os desapontamentos são acompanhados, ainda, da memória (e frustração) com o sistema:

> Sabemos que tem pontos falhos e que a legislação não acompanha, de forma célere, o surgimento dos novos crimes cibernéticos, então as autoridades têm que se desdobrar para 'caçar' os criminosos. (16ES).
> Não é somente a questão da pena. Acredito que todo o mecanismo deixa a desejar, tanto a parte policial (efetivo insuficiente para atender a demanda) [...], alinhado a isso, a legislação é muito rasa aos crimes cibernéticos. (16ES).

Percebe-se essa frustração em razão de os entrevistados referirem e vincularem a eficiência da investigação com a prisão e a pena dos delitos. A ausência da prisão e/ou condenação remete a uma frustração com o próprio trabalho, um 'trabalho para nada', onde a solução seria uma pena restritiva de liberdade como satisfação pessoal para o resultado ser considerado eficiente, o que não é possível em razão das penas baixas nos crimes cibernéticos.

Parte dos entrevistados também reforçou a necessidade de ampliação da sanção penal de delitos contra a honra (arts. 138, 139 e 140, do Código Penal), de exploração da pornografia infanto-juvenil (arts. 241-A e ss. do ECA), da divulgação não consentida da intimidade (art. 218-C do Código Penal), do *stalking* (art. 147-A do Código Penal) e do perfil falso (art. 307 do Código Penal). Em especial, a citação por um dos entrevistados quanto à criação de uma majorante genérica, para todos os crimes, quando da prática do crime com o uso da Internet[66]. Esses resultados podem ser demonstrados pela nuvem de palavras formada a partir das respostas específicas ao questionamento:

Figura 5: Expectativas e frustrações quanto às penas dos delitos praticados no âmbito da Internet



Fonte: Produzido pelo autor (2023).

A frustração, portanto, é bastante direcionada ao resultado dos trabalhos investigativos, muitas vezes morosos e demorados, com resultados ínfimos em relação aos autores do crime. O entrevistado 19DF refere que, dentre dez casos encaminhados ao juizado, um percentual muito baixo chega ao final com condenação:

> Acompanho os casos de condenações, percebo poucas condenações de crimes contra honra, de cada 10 TCs que encaminhamos à justiça, 9,7 não geram condenações, das que geram, são condenações muito pequenas. (19DF)

[66] A majorante já existe, por exemplo, no art. 122 do Código Penal, no seu § 4º: "A pena é aumentada até o dobro se a conduta é realizada por meio da rede de computadores, de rede social ou transmitida em tempo real".

Essa frustração é repetida na fala de outros entrevistados:

> A sensação é de que os criminosos são pouco responsabilizados por esses crimes. Porque os autores não são responsabilizados, tanto faz a pena ser de cinco anos, de dez anos ou de quinze anos, pois se não são responsabilizados esse tempo não faz diferença. (13AL).
> Penso estar sendo radical, mas não vejo esse crime de estelionato praticado pelo meio virtual menos nocivo do que os crimes contra a vida. (02SE).

Outros pontos observados por dois dos entrevistados (16ES, 24PA) remetem à parte processual, qual seja a modificação de regra de competência no caso de estelionato (art. 70, § 4º, CPP, modificado pela Lei nº 14.155/2021), seja a exigência de representação da vítima para processar o estelionatário. Outro entrevistado observa:

> Mas, na questão processual, muitos benefícios acabam impactando no direito penal, por exemplo a pena de um a quatro anos, quem lê pensa que o sujeito vai cumprir aquela pena, mas na verdade, tendo em vista os vários outros institutos de ressocialização e tudo mais, acaba não sendo verídico. (05AC).

Estas observações foram feitas [pelos entrevistados] quando a entrevista ainda estava tratando do direito penal. Assim, as frustrações foram manifestadas tanto em relação à parte penal quanto à parte processual penal, em termos de necessidades evolutivas que repercutam na investigação criminal cibernética.

É esse, portanto, o objetivo do próximo tópico: analisar as observações dos atores de investigação quanto às normas processuais penais e procedimentais e sua repercussão na investigação criminal. Adverte-se, de outra parte, que os projetos legislativos, referenciados como necessidades de tipificações, são analisados ainda neste capítulo e no próximo, assim como os tipos penais agregados à legislação brasileira.

3.2.4 Observar a norma e condicionar procedimentos: frustração cognitiva pela inefetividade nos resultados, com as respostas e com o tempo

Procedimentalizar uma investigação criminal significa, faticamente, agregar provas e evidências da autoria e materialidade delitiva, atendendo às regras processuais penais e constitucionais. No caso dos delitos que são cometidos pela rede [mundial] de computadores, tanto a materialidade quanto a autoria são possíveis de serem obtidas com base nos registros de uma conexão, no caso de provedores de acesso à Internet, ou de uma publicação, uma

mensagem, uma imagem etc., todas publicadas em algum site ou transmitidas, dados estes armazenados em uma aplicação.

Esses registros incluem não só o conteúdo, mas também informações sobre o perfil (dados cadastrais etc.) e sobre a origem do acesso, os *logs* de IP (*Internet Protocol*). Enquanto essas informações de registros são armazenadas pelos provedores de aplicação[67], os provedores de conexão, que fornecem o acesso à internet aos usuários e guardam registros dessas conexões à Internet pelos usuários que contratam o serviço.

Pode parecer simples, mas a complexidade é posta do ponto de vista da própria estrutura e evolução da rede de Internet e, também, da absorção normativa destes conceitos, no caso brasileiro, pelo Marco Civil da Internet e pela Lei Geral de Proteção de Dados, aquele com efeito principal sobre os processos e procedimentos na seara penal (processual). Pela complexidade envolvida – já que o cibersistema da Internet é uma aquisição evolutiva da sociedade –, e tratando-se de alinhamento observável de duas sistemáticas estruturais da Internet e do Direito, objetivou-se observar, a partir do papel de ator de investigação criminal cibernética, vários dos aspectos envolvidos na obtenção de provas e evidências da autoria e materialidade delitiva no espaço cibernético.

Com base na experiência de cada entrevistado, questionou-se sobre serem adequadas ou não as normas procedimentais em relação à realidade das investigações dos crimes cibernéticos. Dos 24 entrevistados, 5 (=20,83%) referiram que as normas estão adequadas, porém com 'incompreensão' por parte do Judiciário (e Ministério Público) sobre determinados aspectos conceituais e procedimentais, bem como a falta de autonomia do delegado de polícia nas investigações, as questões de definição da competência (processual) para o julgamento dos casos e os aspectos regulamentares sobre a cadeia de custódia e rotina das investigações.

Assim, embora 20,83% dos entrevistados concordem que as normas procedimentais sobre as investigações cibernéticas estão adequadas, vários pontos são consonantes com aqueles entrevistados que compreendem não estar adequada a legislação procedimental. Estes, por sua vez, apontam a falta de regras quanto ao prazo de respostas pelos provedores de conexão e de aplicação, a falta de celeridade e agilidade nas respostas às solicitações, bem como a necessidade de judicialização de vários aspectos e fases ('cláusula de reserva

[67] Os conceitos de *provedores de conexão* e *provedores de aplicação* são definidos pelo Marco Civil da Internet, Lei nº 12.965/2014, arts. 13 e 15, respectivamente.

judicial'), ou seja, o não acesso direto pelo delegado de polícia às informações e a necessidade de ordem judicial para o acesso aos dados.

Entrevistados apontam para a necessidade de ajustes nas normas processuais para (a) tornar mais célere o acesso aos dados de registros de conexão e de acesso (aplicações), (b) imprimir uma maior autonomia aos delegados de polícia, (c) definir prazos e rotinas de requisição e respostas pelos provedores, (d) ajustar conceitos sobre 'dados cadastrais', sobre 'porta lógica', (e) atribuir regras mais claras sobre a competência para julgamento dos casos (especialmente do crime de estelionato) e (f) estabelecer uniformidade e procedimentos padronizados junto aos provedores de conexão e de aplicação.

As correlações também apontam, na perspectiva dos entrevistados, para a necessidade de uma legislação específica quanto aos procedimentos processuais penais quando se trate de crimes praticados pela Internet, incluindo prazos de envio do inquérito policial, de diferenciação do prazo nessa remessa, tratando-se ou não de réu preso. A referência, citada pelo entrevistado 02SE, é a legislação sobre drogas (Lei nº 11.343/2006).

Nos termos da legislação processual e procedimental em vigor, segundo os entrevistados, em unanimidade, há condicionamento da rotina dos órgãos às normativas, o que não é ilógico, pois (a) as frustrações dos atores não afetam a validade jurídico-normativa da legislação e orientam o procedimento e (b) há necessidade de coleta e busca de dados da autoria e materialidade atendendo às normas processuais e constitucionais, sob pena de ilegalidades. No entanto, a rotina condiciona também o tempo dos procedimentos, a não uniformidade e a falta de padronização, inclusive no contexto conceitual (ex.: a interpretação sobre dados cadastrais), cujas investigações, apesar da especialização nas polícias, acabam ingressando em uma 'vala' comum dos procedimentos relativos a outros delitos.

O terceiro questionamento realizado foi sobre a coleta e busca de evidências e as dificuldades e os procedimentos encontrados, desde o que é informado pela vítima até o que é buscado no procedimento policial pelos investigadores. A não uniformidade e a ausência de procedimentos padronizados é observável na análise do conjunto de respostas. Embora alguns Estados (MT e DF, por exemplo), tenham Procedimento Operacional Padrão (POP) institucionalizado, essa evolução não atingiu todos os Estados e é dificultada, segundo os entrevistados, pela ausência de normativa específica sobre a cadeia de custódia das 'provas eletrônicas', embasando-se, por outro lado, nas normas ISO (no caso, a norma ABNT NBR ISO/IEC 27.037).

Pelos procedimentos informados quanto à coleta e busca de evidências, em regra as informações levadas pelas vítimas à delegacia são os 'prints' da materialidade,

consubstanciadas e registradas no boletim de ocorrência. Por padrão, poder-se-ia solicitar a preservação dos dados junto aos provedores, mas nem todos os órgãos fazem isso, também "faltando cuidados técnicos, com evidências forenses de dispositivos" (12PI). Quando há necessidade de envolver perícia, os procedimentos são padronizados, porém "a investigação fica prejudicial pela demora" (09MA).

A chamada Lei Anticrime – Lei nº 13.964/2019 – acrescentou a disciplina da cadeia de custódia no Código de Processo Penal, porém não fez referência a procedimentos e cuidados com a evidência no cibersistema da Internet, na forma e nos procedimentos de coleta de evidências junto às aplicações e aos provedores de conexão, tendo-se, somente, a disciplina – nesse aspecto – do Marco Civil da Internet quanto à solicitação da preservação, em relação ao provedor de conexão ou junto à própria aplicação da Internet, por prazo maior do que o previsto legalmente (arts. 13 e 15 do MCI). De outra parte, o MCI recebeu um complemento de proteção de dados pessoais com a LGPD, blindando os dados.

Outro ponto destacado pelos entrevistados é a coleta de dados em fontes abertas e a certificação deles no procedimento, inclusive com utilização de sistemas específicos, como no caso da investigação das situações de pornografia infanto-juvenil na *deep web*, com software CPS (*Children Protection System*)[68], que faz a detecção de trocas de imagens e vídeos entre suspeitos com programas de trocas de arquivo de ponto a ponto (P2P)[69].

Na relação com os provedores, complementando o questionamento anterior, os entrevistados observaram e confirmaram a facilidade da interação com provedores de conexão e provedores de aplicação que possuem plataformas *Law Enforcement*[70], de interação com as forças de Lei, polícia, Ministério Público e Poder Judiciário, com a ressalva, por parte dos participantes da entrevista, de que os sistemas, construídos pelas próprias aplicações, causam o engessamento no cadastro e resposta (às solicitações), e, também, pela falta de padronização e uniformização entre eles.

---

[68] Baseado no programa *Child Rescue Coalition*, disponível em https://childrescuecoalition.org/law-enforcement/, acesso em 4 set. 2022.

[69] Dentre os programas P2P utilizados no Brasil estão Limewire, eMule, Ares Galaxy e Shareaza. O P2P – ou rede *peer-to-peer* – é um sistema que, ao ser instalado em computadores, é responsável pelo compartilhamento, pela troca de documentos, informações e diversos tipos de arquivos, não necessitando de um servidor central, de um servidor principal (EWALLY, 2021). O próprio computador onde está instalado o aplicativo torna-se um servidor, o que lhe possibilita também ser um hospedeiro do arquivo para fins de download por outra máquina conectada na mesma rede e serviço.

[70] Plataformas criadas pelos provedores de conexão e de aplicação para interação com as polícias, membros do Ministério Público e Poder Judiciário. O primeiro a criar uma plataforma foi o Facebook (www.facebook.com/records), sendo seguido por vários outros (WENDT; JORGE, 2021).

Um tema destacado por vários entrevistados é sobre a não existência de regra jurídica que obrigue aos provedores o resguardo da chamada 'porta lógica', que, no caso do protocolo de internet da versão 4 (IPv4), quando há nateamento de IPs (um mesmo IP atribuído, pelo provedor de conexão, a vários usuários), facilita a individualização do acesso e, correspondentemente, a autoria delitiva (BARRETO, 2017). A regra normativa do Marco Civil da Internet não prevê literalmente essa obrigação, embora o § 1º do Art. 10 destaque que o provedor deva passar informações que possam contribuir para a identificação do usuário ou terminal.

De outra parte, o sistema de rede da Internet está assim 'organizado' no Brasil, circunstância reconhecida também pelo Art. 65-J da Resolução nº 738/2020 da Anatel[71], que prevê o resguardo da porta lógica como elemento integrante do registro de conexão e, por tais elementos fáticos e normativos, o Superior Tribunal de Justiça já reconheceu a necessidade de os provedores guardarem essa informação[72].

---

[71] "Art. 65-J. A fim de assegurar a permanente fiscalização e o acompanhamento de obrigações legais e regulatórias, as prestadoras devem manter à disposição da Anatel os dados relativos à prestação do serviço, incluindo, conforme o caso e observada a regulamentação pertinente:

I - documentos de natureza fiscal, dados cadastrais dos assinantes e dados de bilhetagem e das ligações efetuadas e recebidas, bem como data, horário, duração e valor da chamada pelo prazo mínimo de 5 (cinco) anos, nos serviços que permitam a realização de tráfego telefônico; e,

II - registros de conexão à Internet pelo prazo mínimo de 1 (um) ano nos serviços que permitam a conexão à Internet.

Parágrafo único. Para fins do disposto neste artigo, considera-se registro de conexão à Internet o conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal, assim como as portas lógicas utilizadas quando do compartilhamento de IP público, para o envio e recebimento de pacotes de dados".

[72] PROCESSUAL CIVIL. RECURSO ESPECIAL. AÇÃO DE OBRIGAÇÃO DE FAZER. INTERNET. PROVEDOR DE APLICAÇÃO. USUÁRIOS. IDENTIFICAÇÃO. ENDEREÇO IP. PORTA LÓGICA DE ORIGEM. DEVER. GUARDA DOS DADOS. OBRIGAÇÃO. MARCO CIVIL DA INTERNET. INTERPRETAÇÃO TELEOLÓGICA.

1. Ação ajuizada em 15/06/2015. Recurso especial interposto em 17/05/2018 e atribuído a este gabinete em 09/11/2018.
2. Ação de obrigação de fazer cumulada com pedido de tutela antecipada, na qual relata a recorrida que foi surpreendida com a informação de que suas consultoras estariam recebendo e-mails com comunicado falso acerca de descontos para pagamento de faturas devidas à empresa.
3. O propósito recursal consiste em definir a obrigatoriedade de guarda e apresentação, por parte da provedora de aplicação de internet, dos dados relacionados à porta lógica de origem associadas aos endereços IPs.
4. Os endereços IPs são essenciais à arquitetura da internet, que permite a bilhões de pessoas e dispositivos se conectarem à rede, permitindo que trocas de volumes gigantescos de dados sejam operadas com sucesso.
5. A versão 4 dos endereços IPs (IPv4) esgotou sua capacidade e, atualmente, há a transição para a versão seguinte (IPv6). Nessa transição, adotou-se o compartilhamento de IP, via porta lógica de origem, como solução temporária.
6. Apenas com as informações dos provedores de conexão e de aplicação quanto à porta lógica de origem é possível resolver a questão da identidade de usuários na internet, que estejam utilizam um compartilhamento da versão 4 do IP.
7. O Marco Civil da Internet dispõe sobre a guarda e fornecimento de dados de conexão e de acesso à aplicação em observância aos direitos de intimidade e privacidade.

Ainda, um tema complementar é destacado pelos entrevistados: a ausência de prazos, já referida, e não padronização da forma de apresentação das respostas, não uniformes, entre os provedores. Voltam aqui os entrevistados a observar sobre o entendimento do conceito de 'dado cadastral' e, também, em relação a algumas aplicações, a recusa de fornecer esse dado sem ordem judicial, embora prevista a autorização no Marco Civil da Internet.

Pontualmente, operadoras de telefonia (20RR), setor bancário (15TO) e aplicações como o Google (03BA, 11AM, 21RN e 24PA) têm maior resistência em fornecer os dados: "pessoas responsáveis dificultam o trabalho" (22MG). Finalmente, a destacar, é a referência aos provedores de pequeno porte (01GO, 13AL e 24PA), não capazes de fornecer os dados, conforme previsão legal. Ou seja, essas dificuldades pontuais não são consenso entre os entrevistados, embora não se tenha provocado essa análise em questionamento específico.

Assim, percebe-se a frustração dos entrevistados quanto à estrutura não padronizada e não uniformizada, tanto da coleta quanto da preservação de evidências e entrega dos dados de registro de conexão e de acesso, sendo, portanto, expectável uma estabilização das expectativas normativas com procedimentos mais práticos, mais efetivos, na interação com os referidos serviços. Frustrações sobre a interpretação da norma, de maneira a restringir ainda mais o acesso às informações úteis à investigação criminal, com base na LGPD, transparecem de uma considerável parte dos entrevistados.

Nesse processo de obtenção de informações, dados possíveis e úteis na investigação criminal cibernética, podem ser utilizados mecanismos de cooperação, desde a colaboração entre as polícias (troca de dados, realização de depoimentos e interrogatórios, prisões etc.) até auxílios formais, internos e externos ao Brasil.

Pelas respostas dadas pelos entrevistados quanto aos mecanismos de cooperação policial entre polícias dos Estados, prevalece a informalidade na troca de informações e o auxílio na realização de prisões, notadamente pelo contato pessoal entre os atores, especialmente por grupos de mensageria (WhatsApp). A formalização, ou melhor, o aspecto formal da colaboração entre polícias, é referido como moroso e burocrático (ex.: Carta

---

8. Pelo cotejamento dos diversos dispositivos do Marco Civil da Internet mencionados acima, em especial o art. 10, caput e § 1º, percebe-se que é inegável a existência do dever de guarda e fornecimento das informações relacionadas à porta lógica de origem.
9. Apenas com a porta lógica de origem é possível fazer restabelecer a univocidade dos números IP na internet e, assim, é dado essencial para o correto funcionamento da rede e de seus agentes operando sobre ela. Portanto, sua guarda é fundamental para a preservação de possíveis interesses legítimos a serem protegidos em lides judiciais ou em investigações criminais.
10. Recurso especial não provido.

(REsp 1777769/SP, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 05/11/2019, DJe 08/11/2019).

Precatória), sem um protocolo interestadual definido operativamente. O não uso da cooperação, mesmo informal, é pequeno (3= 12,5%), enquanto o uso dessa cooperação é referenciado como utilizado com frequência por 21 (=87,5%) entrevistados, o que é inversamente proporcional à não utilização, pelas polícias civis, da cooperação policial internacional ou, até mesmo, a cooperação penal internacional (arts. 783 e ss. do CPP), sendo esta realizada com base nos tratados e protocolos internacionais, já que são instrumentos utilizados esporadicamente:

- Cooperação policial internacional:
    - não utilizam = 21 (87,5%)
    - sim, utilizaram, porém, apenas recebendo dados de outras polícias ou, no caso de solicitação de auxílio, sem sucesso ou sem resposta = 3 (12,5%)
- Cooperação penal internacional:
    - Nunca utilizou = 19 (79,16%)

O procedimento de cooperação penal internacional, via DRCI/MJSP[73], foi considerado complexo por parte de 7 (=29,16%) entrevistados, e um mesmo número referiu nunca ter tido a demanda, embora tenha tido quem afirmasse as duas situações, ou seja, 'sem demanda, mas complexo'.

Dentre aqueles que já utilizaram o procedimento, destaca-se um Estado com 37 utilizações e POP[74] previsto (19DF), alinhando-se com a complexidade do procedimento previsto em relação a cada país destinatário. De outra parte, o entrevistado 24PA afirmou ter utilizado o procedimento, porém sem sucesso, referindo que prefere "adotar outras técnicas de investigação que fazer cooperação". Já 14PR afirmou ter pagado pelo tradutor juramentado, mas o procedimento foi complexo, enquanto 02SE já adotou o procedimento, mas sem resposta formal e que o "aparato de polícia judiciária" não é adequado.

Assim, quatro entrevistados (=16,66%) utilizaram o procedimento de cooperação penal internacional, que possui, desde 2014, uma cartilha de orientações elaborada pelo Ministério da Justiça e Segurança Pública (SAADI, 2014) e tão-somente um compreendeu a complexidade do procedimento de cooperação penal internacional e se adequou (17DF). Por isso, expectativas referidas são voltadas à Convenção de Budapeste, internalizada no Brasil

[73] Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional da Secretaria Nacional de Justiça (DRCI/Senajus/MJSP) atua como Autoridade Central para a Cooperação Jurídica Internacional.
[74] Procedimento Operacional Padrão.

em 2021 pelo Decreto Legislativo nº 37[75], de 16 de dezembro: "Também sobre a participação do Brasil na Convenção de Budapeste, isto é algo que tem me deixado bastante ansioso e acreditando que alguma coisa vai melhorar [...]" (10SC).

Portanto, procedimentos vários podem ser adotados para a formalização da investigação cibernética, considerados morosos e complexos pelos entrevistados. A facilidade de interação e resposta com relação a alguns provedores de conexão e de aplicação reduz o tempo de formalização do procedimento policial. O crime investigado e a complexidade de dados podem aumentar esse prazo. A noção de "tempo do procedimento" é variável dentre os entrevistados, passando de dias (menos de um mês) a um ano ou mais. A resposta mais comum foi de que o tempo de remessa do procedimento é de 8 meses, ou seja, superior ao previsto no CPP, o que reforçaria a expectativa quanto a uma disciplina normativa específica para os crimes cibernéticos ou sobre os prazos de cumprimento das requisições/determinações.

No entanto, entre a expectabilidade cognitiva dos atores de investigação, que corresponde a uma frustração pela demora ou tempo de resposta dos provedores, a ausência de padronização ou o poder requisitório (diminuído) do delegado de polícia e a possibilidade de câmbio da norma, reestruturando as regras de acordo com as várias expectativas organizacionais envolvidas (dos provedores, do Judiciário etc.), há uma lacuna muito grande, sobre a qual esses policiais, enquanto atores de investigação criminal cibernética, parecem não atuar, não se aprofundar, porquanto a imensa maioria deles desconhece projetos de lei que visem a melhorar e atender a essas expectativas sobre as expectativas normativas. Ou seja, essa comunicação não chega ao sistema legislativo e, por isso, não o irrita e não produz heterroreferência evolutiva.

Não se trata, portanto, de ser o sistema ou os sistemas resistentes às expectativas dos atores de investigação criminal cibernética e de, por isso, essas expectativas sobre expectativas estarem sempre sendo desapontadas. O que não há é comunicação hábil: a seleção dos desapontamentos, a forma de repasse dessas informações, precisa ser explícita para que essas frustrações possam ser conhecidas e, eventualmente, absorvidas pelos demais sistemas de acordo com sua função e código, inclusive os sistemas organizacionais.

Por isso, pretende-se no próximo tópico explorar mais esses aspectos, especialmente a partir da estrutura policial envolvida, das qualificações dos atores, dos investimentos recebidos e da perspectiva e das expectativas e frustrações dos entrevistados a partir de outras

---

[75] Vide mais sobre a Convenção de Budapeste no Capítulo 4.

estruturas organizacionais, especialmente as com o poder de decisão, ou seja, o sistema político (administrativo).

3.3 Estruturas organizacionais e as perspectivas dos atores responsáveis por apresentar resultados na investigação cibernética

No *segundo momento* da entrevista, buscou-se observar, a partir das respostas dos entrevistados, quais as estruturas organizacionais e as perspectivas envolvidas sobre recursos, materiais e humanos, investimentos e definição de atribuições. Esse momento foi dividido em duas partes, as quais podemos definir como *estrutural* e de *investimento*, sequencialmente.

Na parte *estrutural*, procurou-se (a) obter dados sobre o tempo de existência da delegacia/órgão especializado, (b) saber há quanto tempo o entrevistado estava atuando na delegacia, (c) conhecer como é que o público chega à delegacia e se as pessoas sabem que ela existe e qual a função dela, como especializada, (d) ouvir sobre a estrutura existente para investigação de crimes cibernéticos, como o entrevistado percebe ela e qual a experiência que pode advir daí, (e) saber se o local é próprio, locado ou cedido gratuitamente e como são as instalações, (f) saber se o pessoal (efetivo policial) possui conhecimento prévio e se há corpo técnico especializado para as investigações, e (g) saber se os equipamentos e softwares são adequados às necessidades investigativas, finalizando com um questionamento genérico de (h) sobre a existência de alguma sugestão/proposta de melhoria.

Já na parte de *investimento*, buscou-se observar, a partir dos dados conhecidos pelo entrevistado, quais os investimentos direcionados à investigação criminal cibernética, assim, questionando-se (a) o que o entrevistado entende, 'acha' ou conhece, sobre os investimentos na investigação de crimes cibernéticos, (b) se o órgão recebeu verbas e investimentos estaduais, (c) se o órgão recebeu verbas e investimentos federais (e, dependendo do contexto, pedia-se para limitar o tempo de análise na resposta), (d) se o órgão recebeu recursos de doação e apoio de empresas e pessoas privadas nos últimos três anos e, por fim, se o entrevistado (e) queria acrescentar algo sobre os investimentos e sobre qual é a necessidade e/ou expectativa de investimentos que deveriam ser feitos.

A análise do perfil dos entrevistados já foi feita (item 4.1.2), incluindo o tempo de atividade na especialidade de investigação criminal cibernética, o 'tempo de atividade ciber', não se chegando a ter policiais com mais de sete anos de atuação na área. Assim, este questionamento foi analisado em conjunto na observação sobre o perfil dos entrevistados.

Por isso, neste tópico da tese observar-se-á a *estrutura* do órgão a partir (a) dos atos normativos constitutivos e (b) das observações do entrevistado.

3.3.1 Especialização dos órgãos nas polícias civis: antes e depois da Lei nº 12.737/2012

Neste ponto da pesquisa empírica, procurou-se alinhar as respostas dos entrevistados com a documentação coletada a respeito das normativas que previram os órgãos de investigação de crimes cometidos pela rede mundial de computadores em todos os Estados e Distrito Federal.

Assim, verificou-se, de pronto, uma falta de uniformidade tanto na nomenclatura quanto na definição das atribuições em cada Estado, observando-se que as peculiaridades locais, político-administrativas, bem como as terminologias, influenciaram na definição. Nenhum dos órgãos é do século XX, sendo o primeiro, do Estado do Rio de Janeiro, inaugurado no ano de 2000; já o último é do Estado do Acre, porém apenas a previsão e não a efetiva instalação e funcionamento. Com os dados coletados, formatou-se um quadro (ANEXO III), com as informações em ordem alfabética dos Estados e Distrito Federal.

Pelos dados apurados[76], apenas oito Estados possuíam órgãos específicos para a atividade de investigação criminal cibernética antes de 2012, ano da Lei nº 12.737/2012. Outros 18 Estados formataram e incluíram em suas estruturas um setor especializado ou previram a reestruturação administrativa, embora Estados, como Acre, Ceará e Rio Grande do Norte, tenham a previsão da estrutura e não sua efetiva instalação e correspondente atividade diária, com recursos humanos e materiais. Um dos Estados ainda não possui previsão normativa e ou de instalação de órgão específico: Mato Grosso do Sul.

Verifica-se, portanto, que, mesmo que os entrevistados não tenham um conhecimento sobre a Lei nº 12.737/2012, a adequação à sua previsão não deixou de ocorrer no âmbito da estrutura dos Estados, e, mesmo aqueles que já possuíam uma estrutura mínima, ampliaram-na com base no aumento da demanda de trabalho e de novas especialidades, a exemplo de São Paulo, Pará, Maranhão e Minas Gerais.

Observou-se que o Acre, mesmo tendo a normativa criado um Laboratório de Inteligência Cibernética sem uma efetividade prática, após a entrevista[77] acabou por criar uma Delegacia de Polícia e se encaminha para o início das atividades. Também, Bahia, que

[76] Até 6 de setembro de 2022.
[77] Em julho de 2022.

já possuía um laboratório e um grupo especial desde 2012, criou, em agosto de 2022, uma delegacia especializada.

3.3.2 Atender às expectativas do público-vítima e gerenciar a estrutura deficitária: a absorção, a incorporação e o repasse de situações expectantes e frustrantes

As expectativas sociais, em razão da sua complexidade, acabam reproduzindo no legislador uma necessidade de estruturação das expectativas e, por isso, uma utilização maior do direito como mecanismo de contingenciamento e de redução de complexidades. Quando se trata de serviços públicos, como o [papel do] policial investigador, a expectativa social recai sobre a estrutura administrativa de atendimento às vítimas de crimes.

Após normatizada penalmente a previsão sobre a conduta (cibernética), acaba-se por gerar as correspondentes expectativas normativas, tanto pelos sujeitos usuários da Internet quanto pelos operadores da investigação criminal, que têm a função de investigar e 'formar o molde' de enquadramento do fato, da conduta, à norma penal. Essas expectativas normativas tendem a resistir à frustração, pois a norma persiste embora frustrada a expectativa. A mesma lógica se aplica às expectativas sobre a estrutura administrativa consolidada para o atendimento às ocorrências de crimes, assim definidos pelo legislador, ou seja, já estruturados normativamente. A conduta desviante e desapontadora da norma penal passa a ser objeto de observação, a partir da comunicação da ou das vítimas envolvidas, pelos policiais, em função do seu papel inicial na persecução criminal e de acordo com a estrutura organizacional existente, material e humana.

Percebe-se que, no caso das comunicações não selecionadas e normatizadas pelo legislador e/ou administrador local (dos Estados e do Distrito Federal), as expectativas acabam sendo frustradas e assimiladas, possibilitando processos de aprendizado e, assim, geração de outras expectativas que podem encaminhar para uma estruturação, no caso de órgãos policiais específicos para a investigação de crimes cibernéticos. É o caso do Acre, Rio Grande do Norte e Rondônia[78], de acordo com as expectativas e frustrações referidas em observações ditas pelos entrevistados.

Porém, nos demais locais onde já há uma estrutura administrativa consolidada para o atendimento, as expectativas cognitivas sobre as expectativas normativas, estruturadas

[78] Rondônia tem uma situação diferenciada: possui a previsão de um laboratório e atividade com um policial; também possui uma delegacia com foco em investigação de fraudes. Porém, não possui a previsão de uma especializada em investigação de crimes cibernéticos.

administrativamente, são outras. Nestas observações, pretende-se, assim, analisar, sempre a partir da observação dos entrevistados, aspectos inerentes ao atendimento às vítimas de crimes, recursos humanos e materiais, qualificação, perspectivas de melhoria e investimentos.

3.3.2.1 Observar e conhecer o público-alvo dos crimes cibernéticos: atendimento às vítimas, demandas, estruturas e frustrações

"Chegam pessoas com várias demandas, muito mais do que a atribuição" (01GO). A fala resumida do entrevistado condensa a observação sobre a demanda de atendimento às vítimas de crimes cibernéticos e sobre a estrutura e a delineação da atribuição do órgão especializado.

66,67% dos entrevistados (=16) afirmaram que as vítimas conhecem o órgão especializado, sabendo de sua existência, mas não necessariamente das atribuições, e, também, nem todos fazem o atendimento e registro de ocorrências: "público não sabe a função da delegacia" (08PE); "confunde a gente com delegacia pela internet" (08PE); há "uma dificuldade de compreender as atribuições da unidade" (12PI); "nossa função é muito genérica" (14PR); "qualquer crime da internet a população nos procura e a outras delegacias também" (14PR); "muitos fatos não são de nossa atribuição, mas nos procuram para atender" (15TO); "qualquer vítima de crime cibernético chega à delegacia" (06AP); há uma "procura grande", mas "não tem atendimento em massa na delegacia" (19DF); o "público vem por indicação ou por pesquisa na internet" (22MG) ou por "indicação de outras delegacias" (23SP).

Outro entrevistado resume: "o público procura muito" (24PA). Em boa parte desses Estados em que há conhecimento por parte do público, segundo a observação dos entrevistados, é porque há divulgação de campanhas preventivas, de notícias e alertas sobre os crimes cibernéticos (10SC; 16MS; 17MT; 18RO), havendo muita demanda por parte da imprensa quanto ao tema (15TO).

Já nos Estados em que o público desconhece a delegacia/órgão e sua função (8 = 33,33%), as observações destacadas pelos entrevistados são relativas (a) à politização do atendimento (05AC, 11AM)[79], (b) à falta de capacitação dos policiais para o atendimento

[79] Por "politização do atendimento", para fins desta análise, são os casos encaminhados à especializada pelos superiores hierárquicos e/ou por políticos, visando a ter um atendimento preferencial e privilegiado.

correto às vítimas (02SE), (c) à falta de conhecimento interno sobre a função e as atribuições do órgão (09MA) e (d) à deficiência de pessoal especializado (21RN).

A correlação da existência e das atribuições do órgão especializado com a questão político-administrativa fica evidente e clara pela afirmação do entrevistado 11AM: “para ter noção, até nossos chefes de outras delegacias não entendem muito bem [...] trabalhamos em função do próprio governo e a população é muito carente”. Ou seja, além de falta de conhecimento interno sobre as atribuições, também há ingerência para priorização de determinados atendimentos em detrimento de outros.

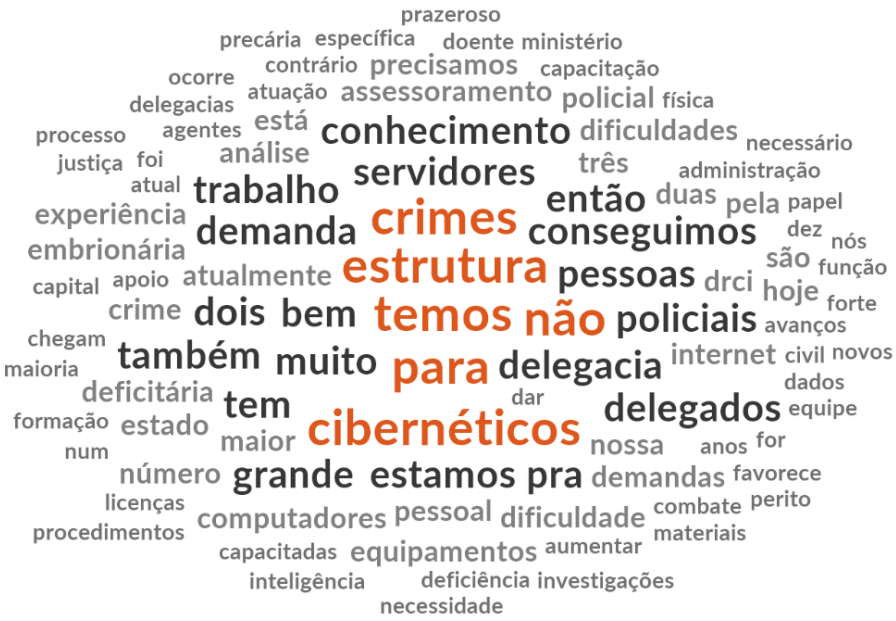
A percepção quanto ao atendimento às vítimas de crimes cibernéticos não fica restrita às possibilidades, aos desafios e ao conhecimento delas e dos integrantes das polícias civis, mas também é relacionada à estrutura física e de recursos materiais e humanos disponibilizada pelo Estado para esse trabalho.

Neste âmbito pontuam-se, então, as principais frustrações, porquanto a referência à deficiência em termos de recursos humanos e materiais foi constante, não havendo servidores suficientes para a atividade fim, de investigação criminal e de assessoramento às investigações realizadas por outras delegacias.

A localização do órgão é referida como forma a dificultar e/ou ampliar a procura por atendimentos outros que não os de atribuição da especializada (06AP), assim como a falta de sensibilidade [e prioridade] dos gestores quanto ao tema, “que não são crimes violentos” (12PI), acaba por desapontar os entrevistados, que também assinalam outras atribuições, conjuntas, mas não correlatas, como a do antissequestro (13AL), prejudicando o andamento e caracterizando a precariedade no atendimento.

A expectativa [e correspondente frustração] é sobre a decisão [político-administrativa] de aumento de efetivo policial, mesmo quando a estrutura física do órgão é satisfatória (15TO). E, mesmo tendo “estrutura excelente”, a sensação de desgaste ocorre em razão da ‘rotina de trabalho’, do ‘crescimento da demanda’ e do ‘número pequeno de servidores’ (22MG). Vários termos são associados a essas expectativas e frustrações:

Figura 6: Expectativas e frustrações quanto às estruturas (administrativa e operacional) de enfrentamento aos crimes cibernéticos



Fonte: Produzido pelo autor (2023).

A expectativa também se estende às necessidades de ampliação e melhoria dos computadores, aquisição de softwares e treinamento do efetivo policial. A afirmação de que "a estrutura nunca será suficiente" (19DF) conforma-se com a demanda recebida no órgão, formando-se uma expectativa generalizada de ampliação da estrutura administrativa do órgão. No entanto, essa percepção específica, observada pelo entrevistado 19DF, não é consonante com os demais entrevistados, especialmente sobre os equipamentos e softwares que seriam adequados à realização das atividades investigativas, porquanto há um direcionamento dos demais observar a falta ou não suficiência deles, faltando, inclusive, conhecimento sobre quais os equipamentos e softwares seriam adequados à atividade.

Aquisição de computadores e softwares representa o anseio dos entrevistados, que também referem ser importante ter equipamentos e sistemas de extração de dados de telefones (a exemplo de 14PR, 16ES). A incapacidade da rede de Internet em suportar a necessidade do trabalho (02SE, 20RR), bem como a utilização de equipamentos pessoais para o trabalho (24PA), são observações reveladoras da incapacidade do Estado de suprir as condições de trabalho, ocasionando uma frustração nos atores de investigação criminal por não conseguirem exercer adequadamente seu papel sem esforço pessoal e paciência.

Finalmente, quanto à estrutura e às condições de trabalho, mesmo atuando em prédios próprios (13)[80], alugados (7) ou cedidos (3), os espaços foram considerados bons, ótimos, satisfatório, adaptados (“antes era um convento” – 13AL), insuficientes, provisórios, precários (“uma sala para todos policiais” – 20RR), necessitando de adequações. Revela-se, assim, uma não uniformidade estrutural também quanto ao espaço físico disponibilizado para a atividade de investigação de crimes cibernéticos.

3.3.2.2 Efetivo e capacidade técnica especializada

A qualificação do ator de investigação criminal cibernética, sob as observações dos entrevistados, é uma expectativa constante. Apesar de em muitos Estados, mesmo nos órgãos especializados, haver apenas um policial com conhecimento na área de Tecnologia da Informação, muitos acabam sendo selecionados e formados internamente, na atividade diária e/ou com treinamentos específicos: “as pessoas foram escolhidas em razão de alguma outra experiência de tinham, ou na área de TI, ou que vinham de investigação de outras delegacias” (06AP); “quando existe a vaga ela será preenchida e o policial aprenderá o trabalho no departamento” (09MA); “alguns colegas, na qual me enquadro, foram removidos para DRCC, não possuem atuação, anteriormente, na área de crimes cibernéticos, assim buscaram conhecimento, se aperfeiçoaram, são proativos e se interessam pelo tema” (15TO).

A busca por autoconhecimento, inclusive com recursos próprios e [não] do Estado, na área de Tecnologia da Informação, segurança cibernética, dentre outros temas, é referida pelos entrevistados como meio de formação e qualificação dos servidores.

Estados, como o Distrito Federal, fazem treinamentos semanais para os integrantes da especializada, fragmentando e especializando os servidores em determinados temas. Outros Estados acabam buscando os conhecimentos de atuação em outros setores, como o da inteligência e/ou o Ciber-Lab do Ministério da Justiça e Segurança Pública. Este setor, aliás, é bastante referenciado nos apoios às investigações e nos treinamentos.

Há, também, observações no sentido de que se “necessita de pessoas com vontade de trabalhar na área” (16ES), de “interessados no tema” (15TO, 18RO), que atuem “por iniciativa própria” (12PI) e de que “não precisa ter conhecimento para estar no departamento” (09MA), mas a seleção de profissionais para atuar nos setores é um caminho para a

[80] Um dos entrevistados considerou a resposta prejudicada por não ter atuação efetiva do órgão, mesmo que indireta.

qualificação do resultado da investigação (06AP, 23SP). Por outro lado, uma vez estando na especializada, acabam se tornando referência e, também, dando treinamentos sobre a investigação cibernética.

3.3.2.3 Investimentos na estrutura de investigação cibernética: União, Estados e iniciativa privada/pública

Dadas as informações sobre deficiências e carências das estruturas físicas e de recursos materiais, procurou-se saber quais as observações dos entrevistados quanto aos investimentos realizados pela União (federal), pelos Estados (estadual) e, também, quais órgãos receberam ou não auxílios do setor privado ou outros órgãos públicos, em doações.

Os investimentos da União nesses órgãos foram destacados por apenas quatro entrevistados, ou seja, 83,33% (=20) deles não percepcionaram investimentos oriundos do governo federal, embora vários tenham mencionado a expectativa de receber recursos em razão de recente preenchimento de questionário demandado por integrantes do Ministério da Justiça e Segurança Pública.

A evidência de falta de investimentos direcionados à investigação cibernética não é somente da União, mas também é constante nos Estados, porquanto somente em oito (=33,33%) houve destinação de recursos, enquanto os demais não tiveram nada direcionado pelos governos estaduais.

A atividade de investigação cibernética tem uma demanda grande de outros setores, privado ou público, o que gera uma interação e interesse de auxiliá-los, seja por projetos específicos (01GO), momentos especiais, como a criação da delegacia (02SE) ou para estruturação do setor (23SP). Bancos ou a Federação de Bancos foram destacados como instituições interessadas em auxiliar, assim como a Receita Federal e o Ministério Público do Trabalho.

Evidencia-se, assim, que a fala do entrevistado 12PI de que os gestores precisam ser convencidos a investir no órgão especializado na investigação cibernética, que “não atende crimes violentos”, é uma observação extensível aos outros Estados.

Mesmo o governo federal, como citado pelos entrevistados, manifestando-se e solicitando o preenchimento de uma planilha com necessidades [em 2022, ano de eleições], não há garantias de investimentos, ou seja, há tão-somente uma expectativa sobre uma ideal estruturação. Por outro lado, há expectativas cognitivas referidas pelos entrevistados quanto

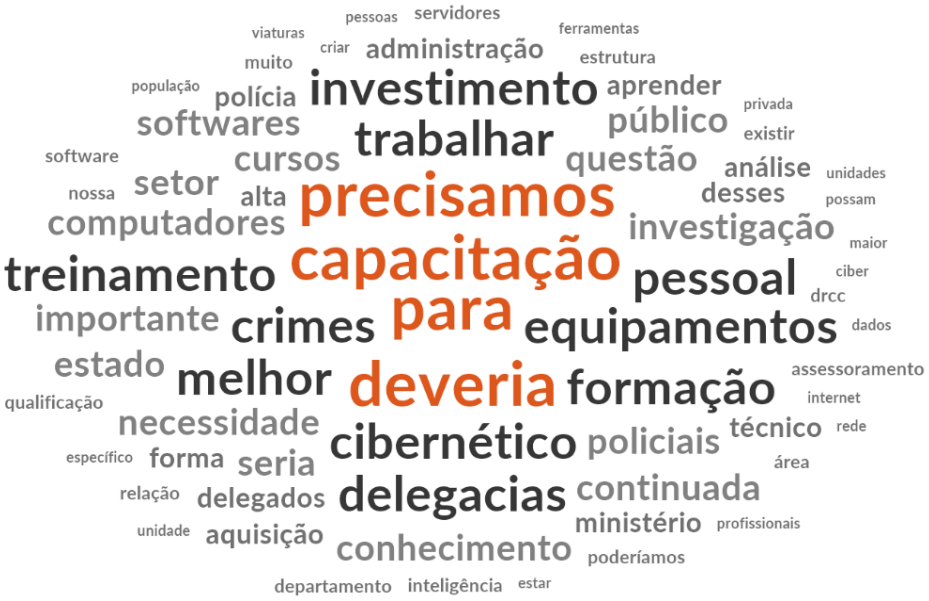
às parcerias público privadas, as denominadas PPPs[81]. Assim, comporta, já no próximo tópico, uma análise dessas necessidades e expectativas sobre as necessidades.

3.3.2.4 Melhoria das condições de realização da atividade de investigação cibernética: entre sugestões e expectativas

Buscou-se, na análise do conteúdo, categorizar as sugestões de melhorias quanto à estrutura do órgão de investigação especializada cibernética, seja elas relacionadas aos recursos humanos e/ou materiais.

Muitos tópicos foram elencados e o que mais foi referido pelos entrevistados é a necessidade de capacitação [continuada] dos policiais, que já deveria iniciar junto à formação inicial deles, não deixando de lado a busca de capacitação no setor privado e a promoção de interação interna de aprendizados. A nuvem de palavras formada a partir dessas observações referência uma amostra da importância dos temas:

Figura 7: Necessidades expectáveis, pelos atores de investigação criminal cibernética, capazes de aprimorar o enfrentamento aos crimes no âmbito da Internet



Fonte: Produzido pelo autor (2023).

[81] A Lei nº 11.079/2004 instituiu normas gerais para licitação e contratação de parceria público-privada no âmbito da administração pública.

Partindo da necessidade de que os gestores compreendam a ‘importância’ da atividade especializada, investindo e destinando recursos, como viaturas, computadores, equipamentos e softwares, os entrevistados reforçaram sugestões de melhoria das ‘condições de trabalho’, ‘investimento em pessoal’, ‘desvinculação administrativa’, ‘aumento de efetivo’, ‘computadores condizentes’ e ‘processadores bons’, ‘potentes’, ou seja, ‘equipamentos compatíveis [com a atividade]’ e de ‘última geração’, capazes de ‘trabalhar com softwares’ e ‘disponíveis para todos os servidores’, aliados à existência de ‘rede elétrica adequada’ e ‘Internet de qualidade’.

Aspectos sobre a localização do setor também foram mencionados como forma de melhorar a atividade e o atendimento ao público, mas também há necessidade de um diagnóstico preciso quanto ao que poderia ser feito pelo Ministério da Justiça e Segurança Pública (17MT).

Aliás, os temas da padronização, centralização e de metodologias, seja de treinamento, de cooperação e intercâmbio de informações, foram elencados pelos entrevistados como um mecanismo complementar e necessário à melhoria da atividade de investigação cibernética. Servidores específicos e com conhecimento sobre o tema são necessários, mas também são necessários, segundo as observações dos entrevistados, profissionais do setor privado, que deveriam ser contratados tendo em vista sua especialidade.

Aliada à necessidade de treinamento e interação entre profissionais e setores, a padronização nacional é referenciada, seja em termos de equipamentos, via incentivo do governo federal, seja para estruturar as unidades, seja para uniformizar procedimentos, inclusive na institucionalização desses padrões a respeito da coleta de evidências, formação de profissionais de *offensive security* (12PI) na aquisição de sistemas e softwares para extração, mineração e análise de dados, possibilitando a criação e manutenção de laboratórios de investigações, inteligência e operações cibernéticas (Ciber-Labs).

A reestruturação do órgão é uma sugestão latente em parcela dos entrevistados, sendo sempre correlacionada à demanda e à importância do tema, o que provoca também a rediscussão sobre a ampliação ou delimitação das atribuições, o que é observado no próximo tópico.

Assim, expectativas cognitivas são geradas sobre a estruturação ideal e adequada, para que os papéis dos atores de investigação criminal cibernética possam ser exercidos de maneira satisfatória e efetiva. A frustração dos entrevistados quanto à configuração de recursos humanos e materiais é latente em face da ausência ou de uma estrutura física condizente, ou de recursos humanos com capacitação na área, ou de equipamentos e

softwares hábeis à realização da atividade, sendo ainda maior quando os três aspectos estão referidos conjuntamente.

3.3.3 Atribuição e atuação: entre realidades e expectativas sobre expectativas normativas de estruturação

Tratou-se nos itens anteriores sobre a estruturação dos órgãos da polícia civil e apontou-se para as normativas estaduais a configuração formal dos órgãos de enfrentamento aos crimes cometidos pela rede mundial de computadores, conforme define a Lei nº 12.735/2012.

A lei em comento não definiu comandos, prazos ou sanções pelo não cumprimento, tampouco estabeleceu diretrizes mais específicas para a efetivação do que previu. Assim, coube às unidades federativas estabelecer diretrizes e delimitar configurações dos referidos setores, como já acontecia.

Objetivou-se, durante a entrevista com os atores de investigação criminal cibernética, conhecer quais os focos de atuação da delegacia/órgão de lotação[82] e se a delimitação formal existente está ou não condizente com a realidade fática, a demanda diária dos crimes cibernéticos[83]. À exceção do Estado onde não há previsão normativa de órgão estruturado para investigação cibernética (RO), embora exista, em modo precário, um Ciber-Lab, todos os entrevistados informaram que existem atos normativos de previsão e funcionamento do setor, que vão desde portarias, resoluções, decretos ou mesmo leis (inclusive complementares), existindo até mesmo 'instruções de serviço' ou 'instruções normativas'.

Verificou-se que, quando se trata de portarias, resoluções ou instruções (normativas ou de serviços), há uma possibilidade maior de alterações, a depender de cada Estado e da gestão da própria Polícia Civil, situação que requer também a observação de limites legais estabelecidos nas Constituições Estaduais e/ou Leis em vigor sobre a estruturação orgânica. Já quando se trata de Decreto ou Lei, a dependência, além de normativa, também é política, porquanto envolve setores além da instituição policial.

---

[82] "- Vocês têm algum foco principal de atuação na delegacia? Como funciona?
- Você diria que vocês têm algum foco principal (em relação aos crimes cibernéticos)? Se sim, por quê? Se não, por quê?
- Qual o foco acessório de vocês (em relação aos crimes cibernéticos)?"

[83] "- Existem atos normativos estaduais delimitando a atuação?
- A atribuição do órgão, no âmbito estadual, está adequada à realidade?"

Assim, procurou-se saber, a partir das observações dos entrevistados, como está delimitada a atuação do órgão a que pertencem, a partir da atribuição normativa, questionando-se o foco efetivo e a adequação à realidade existente. Outros pontos foram levantados, especialmente sobre as relações com órgãos como a Polícia Federal, o Ministério da Justiça e Segurança Pública, o Ministério Público e o Poder Judiciário[84].

Ao final desta série de questões, foi levantado o problema de como dar efetividade à Lei nº 12.735/2012: de certa forma, esta questão acabou sendo uma espécie de síntese sobre as questões anteriores, relacionadas às expectativas de estruturação de maneira geral, administrativa, física, de recursos humanos, de atribuições em si etc.

Metodologicamente, optou-se por separar as análises em dois subtópicos, a fim de melhor descrever as observações.

3.3.3.1 Foco de atuação e delimitação das atribuições do órgão de investigação criminal cibernética: o que é expectável

A atribuição dos órgãos das polícias civis é delineada normativamente e de acordo com [a evolução] de cada instituição no âmbito da sua área de atribuição, ou seja, a unidade federativa correspondente.

Os órgãos são, portanto, cunhados atendendo a alguns critérios político-administrativos do tempo de sua criação e, dentre eles, estão as demandas recorrentes sobre determinados delitos e o interesse político-social, este referido em destaque pelos entrevistados, inclusive para os encaminhamentos de investigações em que pessoas públicas/políticos são vítimas desses delitos (10SC, 22MG), além dos casos de grande repercussão (20RR) e 'clamor social' (22MG), o que requer uma atenção mais direta.

Não é necessariamente uma atribuição normativa atender a casos de clamor social e que envolvem pessoas públicas, embora seja isso referido por entrevistados. Portanto, esse atendimento 'direcionado' pode também ser compreendido como algo que acontece à revelia da norma.

---

[84] "- Como é a relação com a Polícia Federal nas trocas de informações e conhecimentos das práticas investigativas cibernéticas?
- Como é a relação com o Ministério da Justiça e Segurança Pública com relação aos treinamentos e às orientações?
- Como é a relação com MP e PJ? A estrutura desses órgãos é voltada para o cibercrime ou é normal, que atende todos os delitos?"

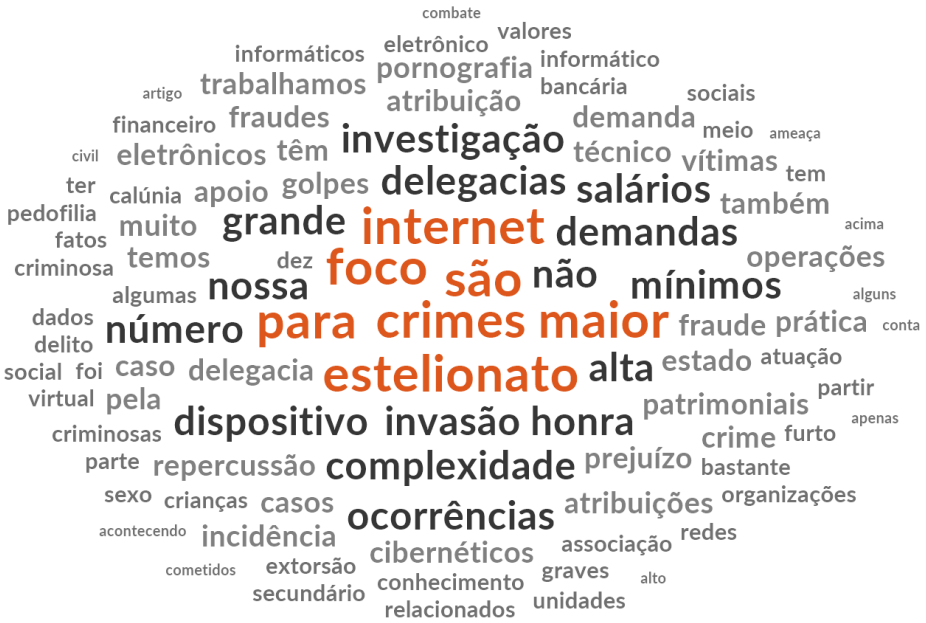
Os controles sobre a designação para a investigação de crimes praticados na Internet podem ser sobre casos individuais, inclusive passando pela gestão da instituição, como no caso referido pelos entrevistados 06AP e 20RR.

Esses controles também podem ser pessoais, como no caso do entrevistado 02SE, que refere ficar "com fraude bancária, *minha atribuição, meu foco é fraude bancária eletrônica*, a equipe faz isso especificamente, mas fazemos atendimento no dia a dia".

As frustrações são elencadas estando ou não a normativa estadual adequada à realidade, porém relacionadas às demandas recorrentes e à falta de efetivo policial para poder atender a todos os casos: "muita coisa passa por aqui" (01GO); "tem muito mais atribuição do que gente trabalhando" (07PB); "são muitas demandas e pelo quantitativo não consegue atender bem" (09MA); "quantidade absurda de ocorrências" (15TO).

A nuvem de palavras geradas a partir desta parte da entrevista demonstra os principais termos mencionados pelos participantes da pesquisa:

Figura 8: Focos de atuação dos órgãos especializados, conforme destaque dado pelos entrevistados



Fonte: Produzido pelo autor (2023).

A maioria dos entrevistados observou ser necessária uma adequação da atribuição do órgão, prevista em diversos tipos de atos normativos diferenciados (14 = 58,33%). O entrevistado 06AP referiu que

> Essa lei foi criada, mais de um ano antes do funcionamento e quando começamos a funcionar, na prática, vimos diversos delitos que não deveriam estar aqui, mas estão, e outros que teriam necessidade de estar, mas não estão. Então, acabamos fazendo trabalhos que não deveriam ser feitos, por exemplo a questão de demanda ínfima, objetos com valor ínfimos, abaixo de cem reais, inevitavelmente fica aqui e ocupando um espaço que deveria ser ocupado com demanda com maior expressividade, caso por exemplo de extorsão, segundo nossa lei não está aqui, mas deveria. (06AP).

Dentre os motivos então apontados à necessidade de adequação da atribuição, um dos critérios mais referidos foi a expectativa de se relacionar a investigação dos órgãos aos casos de maior complexidade investigativa, com abrangência sobre grupos e associações criminosas "de maior expressividade" (06AP). Aliada a essa perspectiva está a de delimitar um valor de prejuízo mínimo, composto por salários-mínimos, para estar ou não sob abrangência de atribuição do órgão de investigação cibernética, atrelando-se, logicamente, aos crimes patrimoniais, especialmente as fraudes eletrônicas. Nesse aspecto, observando-se as observações, estão certos os Estados de Rondônia, com delegacia específica de enfrentamento às fraudes, o Rio Grande do Sul, com a inclusão das fraudes nas atribuições investigativas, e, também, São Paulo, na especialização por áreas.

Partir do interesse pessoal para o institucional, em um processo de convencimento dos atores de investigação criminal cibernética em relação aos gestores institucionais, delineia-se como uma perspectiva [local e nacional] importante na adequação da estrutura normativo-institucional para atender aos casos de crimes praticados no âmbito da Internet. Aliás, a readequação local deve atender aos parâmetros da realidade local, do Estado e, por que não dizer, não se limitar somente à realidade da capital, ondem as 'delegacias cyber' estão localizadas, mas sim correlacionar à realidade de toda a unidade federativa.

Aliar, então, essa redefinição de atribuição com um processo macro, de orientação e auxílio interno aos demais órgãos não especializados na área, seja pela existência de um laboratório de operações ou inteligência cibernética (os Ciber-Labs), seja pela existência da função relacionada à delegacia, ao departamento, à divisão, à diretoria ou à coordenadoria, é considerado fundamental para a evolução no atendimento às situações de investigação em relação aos desvios de conduta, sejam crimes cibernéticos próprios ou impróprios, ou seja, já criados ou não com base neste novo contexto comunicacional da Internet. Nas observações do entrevistado 04RS, há necessidade de "adequar a realidade para toda a Polícia Civil e não apenas para o órgão".

Foco principal ou acessório, definido ou não normativamente, acaba por ser absorvido pela demanda de ocorrências e investigações, para os quais os policiais existentes não são ou

suficientes ou capacitados/especializados, levando a uma expectativa corrente: a de capacitação e qualificação contínua dos policiais. Abrangência e delimitações são necessárias para definir a atuação no órgão especializado, delineado pela Lei nº 12.737/2012, mas não são suficientes para absorver um problema que se tornou mais comum: inúmeros crimes são cometidos com a utilização, em algum ato preparatório ou de execução, da Internet. A função consultiva deste órgão especializado ganha, assim, destaque, pelo fato de os atores, os policiais, terem de auxiliar seus colegas de outras delegacias/setores: essa função de assessoramento para casos em que não há ou há complexidade, e a Internet é usada como um meio, tem um peso bem importante nas expectativas dos atores de investigação cibernética.

Mesmo os estados onde os entrevistados consideram estar adequada a norma sobre a atribuição à realidade fática, há uma expectativa de aumento de efetivo para atender à demanda, de se focar em delitos de maior gravidade (16ES) e dar maior capilaridade à atuação (24PA), ou seja, com mais delegacias especializadas (08PE). Crimes patrimoniais – especialmente estelionato eletrônico, extorsão sexual (*sex extorsion*) e invasão de dispositivo informático –, crimes contra a honra, contra crianças e adolescentes ('pedofilia', pornografia infantojuvenil, abuso etc.) e *fake news* são, juntamente com investigações da criminalidade organizada, objeto de atenção dos atores de investigação criminal cibernética que precisam, por vezes, elencar prioridades (15TO).

Reestruturações atendem às exigências e perspectivas do momento. Mesmo em relação a setores existentes há mais de dez anos, mudanças podem e devem ocorrer em razão da intensificação e massificação do uso da Internet e os efeitos a ela integrados, incluído o desvio de conduta. Este, ampliado o número, deve levar a uma revisão estrutural e normativa. De acordo com 23SP, a reestruturação ocorrida em seu Estado absorveu demandas e delimitou atribuições entre delegacias e outros setores, como uma central de inteligência cibernética e um laboratório de análises, ambos apoiadores nos processos investigativos.

A fragmentação pode ser o caminho neste compasso de tempo presente, com a delimitação, com base na legislação federal vigente, de um setor especializado na investigação e outro no auxílio técnico às investigações em curso. Porém, a fragmentação não será solução única, conforme observado pelos entrevistados, que têm expectativas de transformações frente a outras organizações e papéis, conforme abordar-se-á no próximo subtópico.

3.3.3.2 Interação com outros órgãos de persecução criminal: papéis e organizações

A pesquisa procurou analisar as observações sob o olhar em relação ao entorno dos entrevistados, os quais expectam melhorias e processos uniformes na condução do seu papel. Seus papéis, aliás, são sistematicamente interacionais, presencial ou tecnologicamente, com outros papéis, também ativos na persecução criminal, seja pelo repasse de experiências e orientações (como integrantes da Polícia Federal e do Ministério da Justiça e Segurança Pública), seja pela recepção dos procedimentos policiais e pela compreensão tecno-jurídica do contexto investigado (como integrantes do Ministério Público e do Poder Judiciário).

Ao passo que os entrevistados observam uma tímida relação com integrantes da Polícia Federal na troca de experiências e informações, relatando, em várias oportunidades, a inexistência de interação (‘quase nula’, ‘eles não conversam conosco’, etc.), a percepção é oposta em relação a integrantes do Ministério da Justiça e Segurança Pública, em especial o Laboratório de Operações Cibernéticas, ou seja, há uma interação efetiva, seja na troca de experiências, no treinamento, no repasse de orientações, no apoio às investigações e nas discussões, como as havidas no Ciber Cap.

Já com relação ao Ministério Público e o Poder Judiciário, órgãos envolvidos no sistema de persecução criminal, a percepção e as expectativas são mais evidentes no sentido da necessidade de uma melhora e ampliação. A abertura cognitiva desses sistemas organizacionais ainda não absorveu as comunicações relativas à ampliação da atuação dos agentes delituosos no contexto da Internet, havendo uma adequação mínima por parte dos ministérios públicos e nenhuma adequação no âmbito do judiciário.

A remessa de procedimentos e solicitações de medidas cautelares ao Poder Judiciário não tem uma atenção especializada, ou seja, não existe vara especializada para atender e recepcionar os procedimentos policiais derivados das investigações dos crimes cibernéticos, havendo, pela ótica dos entrevistados, um tratamento comum ao que deveria ser especializado[85]. Em alguns depoimentos, considerou-se ‘inacessível’ o Poder Judiciário, logicamente no processo interacional entre os atores: delegados-investigadores e juízes. O treinamento de integrantes do judiciário é elencado como importante para os entrevistados, visando a compreender as representações e os procedimentos.

[85] Nãos se objetivou fazer um levantamento junto aos Tribunais de Justiça a existência ou não de varas especializadas em processar e julgar os crimes cibernéticos, partindo-se a afirmação a partir das observações dos entrevistados.

Os ministérios públicos, como acenado, cujos membros estão mais envolvidos na persecução da autoria e materialidade delitiva, são referidos como instituições com interesse e de atenção ao tema, mencionados por pelo menos cinco entrevistados, e, pontualmente, criando órgãos especializados em investigação cibernética no âmbito de sua organização[86].

Indaga-se, portanto, se a Lei nº 12.737/2012 é uma lei que foi direcionada unicamente aos Estados e ao Distrito Federal, ou seja, somente às polícias civis, ou também deve ser de atenção do judiciário e órgão ministerial? Os entrevistados respondem ao questionamento, pois, dentre as suas respostas a como dar maior efetividade à referida Lei, citam a necessária especialização na área e incluem Ministério Público[87] e Poder Judiciário, com criação de varas especializadas e treinamento dos juízes e servidores. A efetividade da legislação em tela passa, assim, sob as observações dos entrevistados, por soluções que não são somente funções político-administrativas dos governantes e gestores no âmbito do Estado e DF, mas também ficam sob o crivo e a responsabilidade dos membros e gestores do MP e do judiciário.

Acrescentam eles, especialmente o que reputam importante em âmbito nacional para um efetivo enfrentamento à criminalidade no âmbito da Internet, a partir de 'vontade política': (a) aperfeiçoamento e treinamento dos policiais, ou seja, disseminação do conhecimento; (b) reestruturação/criação de órgãos de investigação e assessoramento às investigações (os Ciber-Labs) no âmbito dos Estados e do DF; (c) estruturação de um setor em âmbito nacional, a cargo do Ministério da Justiça e Segurança Pública, desburocratizado, disponível para auxílios em qualquer momento e que promova interação entre órgãos; (d) estrutura mínima condizente com a demanda dos casos, ampliando o número de servidores policiais para atuar na área; e (e) conscientizar atores de investigação criminal cibernética sobre a cultura investigativa, ampliando os autoconhecimentos na investigação.

Aliás, sobre este último item, conscientização, aliado ao treinamento, há que tecer análises sobre as observações referidas pelos entrevistados, especialmente sobre suas expectativas e frustrações.

---

[86] Em uma consulta realizada no buscador Google, em 16 jan. 2023, com as palavras "Cyber Gaeco" e restrito ao âmbito dos domínios "mp.br", verificou-se que apenas três estados referem a existência do setor: São Paulo, Rio Grande do Sul e Santa Catarina.

[87] Não houve essa pergunta explicitamente, mas a necessidade de especialização do MP foi mencionada espontaneamente pelos entrevistados.

3.3.4 Qualificação e treinamento dos atores de investigação criminal cibernética: realidades expectantes

A investigação criminal tende a ser mais ou menos efetiva em razão da qualificação dos agentes e das autoridades policiais envolvidas sobre procedimentos e técnicas adequadas à situação. A função de 'ator de investigação criminal' não dá ao executor, mesmo tendo um curso de formação logo no ingresso na profissão, uma carta plena de conhecimentos sobre as investigações relacionadas a todos os delitos.

Por outro lado, a fragmentação do processo investigativo, com as especialidades voltadas, por exemplo, à investigação dos crimes de tráfico de drogas e sua relação com os homicídios (REMUS; WENDT, 2022, p. 126-141), ou dos crimes sexuais praticados contra crianças e adolescentes (COSTA; WENDT, 2022, p. 142-157), direciona os treinamentos indicados para cada situação. O mesmo raciocínio deve ser aplicado à investigação dos crimes praticados pela rede mundial de computadores ou, simplesmente, *rede de computadores*, como referido, por exemplo, pelos artigos 122, § 4º, e 154-A, ambos do Código Penal[88].

A qualificação é uma expectativa dentre os entrevistados[89], especialmente que ocorra desde o ingresso na instituição policial (02SE, 03BA, 10SC, 11AM) e que continue no decorrer da vida funcional do ator de investigação criminal cibernética (15TO, 17MT). Aliás, as expectativas relacionadas à qualificação perpassam por vários momentos da entrevista, ou seja, estão além deste bloco específico de questões, sendo a própria expectativa por formação continuada já mencionada anteriormente no subtópico sobre a estrutura do órgão e qualificação dos profissionais lá lotados. A frustração se dá, então, pela não existência de uma formação continuada, embora ela possa ter existido na formação básica do policial (05AC), mas mesmo a existente é considerada 'fraca': "se vira nos trinta, faz o que pode, busca por si" (04RS). Ou seja, "os profissionais acabam buscando a qualificação, não há nada

[88] Sobre conceitos e sua repercussão sobre os tipos penais, vide Costa, Wendt e Campelo (2022).

[89] Questões repassadas aos entrevistados neste *quarto momento*: "Quanto ao treinamento para investigação de crimes cibernéticos:
O que você diz sobre a qualificação profissional dos servidores policiais lotados no órgão onde está lotado:
- Os servidores policiais do órgão receberam treinamento da academia de polícia correspondente nos últimos três anos?
- Os servidores policiais do órgão receberam treinamento de órgão/instituição federal nos últimos três anos?
- Os servidores policiais do órgão realizaram treinamento mediante custeio próprio nos últimos três anos?"

institucional" (05AC), a qualificação é feita de forma pessoal, "nós é que vamos atrás dos cursos" (06AP).

Mesmo nos casos em que a qualificação é considerada boa, "na medida do possível" (07PB), é referida a necessidade de "planejar para evitar que a delegacia fique vazia" no período do treinamento, ou seja, que fique sem andamento nos trabalhos investigativos e no atendimento de ocorrências. O tema é considerado como de não prioridade 'do Estado' (09MA) e sobre essa estrutura estatal que é lançada a expectativa: "precisamos do empenho da administração para nos capacitar" (11AM); a perspectiva é da existência de treinamentos de níveis mais elevados, de maior complexidade (12PI).

Observam os entrevistados que, pela sua experiência profissional na investigação especializada cibernética, acabam ministrando treinamentos aos demais policiais (10SC, 12PI, 13AL, 16ES), mas que, além de ensinarem nas demais delegacias, "precisam aprender e se atualizar" (14PR).

Como "faltam treinamentos específicos de atuação na área de cibercrime e de especialização" (24PA) e têm "dificuldade de encontrar instrutores capacitados para esses treinamentos, precisamos buscar pessoas de fora" (20RR), ou seja, a busca por experiências já construídas, consolidadas, é uma constante, aproveitando-se ofertas de cursos de outros Estados. O curso básico ofertado pela Polícia Civil de Minas Gerais é referido pelos entrevistados como um dos treinamentos aproveitados pelo Estado (05AC, 08PE, 14PR, 24PA). Também os cursos e treinamentos ofertados pelo Ministério da Justiça e Segurança Pública foram mencionados pela maioria dos entrevistados, mas nada se equipara à busca pessoal pelo conhecimento, por meio de recursos próprios.

As observações qualitativas dos entrevistados foram aliadas, de acordo com as perguntas realizadas, às situações objetivas de existência ou não existência de cursos disponibilizados no âmbito estadual, especialmente pela respectiva academia de polícia, ou por órgãos federais, acrescidos da busca por qualificação por meio de recursos próprios. Procurou-se limitar o tempo de análise na resposta a três anos, obtendo-se as seguintes respostas:

Quadro 5: Treinamentos e qualificações recebidos pelos atores de investigação criminal cibernética

Pergunta	Sim	Não
Os servidores policiais do órgão receberam treinamento da academia de polícia correspondente nos últimos três anos?	13	11
Os servidores policiais do órgão receberam treinamento de órgão/instituição federal nos últimos três anos?	17	7
Os servidores policiais do órgão realizaram treinamento mediante custeio próprio nos últimos três anos?	21	3

Fonte: Produzido pelo autor (2023).

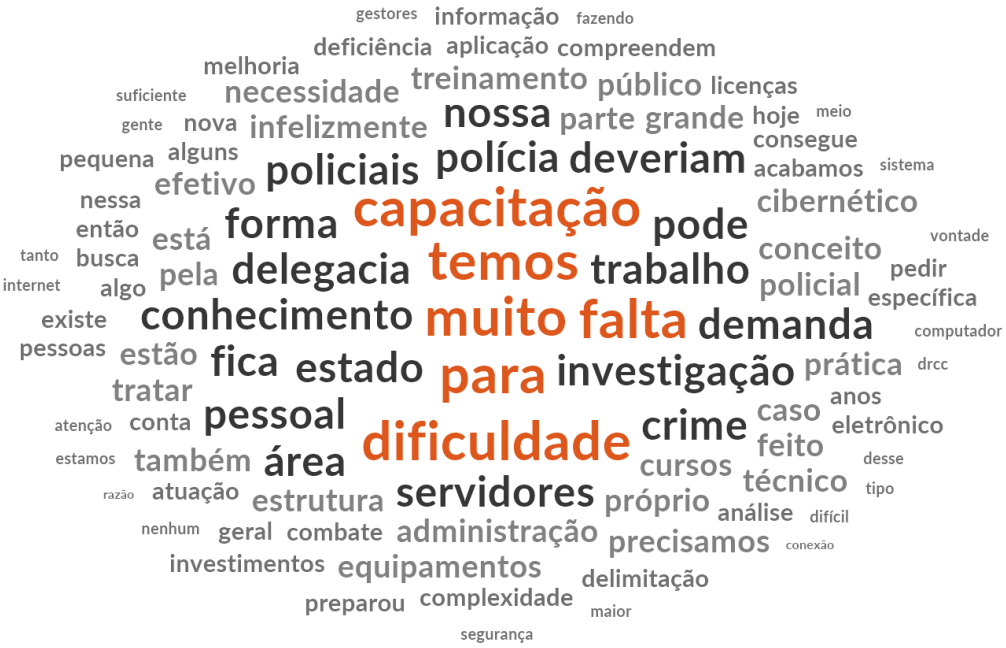
Constata-se, portanto, uma dependência de capacitação em relação aos órgãos federais e da 'busca pessoal' de cada um dos atores de investigação criminal cibernética, remanescendo aos órgãos estaduais um papel secundário, ou melhor, terciário, na qualificação especializada, dependente de decisão político-administrativa para que ocorra. A observação do entrevistado de que "esse curso demorou para acontecer" (09MA) é um misto de frustração e expectativa, sempre em relação à estrutura da unidade federativa, ou seja, da decisão do sistema político.

***

Verificou-se haver, portanto, uma co-reflexividade de expectativas em relação às estruturas federais e estaduais, responsáveis por definir as políticas administrativas capazes de enfrentar efetivamente a criminalidade praticada no contexto da rede mundial de computadores.

Essas expectativas, em regra frustradas em razão da inexistência de uma política contínua de formação e preparo dos atores de investigação criminal cibernética, acabam por refletir no contexto do entorno da sociedade, cujos sistemas psíquicos que estão em seu entorno, veem-se desamparados em razão da ineficiência [declarada pelos entrevistados] do sistema policial para atender a todas as demandas. Esse desamparo do atendimento aos problemas de criminalidade cibernética enfrentados pelas pessoas, portanto, são uma frustração relatada pelos policiais a partir de suas óticas de observação e em face das interações que realizam com elas.

Figura 9: Expectativas e frustrações quanto à capacitação e qualificação dos servidores policiais



Fonte: Produzido pelo autor (2023).

Por outro lado, verifica-se que não apenas o sistema policial investigativo está carente dessas políticas administrativas, estruturais – em termos de recursos materiais e humanos –, procedimentais – em termos de atuação uniforme e padronizada –, educacionais – em termos de capacitação básica, avançada ou contínua. Ministérios Públicos e Poder Judiciário, não atrelados sistemicamente à administração, estão mais atrasados nesse processo evolutivo de atenção à especialização no contexto cibernético, embora já possuam sistemas processuais que atendam às suas situações protocolares. A fragmentação/segmentação voltada à investigação e o processo, derivados da criminalidade cibernética, é um caminhar sem retorno.

3.4 Expectativas cognitivas e expectativas normativas sobre mecanismos (des)estruturados de mitigação de danos cibernéticos e persecução criminal cibernética

O *quinto e último momento* da entrevista buscou observar, a partir da experiência dos entrevistados e do seu autoconhecimento, como lidam com as formas de reduzir e/ou mitigar os danos havidos e relacionados com as condutas divergentes no contexto da rede mundial de computadores e que chegam ao conhecimento das delegacias/setores onde estão em atividade.

A perceber-se, de pronto, que os conhecimentos práticos na atividade policial não são, necessariamente, conectados aos conhecimentos práticos, especialmente quando da usabilidade de uma linguagem técnica. No caso, reduzir ou mitigar danos, por não ser uma atividade vinculada à investigação criminal, que objetiva a apuração da autoria e a comprovação da materialidade delitiva. Então, aspectos considerados complementares, como o resgate do produto do crime, a recomposição financeira em um caso de crime patrimonial ou, ainda, a retirada/remoção de um conteúdo ofensivo à vítima, não necessariamente passam pela atribuição do policial-investigador, pois, em regra, dependem das circunstâncias de cada caso ou situação.

Assim, buscou-se observar esse contexto diferenciado na atividade de investigação cibernética, especialmente voltando à análise de como os atores com essa função dentro da persecução criminal têm atuado em auxiliar as vítimas a reduzirem ou mitigarem os danos que tiveram/estão tendo (pessoais e patrimoniais).

3.4.1 Conhecer e desenvolver estruturas de mitigação e redução de danos: entre reais condições e condições expectantes

O primeiro questionamento realizado nesta fase foi se o entrevistado "já teve experiência com usos de mecanismos de mitigação/redução de danos na Internet". Mas o que seriam "mecanismos de mitigação/redução de danos na Internet"? Poderíamos defini-los como sendo processos realizados, preventiva e reativamente, que auxiliam em restringir, aplacar os danos, a ocorrer ou ocorridos, de uma conduta cibernética divergente, tanto pelo uso de procedimentos tecnológicos quanto pelo uso de procedimentos regrados ou autorregrados, neste caso, respectivamente, pela legislação (Lei ou Decreto) e pelas políticas de privacidade e de uso dos provedores de aplicação e/ou conexão da Internet.

Assim, podem ser mecanismos de mitigação e redução de danos as campanhas e palestras preventivas, ministradas pelos atores de investigação criminal cibernética, ações de orientação às vítimas de crimes, atuação direta com remoção, retirada e suspensão de conteúdo das mídias sociais e demais aplicações, seja por ordem judicial, seja por medida administrativa, prevista ou em norma jurídica ou na política de privacidade e termos de uso das correspondentes aplicações.

Nesse contexto técnico, as observações dos entrevistados sobre suas experiências com a utilização dos mecanismos citados foram as mais diversas, porém, em regra, o questionamento precisou ser explicado a eles em razão do aspecto conceitual utilizado 'ser

distante' do contexto prático. Assim, além de respostas de não experiência, também houve questionamentos por parte dos entrevistados: "Não vou saber responder. Pode me dar um exemplo?" (02SE); "não entendi a pergunta. Pode repetir?" (03BA); "não consegui compreender. O que seria isso?" (05AC); "o senhor pode ser mais específico?" (08PE); "o senhor pode explicar melhor?" (09MA); "não entendi a pergunta" (10SC); "pode citar um exemplo?" (13AL); "por exemplo?" (17MT); "pode deixar mais clara a questão?" (18RO).

No entanto, alguns comentários pós-questionamento já foram no sentido de compreendê-lo: "Ação educativa seria um desses mecanismos?" (12PI); "não. Temos algumas cartilhas" (19DF); "sim. Trabalho de retirada de sites, fraude de falso leilão, desenvolvimento educacional e uso do Instagram da Polícia para campanhas" (23SP); "sim, palestras preventivas em escolas" (24PA).

Assim, em todas as entrevistas buscou-se explicar os mecanismos de mitigação e redução de danos, dando-se exemplos de situações, instigando a memória do participante a recordar situações de sua utilização, o que redundou em reformulações de respostas e aprofundamento das situações possíveis pelos entrevistados.

A remoção ou recuperação de perfis (de redes e mídias sociais), utilizada na prática de crimes, foi um dos tópicos mais citados, inclusive como um "trabalho diário" (06AP). Também foram mencionados: (a) a 'derrubada' de sites usados para golpes, ou seja, sites de conteúdo fraudulento; (b) remoção de sites/postagens com conteúdo sexual (*sex extorsion*), especialmente de exploração sexual infantil; (c) participação em programas de TV com alertas; (d) palestras preventivas; (e) orientação das vítimas quanto às medidas junto aos bancos; (f) orientação das vítimas nos casos de divulgação de conteúdo íntimo; e (g) a necessidade de ordem judicial, inclusive em operações policiais.

As situações mencionadas pelos entrevistados também foram acrescidas de sentimentos de frustrações das expectativas em auxiliar, em razão da "recalcitrância das plataformas" (15TO), de dificuldades com as redes sociais (17MT), também para retirada de conteúdo e exclusão de contas (09MA), não havendo 'vontade' dos provedores em colaborar com a mitigação (10SC).

A experiência diária ajuda, então, a compreender o funcionamento dos mecanismos na prática, havendo necessidade de uma interação constante, após o fato informado pela vítima, com provedores de conexão e de aplicação, que precisam executar medidas quando os fatos já aconteceram ou estão acontecendo, como no caso dos hackeamentos de contas de redes sociais (Instagram, Facebook etc.). Porém, para essa interação entre atores, de investigação

com os das aplicações, há necessidade de conhecimento das regras normativas e das autorregras.

Assim, o segundo questionamento foi se o entrevistado conhecia "atos normativos que ajudem a mitigar/reduzir danos na Internet? Se sim, quais?". Entrevistados foram explícitos em afirmar não saberem quais regras aplicar (8 = 33,33%) às situações aptas a mitigar e reduzir danos provocados às vítimas pelos autores de crimes cibernéticos. Quanto aos demais, citaram (a) o Marco Civil da Internet, (b) a Lei Geral de Proteção de Dados, (c) a Lei Complementar nº 105; (d) o Estatuto da Criança e do Adolescente; (e) o Código de Processo Penal; (f) a Lei do Delegado de Polícia; (g) as regras e políticas de privacidade das plataformas; e (h) a legislação de outros países.

A falta de autoconhecimento padronizado dentre os atores é evidente, correlacionando-se com as expectativas e frustrações já referidas: há necessidade de procedimentos padronizados e de uma qualificação continuada. A efetividade de ferramentas, regulamentadas ou reguladas (autorregras), depende também do seu conhecimento e de formas de aplicação tecnológica.

Por outro lado, as normativas federais não referem quem vai realizar as primeiras medidas de mitigação e redução de danos, exceto nas (a) previsões de reserva judicial, ou seja, de ordem judicial, e na (b) disposição do art. 21 do Marco Civil da Internet, que atribui à vítima ou a seu representante legal a responsabilidade de requerer. Ou seja, não há um comando necessário para que os atores de investigação criminal atuem nessa finalidade, que vai além, como referido, da apuração da autoria e materialidade delitiva.

Por isso, o terceiro tópico da entrevista pretendia observar se o entrevistado entendia "que a investigação criminal é meio hábil para mitigar/reduzir danos na Internet? Se sim, quais as condições para fazê-lo?". A maioria absoluta dos entrevistados (22 = 91,67%) respondeu que "sim", a investigação criminal é um meio hábil que auxilia a mitigar e reduzir danos na Internet, porém, que precisam de condições para que isso se torne mais efetivo.

Dentre as condições referidas como necessárias para a citada atuação estão, em síntese: (a) simplificar e dar possibilidade à autoridade policial de determinar bloqueio/remoção de conteúdo, não necessitando de ordem judicial para a maioria das situações, fazendo a previsão no Marco Civil da Internet; (b) integração (parceria) com setor privado; (c) trabalhar com prevenção e educação digital; (d) melhor conhecimento sobre a linguagem ('palavreado') da Internet (04RS); (e) vincular à questão da punição, responsabilização do autor dos crimes e/ou organizações criminosas envolvidas; (f) melhorar o canal de comunicação e o tempo de resposta às requisições pelos provedores de conexão, de aplicação

e operadoras de telefonia; (g) equipamentos e softwares melhores, assim como uma conexão de Internet mais rápida; (h) qualificação do pessoal; (i) investir em segurança cibernética, com criação de cartilha para a população, especialmente focada para escolas, e divulgação ampla às vítimas; (j) melhorar o canal de comunicação com o Poder Judiciário; (k) trabalho emergencial junto aos bancos; (l) tornar a legislação mais clara; (m) ter um protocolo rígido de atuação, de como e quando fazer o procedimento, ou seja, mecanismos claros de atuação policial, com capacitação de pessoal.

Pelas observações dos entrevistados, para que possam auxiliar adequadamente as vítimas de crimes cibernéticos a reduzir/mitigar danos, as condições expectantes vão além da sua função, sendo dependentes ou de uma decisão judicial ou de uma decisão, seja dos provedores de aplicação e/ou de conexão, seja das operadoras de telefonia, seja também do setor financeiro, não havendo sequer um protocolo de atuação, ou seja, processos instituídos e que tenham tal finalidade, embora existam focos de atuação preventiva, proativa, em relação às situações constatadas e divulgadas, seja na mídia ou em palestras, evitando-se novas vítimas.

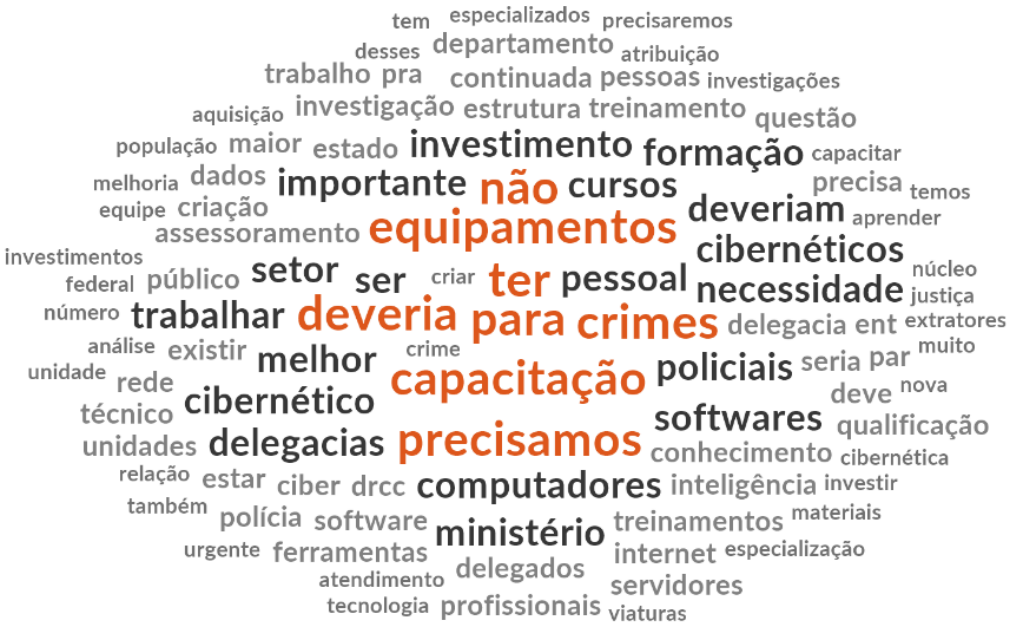
A reflexividade das expectativas aqui é recorrente, pois se dá sobre estruturas já formadas, sejam elas normativas (a exemplo da necessidade de ordem judicial para remoção de conteúdo), sejam elas organizacionais (a exemplo da organização e burocracia do Poder Judiciário e das autorregras procedimentais das plataformas).

Frustram-se as expectativas e elas continuam mantidas, e, no caso da reorganização interna nas polícias quanto aos procedimentos cabíveis, preserva-se a possibilidade de aprendizado e construção de estrutura, procedimental e material, para atuação mais efetiva em auxílio às vítimas.

3.4.2 Perspectivas ideais da persecução da criminalidade cibernética: observações integrativas

Cada questionamento da entrevista, e a sequência preconizada, foi idealizado numa linha estratégica de provocação e reflexão sobre as condições normativas, materiais e procedimentais de execução da investigação criminal cibernética no Brasil, procurando-se observar sistemática e integrativamente os contextos no entorno do ator dessa investigação criminal especializada: o policial civil, agente ou delegado, designado para esta função. A nuvem de palavras, formadas a partir da parte final da entrevista, dá a dimensão da complexidade que o tema envolve:

Figura 10: Perspectivas de atuação na persecução criminal elencadas pelos atores de investigação cibernética



Fonte: Produzido pelo autor (2023).

Todos os questionamentos e respostas levaram, portanto, a uma reflexão final, condicionada pela pergunta: “Finalmente, qual o caminho ideal para melhorar a persecução da criminalidade no âmbito da Internet?”

Para melhor compreensão, as respostas foram categorizadas em (a) expectativas cognitivas, ou seja, não necessariamente vinculadas às estruturas administrativas e/ou normativas; (b) expectativas normativas, relacionadas às estruturas já formadas administrativa ou normativamente; e, também, (c) expectativas cognitivas sobre expectativas normativas, porquanto há expectativas de mudanças das estruturas.

3.4.2.1 Expectativas cognitivas relativas à investigação criminal cibernética

As expectativas cognitivas envolvidas e citadas pelos atores de investigação cibernética demarcaram sua perspectiva sobre a efetividade no atendimento da sua função. Destaca-se que a busca por conhecimento [expectativa] se correlaciona, no oposto, à inexistência de perspectiva de encontrar um caminho ideal para a investigação criminal cibernética [frustração].

Cognitivamente, então, esperam os entrevistados que, com base em conhecimento autoadquirido, possam dar uma efetividade maior ao atendimento e ao repasse de orientações e informações à população, prospectando uma responsabilidade maior de todos os envolvidos.

Contingencialmente, espera-se, então, mais e além do que a estrutura pode ofertar, porém, com base na absorção de conhecimentos pela qualificação igualitária dos policiais e aplicação prática da construção teórica recebida, também com uma redução da "distância entre as polícias" (03BA).

Também expectam como caminho ideal na melhoria dos trabalhos a dedicação à educação digital/cibernética, à prevenção e à divulgação, nos meios de comunicação em massa, dos trabalhos e de eventuais condenações de autores de crimes cibernéticos. Isso se substancia na construção de políticas macro de atuação e na participação de policiais nos debates, aptos a auxiliar na estruturação ideal para resolução do problema da insegurança cibernética.

Em resumo, expectam que o problema seja reconhecido e que seja resolvido, embora possam não ter as mesmas indicações de solução, mas que possam ser debatidas e colocadas à seleção, que possam ser selecionadas ou não como formas de solução, auxiliares na efetividade da persecução da criminalidade cibernética.

Porém, não é só isso, pois que às expectativas cognitivas também se agregam as expectativas normativas, especialmente no preenchimento das lacunas legislativas.

3.4.2.2 Expectativas normativas vinculadas ao tema da persecução da criminalidade cibernética

As expectativas normativas citadas, por sua vez, indicaram as perspectivas relacionadas aos demais atores envolvidos, tanto na estrutura de persecução criminal quanto nas normas relativas à produção de provas e evidências.

Em relação à estrutura organizacional existente, destacam a expectativa normativa relacionada à melhora das questões processuais e procedimentais, com acesso mais rápido às informações aptas a auxiliar na resolução dos casos. Mais, que as sanções e o sistema de ressocialização sejam revistos e que haja leis mais rígidas para 'combater' os crimes cibernéticos. Então, a reflexividade das expectativas se torna evidente e guindada à

ampliação legislativa, procedimental e material, o que, expectam cognitivamente e simbolicamente, daria maior efetividade à investigação criminal cibernética.

Como já delineado, a frustração nesse contexto normativo é que, em face da forma como estão as redações das normas processual penal e vinculadas à obtenção de dados telemáticos, não há um padrão de atuação em termos de tempo e de procedimento, especialmente nos casos dos provedores de conexão, provedores de aplicação, operadoras de telefonia e setor financeiro (bancário).

3.4.2.3 Expectativas cognitivas sobre as expectativas normativas relativas à estrutura da persecução da criminalidade cibernética

Complexificando as várias expectativas, foram notadas, em relação às observações elencadas pelos entrevistados, expectativas cognitivas sobre expectativas normativas já consolidadas, já estruturadas, seja administrativamente, seja normativamente. Assim, consolidam-se as observações em cada um dos tipos de expectativas:

- Expectativas sobre expectativas normativas sobre regras jurídicas existentes:

1 – Fornecimento de informações (dados cadastrais e de acesso) às autoridades policiais: a necessidade de vênia judicial para o repasse de informações sobre acessos (*logs* de conexão e de acesso), no entender dos atores de investigação criminal cibernética, retarda a resolução dos casos e a efetividade da função administrativa de produção de provas e da autoria (01GO; 17MT)[90];

2 – Comunicação mais ágil com outras organizações do sistema de persecução criminal, especialmente o Poder Judiciário: a frustração é não existir uma especialização no órgão judicial nem um procedimento específico e célere previsto em relação à temática dos crimes cibernéticos (09MA);

3 – Aprimoramento da legislação, com participação da sociedade e dos atores estatais (22MG; 24PA), visando a: (a) revisão de forma geral e não necessariamente da parte penal (14PR); (b) inserção de controle no sistema de telefonia celular (09MA, 14PR); (c) controle por uso e cadastro de *wi-fis* públicas (14PR); (d) institucionalização normativa de prazo maior

[90] Em fevereiro de 2023 o STF emitiu decisão em relação aos dados cadastrais, definindo que a requisição de dados de provedores de internet com sede fora do Brasil pode ser feita tanto pela via diplomática, à autoridade do país sede da empresa, ou seja, seguindo o protocolo de cooperação internacional, quanto diretamente a seus representantes no Brasil ou no exterior (RODAS, 2023).

de resguardo de dados pelos provedores de conexão e de aplicação (14PR); e (e) prazo para fornecimento desses dados e mecanismos mais claros de atuação policial (23SP).

- Expectativas sobre expectativas normativas relativas à estrutura administrativa (policial estadual) e procedimental:

1 – Criação de boas práticas e de metodologia de atuação unificada: a expectativa é sobre a reorganização administrativa, que precisaria ser melhorada e direcionada a padrões de atuação no âmbito dos Estados e da União, ou seja, por outro lado, a frustração é pela inexistência dessa metodologia (02SE; 03BA; 17MT);

2 – Aperfeiçoamento dos gestores e investimento na Polícia Civil: a frustração está, atualmente, relacionada à falta de conscientização do gestor público em priorizar e aprimorar a estrutura de investigação dos crimes cibernéticos. Portanto, expectam os entrevistados que os gestores político-administrativos sejam formados e condicionados a percepcionar essa transformação advinda do uso da Internet e o impacto dos crimes cibernéticos sobre a população, promovendo ou readequando políticas públicas voltadas ao tema, especialmente à delegacia especializada (04RS; 05AC; 07PB; 08PE; 15TO);

3 – Investimento em recursos humanos e na formação do policial: a ampliação de servidores, a qualificação permanente, incluindo as ferramentas necessárias à investigação criminal cibernética, com acréscimo do número de servidores treinados, é expectada para ampliar a efetividade da estrutura já formada (03BA; 06AP; 07PB; 11AM; 15TO; 16ES; 20RR; 21RN; 24PA);

4 – Investimento em recursos materiais e melhoria da estrutura dos órgãos especializados: expectam os entrevistados a ampliação e melhoria de equipamentos e softwares para ampliar a efetividade do trabalho policial (07PB; 08PE; 09MA; 15TO; 16ES);

5 – Restruturação ou ampliação administrativa: expectam os entrevistados que, para construção do caminho ideal na persecução da criminalidade cibernética, seria necessária a remodelação do órgão especializado, com a sua transformação administrativa para um departamento ou divisão, incluindo-se aí (a) delegacias com temas específicos, (b) um Ciber-Lab (Laboratório de Inteligência ou Operações Cibernéticas), e (c) setor de perícias forenses, ou seja, a transformação burocrática desses órgãos (07PB; 09MA; 16ES);

6 – Consolidação de parcerias público-privadas para fornecer melhores subsídios e qualificar a investigação criminal cibernética (10SC).

- Expectativas sobre expectativas normativas relacionadas ao sistema político-administrativo além da esfera policial estadual:

1 – Construção de um programa de educação digital e inserção efetiva na grade curricular das escolas (10SC), de acordo com o previsto no Marco Civil da Internet (arts. 26 e 27);

2 – Integração entre os Estados, com criação de um órgão central e uma política de investigação cibernética: expectativas são direcionadas à necessidade de uma estrutura central no Brasil que promova a integração e a colaboração entre os órgãos policiais e atores de investigação criminal cibernética (13AL; 20RR);

3 – Criação de um canal de interação 24/7 com instituições financeiras, para troca de dados sobre fraudes e atuação no congelamento de contas e bloqueio de valores, com possibilidade de mitigação dos danos à vítima (17MT);

4 – Capacitação de integrantes do Ministério Público e do Poder Judiciário, ou seja, de todos os atores envolvidos na investigação criminal cibernética e na recepção do resultado dela (18RO).

***

Percepciona-se assim, a partir das observações realizadas pelos entrevistados, que as expectativas e as expectativas sobre expectativas são relacionadas ao entorno do seu papel como investigador criminal cibernético. Não se observou para além dessa estrutura, pois o espectro de análise pautava-se sobre a visão desse ator e não atores de outros sistemas organizacionais, como integrantes do Ministério Público, do Poder Judiciário e da Polícia Federal, embora tenha se questionado sobre as relações entre atores desses sistemas [organizacionais].

Também, importante mencionar que esta tese não se pautou por analisar as observações sob a perspectiva da criminologia crítica ou da política criminal, o que também poderia ser feito em outro momento. Poder-se-á sugerir, por esses vieses, que o conservadorismo nas respostas dos entrevistados é condicionado à integração deles no sistema, pautado pela Lei, e, por isso, não conseguem pensar o problema criminal para além da Lei, já que todos ainda ficam amarrados na estrutura legalista do próprio Direito [penal e processual penal].

Numa análise crítica, observa-se que essas expectativas e frustrações são geradas como um próprio condicionamento do sistema de Justiça Criminal ou do sistema de persecução criminal adotado no Brasil, que engessa os seus atores a pensarem o próprio sistema no entorno da Lei e tão-somente a Lei. Não somente o sistema de persecução criminal, pautado por princípios constitucionais, mas as próprias estruturas organizacionais e funcionais são

formatadas normativamente, delineando os papéis dos atores e direcionando as suas condutas.

No entanto, mesmo esse engessamento normativo, sobre o qual as expectativas são mantidas normativamente, gera frustrações especialmente cognitivas, internas [da consciência], dos atores de investigação cibernética, que, embora consigam processar a informação sobre as expectativas e frustrações, não conseguem estabelecer o meio adequado de emissão para que essa comunicação chegue ao receptor adequado, ou seja, ao subsistema social que teria a função de recepcionar, compreender e/ou absorver ou não essa comunicação de acordo com sua operatividade interna. Por isso, confirma-se a primeira hipótese desta tese, de que as frustrações e os desapontamentos em relação às estruturas administrativas e normativas relacionadas aos crimes cibernéticos são mais latentes do que as expectativas, cognitivas e/ou normativas, e a comunicação destas [pelos atores de investigação cibernética] não chega até os demais sistemas sociais, especialmente o Político, sendo apenas ruído comunicacional, quando não apenas um reclame da própria consciência.

Esses subsistemas sociais, a Política (Legislativo e Executivo) e o Direito, não conseguem, portanto, recepcionar a comunicação não feita pelas consciências dos atores de investigação cibernética. Portanto, precisam eles estabelecer uma linguagem e um *médium* adequado para que essa comunicação seja não só um projeto ou um ruído de comunicação, mas que [ela] possa gerar acoplamento estrutural com os subsistemas referidos.

O condicionamento da atuação dos policiais responsáveis pela investigação cibernética ao contexto legal não é só sobre como, quando e por que atuar, mas também sobre suas expectativas relacionadas à efetividade do exercício da função. Porém, não podem desconhecer que a satisfação ou frustração não deve necessariamente estar na finalização da investigação com prisão e condenação, porquanto o procedimento policial, de acordo com o Código de Processo Penal, é peça informativa. Compreende-se, por outro lado, a frustração pela inefetividade e ausência de prisão/condenação, pois que a ela corresponde especialmente uma cobrança social realizada, em primeiro lugar, sobre os órgãos policiais de segurança pública.

Aliás, conforme observam Finco e Martini (2022), as normas existem e podem vir a ser rompidas, o que não significa serem desnecessárias: “ao contrário, precisamente se e quando não forem respeitadas – isto é, quando as expectativas normativas são “desiludidas” –, elas sinalizam uma ruptura na ordem social e, portanto, a necessidade de intervenção de sanções”. Embora, como traçado pelos entrevistados, as sanções não sejam necessariamente adequadas, ao que corresponde uma sequencial frustração ou desilusão.

Confirma-se, pelas observações sobre as observações dos entrevistados, outra hipótese, de que o quadro estrutural atual das Polícias Civis brasileiras não comporta unicidade, padronicidade ou uniformidade, sendo fundamental o estabelecimento de uma diretiva única e de protocolos uniformizados e padronizados no enfrentamento à criminalidade em rede de computadores, dispositivos de comunicação ou sistemas informatizados [criminalidade cibernética], sem os quais torna-se difícil aprimorar a investigação criminal cibernética, já que a organização administrativa é local nas unidades federativas e as decisões nesse âmbito não são uniformizadas, gerando também frustrações e desapontamentos quanto à efetividade da resposta procedimental.

Por outro lado, aventou-se a hipótese de que os atores de investigação policial cibernética não possuem consenso quanto às necessidades de normatividade de medidas procedimentais e mecanismos efetivos na redução/mitigação dos danos cibernéticos. Aqui cabem observações que podem ser complementadas no próximo capítulo, mas que podem ser desde já delineadas.

No que diz respeito às necessidades de normatividade de medidas procedimentais, conforme análise anterior, os atores de investigação criminal encaminham suas observações para uma mesma direção, o que se poderia dizer que há um determinado consenso, não só quanto às expectativas, mas também quanto às frustrações. Porém, em relação aos mecanismos efetivos na redução/mitigação dos danos cibernéticos, ainda resta um caminhar de autoconhecimento e consenso, especialmente quando à sua efetiva prática no âmbito da investigação criminal cibernética. Esse tema será retomado no próximo capítulo.

Por tudo isso, compreender quais são [e como repercutem comunicativamente] as expectativas cognitivas e as expectativas normativas desses atores atuantes na investigação criminal cibernética, foco principal desta tese, ajuda a compreender como estão se moldando em termos de comunicação/atuação no entorno do cibersistema da Internet. Também, como estão coevoluindo, especialmente a partir dos sistemas sociais do Brasil, não se deixando de observar o sistema da sociedade mundial, porquanto a rede de computadores, com linguagem única, está inserida internacionalmente. As repercussões convergentes ou divergentes podem se irradiar para além das fronteiras físicas dos países e dos aspectos da soberania nacional envolvidos.

Observar e analisar, portanto, como se deu a construção da realidade socionormativa cibernética no Brasil ajuda a compreender por que as expectativas dos atores de investigação criminal cibernética são mais condicionadas ao sistema de persecução criminal brasileiro, ou seja, à Lei, que ao entorno da Lei. É o tema do próximo capítulo, pautado numa análise dessa

construção social da realidade normativa brasileira, em linha linear do tempo, especialmente sobre as normas penais e processuais penais que tratam da Internet e dos crimes cibernéticos.

4 A INTERNET E A CONSTRUÇÃO DA REALIDADE NORMATIVA NO BRASIL

"Não existe uma lei específica sobre os crimes cibernéticos ou pedofilia na internet, mas há legislação pertinente". (FLÁVIO, 2019). A fala jornalística de uma agência de governo no Distrito Federal é de um ambiente com ausência de regras e de necessidade de impô-las como forma de controle e, mais, como forma de segurança. Esse processo informativo-observacional de um veículo de comunicação tem o viés de acabar por construir uma realidade social que é absorvida por outros sistemas da sociedade, ou seja, pessoas e os sistemas sociais, especialmente o sistema político, que recebe tal comunicação, analisa de acordo com cada função específica e reproduz a realidade, no caso do Legislativo, por meio de normas.

Por isso, é importante pensar a Internet sob o ponto de vista sistêmico, tendo ela no seu entorno, na sua ambiência, outro sistema, o psíquico, ou seja, eu, eles, nós, vocês, os outros, os seres humanos, que operam pela consciência. Também, é preciso considerá-la na ambiência de um sistema maior, a Sociedade. Esta, por sua vez, tem inúmeras ambiências sistêmicas no seu entorno, incluindo a Internet, que é, atualmente, a principal forma de armazenamento de dados e informações, capazes de comunicar e realizar acoplamentos estruturais com os diversos sistemas e subsistemas, como o Político, a Moral, o Direito, a Religião, dentre tantos.

A ideia de transversalidade, interacionalidade (e internacionalidade) e interatividade instantânea, característica principal da "Teia de Alcance Mundial" (CASTELLS, 1999, p. 379), é semelhante a um objeto perfurante, um objeto que tem o condão de impactar, de introjetar, e, no caso da Internet, romper e ampliar o horizonte da disponibilidade do dado e da informação. A partir dos estudos da cibernética, condensados por Losano (2019) e já referidos no primeiro capítulo, percebem-se a evolução e a adaptação de sistemas cibernéticos, especialmente a Internet, capazes de ampliar o horizonte da comunicação e provocar uma transformação cultural, social, política e econômica, na qual os algoritmos condicionam tarefas, gostos, aquisições etc.

Esse conjunto evolutivo a partir da rede de computadores, associado às questões de Estado, soberania, política, segurança etc., em tempos de globalização, compartilhamentos e *likes*, tem gerado incertezas e demandado soluções nos mais diversos âmbitos, governamental, cultural, econômico, político etc. Essa comunicação, advinda de dados e informações constantes na Internet, gera expectativas, cognitivas e normativas, respectivamente sem e com aceitação de frustrações, especialmente pelo fato de que a rede

mundial de computadores foi criada com a lógica da liberdade da rede e assim deveria permanecer. Porém, não se pode mais discutir 'se vai ou não' ser regulada pelo Direito, mas sim 'como' será regulada (SVANTESSON, 2020).

A 'insegurança' gerada/sentida a partir da (utilização da) Internet tem 'guindado', por que não dizer, direcionado governos, organizações e pessoas a procurar soluções no sistema do Direito como se fosse o principal ponto de apoio e de resolução da insegurança contemporânea, motivada pela expansão e utilização da rede mundial de computadores. São as 'irritações', a partir das comunicações, provocadas por um sistema em outro sistema, demandando sua atenção em face da codificação/função e, em alguns casos, demandando mudanças internas[91]. Para tanto, é necessário o conhecimento sobre o ambiente, o entorno e suas transformações culturais e as expectativas envolvidas, e, por isso, a necessidade de observações pautadas na cibersociologia[92].

As questões de 'segurança' relativas à Internet precisam ser ponderadas sob o ponto de vista da análise do 'risco', embora possa ele não ser mensurado corretamente, em sua plenitude. Sendo o risco também construído socialmente, a partir das observações dos observadores, e mesmo que haja uma possibilidade de análise e calculabilidade inicial, a percepção social e as peculiaridades das percepções individuais acabam por refletir nos efeitos do risco analisado: o olhar do observador constrói a realidade social e, no caso, também sobre o risco. Por outro lado, pode-se afirmar que, em relação à Internet, o risco é ao menos gerenciável.

Assim, de uma maneira genérica e resumida, três aspectos sobre o 'risco' à segurança na Internet parecem guindar todas as demais: (a) o que é colocado na Internet pelo usuário, por vontade própria, usando do direito de autoviolação ou autorrevelação da intimidade, o direito à extimidade, (b) o que é coletado a respeito do usuário, em razão do uso de dispositivos e aplicações na Internet e (c) o que é colocado na Internet por uma ação de terceiros, sejam eles pessoas físicas ou jurídicas. Nos três casos ou a atenção se volta à possível vítima ou foca em relação ao potencial causador do dano [autor da conduta

---

[91] Os termos "irritação", "irritações", "autorreferenciais", "expectativas normativas" são próprios da teoria sistêmica, desenvolvida por Niklas Luhmann (1980; 1983; 1990; 2014).

[92] No dizer Soro (2006, p. 11), para compreendermos esse novo espaço, o ciberespaço, teria o pesquisador que se 'converter' em um cibersociólogo e, necessariamente, ser um cibernauta, pois precisa compreender como usar e como funciona a Internet: "Con la apertura del Ciberespacio como otro contexto donde observar procesos de interacción social se abre un campo de análisis para la Sociología. [...] Este cibersociólogo no puede ser otra cosa que un "cibernauta" avezado ya que no es posible estudiar la vida en el Ciberespacio sino es dentro del mismo".

divergente], ou, ainda, em ambos, vítima e autor. As expectativas, sociais/cognitivas e normativas, também são diferentes em relação a cada uma das situações elencadas.

Previamente, pode-se ponderar que a autorrevelação da intimidade poderia ser observada sob a ótica da ética da alteridade, mas em regra – e quanto aos sistemas sociais ocidentais e também orientais – tem sido analisada, conforme crítica de Herrera Flores (2009), sob a ética da liberdade, ou seja, "a minha liberdade termina onde começa a do outro". Tudo isso, porém, ainda sob um viés contemporâneo, no qual se propugna e se busca uma 'segurança' e se tem em mente que todos, indistintamente da cultura, da moral, da religião etc., têm de seguir um (determinado) modelo, convergentemente esperado.

Desde a Internet, principalmente, toda essa lógica, se já não antes, é contestada. Pode-se dizer que na Internet prevalece a alteridade, e as alterações culturais e sociais são sentidas e intensificadas quase que instantaneamente: "a minha liberdade começa onde [e quando] começa a do 'outro'"[93]. A esse novo olhar sobre os direitos (humanos) no acesso e uso da Internet a aplicação da teoria crítica de Herrera Flores (2009) é importante, porquanto as *posições* e *disposições* em que se encontram os usuários da rede são distintas e, ainda, poucos têm a consciência de todos seus direitos "achados na rede" (SANTARÉM, 2010), ou seja, desconhecem e não formam expectativas cognitivas e/ou expectativas normativas em relação às estruturas já existentes.

A rede da Internet propicia, portanto, processos colaborativos e não coordenados, instantâneos, involuntários e incontroláveis aos olhos, aos ouvidos e às ações dos integrantes do poder dominante, ou seja, dos demais sistemas sociais e psíquicos. Os *haters* das redes sociais, com suas condutas divergentes das esperadas [social e normativamente], são o principal exemplo dessa contemporaneidade complexa, na qual princípios, *v.g*, da proteção da vida privada e liberdade de expressão, de comunicação, de informação e de opinião têm de ser ponderados frente a situações concretas, do dia a dia das interações virtuais.

Qual a solução para esse contexto? Para parcela da sociedade, sejam os legisladores, sejam os agentes de controle social formal, o sistema do Direito parece ser a principal solução, tanto é que as comunicações oriundas do sistema social irritam o sistema político na busca de formatação de mais regras jurídicas. Para eles, o Direito é vislumbrado então como uma ferramenta de controle, de coerção, ao que Luhmann (1983) repudia, face a desconsiderar a verdadeira função do direito, de estabilizar expectativas normativas congruentemente generalizadas. Por outro lado, nem a 'governança' nem a 'regulamentação',

[93] Com base em Herrera Flores (2009).

mundial (global) ou tribalista (local)[94], pode ser capaz de resolver essas diferenças, que são próprias de cada ser humano, de cada sistema psíquico, motivo pelo qual a dimensão prática sobre os papéis [ator de investigação criminal, fiscal da lei, juiz etc.] e organizações [polícia, ministério público, judiciário etc.] deve se sobressair em relação às pessoas e aos valores envolvidos. Ademais: o contingenciamento jurídico pode não evitar que essas circunstâncias comportamentais divergentes continuem a ocorrer e as expectativas sociais, culturais, econômicas e normativas sejam frustradas.

No entanto, em relação ao outro ponto, a coleta de dados pessoais pelos provedores de conexão e de aplicação, trata-se de segmento que pode causar danos em largas proporções e precisa, realmente, de uma atenção maior dos países, que devem/tendem a tratar da regulação interna/regional da proteção de dados pessoais[95].

A despeito da citação inicial realizada já neste capítulo, o legislador brasileiro vem produzindo legislação na temática da Internet. Compreender como se deu/dá a construção da realidade do direito legislado/normatizado sobre a Internet no Brasil é fundamental para podermos responder aos questionamentos sobre a cibercriminalidade no Brasil ou, mais especificamente, se ela atende às expectativas cognitivas dos atores de investigação criminal cibernética no Brasil e se há necessidade de continuar a criminalizar ou aumentar penas ou, por outro lado, fortalecer políticas públicas de prevenção e investigação criminal. De onde deve partir esse olhar e essa construção social-normativa? Dos Estados? Dos atores da investigação criminal? De dentro e para dentro da arena cibernética? É nesse ponto que se concentra, então, este capítulo, partindo da análise do contexto legislativo e normativo, já consolidado e em discussão, que relaciona o direito penal e processual penal, incluindo políticas públicas, com a Internet e a tecnologia comunicacional advinda com ela.

A metodologia adotada neste capítulo é de, além de revisão bibliográfica sobre o cibercrime no Brasil, desde sua perspectiva tradicional e crítica, uma pesquisa empírica da linha do tempo sobre o direito legislado no Brasil, pois é necessário compreender como foi

---

[94] Por isso, pode-se dizer que 'governança', derivada de *multistakeholders* (múltiplos interessados), é o caminho, por assim dizer, 'saudável' para o exercício de controles sobre que é coletado pelos 'intermediários da Internet' e, também, sobre os serviços (de segurança e defesa) dos Estados, que têm pretensão de coleta massiva de dados, justificando sua ação com base em uma segurança e defesa nacional ou, ao menos, regional. Não se trata, pois, como dito, de regular ou não, mas de como regular. Porém, esses setores – e sequer os *backbones* – não podem ser atrelados a um único país [veja-se mais sobre *backbone*, sua explicação e sobre outros componentes da rede de Internet, por Torres (2015, p. 29 e ss.)] como ocorre atualmente (10 são baseados nos Estados Unidos!). As regras de regulação têm de partir de um acordo global, por exemplo, de um debate na Cúpula Mundial sobre a Sociedade da Informação (WSIS: http://www.itu.int/wsis/index.html) e/ou do IGF (*Internet Governance Forum*: http://www.intgovforum.org/cms/)

[95] Não é o objetivo desta tese focar na proteção de dados pessoais e sua regulação.

construída a *timeline* da discussão e da produção legislativa no Brasil no que diz respeito ao ciberespaço, ou seja, o sistema digital da rede [mundial] dos computadores: a Internet. Junto a essa abordagem historiográfica-normativa de discussão legislativa e normativa seguirá a abordagem sobre eventuais elementos de construção/formatação prática de expectativas normativas, com base em Niklas Luhmann, já existentes quanto a normas vigentes (*revenge porn*, *stalking*, proteção de dados públicos, automutilação, fraude eletrônica etc.), bem como as expectativas cognitivas sobre temas atuais e em discussão legislativa, como o *bullying* e as *fake news*.

O método, como referido introdutoriamente, é hipotético-dedutivo, partindo-se do geral para o particular, buscando contextualizar criticamente e propor uma leitura e avaliação não necessariamente dogmático-normativa, mas social-normativa, assim baseada no contexto cyber-social e linear da produção normativa brasileira e a comunicação que ocorre a partir de dados e informações produzidos, armazenados e transmitidos algoritmicamente. Finalmente, utiliza-se, em determinados tópicos, o confronto de óticas de criminalização e não criminalização como mecanismos de controle hegemônico e perpetuação do *status quo* vigente, ou seja, de uma atenção primordial à Lei.

4.1 Construção da realidade normativa sobre a Internet no Brasil: análise macro

Importa ponderar, inicialmente, que não se trata de fazer uma varredura e análise completa sobre os principais aspectos normativos e legislados sobre a Internet no Brasil, mas focar naqueles que têm relação com a presente análise sobre a construção sociocultural normativa, ou seja, com conexão com a investigação criminal cibernética e o direito penal, tanto material quanto substantiva.

Da mesma forma, não se pretende retroceder *ad eternum* no tempo, mas analisar o período pré/pós-Constituição Federal de 1988 e, principalmente, o período da era comercial da Internet.

De pronto, cabe referir que o Brasil somente em 2021[96] aprovou a adesão e, assim, ratificou formalmente a Convenção de Budapeste[97]. Porém, acabou legislando e sancionando normativas penais no decorrer do tempo, criminalizando condutas no âmbito da Internet. Em meio às opções criminalizantes, normativas com direitos civis e aspectos regulatórios foram solidificando a regulamentação da Internet no território brasileiro.

> O Comitê de Ministros do Conselho da Europa convidou o Brasil a aderir à Convenção sobre Crimes Cibernéticos, também conhecida como Convenção de Budapeste, celebrada em 2001. O processo foi iniciado em julho último [2019], quando o Governo brasileiro manifestou sua intenção de aderir ao instrumento internacional. **O ingresso nesse acordo de cooperação proporcionará às autoridades brasileiras acesso mais ágil a provas eletrônicas sob jurisdição estrangeira, além de mais efetiva cooperação jurídica internacional voltada à persecução penal dos crimes cibernéticos**.
> Trata-se de iniciativa decorrente de trabalho de coordenação interinstitucional, constituído para esse fim, entre o Ministério das Relações Exteriores, a Polícia Federal (PF) e o Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI) – ambos do Ministério da Justiça e Segurança Pública –, o Gabinete de Segurança Institucional da Presidência da República, a Agência Brasileira de Inteligência e o Ministério Público Federal.
> [...]
> O Brasil deverá tomar as providências legais internas necessárias à adesão à Convenção, podendo, contudo, desde já, participar, como observador, das reuniões sobre a Convenção e seus protocolos. Uma vez signatário, o Brasil se unirá a grupo internacional que inclui países como Argentina, Austrália, Canadá, Chile, Costa Rica, Estados Unidos, Japão, Paraguai, República Dominicana e membros da União Europeia, entre outros. (MINISTÉRIO DAS RELAÇÕES EXTERIORES, 2019, grifos nossos).

Em 2021, o Projeto de Decreto Legislativo (PDL) nº 255/2021 foi aprovado na Câmara dos Deputados, tendo por base o texto da Convenção sobre o Crime Cibernético, acordo que tem por objetivo facilitar a cooperação internacional no combate a delitos cometidos por cibercriminosos (JÚNIOR, 2021). A Mensagem nº 412/20, do Poder Executivo brasileiro, deu início a esse debate, conforme referido. O aceite dos termos da Convenção de Budapeste, consubstanciado pelo Decreto Legislativo nº 37, de 16/12/2021[98], demanda análise e ajustes na legislação brasileira, especialmente no que concerne à parte procedimental e de

---

[96] No Brasil, a discussão foi longa, tendo a Convenção sido relegada a um 'plano secundário' de prioridades. Mesmo assim, participou de discussões sobre o tema. Os representantes da Justiça da Comunidade dos Países de Língua Portuguesa (CPLP) terminaram, em novembro de 2019, as jornadas de trabalho com recomendações alinhadas de combate ao cibercrime nos Estados membros. Segundo o site Expresso das Ilhas (2019), "O seminário internacional, subordinado ao tema 'Cibercrime e prova electrónica: Harmonização de legislação e a Convenção de Budapeste na Comunidade dos Países de Língua Portuguesa', tinha na agenda nove sessões de trabalhos, comportando três eixos considerados de 'grande interesse e relevância', visando preparar a todos para os desafios futuros em matéria de prevenção e combate ao cibercrime".

[97] Vide análise sobre os contextos peruano e mexicano e a adesão à Convenção de Budapeste em Covarrubias (2020).

[98] O DL nº 37/2021 foi publicado no DOU em 21/12/2021.

cooperação internacional, aliás, o que é referido como expectativa por parte de entrevistados[99]. Ademais, também deverá ser necessária a análise do protocolo adicional, já validado âmbito da comunidade europeia (COUNCIL, 2021).

Em relação à produção legislativa atinente à Internet, em pesquisa anterior divulgou-se o quanto a sociedade brasileira põe sua expectativa no Direito para resolver problemas da tecnologia. (WENDT, 2017b, p. 85-128). Risco e medo podem influenciar nesse sentido, porém não são completamente determinantes. A cultura brasileira, por sua vez, é de regulamentação, mesmo desconhecendo as normativas existentes:

> 92,2% dos participantes da pesquisa entendem que deve haver algum tipo de regulação da Internet, seja através de atualização das regras existentes, seja sobre direitos e deveres dos usuários, seja em relação a provedores de conexão e de aplicação, ou, ainda, de provedores e usuários da Internet:
> mesmo entre quem não considera arriscado usar a Internet (= 134), 82,8% entendem que há necessidade de algum tipo de regulação na Internet;
> mesmo entre os que não sentem medo em usar a Internet (= 436), 88,5% compreendem que deve haver algum tipo de regulação na Internet. (WENDT, 2017b, p. 126).

Não se pode negar o fator influenciador da mídia nesse processo, de construção de uma realidade social em que é necessária a presença 'forte' e de controle do Direito, pois "mesmo entre aqueles que não consideram arriscado usar a Internet, a tendência é pelo incremento dos tipos penais" (WENDT, 2017b, p. 126). A necessidade de 'controle' pelo Direito passa, por outro lado, pelo desconhecimento interdisciplinar da Internet, já que este não tem uma análise mais acentuada dos *mass media*, que pautam a divulgação de fatos que têm a atenção maior do público-leitor, os sistemas psíquicos com seus papéis em vários sistemas diferenciados, que acabam por receber essa comunicação de acordo com sua função/código.

No entanto, no processo evolutivo da regulação e regulamentação da Internet, a primeira foi necessária em termos de estruturação dos setores/entidades responsáveis pela sua organização, o que é objeto da análise a seguir.

4.1.1 Regulação e estruturação da gestão e governança da Internet

Tal qual referido, o movimento regulamentador é mais recente, tendo sido precedido de processos de governança e regulação. A comercialidade da Internet e sua governança global exigiram dos continentes e países a criação de órgãos de gestão e governança da *rede*,

---

[99] Vide tópico 3.2.4.

que passaria a se tornar o principal meio de comunicação global e necessitava, então, de regulação. Após 1980, entidades não governamentais assumiram a regulação do ciberespaço, estabelecendo padronizações e regras. Duas dessas entidades são a ICANN – *Internet Corporation for Assigned Names and Numbers* – e a IANA – *Internet Assigned Numbers Authority* –, sendo esta última responsável pela distribuição/organização de "números" na Internet, como os endereços dos protocolos de internet – IP – e portas de comunicação[100].

Assim, também por exigir uma organização local da Internet, em cada país foi atribuída a uma entidade a função de coordenação e integração dos serviços de Internet. A escolha dessa "entidade" não é padronizada mundialmente. No Brasil, a *rede* passou a ser mais usual após 1995, deixando de ser exclusividade das universidades e unidades militares, passando a ter acesso público e comercial. O domínio ccTLD[101] *.br* foi registrado somente em 1989 (NEVES, 2015, p. 59), enquanto outros domínios "conhecidos do mundo da tecnologia, como Xerox.com, HP.com, Siemens.com, Adobe.com e Apple.com" já haviam sido registrados entre 1985 e 1987" (CABRAL, 2018).

Seis anos após o registro do ccTLD *.br*, foi criado o Comitê Gestor da Internet no Brasil (CGI.br) pela Portaria Interministerial (MCT/MC) nº 147, de 31 de maio de 1995, alterada pelo Decreto Presidencial nº 4.829, de 3 de setembro de 2003.

O Comitê Gestor da Internet no Brasil passou, a partir do Decreto de 2003, a ter atribuições de estabelecer diretrizes (a) estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, (b) para a organização das relações entre o Governo e a sociedade, na execução do registro de Nomes de Domínio, na alocação de Endereço IP (*Internet Protocol*) e na administração pertinente ao Domínio de Primeiro Nível (*ccTLD – country code Top Level Domain*), "**.br**", no interesse do desenvolvimento da Internet no país. Também, de (c) propor programas de pesquisa e desenvolvimento relacionados à Internet, que permitam a manutenção do nível de qualidade técnica e a inovação no uso, bem como estimular a sua

---

[100] Fazem parte da governança da Internet os protocolos IP (*Internet Protocol*), os sistemas de nomes de domínio (TLD – *Top Level Domain* – e ccTLD – *country-coded TLD*: Domínios de Primeiro Nível (.com, .net, .org, .biz, .info, .museum, .aero, .cat etc.) e Domínios de Primeiro Nível geográficos (nacionais), estabelecidos e relacionados a países, com terminações relativas a uma entidade nacional, como, por exemplo, .br, .py, .uy, .pt, .mx, .fr, .de, .uk, .us etc.). A IANA é responsável pela coordenação global do DNS raiz (sistema de nomes de domínio), pelo endereçamento IP e por outros recursos de protocolo Internet. O banco de dados "Root Zone Database" (acessível através do link <http://www.iana.org/domains/root/db>) representa os detalhes da delegação de domínios de nível superior, incluindo gTLDs como ".com" e códigos de país TLDs como ".br".

[101] Conforme nota anterior, o ccTLD é *country code Top Level Domain*, ou seja, o domínio de topo na Internet geralmente usado ou reservado para um país ou um território: corresponde ao domínio de primeiro nível geográfico, sendo o *.br* o correspondente ao Brasil.

disseminação em todo o território nacional, buscando oportunidades constantes de agregação de valor aos bens e serviços a ela vinculados.

A (d) promoção de estudos e recomendação de procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de Internet, acompanhando a crescente e adequada utilização pela sociedade, e (e) a articulação das ações relativas à proposição de normas e procedimentos atinentes à regulamentação das atividades inerentes à Internet estão dentre suas funções de conexão entre sociedade e sistema organizacional do CGI.br. Administrativamente, cabe-lhe (f) ser representado nos fóruns técnicos nacionais e internacionais concernentes à Internet e (g) deve adotar os procedimentos administrativos e operacionais necessários para que a gestão da Internet no Brasil se dê segundo os padrões internacionais aceitos pelos órgãos de cúpula da Internet, podendo, para tanto, celebrar acordo, convênio, ajuste ou instrumento congênere. Finalmente, tem o privilégio de (h) deliberar sobre quaisquer questões a ele encaminhadas, relativamente aos serviços de Internet no país.

As funções cresceram oito anos após a edição da portaria interministerial criando o CGIbr, pois que tinha como atribuições principais o fomento do desenvolvimento de serviços Internet no Brasil e a recomendação de padrões e procedimentos técnicos e operacionais. Uma das funções a destacar do CGIbr é o acompanhamento dos incidentes da Internet, categorizados pelo CERT.br[102], que é um Centro de Resposta a Incidentes de Segurança em Computadores, de âmbito nacional e de "último recurso"[103], e que contempla dados estatísticos[104] sobre notificações voluntárias de incidentes ocorridos em redes, além de outros dados estatísticos.

Dentre as notificações possíveis e que são orientadas pelo CERT.br[105], estão aquelas em que há possibilidade de remoção de artefatos maliciosos [utilizados em subtração de identidades, em tentativas e ataques às aplicações web etc.], de páginas de *phishing scam* [pescaria virtual, com coleta de dados de pessoas e organizações, seja por infecção seja por preenchimento de formulários], dentre outras várias possibilidades de notificações [vazamento de dados, escaneamento de redes etc.]. Todas elas, em verdade, são formas não judiciais de redução e mitigação de danos cibernéticos, que são, conforme demonstrado na

---

[102] Vide https://cert.br/.
[103] Vide https://cert.br/csirts/.
[104] Vide https://cert.br/stats/.
[105] Vide https://cert.br/docs/whitepapers/notificacoes/.

pesquisa empírica descrita no capítulo anterior, de desconhecimento dos atores de investigação criminal (vide tópico 3.4).

Complementando as funções estruturantes do CGIbr, ressalta-se que durante estes mais de 25 anos vários atos normativos internos, de recomendações, orientações e padronizações, foram expedidos[106], assim como houve, paralelamente, uma constante produção legislativa e normativa nas áreas penal e processual penal.

4.2 Como se deu a construção da legislação penal e processual penal relacionada à Internet no Brasil?

Neste tópico objetiva-se demonstrar como ocorreu a construção socionormativa das legislações penais e processuais penais que mencionam direta e indiretamente a rede de computadores, a Internet, procurando regulamentar aspectos de direito material e subjetivo.

A primeira norma jurídica, ainda anterior à CF88, a tratar das questões informáticas foi a Lei de Software – Lei nº 7.646, de 18 de dezembro de 1987 –, tendo o Projeto de Lei nº 8.551 sido encaminhado no ano anterior (1986). A Lei nº 7.646/1987 viria a ser a primeira a criminalizar, através dos arts. 35 e 37, condutas de violação no contexto informático brasileiro[107]. Porém, a Lei de Software veio a ser revogada pela Lei nº 9.609, de 19 de fevereiro de 1998, prevendo sobre a proteção da propriedade intelectual de programa de computador sua comercialização no país, ou seja, com regras sobre a proteção/registro do software e a criminalização de condutas quanto a sua violação (art. 12)[108].

Posteriormente, em 1990, duas leis de destaque são aprovadas[109]: (a) Lei nº 8.069, de 13 de julho de 1990, o Estatuto da Criança e do Adolescente (ECA)[110]; e (b) Lei nº 8.078, de 11 de setembro de 1990, dispondo sobre a proteção do consumidor (CDC)[111]. Ambas normativas, embora contemporâneas – pelo ano de seu sancionamento –, não contemplaram 'o que seria e como tratar' a Internet, embora, (a) no caso do consumidor, são plenamente

---

[106] Vide https://cgi.br/portarias/ano/.

[107] "Art. 35. Violar direitos de autor de programas de computador:
Pena - Detenção, de 6 (seis) meses a 2 (dois) anos e multa.
Art. 37. Importar, expor, manter em depósito, para fins de comercialização, programas de computador de origem externa não cadastrados:
Pena - Detenção, de 1 (um) a 4 (quatro) anos e multa".

[108] A Lei nº 9.609/1998 foi baseada no PL nº 200/1995.

[109] Ambas são instituidoras de proteção, com direitos e garantias, em diferentes áreas: criança e adolescente e consumidor.

[110] O ECA é oriundo do PL nº 5.172/1990 e do PLS nº 193/1989.

[111] O CDC é oriundo do PL nº 3.683/1990 e do PLS nº 97/1989.

aplicáveis à proteção de dados penais os arts. 72 e 73[112] [pela previsão do 'banco de dados'], e, (b) no caso do ECA, era aplicável o então art. 241 [nos casos de publicação de cena de sexo explícito envolvendo criança e adolescente][113]. Porém, tais contextos foram alterados/acrescentados na sequência evolutiva[114] da legislação no Brasil.

No caso do ECA, especificamente em relação à Internet e possíveis efeitos, houve dois acréscimos:

1. Lei nº 11.829, de 25 de novembro de 2008[115], que teve por objetivo "aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet", alterando os arts. 240 e 241 e acrescentando outros cinco artigos[116];
2. Lei nº 13.441, de 8 de maio de 2017, que também alterou o ECA, para "prever a infiltração de agentes de polícia na Internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente", acrescentando uma nova Seção à Lei e cinco artigos, disciplinando a infiltração de agentes policiais na Internet visando ao enfrentamento dos delitos praticados em desfavor de crianças e adolescentes[117].

Essa evolução[118] relativamente ao ECA traz à *linha do tempo* construída do direito sobre a Internet no Brasil um dos poucos atos normativos prevendo procedimentos (de investigação) em relação aos delitos cometidos no ambiente da rede de Internet brasileira e/ou com efeitos no território brasileiro: a infiltração de agentes policiais na Internet[119].

---

[112] "Art. 72. Impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros:
Pena - Detenção de seis meses a um ano ou multa.
Art. 73. Deixar de corrigir imediatamente informação sobre consumidor constante de cadastro, banco de dados fichas ou registros que sabe ou deveria saber ser inexata:
Pena - Detenção de um a seis meses ou multa".

[113] O art. 241 teve duas modificações, em 2003 e 2008, porém tinha como redação original a seguinte: "Art. 241. Fotografar ou publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
Pena - reclusão de um a quatro anos".

[114] *Evolução* não no sentido de melhora, mas no sentido de mudanças decorrentes do tempo e da ação legislativa.

[115] Antes da Lei nº 11.829/2008, a Lei nº 10.764, de 2003, já havia alterado os tipos penais dos arts. 239, 240, 241, 242 e 243 do ECA.

[116] A Lei nº 11.829/2008 é oriunda do PL nº 3.773/2008 e do PLS nº 250/2008.

[117] A Lei nº 13.441/2017 é oriunda do PLS nº 100/2010 e do PL nº 1.404/2011.

[118] Aqui, sim, o sentido de *evolução* pode ser empregado no sentido de melhora legislativa e de compreensão e adaptação da realidade frente ao curso dos acontecimentos e usos da Internet em relação a crianças e adolescentes.

[119] Como será visto no subtópico 4.2.2.4, a Lei nº 13.964/2019 estendeu a infiltração de agentes policiais para os casos de investigações de organizações criminosas e lavagem de dinheiro.

Já a modificação anterior, acrescentando dispositivos penais no ECA, foi resultado da ampla discussão no âmbito CPI da Pedofilia, cujo relatório foi concluído em 2010. Apesar de tais modificações, conforme ressaltado na pesquisa empírica, a frustração dos atores de investigação cibernética recai sobre a pena, especialmente no caso de armazenamento de conteúdo contendo cena de sexo explícito envolvendo criança e adolescente, que é de um a quatro anos, conforme art. 241-B[120] (vide tópico 3.2: especificamente, os entrevistados 07PB e 10SC).

Já o Código de Defesa do Consumidor nada dispôs na sua concepção sobre a Internet e somente após treze anos passou a regular o assunto por meio do Decreto nº 7.962, de 15 de março de 2013, "para dispor sobre a contratação no comércio eletrônico", abrangendo os aspectos delineados, ou seja, (a) informações claras a respeito do produto, serviço e do fornecedor, (b) atendimento facilitado ao consumidor e (c) respeito ao direito de arrependimento.

A contextualização inicial deste tópico serve, então, para demonstrar como foi, exemplificativamente, o processo de adaptação das legislações ao contexto da 'novidade' comunicacional da Internet no Brasil. No entanto, cumpre fazer uma análise historiográfica das legislações que incrementaram a parte penal e processual penal quanto à informática, à tecnologia da informação e, especificamente, quanto à Internet no território brasileiro. *A posteriori*, também objetiva-se construir uma análise crítica quanto aos principais projetos legislativos em andamento, especialmente sobre *bullying* e *fake news*.

4.2.1 *Timeline* da estruturação da legislação penal quanto à Internet no Brasil

Um dos primeiros projetos de lei que visavam a criminalizar condutas no âmbito da tecnologia da informação no Brasil, com a preocupação quanto aos dados e às informações e sua violação, foi o PLS nº 152/1991, transformado no PL nº 4.102/1993. A pretensão da proposta procurou instituir crimes de violação de dados e sua comunicação, ou seja, perpetrados por computador. Tal PL encontra-se ainda em debate no Congresso brasileiro, tendo como última movimentação importante a apresentação de um substitutivo em 2003[121].

---

[120] "Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa".

[121] Consulta feita em 06 jan. 2023 revela que o PL ainda aguarda designação de relator na Comissão de Constituição e Justiça e de Cidadania (CCJC) da Câmara dos Deputados.

Visando a compreender a absorção do tema ‘Internet’, as comunicações geradas no seu entorno e sua ‘proteção penal’ pelo legislador, analisaremos a linha do tempo das normas de caráter penal e que levaram em conta a mudança cultural e social em razão da rede mundial de computadores e da comunicação propiciada por ela a partir de dados e informações, cuja realidade foi sendo construída, reproduzida e disseminada pelos meios de comunicação social, os *mass media*.

Essa análise da *timeline* não tem o objetivo de esgotar os temas, mas não pode deixar, de outra parte, de considerar alguns aspectos legislativos e normativos que demonstram a atuação do legislador brasileiro frente ao crescente uso da Internet no Brasil, considerando o dano e o autor do dano, ou seja, o crime e o criminoso, num contexto criminológico tradicional e vicioso, reproduzindo o sistema hegemônico vigente.

Para auxiliar a compreensão, dois quadros representando a estruturação normativo-penal dos principais aspectos considerados pelo legislador brasileiro, pontuando-se que o detalhamento ocorrerá nas análises específicas a serem produzidas (subtópicos).

Quadro 6: *Linha do tempo* da estruturação da legislação penal quanto à Internet no Brasil – parte 1

1987	**1997**	**1998**	**2000**	**2003**	**2008**	**2012**	**2013**
Lei nº 7.646	**Lei nº 9.504**	**Lei nº 9.609**	**Lei nº 9.983**	**Lei nº 10.695**	**Lei nº 11.829**	**Lei nº 12.737**	**Lei nº 12.891**
[Lei de Software] (revogada) Arts. 35 e 37	[Lei Eleitoral] Art. 72	[Lei de Programa de Computador] Art. 12	Servidor público e proteção de dados [CP] Arts. 313-A e B, 153, §1-A	[CP] Art. 184 [CPP] Art. 530 A até I	[ECA] Arts. 241-A a E	[CP] Art. 154-A – Art. 266	[Lei Eleitoral] Art. 57-H

Fonte: Produzido pelo autor (2023).

Quadro 7: *Linha do tempo* da estruturação da legislação penal quanto à Internet no Brasil – parte 2

2018		**2019**		**2021**			**2022**	**2023**
Lei nº 13.718	**Lei nº 13.772**	**Lei nº 13.834**	**Lei nº 13.968**	**Lei nº 14.132**	**Lei nº 14.155**	**Lei nº 14.197**	**Lei nº 14.478**	**Lei nº 14.532**
[CP] Arts. 215-A, 217, §5º, 218-C, 225, 226, II e IV, e, 234-A, III e IV	[CP] 216-B [Lei Maria da Penha] Art. 7º, II	[Lei Eleitoral] Art. 326-A	[CP] Art. 122, caput, e §§ 4º e 5º	[CP] Art. 147-A	[CP] Arts. 154-A, 155, §§4º-B e C, e 171, §§ 2º-A e B.	[CP] Art. 359-N	[CP] Art. 171-A	[Lei 7.716/ 1989] Art. 2º-A Art. 20, §2º, §2º-A, §2º-B, §3º Art. 20-A Art. 20-B Art. 20-C Art. 20-D [CP] Art. 140, §3º

Fonte: Produzido pelo autor (2023).

A linha do tempo, portanto, dessa evolução, estende-se por 35 anos, sobre a qual seguem as análises, de acordo com os quadros expostos.

4.2.1.1 Estruturação normativo-penal da proteção de software e direitos autorais

Como destacado anteriormente, a Lei do Software foi a primeira envolvendo a área tecnológica e voltada à proteção da propriedade dos programas de computador, tendo sido modificada em 1998 pela Lei nº 9.609. Esta Lei veio a criminalizar a violação dos direitos do autor de programa de computador no seu art. 12[122], considerando mais grave a

[122] "Art. 12. Violar direitos de autor de programa de computador:
Pena - Detenção de seis meses a dois anos ou multa.
§ 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente:
Pena - Reclusão de um a quatro anos e multa.
§ 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.

"reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente". Por outro lado, não só a reprodução de programa de computador sem autorização e com violação de direito autoral foi criminalizada, mas a venda, a exposição à venda, a introdução no País, a aquisição, a ocultação ou o depósito, desde que 'para fins de comércio'.

Nessa mesma esteira e paralelamente no tempo, discutiu-se a proteção de direitos autorais de outras produções intelectuais, surgindo a Lei nº 10.695/2003, derivada de uma proposta do governo em 1996 com o PL nº 2.681[123], visando a tipificar e criminalizar a pirataria, inclusive a sua exploração pelos meios de comunicação digital, instituindo, também, o procedimento quanto à apreensão e destruição dos 'bens intelectuais'.

A referida Lei nº 10.695/2003, que alterou o art. 184 do Código Penal[124], criminalizou não só a violação dos direitos do autor e os que lhe são conexos, mas deu ênfase penal à exploração direta e indireta, sem autorização do autor ou responsável, de obra intelectual ou fonograma reproduzido com violação do direito de autor, do direito de artista intérprete ou executante ou do direito do produtor de fonograma, bem como o

---

§ 3º Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo:
I - quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público;
II - quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo.
§ 4º No caso do inciso II do parágrafo anterior, a exigibilidade do tributo, ou contribuição social e qualquer acessório, processar-se-á independentemente de representação".

[123] O PL nº 2.681/1996 transformou-se no PLC nº 11/2003 no Senado Federal.

[124] **Violação de direito autoral**
Art. 184. Violar direitos de autor e os que lhe são conexos:
Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa.
§ 1º Se a violação consistir em reprodução total ou parcial, com intuito de lucro direto ou indireto, por qualquer meio ou processo, de obra intelectual, interpretação, execução ou fonograma, sem autorização expressa do autor, do artista intérprete ou executante, do produtor, conforme o caso, ou de quem os represente:
Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
§ 2º Na mesma pena do § 1º incorre quem, com o intuito de lucro direto ou indireto, distribui, vende, expõe à venda, aluga, introduz no País, adquire, oculta, tem em depósito, original ou cópia de obra intelectual ou fonograma reproduzido com violação do direito de autor, do direito de artista intérprete ou executante ou do direito do produtor de fonograma, ou, ainda, aluga original ou cópia de obra intelectual ou fonograma, sem a expressa autorização dos titulares dos direitos ou de quem os represente.
§ 3º Se a violação consistir no oferecimento ao público, mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro, direto ou indireto, sem autorização expressa, conforme o caso, do autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente:
Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
§ 4º O disposto nos §§ 1º, 2º e 3º não se aplica quando se tratar de exceção ou limitação ao direito de autor ou os que lhe são conexos, em conformidade com o previsto na Lei nº 9.610, de 19 de fevereiro de 1998, nem a cópia de obra intelectual ou fonograma, em um só exemplar, para uso privado do copista, sem intuito de lucro direto ou indireto.

> oferecimento ao público, mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro (BRASIL, 2003).

Ficou, assim, sob o ponto de vista do legislador e dos detentores dos direitos autorais, intelectuais e culturais, completo o 'ciclo de proteção penal' quanto aos programas de computador e direitos de autor de obras intelectuais, sejam livros, artigos, músicas, filmes, dentre outros, e sua exploração comercial, exposição e difusão sem a devida autorização[125].

Estipulou a norma que o processamento do autor da violação ocorra, em regra, por vontade expressa do autor da obra intelectual, porém, no caso da exploração direta ou indireta, incluindo o uso da Internet para esse fim, a ação penal é pública incondicionada. Atendeu o legislador a uma reivindicação econômica de que era necessário o combate à pirataria também no ambiente *on-line*, sobrepujando os aspectos atinentes ao acesso à cultura, à informação e ao interesse público sobre as obras[126].

A legislação, então, manteve firme o propósito de defesa da "propriedade intelectual", que firma e sustenta o "monopólio de distribuição de obras" (VIANNA, 2006, p. 939), não necessariamente o seu uso e sua disseminação do conhecimento aos usuários, leitores, ouvintes e espectadores, que foram preteridos no processo de produção normativa.

Se foi uma das primeiras normativas penais brasileiras, por outro lado não é o foco de atenção e preocupação dos entrevistados, porquanto apenas um (16ES) informou dominar seus aspectos penais. Por consequência, pode-se afirmar, mesmo sem dados sólidos e com base nas entrevistas, que a violação de programas de computador e propriedade intelectual não é objeto de atenção dos investigadores cibernéticos, mesmo porque, em regra, depende de um encaminhamento da notícia do crime para o início da investigação criminal.

Por outro lado, observou-se que, capitaneadas pelo Ministério da Justiça e Segurança Pública, foram desencadeadas, desde 2019, quatro operações policiais de enfrentamento à pirataria. A Operação 404[127] centrou seu foco em "plataformas piratas para assistir, via Internet, filmes, séries ou mesmo partidas de futebol". Peduzzi (2019) destaca dois aspectos

---

[125] Sobre a propriedade intelectual, foi um acordo internacional, denominado *Agreement on Trade-Related Aspects of of Intellectual Property Rights, TRIPs*, ou Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio. Ele foi celebrado em 1994, durante a Rodada Uruguai, do GATT (*General Agreement on Tariffs and Trade* ou, em português, Acordo Geral sobre Tarifas e Comércio).

[126] Vianna (2006, p. 940) defende que sob "o pretexto de se tutelar os "direitos de autor", o combate à pirataria é tão-somente um instrumento de reafirmação da velha ideologia da "propriedade intelectual", única capaz de legitimar o monopólio do direito de cópia dos detentores dos meios de produção".

[127] O nome faz referência ao código de resposta do protocolo HTTP para indicar que a página não foi encontrada ou está indisponível.

levantados na investigação: primeiro, que "boa parte dessas pessoas sequer sabe que se trata de um serviço ilegal, a ponto de ligar para autoridades do setor para reclamar do serviço mal prestado por esses contraventores"; segundo, que a "estimativa [...] aponta que, só com a propriedade audiovisual, haja um prejuízo de R$ 9 bilhões por ano para o Brasil".

As quatro fases da Operação 404 (2019, 2020, 2021 e 2022) cumpriram mandados de busca e apreensão em vários Estados no Brasil e, durante as últimas duas operações, também houve participação de outros dois países: Reino Unido e Estados Unidos. Além dos mandados de busca e prisão, houve bloqueio de sites e de aplicativos de *streaming* ilegal de conteúdo (OPERAÇÃO, 2022).

Objetivou-se trazer essa correlação entre o não foco dos entrevistados com a atuação e gestão operacional em nível federal, pois esta é uma das expectativas acentuadas pelos entrevistados, sendo também uma frustração a ausência de processos de gestão e padronização em nível nacional, já que atuações nos Estados são casos isolados quanto ao tema. Além das operações sequenciais citadas, a Operação Brick teve objetivos similares, com a desarticulação de organizações criminosas dedicadas à prática de crimes de pirataria de videogames (CARONE; PINHEIRO, 2021)[128]; também, a Operação Last Page, que foi focada em reprimir crimes praticados contra a propriedade intelectual, por meio da divulgação de livros, violando os direitos dos autores em sites ilegais de *download* (PIRATARIA, 2022)[129]. Em ambas, a mobilização foi efetivada pelo Ministério da Justiça e Segurança Pública (MJSP), por intermédio do Laboratório de Operações Cibernéticas (Ciber-Lab).

4.2.1.2 Estruturação normativo-eleitoral e incremento penal em face da Internet

A legislação penal eleitoral também foi apenas citada por um dos entrevistados (08PE), vinculando-a à circulação de *fake news* e à possibilidade de enquadramento penal tão-somente para fins de "crime eleitoral, mas deveria existir, também, prá [sic] injúria e difamação, mas tem que adaptar". Assim, há expectativas cognitivas sobre a estrutura normativa, porém não necessariamente sobre a legislação eleitoral, que tem recebido

[128] A Operação Brick contou com a participação dos Estados de São Paulo, Mato Grosso do Sul e Minas Gerais. Foram cumpridos, por determinação judicial, 7 mandados de busca e apreensão, 34 bloqueios e/ou suspensão de sites e exclusão de perfis em plataformas de comércio eletrônico.

[129] As Polícias Civis dos estados do Maranhão (MA), Paraná (PR), Espírito Santo (ES) e Minas Gerais (MG) cumpriram, no dia 30/11/22, seis mandados de busca e apreensão e quatro ordens judiciais para bloqueio e/ou suspensão e desindexação de sites ilegais de *download* e exclusão de perfis em plataformas de redes sociais.

incremento de tipos penais ao longo do tempo, também em relação à Internet. Por isso, merece observações críticas.

O Código Eleitoral foi instituído pela Lei nº 4.737/1965, elencando as normas gerais sobre as eleições no Brasil, incluindo a tipificação dos crimes. Dentre os delitos previstos estão, também, os relativos à proteção à honra dos envolvidos no processo eleitoral, especialmente dos candidatos a algum cargo eletivo. Injúria, calúnia, difamação foram adequadas e implantadas nos termos e em razão do processo eleitoral, sua proteção e lisura. Evolutivamente[130], algumas alterações foram feitas no Código Eleitoral nesse período (55 anos).

Três décadas depois da instituição do Código Eleitoral foi aprovada a Lei nº 9.504/1997[131], que estabeleceu normas para as eleições realizadas a partir de então. Essa norma define e informa, então, as principais regras para os processos eleitorais, sendo ela a que sofreu o maior número de alterações em razão da comunicação e interação digital propiciada pela Internet. Tal lei, no entanto, já previu no art. 72, como crime de reclusão, punível com pena de cinco a dez anos, o fato de alguém

> [a] obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos [...]
> [b] desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral. (BRASIL, 1997).

Estabeleceu-se, então, uma ‘proteção penal’ ao sistema eletrônico/digital eleitoral de votação adotado no Brasil, especialmente quanto aos dados gravados e/ou a transmitir, bem como a manipulação dos resultados constantes em sistema de tratamento automático do banco de dados das eleições em andamento.

Para melhor compreensão das modificações realizadas na sequência temporal pós Código Eleitoral e Lei Eleitoral, expõem-se, em itens, as principais alterações havidas e que são relativas ao tema em pesquisa e estudo: a Internet e a estruturação normativa [da cultura política] brasileira. Desta forma, citam-se as alterações na legislação eleitoral e que levam em conta as regras de conduta e normas proibitivas em razão da Internet[132]:

---

[130] Evolutivamente, não necessariamente num sentido positivo nem negativo. Evolução no sentido de adequação com o decorrer do tempo e debates sobre os temas.

[131] A referida Lei Eleitoral é originária do PL nº 2.695/1997 e do PLC nº 37/1997. Ou seja, os projetos são do mesmo ano da aprovação e sanção da Lei Eleitoral.

[132] A Lei dos Partidos Políticos, Lei nº 9.096/1995, também sofreu alterações concomitantes, mas não serão analisadas no decorrer desta pesquisa.

- Lei nº 12.034/2009[133]: alteração no Código Eleitoral (1965) e na Lei Eleitoral (1997), estabelecendo normas quanto à propaganda eleitoral na Internet e ao recebimento de doações de campanha por esse meio. As principais normas relativamente à propaganda na Internet estão nos arts. 57-A a 57-H, inseridos na Lei nº 9.504/1997. Nessa primeira norma prevendo a Internet como meio de comunicação entre candidatos e eleitores não foi previsto nenhum tipo de crime, mas o descumprimento, com a violação das regras, poderia levar a aplicação de multas elevadas[134].

- Lei nº 12.891/2013[135]: também trouxe alterações no Código Eleitoral (1965) e na Lei Eleitoral (1997), visando a diminuir os custos da eleição, inclusive com o uso e em razão da Internet. Trouxe modificações procedimentais e penais relativamente à Internet, a destacar: a) acrescentou o §3º no art. 57-D da Lei nº 9.504/1997, estipulando, além da multa prevista no §2º pela violação do dispositivo, a possibilidade de a Justiça Eleitoral "determinar, por solicitação do ofendido, a retirada de publicações que contenham agressões ou ataques a candidatos em sítios da Internet, inclusive redes sociais"; b) Incrementou o art. 57-H, que já considerava a prática "de quem realizar propaganda eleitoral na Internet, atribuindo indevidamente sua autoria a terceiro, inclusive a candidato, partido ou coligação" uma conduta com sanção pecuniária, considerando crime quem: 1) contratar direta ou indiretamente de grupo de pessoas com a finalidade específica de emitir mensagens ou comentários na Internet para ofender a honra ou denegrir a imagem de candidato, partido ou coligação, prevendo a punição com detenção de dois a quatro anos; e 2) as pessoas contratadas com a finalidade específica de emitir mensagens ou comentários na Internet para ofender a honra ou denegrir a imagem de candidato, partido ou coligação, prevendo a punição e detenção de seis meses a um ano, com alternativa de prestação de serviços à comunidade pelo mesmo período. Em ambos os casos também pode ser atribuída multa pecuniária.

- Lei nº 13.165/2015[136]: considerada uma 'minirreforma' eleitoral, teve por finalidade "reduzir os custos das campanhas eleitorais, simplificar a administração dos Partidos Políticos e incentivar a participação feminina". Alterou poucos aspectos da campanha eleitoral pela Internet e a forma de captação de recursos, incluindo cartão de crédito, bem como em relação ao direito de resposta em razão de postagens na Internet e outros meios.

---

[133] A Lei nº 12.034/2009 é originária do PL nº 5.498/2009 e do PLC nº 141/2009.
[134] Arts. 57-C, 57-D, 57-E e 57-H da Lei nº 9.504/1997.
[135] A Lei nº 12.891/2013 é originária do PLS nº 441/2012 e do PL nº 6.397/2013, sendo este devolvido ao Senado Federal com texto substitutivo, gerando reanálise do tema.
[136] A Lei nº 13.165/2015 é originária do PL nº 5.735/2013 e do PLC nº 75/2015.

- Lei nº 13.488/2017[137]: produziu alterações em relação à legislação anterior, promovendo uma "reforma no ordenamento político-eleitoral". Especificamente, trouxe regras quanto (a) ao financiamento coletivo via Internet, por aplicativos eletrônicos e outros recursos similares (art. 23, IV, Lei nº 9.504/1997), e (b) ao impulsionamento de conteúdo na Internet (art. 26, XV e § 2º; art. 39, IV; art. 57-B, IV, §§ 3º e 4º; e art. 57-C, todos da Lei nº 9.504/1997), inclusive o impulsionamento de publicação de direito de resposta em razão da ofensa gerada na Internet (art. 58, §, IV, "a", da Lei nº 9.504/1997).

- Lei nº 13.834/2019[138]: promoveu a criminalização da denunciação caluniosa com objetivos e fins eleitorais e acrescentou o Art. 326-A no Código Eleitoral[139].

Assim, toda e qualquer pessoa que der causa à instauração de investigação criminal, processo judicial e, inclusive, investigações administrativas, inquérito civil ou ação de improbidade administrativa, com a finalidade eleitoral, pode ser alvo de um processo crime que pode levar à punição de 2 a 8 anos de reclusão. Incorre no mesmo crime quem faz a divulgação e/ou propala, por qualquer meio ou forma – aqui se incluem as aplicações de Internet, sites, mídias sociais, comunicadores instantâneos etc. –, o ato ou fato que foi atribuído falsamente ao denunciado inocente, exigindo-se, no entanto, que tenha ciência dessa inocência.

Ingressou aqui o legislador numa seara discutida em inúmeras eleições mundiais e uma prática muito comum: as *fake news* ou 'notícias falsas'. A discussão sobre a criminalização inserida no contexto eleitoral, diferente das demais relativas às regras eleitorais, transcorreu nas casas legislativas por oito anos: em regra, as propostas de modificações de normas eleitorais são bastante rápidas, com propostas e aprovações realizadas no mesmo ano, demonstrando o intento do legislador brasileiro em autoproteção. Portanto, juntamente com a Lei nº 13.165/2015, são duas leis eleitorais que tiveram um período de discussão maior do que um ano para sua aprovação e sanção, ou seja, 'a regra de tempo' de debates e aprovações de leis eleitorais é de no máximo um ano.

---

[137] A Lei nº 13.488/2017 é originária do PL nº 8.612/2017 e do PLC nº 110/2017.

[138] A Lei nº 13.834/2019 é originária do PL nº 1.978/2011 e do PLC nº 43/2014.

[139] Art. 326-A. Dar causa à instauração de investigação policial, de processo judicial, de investigação administrativa, de inquérito civil ou ação de improbidade administrativa, atribuindo a alguém a prática de crime ou ato infracional de que o sabe inocente, com finalidade eleitoral:

Pena - reclusão, de 2 (dois) a 8 (oito) anos, e multa.

§ 1º A pena é aumentada de sexta parte, se o agente se serve do anonimato ou de nome suposto.

§ 2º A pena é diminuída de metade, se a imputação é de prática de contravenção.

§ 3º Incorrerá nas mesmas penas deste artigo quem, comprovadamente ciente da inocência do denunciado e com finalidade eleitoral, divulga ou propala, por qualquer meio ou forma, o ato ou fato que lhe foi falsamente atribuído.

Por outro lado, a temática das notícias falsas/desinformação foi recorrente nos últimos anos e teve seu ápice no Brasil em 2018, no mês de outubro, em face do pleito eleitoral presidencial[140].

- Lei nº 14.197/2021[141]: inseriu, no Código Penal, no capítulo dos crimes contra o funcionamento das instituições democráticas no processo eleitoral, o crime de interrupção do processo eleitoral. Segundo o art. 359-N, comete o crime, com pena de três a seis anos, quem impedir ou perturbar a "eleição ou a aferição de seu resultado, mediante violação indevida de mecanismos de segurança do sistema eletrônico de votação estabelecido pela Justiça Eleitoral".

Para complementar esta breve análise temática da linha [estrutural] do tempo das modificações da legislação eleitoral em relação à Internet, estas são reproduzidas em um quadro analítico:

Quadro 8: Linha do tempo da legislação eleitoral no Brasil e a relação com a Internet

1965	**1997**	**2009**	**2013**	**2015**	**2017**	**2019**	**2021**
Lei nº 4737	**Lei nº 9504**	**Lei nº 12.034**	**Lei nº 12.891**	**Lei nº 13.165**	**Lei nº 13.488**	**Lei nº 13.834**	**Lei nº 14.197**
Código Eleitoral	Lei Eleitoral	Propaganda eleitoral na Internet e recebimento de doações de campanha por esse meio	Lei Eleitoral: Arts. 57-D, §3º, e 57-H	Reduzir os custos das campanhas eleitorais, simplificar a administração dos Partidos Políticos e incentivar a participação feminina	Financiamento coletivo via Internet, por aplicativos eletrônicos e outros recursos similares (Art. 23, IV, Lei nº 9.504/1997), e (b) ao impulsionamento de conteúdo na Internet. Suspensão de conteúdo – Art. 57-I, Lei nº 9.504/1997.	Lei Eleitoral: Art. 326-A	Acréscimo, no Código Penal: Art. 359-N

Fonte: Produzido pelo autor (2023).

[140] O acompanhamento do termo *fake news* e sua exploração na Internet pode ser feito no Google Trends. Nos últimos cinco anos, pelo link disponível em https://trends.google.com/trends/explore?date=today%205-y&geo=BR&q=fake%20news, pode-se visualizar que o período de maior ênfase no tema é nas três semanas antes do segundo turno do processo eleitoral de 2018, de 07 a 27 de outubro, e durante o período eleitoral de 2022, especialmente de 18 de setembro até 5 de novembro.

[141] A Lei nº 14.197/2021 é originária do PL nº 2.462/1991, ou seja, teve trinta anos de trâmite no legislativo brasileiro.

O assunto sobre a desinformação/*fake news* também será abordado no tópico relativo aos projetos de lei existentes no Congresso Nacional e que tratam da tentativa de estruturação penal, ou seja, de criminalização/regulação do tema.

4.2.1.3 Estruturação da proteção penal aos bancos de dados da Administração Pública e criminalização das condutas dos servidores

Observa-se, de pronto, que, embora os bancos de dados da Administração Pública no Brasil sempre fossem objeto de atenção e de exploração, podendo-se dizer que cercado de componentes que indicavam e indicam a vulnerabilidade e facilidade de acesso aos sistemas, a mesma atenção e expectativa não é referida pelos entrevistados da pesquisa empírica, exceto pela conduta de invasão de dispositivos informáticos, assunto do próximo subtópico.

Por outro lado, as ações hacktivistas têm um olhar, por assim dizer, especial para os bancos de dados públicos, visando, muitas vezes, à divulgação de dados que deveriam estar disponíveis à população pelo mecanismo da transparência. O melhor exemplo dessa exploração cotidiana pelas ações hacktivistas é o site Zone-H[142], que reproduz cotidianamente as vulnerabilidades nos principais sítios governamentais brasileiros. Assim, o legislativo brasileiro absorveu essas comunicações que circundavam no seu entorno e estabeleceu mecanismos de proteção penal na estrutura da legislação penal brasileira.

Em 1999, o Governo brasileiro encaminhou à Câmara dos Deputados um projeto prevendo a criminalização de várias condutas que, segundo o texto, visavam a dar proteção jurídico-penal aos bancos de dados da administração pública federal, estadual e municipal, direta e indireta. O PL nº 933/1999 teve *start* em maio de 1999 e com regime de urgência na tramitação, sendo aprovado no mesmo ano e no ano seguinte seguindo ao Senado Federal (PLC nº 23/2000). Em julho de 2000, ou seja, 1 ano e 2 meses após a apresentação da proposta, estavam aprovadas a modificação no Código Penal e a inserção de quatro novos tipos penais, além de incremento em vários outros.

O objetivo principal, segundo a ementa do PLC no Senado Federal, era a "tipificação de condutas que constituem crimes contra a Previdência Social", surgindo, então, no Código Penal, os arts. 168-A e 337-A, de apropriação indébita e sonegação previdenciária. Além disso, outros tipos penais foram integrados. De destaque para o presente estudo são quatro

[142] Vide arquivo com as divulgações dos sites que, explorados em sua segurança cibernética, apresentaram falhas: http://br.zone-h.org/archive/special=1 (acesso em 09 jan. 2023).

tipos penais "gerados" e incorporados ao Código Penal e que são relativos aos bancos de dados dos serviços públicos, diretos ou delegados, no Brasil, a referir:

- *Inserção de dados falsos em sistema de informações*: poder-se-ia denominar o art. 313-A de "corrupção eletrônica", pois que visa a punir o agente público que obtém vantagem indevida ou que queira causar dano a outra pessoa com a prática de (a) inserção ou (b) facilitação da inserção de dados falsos, (c) alteração ou (d) exclusão indevida de dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública. A proteção à integridade de dados pessoais, de todos os brasileiros, constantes em bancos de dados públicos, é clara, punindo o agente público que vise a inserção, alteração ou exclusão de dados ou informações com objetivos ilícitos[143].

- *Modificação ou alteração não autorizada de sistema de informações*: o art. 313-B inseriu uma proteção genérica quanto aos dados e informações dos bancos de dados e sistemas públicos, porquanto a modificação ou alteração deles ou de programa de informática, sem autorização ou solicitação, pode levar à punição do funcionário público[144], tendo, também, um acréscimo de pena no caso de resultar em dano para o cidadão ou para a Administração Pública.

- *Divulgação, sem justa causa, de informações sigilosas ou reservadas*: a divulgação de segredo já era um tipo penal integrado ao Capítulo dos Crimes Contra a Inviolabilidade dos Segredos do Código Penal, aplicável especialmente ao ambiente corporativo e mediante o interesse da vítima, ou seja, do 'dono do segredo'. A Lei nº 9.983/2000 inseriu no art. 153 o §1-A[145], instituindo como crime a violação de segredo constante em bancos de dados públicos e que são consideradas informações sigilosas ou reservadas, estipulando que no caso de dano à Administração Pública (não fala em 'administrado' ou cidadão) a ação penal é pública incondicionada. Esta previsão, pelo contexto e pelo que visa a proteger, poderia estar

---

[143] "Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano:
Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa".

[144] "Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:
Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa.
Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado".

[145] "§ 1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública:
Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa.
§ 2º Quando resultar prejuízo para a Administração Pública, a ação penal será incondicionada".

nos Crimes Contra a Administração Pública, especialmente nos relativos à violação do sigilo funcional.

- *Fornecimento e empréstimo de senha*: a condição de funcionário/servidor público lhe 'empresta' o dever de zelar no trato dos dados e bens públicos, e qualquer violação de sigilo funcional pode redundar em processos civil, criminal e administrativo. A Lei nº 9.983/2000 inseriu no §1º do art. 325 do Código Penal (Violação do Sigilo Funcional) a tipificação para quem (a) permitir ou facilitar, "mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública" e para quem (b) utilizar, indevidamente, o acesso restrito.

A proteção penal proposta com a Lei nº 9.983/2000 visou a contemplar vários verbos e condutas que são violadoras dos dados dos cidadãos, ora contingenciando a proteção destes, ora a proteção dos próprios dados e incentivando a reserva de informação sobre eles. Trata-se, portanto, de uma proteção *penal* aos dados pessoais e governamentais/de Estado. Essa proteção penal de dados, aliás, ocorre pelo menos 20 anos antes da proteção civil e constitucional de dados (EC nº 115/2022).

4.2.1.4 Invasão de dispositivo informático e sistemas: entre estruturações, expectativas e frustrações

Há similitude, em três aspectos, da legislação tratada no item anterior, relativa aos dados e informações constantes em bancos de dados da Administração Pública, com a introduzida no Código Penal em 2012, na aprovação e sanção da Lei nº 12.737, denominada 'Lei Carolina Dieckmann': (a) visam à proteção de dados e informações constantes em bancos de dados, naquele caso os públicos, neste caso os privados; (b) focam no acesso indevido e/ou manipulação (alteração ou exclusão) de dados e informações; e (c) as Leis foram aprovadas e sancionadas em tempo considerado muito curto para maturação e discussão de criminalização de condutas: 1 ano e 2 meses, no caso da Lei nº 9.983/2000, e 1 ano e 1 dia, no caso da Lei nº 12.737/2012.

As três observações firmadas no parágrafo anterior também são cabíveis à Lei nº 14.155/2021, que veio a modificar os artigos 154-A, 155 e 171 do Código Penal. O Projeto de Lei nº 4.554/2020 foi protocolado em 14/09/2020 no Senado Federal, passando pela aprovação na Câmara dos Deputados, sendo sancionada em 27/05/2021, ou seja, em menos

de 9 (nove) meses de discussão e trâmite legislativo. Voltaremos a ela *a posteriori* (contextos materiais e processuais penais).

A 'Lei Carolina Dieckmann' acrescentou à legislação penal um dispositivo completo e fez dois acréscimos em outros dispositivos:

- *Invasão de dispositivo informático*: a tipificação do art. 154-A, do Código Penal, modificada em 2021, previu a prática delitiva no caso de (a) invasão a dispositivos informáticos e (b) a instalação de vulnerabilidades. Em todos os casos, o delito ocorre quando não há o consentimento do possuidor dos dispositivos de informática ou telemática, havendo acesso indevido e forçado para obtenção, adulteração ou exclusão de dados, sendo o mais comum a obtenção do dado/informação[146].

A pena estipulada é maior nos casos de a invasão resultar na obtenção de "conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido". O lógico é de que quanto mais íntimos ou privados os dados, maior seria a proteção penal e maior a punibilidade. Essa lógica de redação legislativa não foi modificada com a alteração introduzida pela Lei nº 14.155/2021, que, em relação ao dispositivo em questão, retirou a exigência de que a invasão seja realizada mediante violação de mecanismo de segurança, bem como retirou a condição de propriedade alheia e exigiu apenas que o dispositivo seja de uso alheio.

Inúmeras considerações foram – e ainda podem – ser feitas quanto a esse tipo penal, especialmente quanto à abertura conceitual existente (WENDT, 2017b): o que é dispositivo

---

[146] Redação original, de 2012, com base na Lei nº 12.737: "Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
I - Presidente da República, governadores e prefeitos;
II - Presidente do Supremo Tribunal Federal;
III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal".

informático? Qual a amplitude do conceito de obter?[147] A aplicação abrangente dos conceitos previstos, especialmente por parte dos entrevistados, também é direcionada a uma expectativa de melhor redação do dispositivo penal, embora já tenha ocorrido recentemente.

A *quaestio* principal em face da pandemia da Covid-19 é quanto ao incremento dos delitos em meio cibernético e seu potencial risco (MELLO JR., 2021), bem como a irritação que o tema provoca no sistema legislativo, acarretando a revisão e o incremento dos tipos penais já existentes. No caso em tela, o tipo penal base do art. 154-A sofre uma alteração de pena, inicial, de três meses para um ano, e, final, de um ano para quatro anos, ou seja, o que era a pena final anteriormente passa a ser a pena inicial a partir da publicação da Lei (28/05/2021).

Os aumentos de pena também se estenderam para os casos de a invasão resultar em prejuízo econômico (entre 1/6 a 1/3 em 2012 para 1/3 a 2/3 da pena em 2021) e se a invasão resultar em "obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido", quando a pena mínima atual prevista (2021) parte também da máxima prevista anteriormente (2012), ou seja, de dois anos, podendo chegar a cinco anos de reclusão.

Resumindo, em relação ao art. 154-A do Código Penal, a Lei nº 14.155/2021 produziu (a) a modificação da redação do caput, ampliando a incidência do tipo penal, (b) a majoração da pena do crime na sua forma básica (caput do art. 154-A), (c) a majoração dos limites da causa de aumento de pena do § 2º e (d) a majoração da pena da qualificadora do § 3º.

Não obstante as alterações substanciais no delito emergencialmente criado em 2012, expectativas e frustrações dos investigadores cibernéticos são relacionadas (a) a redação normativa, que deveria ser melhorada ou aprimorada, e (b) à pena privativa de liberdade, que, embora ampliada na redação de 2021, não é reconhecida como "efetiva" pelos policiais, especialmente por não gerar decretação e a consequente prisão dos autores:

---

[147] Redação com base na Lei nº 14.155/2021: "Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
[...]
§ 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.
§ 3º [...]
Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa".

> ainda vira um Termo Circunstanciado, ainda é de menor potencial ofensivo, isso acaba sendo muito pouco. (04RS).
> por exemplo a questão de invasão a dispositivo informático, aqui temos encarado muitos casos referentes à invasão de dispositivo, principalmente, em relação à rede social. Temos enxergado, que atualmente, a penalidade aplicada não está sendo o suficiente. (06AP).
> mas nesse estelionato (invasão de dispositivo informático) a lei deveria ter mais rigor. (09MA).
> acredito que a pena, principal, é em relação ao artigo 154-A (invasão do dispositivo informático), está bem branda, passível de não persecução penal. (10SC).
> deveríamos incrementar a pena no delito de invasão de dispositivo informático e estelionato. (12PI).
> A interpretação, extensiva ou analógica, compreende as redes sociais como dispositivos informáticos, então temos enfrentado dificuldades nesse sentido, pois têm magistrados que entendem dessa forma, outros não, de enquadramento da rede social como dispositivo informático, em que esse fato se insere num vácuo legislativo. (15TO).
> no crime de invasão de dispositivo informático verificamos que o legislador foi tímido ou modesto ao prever a sanção penal. [...] Também a questão da invasão do dispositivo informático, em que a pena é muito branda. (17MT).
> a pena é pequena para invasão de dispositivo informático. (18RO).
> nos crimes do artigo 154-A, temos várias situações, por exemplo, no Tribunal de Justiça do DF, entendiam que um perfil não era um dispositivo informático, assim não aplicávamos o 154-A, recentemente decidiram que um perfil é dispositivo informático e temos que aplicá-lo. Então, na invasão do Instagram, em tese é o artigo 154-A, o mesmo que tratará de uma invasão de um servidor de uma empresa, em que foram deletados arquivos importantes, ou seja, o artigo 154-A atende uma situação muito simples de perfil, como atende uma situação muito complexa e tudo isso dentro de uma única pena. Então, acredito que deveria ter, algum tipo de diferenciação, além de definir bem a questão do dispositivo informático. (19DF).
> trabalhamos, muito, com artigo 154-A, que dispõe de invasão de dispositivo informático, existe um debate dentro da polícia sobre as dificuldades de conceituação de dispositivos, inclusive eu oscilo entre um entendimento e outro, conforme o tempo e a amplitude do debate. [...] entendo que há necessidade de delinear melhor as condutas típicas, classificar com mais técnica legislativa. Uma delas seria a conceituação de dispositivo informático, pois debatemos muito a questão de sistema, se ele pode ser considerado um dispositivo informático, também sobre a invasão de rede social, se pode ser dispositivo informático. Pois pelo significado da palavra, presumisse que dispositivo é um bem material (palpável). Então, quando alguém invade um sistema, por exemplo uma rede social, como deve ser tipificado, nesse sentido encontramos dificuldades. (22MG).

Fica claro, pelas expectativas relatadas pelos entrevistados, que o mesmo tipo penal de invasão de dispositivo informático pode ser aplicado a situações simples e a fatos complexos, porém, penalmente (tipo penal e sanção) tem o mesmo tratamento, não existindo uma diferenciação normativo-penal.

- *Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública*: o acréscimo do §1º ao art. 266 do Código Penal considera crime a interrupção de serviço telemático ou de informação de utilidade pública

ou, igualmente, quando alguém impede ou dificulta o restabelecimento desse serviço que envolve telefonia e informática ou que presta informação de utilização pública[148].

- *Falsificação de cartão de crédito ou débito*: o acréscimo no art. 298 do Código Penal equiparou a documento particular o cartão de crédito ou débito, os meios mais comuns de pagamento nas duas primeiras décadas do século XX[149].

Finalmente, há que se frisar dois aspectos sobre essa Lei em específico: primeiro, que os entrevistados referem inúmeras vezes o crime de invasão de dispositivo, mas não referem nenhum dos outros dois mencionados; segundo, o papel da imprensa na aprovação das leis em comento, tanto a de 2012 quanto a de 2021.

No caso da discussão e aprovação da Lei nº 12.737/2012, os veículos de comunicação brasileiros tiveram um papel condutor na construção de uma realidade não verdadeira: a inexistência de tipificação penal para os casos como o da atriz Carolina Dieckmann (WENDT, 2017b), que foi vítima de extorsão e não necessariamente de algum tipo de invasão de dispositivo informático ou telemático. Essa circunstância levou o legislador a aprovar rapidamente o PL nº 2.793/2011 (PLC nº 35/2012), sem maiores discussões e com conceitos abertos e abrangentes[150].

No cenário pandêmico, em razão da Covid-19, com o incremento dos casos de violação de dados e ataques remotos (ROLFINI, 2020), de sequestro de dados e *phishing* (VITTA, 2020; SANTINO, 2020), as comunicações chegam e são absorvidas pelo legislador brasileiro, que pauta a temática[151]. Dentre as propostas, no Senado Federal é protocolado, em setembro de 2020, o PL nº 4.554, que, após menos de 3 meses de trâmites, com nove emendas e debates[152], é aprovado e remetido à Câmara dos Deputados[153]. Em 5 meses de trâmites e discussões, o PL nº 4.554/2020 é aprovado com alterações pelos deputados, voltando ao

---

[148] "Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
Pena - detenção, de um a três anos, e multa.
§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
§ 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública".

[149] "Art. 298. Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
Pena - reclusão, de um a cinco anos, e multa.
Falsificação de cartão
Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito".

[150] Sobre os pontos críticos, além de Wendt (2017b), ver também Sydow (2013, p. 279-316).

[151] As notícias citadas são todas de julho e agosto de 2020.

[152] No Senado Federal, o PL nº 4.554/2020 tem a ele anexado o PL nº 4.287/2019.

[153] O PL nº 4.554/2020 teve dois outros PLs apensados no transcorrer das discussões na Câmara dos Deputados: PL nº 2.638/2020 e PL nº 3.363/2020.

Senado Federal para nova discussão, de menos de mês, quando foi aprovado e encaminhado à sanção.

É certo que a pandemia acelerou a utilização das mídias e sistemas informáticos, sendo lógico que houvesse uma expectativa social e midiática sobre o legislador quanto à maior proteção penal dos dados, o que acabou se concretizando com a aprovação da Lei nº 14.155/2021, na qual restou incluída a modificação do crime de invasão de dispositivo informático. A referida lei será ainda analisada em um subtópico quanto à proteção penal decorrente da subtração e da obtenção indevida de vantagem financeira, pois tipificou o furto mediante fraude e a fraude eletrônica. Porém, seguiremos com a linha do tempo estruturada pelo legislador nacional.

4.2.1.5 O contingenciamento penal quanto à produção e divulgação não consentida de intimidade: pornografia de vingança e violação da privacidade

A violência de gênero não é restrita ao mundo físico, que muitos chamam de mundo real[154]. Pelo contrário, as redes sociais e os comunicadores instantâneos propiciaram uma plena ampliação das práticas de abusos masculinos, em especial a pornografia de vingança (*revenge porn*) e o *cyberbullying*. Imagens, vídeos, textos e áudios são explorados em comportamentos divergentes, por isso, tornando-se mecanismos propulsores de danos, tanto na produção quanto na divulgação não consentida de aspectos inerentes à intimidade das pessoas. Por outro lado, o *sexting*, ativo e passivo (envio e recebimento de imagens e vídeos de conteúdo íntimo), é uma prática rotineira entre jovens e depende de processos orientativos (CARDOSO; FALCKE; MOSMANN, 2019).

O caso Rose Leonel é tido como um dos primeiros (ocorreu em 2006) em que, com repercussão em mídias diversas, demonstrou os reais efeitos desse tipo de violência contra a mulher na era da Internet (GUILLEN, 2011). No caso em tela, o homem a anunciava como garota de programa e colocava os telefones pessoais dela para contato, fazendo com que a vítima recebesse mais de 500 ligações por dia de homens interessados nas divulgações. O autor encaminhou fotografias íntimas dela por e-mail para diversas pessoas e publicou as imagens em diversos sites nacionais e internacionais de conteúdo pornográfico. O autor foi

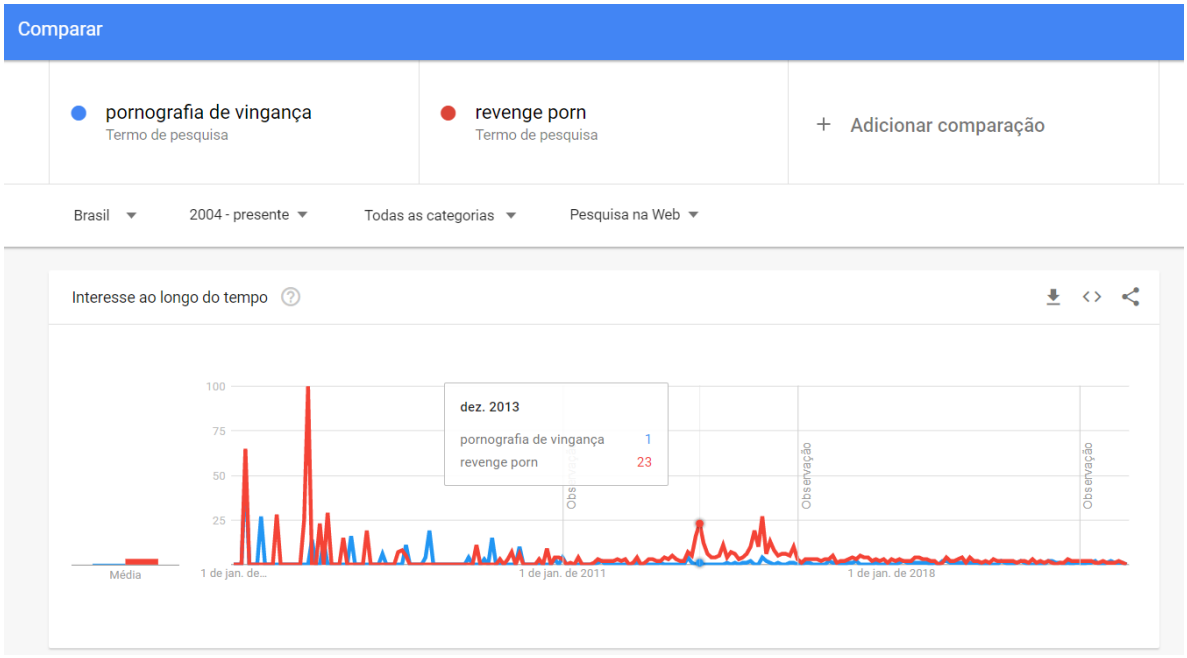
[154] Sobre os aspectos do mundo real-real e real-virtual, vide Ziemer *et al.* (2009). As análises nesse sentido podem ir além do contexto cultural e adentrar nos aspectos filosóficos, porquanto este não é o objetivo da pesquisa. Para fins deste estudo, considera-se o ambiente da Internet o ambiente 'digital' (ou virtual) para diferenciá-lo do ambiente 'físico' (ou real).

condenado, em 2011, por injúria e difamação (SETE, 2013), além de ter de pagar uma indenização (EMPRESÁRIO, 2011; GUILLEN, 2011). Porém, os efeitos foram diversos, tais como depressão, isolamento e, ainda, perda do emprego (ENCONTRO, 2014).

Aliás, Rose Leonel foi uma das principais articuladoras da existência de um tipo penal específico e não somente o enquadramento citado, como ocorreu no caso em que foi vítima (WENDT, 2015a), tanto que o projeto de normativa no Senado Federal levou o seu nome quando da análise, a partir de 2013. O Projeto de Lei da Câmara nº 18, de 2017, foi denominado de "Projeto de Lei Rose Leonel" e derivou do PL nº 5.555/2013, gerando a Lei nº 13.772/2018.

O destaque do tema pode ser buscado, também, pelo volume de pesquisas feito no principal mecanismo de busca, o Google, tendo tido, nos períodos de 2004 a 2006 e 2013 a 2015, uma maior incidência de buscas dos termos 'pornografia de vingança' e seu correlato em inglês '*revenge porn*':

Figura 11 - *Google Trends (Topics) - Pornografia de vingança e revenge porn*



Fonte: Acesso Google Trends em 09 jan. 2023 (REVENGE, 2023).

Segundo Buzzi (2015, p. 11), os termos[155] citados são usados "para nomear a divulgação, sobretudo na *Internet*, de fotos, vídeos, áudios, montagens, em suma, qualquer material sexualmente gráfico, íntimo e privado de uma pessoa, sem sua autorização". Já se

[155] Ver mais sobre os termos utilizados e histórico em Buzzi (2015, p. 29-36).

deixa claro, portanto, que os termos, em português ou inglês, não são exclusivos do ato de vingança de exposição de pornografia de mulheres, abrangendo também homens como vítimas, além de gays, lésbicas, travestis e transexuais. No entanto, deve-se acrescentar que a cibervingança também pode ter como objetivo causar humilhação da vítima (WENDT, 2015b), além do compartilhamento de imagens com conteúdo não necessariamente de nudez explícita, como fotos de biquíni e mesmo sem mostrar rosto (ALVES, 2020).

A tipificação até então adequada às hipóteses de postar, divulgar, compartilhar na Internet fotos íntimas de ex-parceira(o) era a prevista nos arts. 139 e 140 do Código Penal, respectivamente, difamação (pena de 3 meses a 1 ano) e injúria (pena de 1 a 6 meses), com possibilidade de aumento de pena do art. 141, III, ou seja, a utilização de meio que facilite a divulgação da difamação ou da injúria, no caso, a rede de computadores. A situação fica(va) mais evidente, como no caso Rose Leonel, quando o compartilhamento de fotos íntimas se dá em conjunto com textos retratando a vítima como prostituta, "expondo-a para angariar clientes e programas"[156]. Já quando a vítima é menor de idade, o direcionamento de aplicação é em relação aos artigos penais do Estatuto da Criança e do Adolescente (arts. 241 e ss.), conforme modificações normativas de 2008, já analisadas.

Antes mesmo da existência de um tipo penal específico, em 2014, a vítima de exposição indevida da sua intimidade foi beneficiada com a possibilidade de notificar o provedor no qual está o conteúdo armazenado para que o delete e preserve as evidências. Tal providência está prevista no art. 21 da Lei nº 12.965/2014, o Marco Civil da Internet, devendo os provedores de aplicações retirar imagens, vídeos e outros materiais, contendo nus e atos sexuais, tão logo notificado:

> Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.
> Parágrafo único. A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

[156] Apelação Criminal nº 756.367.3 (TJ-PR).

Em não atendendo a solicitação, também pode a vítima propor uma ação cível, que pode ser, conforme o art. 22 do Marco Civil da Internet, protocolada no Juizado Especial[157].

A existência de um expediente rápido de remoção do conteúdo publicado indevidamente não desmobilizou o público feminino, cuja comunicação 'provocou' a discussão legislativa, levando à edição de duas Leis que abrangem o tema: Lei nº 13.718 e Lei nº 13.772.

Embora a Lei nº 13.772/2018 tenha sido aprovada e sancionada depois da Lei nº 13.718/2018, as discussões sobre o que propunha começaram antes, em 2013 – estando, a partir daí, nos *Trending Topics* do Google –, com o 'Projeto de Lei Rose Leonel', o PL nº 5.555/2013, transformado em PLC nº 18/2017, conforme referido. A sanção foi concomitante a um conjunto de quatro normas federais de proteção às mulheres (NOBRE, 2018), destacando-se a Lei nº 13.772/2018 por incluir no Código Penal o art. 216-B[158], punindo os casos de "registro não autorizado da intimidade sexual", incluindo a montagem em fotografia, vídeo ou áudio.

A Lei nº 13.772/2018 também inseriu a "violação da intimidade" da mulher como forma de violência psicológica[159] para fins de aplicação da Lei Maria da Penha (Lei nº 11.340/2006) e deferimento de medidas protetivas de urgência. Diferentemente, a Lei nº 13.718/2018 teve sua origem no Senado Federal com o PLS nº 618/2015 e, no ano seguinte, foi enviado, passando, sob o PL nº 5.452/2016, por dois anos de discussões, período em que um projeto substitutivo foi aprovado na Câmara dos Deputados. Em razão disso, voltou ao Senado Federal, sob o Substitutivo da Câmara dos Deputados nº 2/2018, sendo aprovado e sancionado em setembro de 2018. Com a Lei nº 13.718/2018, dois artigos foram incluídos no Código Penal e outros foram incrementados, com destaque ao que se relaciona ao presente

---

[157] Alguns provedores, como a Microsoft, estão possibilitando procedimentos ágeis de retirada de links com *revenge porn* (MOREIRA, 2015). As aplicações possuem, na maioria dos casos, orientações e procedimentos diretos de remoção, sem necessidade de ordem judicial, por também entenderem ser algumas condutas violadoras de suas autorregras.

[158] "Art. 216-B. Produzir, fotografar, filmar ou registrar, por qualquer meio, conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado sem autorização dos participantes:

Pena - detenção, de 6 (seis) meses a 1 (um) ano, e multa.

Parágrafo único. Na mesma pena incorre quem realiza montagem em fotografia, vídeo, áudio ou qualquer outro registro com o fim de incluir pessoa em cena de nudez ou ato sexual ou libidinoso de caráter íntimo".

[159] "Art. 7º [...]

II - a violência psicológica, entendida como qualquer conduta que lhe cause dano emocional e diminuição da autoestima ou que lhe prejudique e perturbe o pleno desenvolvimento ou que vise degradar ou controlar suas ações, comportamentos, crenças e decisões, mediante ameaça, constrangimento, humilhação, manipulação, isolamento, vigilância constante, perseguição contumaz, insulto, chantagem, **violação de sua intimidade**, ridicularização, exploração e limitação do direito de ir e vir ou qualquer outro meio que lhe cause prejuízo à saúde psicológica e à autodeterminação". (grifo nosso)

estudo: a “divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia”.

O art. 218-C tornou crime a conduta de “oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio – inclusive por meio de comunicação de massa ou sistema de informática ou telemática” –, fotografia(s), vídeo(s) ou outro(s) registro(s) audiovisual(is) que contenha(m) cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, ainda, “sem o consentimento da vítima, cena de sexo, nudez ou pornografia”, sendo este o caso de enquadramento principal nos casos de pornografia de vingança, especialmente se associado ao §1º do mesmo dispositivo, quando o crime é “praticado por agente que mantém ou tenha mantido relação íntima de afeto com a vítima ou com o fim de vingança ou humilhação”, ocorrendo neste caso um aumento de pena.

Diferente do que estabeleceu o legislador penal quanto à indução ou instigação à automutilação e ao suicídio (art. 122 do Código Penal), objeto de análise no próximo subtópico, não há nos tipos penais de 2018 (216-B e 218-C do Código Penal) uma gravidade maior no caso de transmissão pela Internet.

O óbvio paira na resposta, pois que os verbos destes tipos penais já são circunscritos às práticas do ambiente da ‘virtualidade real’ da web. Por outro lado, quando se tratar de criança e adolescente, a proteção vem do estatuto próprio, o Estatuto da Criança e do Adolescente, especialmente a partir de 2008, com os arts. 241-A e seguintes, conforme já observado.

Quadro 9: Linha do tempo da legislação tratando sobre violação não consentida da intimidade

1942	**2008**	**2014**	**2018**	
Código Penal	**Estatuto da Criança e do Adolescente**	**Lei nº 12.965**	**Lei nº 13.718**	**Lei nº 13.772**
Crimes contra a honra e lesão corporal (violência psicológica)	Crimes do art. 241-A e seguintes	Remoção de conteúdo – Art. 21 Ação nos Juizados Especiais – Art. 22	Divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia – Art. 218-C	Registro não autorizado da intimidade sexual – Art. 216-B CP Violação da intimidade = violência psicológica – Art. 7, II, Lei Maria da Penha

Fonte: Produzido pelo autor (2023).

Há que se perceber que, quanto a este tema de proteção à intimidade da mulher, visando a criminalização da pornografia de vingança e a exposição íntima de pessoas, o movimento feminista o auxiliou a formatar, pois o "*revenge porn*, além de denunciar a identidade social em uma logística patriarcal e secundária, também revela uma violência de gênero no contemporâneo que conduz a um dispositivo de poder" (SALES; ELIHIMAS; ELIHIMAS, 2018, p. 105). O foco, então, desse processo criminalizante é de desafiar o sistema patriarcal dominante e estabelecer a igualdade normativa como condição de igualdade efetiva e real da mulher.

De outra parte, numa análise feita por Sydow (2016, p. 23), então referente aos projetos de lei que buscavam a criminalização da conduta sob óticas diversas,

> As figuras penais propostas com cuidado trazem importante avanço vitimodogmático ao apresentar que o delito é considerado consumado mesmo que a vítima tenha consentido na captura ou armazenamento da imagem ou comunicação, no sentido de que sua contribuição no cometimento do delito está limitada àquilo sob seu controle, mas não às consequências ilícitas advindas de seu ato.

Referia-se o autor a três projetos diferentes: PL nº 1.676/2015 (objetivava criminalizar a publicação/divulgação sem autorização ou com "objetivos não lícitos"); PL nº 6.630/2013 (objetivava criminalizar a "divulgação indevida de material íntimo"); e PL nº 7.377/2014 (objetivava criminalizar a "violação da privacidade"). O PL nº 6.630/2013, que tinha como apenso o PL nº 7.377/2014[160], teve declarada sua prejudicialidade em face dos encaminhamentos dados ao PL nº 5.555/2013; já o PL nº 1.676/2015, que tem 28 projetos apensados a ele, está anexado ao PL nº 2.630/2020[161], ou seja, ainda segue em análise. Como apontado por Sydow (2016), os enfoques dos projetos, não considerados pelo tipo penal, continham um propósito vitimodogmático, o que é importante no contexto dos estudos sobre cibercriminalização [a partir da criminologia crítica].

Por outro lado, em correlação às observações sobre a estruturação normativo-penal da conduta divergente de registro ou divulgação não consentida da intimidade, integrando-a às observações realizadas pelos entrevistados, verifica-se que, além de ocorrerem vários casos (07PB, 12PI, 24PA), entendem eles que poderia haver um aumento de pena para os casos de

---

[160] Além do PL nº 7.377/2014, o PL nº 6.630/2013 tinha como apensos: PL nº 6.713/2013; PL nº 6.831/2013 (1); PL nº 5.647/2016; PL nº 3.158/2015 (1); PL nº 5.862/2016; PL nº 5.632/2016; PL nº 6.668/2016.

[161] Pesquisa feita em 09 jan. 2023. O PL 2630/2020 tem outros 87 projetos de lei apensados. Este tema será analisado no tópico de projetos de lei sobre *fake news* (ver 4.3.2).

compartilhamento e armazenamento de pornografia (07PB). Novamente, há a compreensão de que a efetividade da persecução criminal ocorre em razão da restrição da liberdade.

4.2.1.6 Da informação e comunicação via Internet ao induzimento, à instigação ou ao auxílio a suicídio ou a automutilação [autolesão]

O crime de indução e instigação ao suicídio não é recente. Porém, o tema da instigação e do induzimento ao suicídio ou à automutilação ganhou espaço na mídia no decorrer da segunda década deste século, com os 'jogos mortais' chamados de 'baleia azul'[162] e 'jogo da asfixia'[163]. O debate legislativo perdurou por 4 anos no Congresso Nacional, iniciando-se uma discussão por dois anos no Senado Federal, com o PLS nº 664/2015, passando por um período similar na Câmara dos Deputados, casa legislativa na qual tramitavam 19 projetos sobre o assunto[164]. O PL nº 8.833/2017 foi aprovado, porém somente com a tipificação penal, deixando de lado, por exemplo, a proposta prevista no PL nº 6.989/2017 (alteração do Marco Civil da Internet, Lei nº 12.965/2014), para incluir procedimento de retirada de conteúdos que induzam, instiguem ou auxiliem a suicídio de aplicações de Internet.

Em razão da aprovação de um substitutivo na Câmara dos Deputados, o PL nº 8.833/2017 retorna ao Senado Federal como PL nº 6.389/2019, sendo aprovado em dois meses, transformando-se na Lei nº 13.968/2019, que trouxe a modificação da redação do art. 122 do Código Penal, tratando não só do induzimento, da instigação ou do auxílio a suicídio, mas também da automutilação (por exemplo, os casos provocados pelo jogo 'baleia azul').

As punições previstas são maiores no caso de resultado com lesão corporal grave ou morte, podendo-se aplicar a pena (a) em dobro nos casos de a conduta ser realizada por meio da rede de computadores, de rede social ou transmitida em tempo real (art. 122, § 4º) e, ainda, (b) aumentá-la em metade se o agente é líder ou coordenador de grupo ou de rede virtual (art. 122, § 5º). As condições de vulnerabilidade também foram consideradas, assim como os

---

[162] 'Jogo' virtual surgido de uma falsa notícia e que, segundo Barreto Júnior e Lima (2017), "consiste em cinquenta desafios diários enviados por um curador, sendo que o último desafio consiste em retirar a própria vida".

[163] Conforme Guilheri, Andronikof e Yazigi (2017, n.p) "Os 'jogos de asfixia' ou de não oxigenação são comportamentos de risco autoinfligidos individual ou coletivamente, por crianças ou adolescentes, por meio do uso de técnicas de apneia, de estrangulação ou de compressão afim de obter um breve estado de euforia, podendo conduzir a um desmaio voluntário ou acidental, às vezes letal".

[164] PL nº 6.989/2017 (14), PL nº 7.047/2017 (9), PL nº 7.430/2017 (3), PL nº 7.506/2017, PL nº 7.538/2017, PL nº 3.632/2019, PL nº 7.441/2017 (1), PL nº 310/2019, PL nº 1.570/2019 (2), PL nº 1.670/2019 (1), PL nº 4.930/2019, PL nº 7.458/2017 (1), PL nº 3.496/2019, PL nº 7.460/2017, PL nº 7.917/2017; PL nº 511/2015 (2), PL nº 10.603/2018 e PL nº 5.197/2019.

casos de lesão corporal grave ou gravíssima e os casos de morte de pessoas com menos de 14 anos são consideradas, respectivamente, lesão corporal de natureza grave ou gravíssima e homicídio.

Neste caso não se levou em conta nenhum estudo acadêmico para criminalizar a indução à automutilação, pois meios de comunicação de massa (MCM), os *media*, exerceram o protagonismo da informação (BUDÓ, 2008; 2012; 2013), e as teorias da comunicação propiciam(ram) a notícia em detrimento da opinião científica. Os casos 'baleia azul' eram noticiados cotidianamente sob a ótica do induzimento e nenhum trabalho acadêmico relevante pode ser considerado, tendo o auge da exploração pelos *media* no ano de 2017[165]. Ou seja, a realidade social foi moldada tão-somente a partir dos meios de comunicação e foi absorvida como 'verdade' pelo sistema político em seu processo legislativo.

Por outro lado, em trabalho publicado na Espanha, Guadix *et al.* (2020, p. 12) observam que

> Las motivaciones más frecuentes para implicarse en autolesiones online fueron: 1) hacerlo como una expresión de malestar; 2) buscar desahogo o alivio; 3) buscar la atención y comprensión de otros; 4) ver la reacción de otros; 5) porque consideraban que era gracioso; y 6) porque otros lo hacen o es "una moda".

Ou seja, segundo o estudo hispânico, as autolesões não foram induzidas dolosamente por outras pessoas, embora fossem praticadas porque outros a praticam. A influência dos *media* no Brasil, então, produziu mais efeitos na criminalização que eventuais estudos técnicos, que sequer foram considerados para a produção normativa. Também, dados estatísticos podem sequer ter sido levantados a respeito para análise legislativa da proposta de tipificação. Observa-se, ainda, a partir das entrevistas, que nenhum dos entrevistados menciona essas circunstâncias factuais como foco principal ou acessório dos órgãos de investigação cibernética.

4.2.1.7 Perseguição em tempos cibernéticos e a construção do tipo penal de *stalking*

[165] O Google Trends indica que o tópico 'baleia azul', como assunto pesquisado na Internet, bem como as variações de sua pesquisa, esteve no auge, no Brasil, no início de 2017, conforme indica o link disponível em https://trends.google.com.br/trends/explore?date=all&geo=BR&q=%2Fg%2F11c7190bky (acesso em 09 jan. 2023), justamente quando houve a apresentação de muitos projetos legislativos e no ano em que houve a aprovação do substitutivo na Câmara dos Deputados. O tema continuou, a partir de então, a ser objeto de pesquisa constante no Brasil (BALEIA, 2023).

"A gente tem amadurecido um pouco, incluindo o crime de *stalking*, que também precisava de um normativo pra responsabilizar pessoas que perseguiam outras na Internet". A observação de 02BA sobre a perseguição virtual deixa evidente a expectabilidade quanto ao tipo penal, embora também haja frustração quanto à pena a ele prevista, conforme refere 16ES: "para os crimes *stalking*, as penas são muito baixas".

Expectável, a proposta de criminalização do *stalking* vinha sendo discutida desde 2009, com base no PL nº 5.419/2019, que possuía agregados outros onze projetos normativos[166]. Um deles, o PL nº 1.369/2019, acabou por se tornar a principal referência de discussão legislativa e foi transformado, após aprovação no Senado Federal, na Lei nº 14.132/2021.

A proposta que acabou transformada em Lei e que alterou o Código Penal foi oriunda do Senado Federal (PL nº 1.369/2019), voltando àquela casa em virtude da alteração proposta na Câmara dos Deputados. A aprovação da nova norma penal também foi pauta do movimento feminista (SENADO, 2021a), com movimento direcionado no Dia Internacional da Mulher e votação do dia subsequente (SENADO, 2021b). Além de definir o delito de 'perseguição' reiterada[167], também a Lei nº 14.132/2021 revogou o art. 65 da Lei de Contravenções Penais, ou seja, o delito de perturbação da tranquilidade, um dos meios aptos de enquadramento até então existentes.

O *cyberstalking* (PIRES; SANI; SOEIRO, 2018), conduta danosa provocada com utilização de criação sistemática de perfis falsos, comentários, *folows*, rastreamentos indevidos, monitoramentos digitais, envio reiterado de e-mails etc., está contemplado na nova redação. Também o envio reiterado de PIX (meio de pagamento rápido), com ameaças (DUTRA, 2022; SANDRE, 2022) e mensagens, também pode configurar a perseguição reiterada e, inclusive, possibilitar a aplicação da Lei Maria da Penha [em razão da violência psicológica envolvida].

---

[166] Apensados ao PL nº 5.419/2009 (11): PL nº 5.499/2009 (1), PL nº 946/2019; PL nº 1.291/2019; PL nº 2.332/2019 (1); PL nº 2.332/2019; PL nº 3.544/2019; PL nº 2.723/2019; PL nº 3.484/2019 (1), PL nº 6.521/2019; PL nº 3.042/2019; PL nº 1.696/2019; e PL nº 4.411/2020.

[167] Definição penal do delito de "perseguição":

"Art. 147-A. Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade.

Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa.

§ 1º A pena é aumentada de metade se o crime é cometido:

I – contra criança, adolescente ou idoso;

II – contra mulher por razões da condição de sexo feminino, nos termos do § 2º-A do Art. 121 deste Código;

III – mediante concurso de 2 (duas) ou mais pessoas ou com o emprego de arma.

§ 2º As penas deste artigo são aplicáveis sem prejuízo das correspondentes à violência.

§ 3º Somente se procede mediante representação".

Mas a construção da realidade normativo-penal em razão da utilização da rede de computadores, seja privada, seja mundial, não parou por aí, tendo havido, no período da pandemia, um aumento do uso da Internet e uma migração criminal, conforme se observa no subtópico a seguir.

4.2.1.8 Tipologias específicas inseridas na estrutura normativo-penal brasileira: furto mediante fraude e fraude eletrônica

Conforme análise no capítulo anterior, as expectativas e frustrações dos atores de investigação cibernética são constantemente relacionadas aos casos de estelionatos e fraudes cometidos pela Internet, especialmente por, em regra, não gerar prisão dos autores identificados na investigação policial. Cumpre compreender, no entanto, como se deu a construção socionormativa, a partir das notícias e do legislativo brasileiro, dessas condutas específicas, que afetam pessoas, mas sobretudo o sistema financeiro brasileiro (bancos e *fintechs*), que contemplam um fator de influência econômica sobre os sistemas sociais no Brasil[168].

A Lei nº 14.155/2021, já tratada no tópico sobre invasão de dispositivo informático (4.2.1.4), trouxe duas inovações penais para o código penal: (a) o furto mediante fraude cometido por meio de dispositivo eletrônico ou informático e (b) o estelionato eletrônico [como mencionam os entrevistados], ou melhor, a fraude eletrônica [como diz o texto legal]. Antes de analisar especificamente os tópicos, há que se reafirmar, por observações de segunda ordem, o papel construtor da realidade social, sobre o cibercrime durante a pandemia da Covid-19, dos *mass media*.

Então, a contextualização sobre a construção social da realidade (AUGSTEN; WENDT, 2021, p. 1535-1541), para o cenário da pandemia e a exploração do aumento dos casos de crimes praticados no contexto da Internet, passa pela constatação de que a comunicação do sistema específico dos *media* com o cibersistema da Internet e o sistema Político, cada um por meio de suas funções, gera o acréscimo normativo no sistema do Direito, estruturando aquelas expectativas advindas dos demais sistemas psíquicos e sociais. Veja-se estruturalmente uma linha do tempo, em quatro atos, dada como exemplo:

---

[168] Sobre a influência dos agentes econômicos na formatação dos demais sistemas, vide (GARCÍA LUNA; PEÑA LABRIN, 2017).

1 – No ano de 2020 várias notícias são veiculadas com os enfoques de aumento da criminalidade cibernética. Foram selecionadas sete notícias, a partir de abril de 2020: “PF alerta para aumento nos crimes cibernéticos durante a pandemia” (PF ALERTA, 2020); “Criminosos aproveitam pandemia de Covid-19 para aplicar golpes virtuais” (COLUCCI, 2020); “Cibercrime: ataques no Brasil aumentam mais de 300% com a pandemia” (ROLFINI, 2020); “Interpol alerta para crescimento de crimes virtuais durante a pandemia” (VITTA, 2020); “A pandemia de cibercrime: por que os ataques de *ransomware* estão disparando?” (SANTINO, 2020); “País tem aumento de crimes virtuais durante a pandemia” (IMENES, 2020); “Prejuízo global do cibercrime passa de US$ 1 trilhão, diz McAfee” (ARBULU, 2020). Esta última notícia foi veiculada no dia 07/12/2020, quando proposto o PL referido no tópico seguinte;

2 – No final de 2020 (07/12/2020), o PL nº 4.554/2020 é analisado na Câmara dos Deputados, tendo passado por análise anterior do Senado Federal, conforme já abordado, objetivando alterar o Código Penal e tornar mais graves os crimes de violação de dispositivo informático, tipificar o furto mediante fraude e a fraude eletrônica, todos cometidos de forma eletrônica ou pela Internet;

3 – Após a proposta de lei e no decorrer do primeiro semestre de 2021, várias outras notícias são divulgadas pelos veículos de âmbito nacional sobre o aumento da criminalidade no ambiente cibernético: “Brasil figura como um dos países com mais ameaças cibernéticas do mundo em 2020” (BRASIL FIGURA, 2020); “Ameaças cibernéticas crescem 394% durante a pandemia” (MANSUR, 2021); “Com 17.843 ocorrências, crimes cometidos pela internet sobem 87,1% em 2020” (DIOGO, 2021); “Estelionato na internet cresceu mais de 1.200% no DF durante pandemia” (CARONE, 2021); “Crimes cibernéticos contra mulheres aumentam durante pandemia” (CRIMES CIBERNÉTICOS, 2021); “Crimes digitais têm forte alta em vários estados; saiba como prevenir” (GOUSSINSKY, 2021); “A pandemia de golpes digitais no Brasil” (TONDO, 2021).

4 – No final de maio de 2021 é sancionada a Lei nº 14.155/2021, incrementando tipos e penas no Código Penal e modificando a competência no Código de Processo Penal:

> Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato (BRASIL, 2021b).

Com a alteração legislativa, com trâmite célere nas duas casas legislativas – 9 meses – , estruturou-se a:

Tipologia de furto mediante fraude: houve inserção de dois parágrafos no art. 155 do Código Penal, sendo um principal e outro de acréscimo de penas:

> Art. 155. [...]
> § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
> § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
> I – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional;
> II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável.

O § 4º-B do art. 155 do Código Penal reproduziu a pena do furto qualificado e é um tipo penal consolidativo do já entendimento jurisprudencial brasileiro (BRASIL, 2007[169]; BRASIL, 2008[170]) no sentido de que o acesso indevido e a subtração de valores de contas bancárias se caracterizam como furto mediante fraude, sejam eles baseados ou não em violação de mecanismos de segurança, do dispositivo ou sistemas informáticos, ou com "utilização de programa malicioso", ou seja, programa com captação de informações hábeis à prática da subtração. Ainda previu a prática da subtração com a atuação criminosa prévia mediante a utilização de "qualquer outro meio fraudulento análogo", ou seja, inserindo a prática delitiva da pescaria virtual (*phishing scam*) com consequente subtração de valores.

Tipologia de fraude eletrônica: houve o acréscimo, no art. 171 do Código Penal, de dois parágrafos e a alteração de outro:

---

[169] CONFLITO DE COMPETÊNCIA. TRANSFERÊNCIA BANCÁRIA FRAUDULENTA VIA INTERNET. FURTO QUALIFICADO. COMPETÊNCIA - LOCAL DA CONSUMAÇÃO. 1. A transferência bancária fraudulenta operada por via virtual constitui crime de furto qualificado, previsto no artigo 155, § 4º, do Código Penal. 2. Dá-se a consumação do delito quando o bem subtraído sai da esfera de disponibilidade da vítima, mediante o débito lançado na conta em poder da instituição financeira depositária. 3. A competência é definida pelo juízo com jurisdição no local em que situada a agência bancária detentora da conta alcançada. 4. Precedentes (STJ e TRF4ªR). (TRF-4 - CC: 16796 PR 2007.04.00.016796-0, Relator: AMAURY CHAVES DE ATHAYDE, Data de Julgamento: 24/09/2007, QUARTA SEÇÃO, Data de Publicação: D.E. 10/10/2007)

[170] PENAL. FURTO QUALIFICADO (FRAUDE). ART. 155, § 4º, II, DO CP. TRANSFERÊNCIA BANCÁRIA FRAUDULENTA VIA INTERNET. Responde pelo delito de furto qualificado pela fraude aquele que, sem autorização do titular da conta corrente, realiza transferências de valores depositados em agência bancária, por meio da internet. (TRF-4 - ACR: 14815 PR 2002.70.00.014815-4, Relator: ARTUR CÉSAR DE SOUZA, Data de Julgamento: 30/07/2008, OITAVA TURMA, Data de Publicação: D.E. 13/08/2008)

> Art. 171. [...]
> Fraude eletrônica
> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.
> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.
> [...]
> Estelionato contra idoso ou vulnerável
> § 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso.

Os dois primeiros parágrafos tratam de penas específicas e aumento de pena, respectivamente, § 2º-A e § 2º-B do art. 171, para os casos de estelionato cometidos com a utilização de informações coletadas por meio das redes sociais, contatos telefônicos ou e-mails, fornecidas pela vítima ou terceiro induzido a erro. Também, há prática do delito se há utilização de qualquer outro meio fraudulento para obtenção do dado, como, por exemplo, a utilização de aplicativos com autenticação em redes sociais e/ou telefones e e-mails, ou, ainda, por meio de páginas de cadastros e coleta de dados (*phishing scam*).

Já o §4º do art. 171 sofreu uma alteração para contemplar o aumento de pena no caso da prática de crimes contra idosos ou vulneráveis, "considerada a relevância do resultado gravoso". Há que se considerar que o § 5º não sofreu alteração, exigindo, em regra, a representação para que o crime de estelionato seja investigado.

Não bastasse a tipificação, ainda restam, por parte dos entrevistados, expectativas cognitivas sobre condutas que não seriam necessariamente enquadráveis nos referidos delitos ("A questão dos bancos (PIX)", conforme 11AM). Outras observações dos entrevistados merecem destaque:

> As leis não são suficientes para o estelionato, furto mediante fraude, furtos eletrônicos, porque mesmo responsabilizando os autores, mesmo presos, continuam cometendo o crime, até de dentro do presídio. [...] o estelionato e furto mediante fraude tiveram aumento de pena, recentemente, para diminuição de crimes cometidos pela Internet, porém, na prática, a sensação é que nada mudou. Porque os autores não são responsabilizados, tanto faz a pena ser de cinco anos, de dez anos ou de quinze anos, pois se não são responsabilizados, esse tempo não faz nenhuma diferença. (13AL).

Porém, há também observações sobre e melhoria em relação aos enquadramentos às situações fáticas:

> O furto qualificado usamos para invasão de contas correntes, não sei se necessita de tipo penal. O estelionato, agora com a fraude eletrônica, melhorou, ajudou

> muito, a própria alteração do crime de invasão, em que tirou a especificidade "mediante violação de mecanismo de segurança", ficou muito bom. (14PR).
> Pensando nos crimes penais mais comuns que utilizo, a fraude eletrônica (artigo 171, parágrafo A) e o furto qualificado mediante dispositivo eletrônico (artigo 4ºB), esse melhorou a pena, mas a pena de fraude eletrônica é muito pequena. (18RO).
> Por exemplo essa parte de crimes patrimoniais, recentemente, houve aumento de penas, de estelionato pela Internet e de furto mediante fraude, então isso veio a corrigir uma distorção, porque tínhamos furto de objeto comum comparado com furto pela Internet, na qual é muito mais complexo. Então, acredito que nos crimes patrimoniais, na parte de direito penal, nossa legislação atende bem. (19DF).

A realçar, também, sobre as observações dos entrevistados, que apenas três não se referem à palavra estelionato (05AC, 10SC e 23MG), porém, se referem ao termo fraude. Este termo, por sua vez, não é referido por apenas quatro entrevistados (01GO, 20RR, 21RN e 24PA). Já a palavra furto é referida por metade dos entrevistados. A partir das observações sobre as perspectivas dos entrevistados é que se optou por analisar em conjunto esses dois tipos penais estruturados no Código Penal em 2021. Da mesma forma, a partir da observação de um entrevistado apenas, que expectava um tipo penal em específico, é que se optou por analisar a fraude relacionada a criptoativos no próximo subtópico.

4.2.1.9 A estruturação normativa sobre os ativos virtuais e a tipificação penal de fraude com sua utilização

A utilização de criptomoedas ou criptoativos nas ações criminosas na rede de computadores é uma preocupação por parte dos entrevistados, por três motivos: primeiro, pela falta de conhecimento e softwares capazes de monitorá-los; segundo, pela dificuldade investigativa; terceiro, a regulamentação [penal etc.].

O entrevistado 07PB refere que "tem grande demanda envolvendo crimes de criptoativos na *dark web* e temos muitas dificuldades com essas investigações". Já o entrevistado 16ES menciona que "os crimes de criptomoedas são poucos, não temos ferramenta de análise boa". Aliás, esta falta de ferramentas de análise é referida também pelos entrevistados 01GO e 14PR.

Já o entrevistado 23SP, cuja delegacia em que trabalha tem a função de investigar casos de lavagem de dinheiro no contexto da Internet, tenciona que

> em razão da atribuição da delegacia, trabalhamos com questões de lavagem de dinheiro. Dentro desse cenário, o que está sendo mais desenvolvido tem a ver com a utilização de criptoativos (criptomoedas). Então estamos buscando um

> aprendizado constante, porque a utilização desses recursos, para investigação da polícia, é algo novo.
> [...]
> Não temos uma regulamentação na utilização das criptomoedas, dos criptoativos, consequentemente, traz dificuldade para investigação, também para localização e rastreamento para seguir esses valores e recuperá-los. Então, são utilizados mecanismos jurídicos postos à disposição dos crimes mais comuns para que consigamos adequar e dar o resultado efetivo à sociedade, mas faltam algumas coisas. Por exemplo a regulamentação (questão regulatória) de utilização de criptoativos, que permitiria maior eficiência nas investigações ou o entendimento mais fácil do seu funcionamento. (23SP).

O entrevistado 20RR comunga do mesmo pensamento, especialmente com relação à regulamentação penal:

> Mas nos crimes de lavagem de dinheiro com criptomoedas, ainda estão muito incipientes, tentamos colocar na lavagem de dinheiro essa utilização das criptomoedas, mas fica vago, a investigação é difícil, nesse sentido, acredito que deveria ter um tipo penal de lavagem de dinheiro com criptomoedas, com pena maior, com majorante, com qualificadora, como está sendo atendido na maioria dos crimes cibernéticos. (20RR).

Seis entrevistados teceram observações sobre os criptoativos, expectando cognitivamente regulamentação e, também, solução investigativa. Após a realização das entrevistas, acabou sendo aprovada, em legislação específica, por meio da Lei nº 14.478/2022[171], a definição de "ativo virtual", que é, segundo art. 3º, a "a representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para realização de pagamentos ou com propósito de investimento". A mesma lei regulamentou a prestação de serviços envolvendo ativos virtuais.

Ainda, veio a estruturar o tipo penal de "fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros", previsto no art. 171-A[172], bem como incrementar a pena do crime de lavagem de dinheiro (art. 1º, §4º, Lei nº 9.613/1998)[173], ou seja, a expectativa dos entrevistados foi contingenciada com a estruturação penal referida: novo tipo penal e aumento da pena privativa de liberdade.

No período de tramitação, o então PL nº 2.303/2015 (PL nº 4.401/2021) passou por vários estágios e discussões (GUIMARÃES, 2022), com múltiplas audiências públicas, nas

---

[171] A Lei nº 14.478/2022 originou-se na Câmara dos Deputados com o PL nº 2.303/2015 – que recebeu numeração nova em 2021: PL nº 4.401/2021 (Câmara e Senado).

[172] Diz o tipo penal do art. 171-A, com pena de quatro a oito anos: "Organizar, gerir, ofertar ou distribuir carteiras ou intermediar operações que envolvam ativos virtuais, valores mobiliários ou quaisquer ativos financeiros com o fim de obter vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento".

[173] Sobre a correlação de criptoativos e lavagem de dinheiro, vide (WEISHEIMER *et al.*, 2022).

quais também foram ouvidos Delegados de Polícia Civil e Federal, pesquisadores e doutrinadores, empresários e investidores em criptoativos.

No entanto, permanecem as expectativas sobre a estrutura de investigação, capaz de auxiliar na efetividade da resposta na persecução desse e outros delitos em que os ativos virtuais, os criptoativos, são utilizados. As expectativas cognitivas em relação à qualificação dos servidores policiais, que podem ocorrer no âmbito dos Estados ou da União, bem como buscada no setor privada, podem ser supridas com decisões dos sistemas organizacionais nesse âmbito, tal qual delineado no Mato Grosso, como "aprendizado obrigatório de novos agentes" (BERTOLUCCI, 2022).

> No caso das criptomoedas, o ensino sobre o tema deve ocorrer para os cargos de Delegado, Escrivão e Investigador. Ou seja, todos os novos agentes da polícia civil devem obrigatoriamente aprender sobre a tecnologia financeira, na área temática de "Inteligência Policial".
> Durante a disciplina que contém as criptomoedas, os agentes também estudam sobre Inteligência financeira, afastamento de sigilo bancário e fiscal, análise de vínculos, entre outros mais. (BERTOLUCCI, 2022, n.p.).

Sobre a capacitação nessa área específica de investigação cibernética, a dos criptoativos, o treinamento de habilidades conjuntas é destacado por Wendt e Zumas (2022, p. 21):

> De longe inferimos que equipes especializadas em investigações cibernéticas e financeiras não serão capazes de ser bem-sucedidas em investigações envolvendo criptoativos, pelo contrário, apontamos a real necessidade da união de conhecimentos em ambas as searas a fim de potencializar a eficiência das ações repressivas.
> Habilidades complementares (*ciber* e financeira) somadas a conhecimentos pontuais do ecossistema cripto são a chave para o sucesso. A interdisciplinaridade revela-se de suma importância no combate à criminalidade atual, que vem se aproveitando do desconhecimento estatal para investigar ações criminosas envolvendo criptoativos.

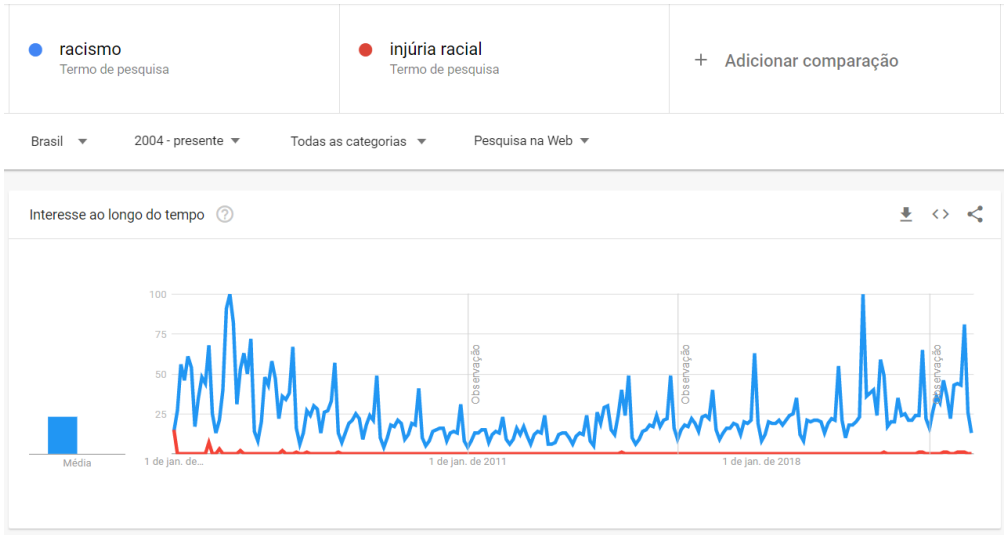
A qualificação dos policiais torna-se, então, necessária e é pautada, segundo Amaro (2020), por projeto que objetiva incentivar e promover a capacitação de agentes em Cooperação Jurídica Internacional. O projeto Grotius Brasil, iniciado em 2010, foi renovado em 2021[174], mantendo uma correlação entre os temas da investigação cibernética, cooperação penal e lavagem de dinheiro (BRASIL, 2022b).

[174] O GROTIUS teve renovada recentemente a sua base normativa por meio da Portaria Senajus/MJSP nº 36, de 10 de dezembro de 2021 (BRASIL, 2022).

4.2.1.10 Racismo e injúria racial: a reestruturação dos tipos penais e o cibersistema da Internet

O racismo é uma conduta bastante destacada pela mídia no Brasil, em vários aspectos, incluindo futebol e mídias sociais. Também é um termo frequentemente pesquisado na Internet, conforme dados do Google Trends:

Figura 12: Incidência das pesquisas sobre racismo no Brasil



Fonte: Google Trends, período de janeiro de 2004 a janeiro de 2023.[175]

Como se abordará no próximo tópico, relativo à parte processual, a Lei nº 7.716/1989, dos crimes de preconceito, contempla formas de remoção e retirada de conteúdo racista, em razão de dois acréscimos normativos, em 2010 e 2012. No início de 2023 foi sancionada a Lei nº 14.532[176], que alterou o Código Penal e a Lei em comento.

Com a nova norma sobre racismo e injúria racial, este delito, antes previsto no Código Penal, foi 'transportado' para a lei dos crimes de preconceito, porém com uma pena maior e com a característica de inafiançabilidade, expressamente prevista constitucionalmente (art. 5º, XLII, CF). Diz o dispositivo sobre o crime de injúria:

[175] Pesquisa feita em 12 jan. 2023 mostra um constante interesse no tema do racismo por parte dos internautas. Vide Google Trends: https://trends.google.com.br/trends/explore?date=all&geo=BR&q=racismo,inj%C3%BAria%20racial.

[176] A lei derivou do antigo PL nº 1.749/2015 da Câmara dos Deputados, recebendo nova numeração em 2021: PL nº 4.566/2021, com trâmite de sete anos nas casas legislativas.

> Art. 2º-A Injuriar alguém, ofendendo-lhe a dignidade ou o decoro, em razão de raça, cor, etnia ou procedência nacional.
> Pena: reclusão, de 2 (dois) a 5 (cinco) anos, e multa.
> Parágrafo único. A pena é aumentada de metade se o crime for cometido mediante concurso de 2 (duas) ou mais pessoas.

Com a alteração advinda da nova lei, a injúria qualificada, prevista no Código Penal, será tão-somente a correspondente aos "elementos referentes a religião ou a condição de pessoa idosa ou com deficiência", ou seja, as referências à religiosidade, etarismo e capacitismo (art. 140, §3º, do CP), com pena de um a três anos de reclusão, além da multa. Então, os casos de injúria, com ofensa à dignidade ou ao decoro, decorrentes da raça, etnia ou procedência nacional ('racismo regional'), possuem, a partir do art. 2º-A, uma pena de reclusão de dois a cinco anos, além da multa, podendo ser aumentada se cometida em concurso de agentes.

A nova lei também previu pena similar, acrescida da proibição de frequência, para os casos em que a prática, a indução ou incitação à discriminação[177] ou preconceito de raça, cor, etnia, religião ou procedência nacional, for "cometida no contexto de atividades esportivas, religiosas, artísticas ou culturais destinadas ao público" (art. 20, caput, e § 2º-A, da Lei nº 7.716/1989).

A pena de reclusão e multa é prevista também quando estes crimes forem cometidos "por intermédio dos meios de comunicação social, de publicação em redes sociais, da rede mundial de computadores[178] ou de publicação de qualquer natureza" (art. 20, caput, e § 2º, da Lei nº 7.716/1989).

Finalmente, cumpre destacar que se os crimes de injúria racial ou racismo forem cometidos ou por funcionário público (art. 20-B da Lei nº 7.716/1989) ou quando "ocorrerem em contexto ou com intuito de descontração, diversão ou recreação" (art. 20-A da Lei nº 7.716/1989), haverá também um aumento de pena ao autor da conduta divergente.

Embora, nas entrevistas, apenas três atores de investigação cibernética tenham referido o termo "racismo", somente um (16ES) esboçou expectativa quanto ao aumento de pena relativa ao delito analisado, embora tenha mencionado como suficientes os tipos penais existentes e possíveis de enquadramento às situações fáticas registradas na sua delegacia,

---

[177] O legislador entendeu por delinear o contexto-conceitual de "atitude discriminatória" como "qualquer atitude ou tratamento dado à pessoa ou a grupos minoritários que cause constrangimento, humilhação, vergonha, medo ou exposição indevida, e que usualmente não se dispensaria a outros grupos em razão da cor, etnia, religião ou procedência" (art. 20-C da Lei nº 7.716/1989).

[178] Sobre os aspectos conceituais de rede de computadores e rede mundial de computadores, vide Costa, Wendt e Campelo (2022).

mencionando expressamente, além de outros delitos, também o delito de injúria racial. Assim, embora não expectável pelos atores de investigação cibernética, a previsão de aumento de pena quando da prática dos delitos no âmbito da Internet restou possível, especialmente por se referir à "rede mundial de computadores".

***

Analisados, assim, os aspectos penais em dez subtópicos, especialmente sobre as alterações e mutações nos tipos penais brasileiros sob a influência da transformação tecnológica a partir da Internet, há que se focar, também, nas alterações normativas de caráter processual, naturalmente sob a mesma ótica da irritação provocada no sistema jurídico pela comunicação advinda dos sistemas sociais e do cibersistema da Internet, em razão da ampliação do uso da tecnologia digital.

Ainda não há, portanto, elementos para confirmar ou não outra hipótese desta tese: que o legislador brasileiro possui um foco direcionado à área penal, à produção de direito material penal, circunstância que é refletida sobre o sistema de persecução criminal, com medidas limitadas na área processual penal, capazes de reduzir ou mitigar os danos e riscos no ambiente cibernético. Portanto, necessárias são as observações sobre a estruturação normativo-processual penal no Brasil, especialmente no que tange aos mecanismos processuais investigativos e relativos à rede de computadores.

4.2.2 *Timeline* da estruturação da legislação processual quanto à Internet no Brasil

Não há como desprender a legislação penal da previsão de procedimentos adequados constitucionalmente e dentro das regras de respeito aos direitos humanos e fundamentais. Também não há como não vincular os temas, especialmente se partirmos das observações dos atores de investigação criminal, que, em vários momentos, referem suas expectativas e frustrações quanto ao direito penal e processual penal estruturados em relação à investigação cibernética.

Ab initio, importa afirmar que a correta previsão e normatização de procedimentos adequados à formação de provas e à coleta de indícios em investigações criminais e processos, sejam cíveis, sejam criminais, sejam administrativos, evita a violação de direitos e garantias individuais dos investigados.

Por outro lado, a não previsão de medidas procedimentais adequadas pode acarretar um prejuízo à não consecução da persecução criminal, com identificação – célere e em tempo hábil – de provas e evidências que levem à autoria e à materialidade delitiva cibernética. Sob a ótica dos atores de investigação criminal cibernética no Brasil, foram delineadas e condensadas suas expectativas cognitivas sobre as expectativas normativas relativas à estrutura da persecução da criminalidade cibernética (subtópico 3.4.2.3).

A análise da evolução da estrutura normativa atual, tendo por referência a relação com a Internet, ajuda a compreender, por outro lado, como a cultura tecnológica influenciou a formação de uma nova cultura jurídica, especialmente atenta às situações de uso da tecnologia da informação e comunicação para fins de interação social, cultural, econômica e política, não absorvendo, no entanto, as expectativas principais e atuais dos atores de investigação cibernética.

Assim, com base na *timeline* (linha do tempo) a seguir disposta, neste tópico analisar-se-á criticamente esse contexto evolutivo, focado nos aspectos processuais penais brasileiros. Naturalmente, enfoca-se nas normativas que já tenham relação direta e indireta com o sistema da Internet, com recorte nas normativas brasileiras já estruturadas.

Quadro 10: Linha do tempo da legislação processual (procedimental) quanto à Internet no Brasil

1996	**2003**	**2012**	**2013**	**2014**	**2016**	**2017**	**2019**	**2021**
Lei nº 9296	**Lei nº 10695**	**Lei nº 12683**	**Lei nº 12850**	**Lei nº 12965**	**Lei nº 13344**	**Lei nº 13441**	**Lei nº 13964**	**Lei nº 14.155**
Interceptação telefônica, telemática e de informática	CPP – Art. 530 A até I (propriedade intelectual)	Lei de Lavagem de Dinheiro – Art. 17-B	Crime Organizado – Art. 15	Marco Civil da Internet – Arts. 10 e ss.	Lei de Tráfico de Pessoas. Alteração CPP, arts. 13-A e 13-B	Infiltração de Agentes Policiais na Internet – Pedofilia	Infiltração de Agentes Policiais na Internet – Organizações Criminosas e Lavagem de Dinheiro	Art. 70, § 4º: local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção

Fonte: Produzido pelo autor (2023).

O quadro é, no entanto, apenas um referencial para que os tópicos seguintes possam ser aprofundados. Segue-se a análise pontual e conjunta de cada um.

4.2.2.1 Interceptação telefônica, telemática e de informática e captação ambiental de sinais eletromagnéticos, ópticos e acústicos

A Lei nº 9.296/1996 foi sancionada após discussão da regulamentação do inciso XII, parte final, do art. 5° da Constituição Federal, para estabelecer as regras de exceção à inviolabilidade do sigilo das comunicações telefônicas, com exigência de ordem judicial, para fins de investigação criminal ou instrução processual penal. A discussão para aprovação foi de 9 meses, sendo iniciada pelo PL nº 1.156/1995, seguindo para o Senado Federal (PLC nº 4/1996).

A referida normativa estipulou regras de (a) aplicação (concessão e rito processual) da interceptação do fluxo de comunicações telefônicas de qualquer natureza e, também, em sistemas de informática e telemática – arts. 1º ao 9º – e (b) tipo penal quando da violação das comunicações sem a devida autorização – art. 10[179]. Com o advento da Internet e da comunicação por pacote de dados, a interceptação informática ou telemática passou a também ser utilizada, sendo referida por vários entrevistados (nove, ao todo).

No decorrer de mais de 20 anos, vários projetos visaram a alteração, incremento e revogação da Lei nº 9.296/1996, tendo subsistido a ideia de seu incremento processual e penal e de restrição de uso, respectivamente, com a Lei nº 13.964/2019 (Pacote Anticrime)[180] e com a Lei nº 13.869/2019 (Lei de Abuso de Autoridade)[181].

A Lei nº 13.964/2019 inseriu na Lei de Interceptações a regulamentação de outro instituto possível nas investigações criminais, a captação ambiental de sinais eletromagnéticos, ópticos ou acústicos – art. 8º-A –, estipulando regras básicas e possibilitando o uso subsidiário das regras atinentes às interceptações. Assim, é possível a captação ambiental com autorização judicial nos casos de (a) a prova não puder ser feita por

---

[179] Nova redação: "Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei:
Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
Parágrafo único. Incorre na mesma pena a autoridade judicial que determina a execução de conduta prevista no **caput** deste artigo com objetivo não autorizado em lei".

[180] A Lei nº 13.964/2019 teve origem no PL nº 10.372/2018 (Câmara dos Deputados) e no PL nº 6.341/2019 (Senado Federal), ao total com 1 ano e 6 meses de tramitação e debates.

[181] A Lei nº 13.869/2019 teve origem no PLS nº 85/2017 (Senado Federal) e no PL nº 7.596/2017 (Câmara dos Deputados), ao total com mais de dois anos e meio de tramitação e debates.

outros meios disponíveis e igualmente eficazes, (b) houver elementos probatórios razoáveis de autoria e participação em infrações criminais cujas penas máximas sejam superiores a 4 (quatro) anos ou em infrações penais conexas e (c) o requerimento deverá descrever circunstanciadamente o local e a forma de instalação do dispositivo de captação ambiental.

A Lei nº 13.964/2019 também trouxe um novo tipo penal. O art. 10-A tipifica a conduta de, sem autorização judicial, realizar captação ambiental de sinais eletromagnéticos, ópticos ou acústicos para investigação ou instrução criminal[182].

Não diferente, a Lei nº 13.869/2019 também incrementou a Lei de Interceptações com a modificação do único tipo até então existente na norma, ampliando o espectro da ilicitude da conduta para os casos de 'escuta ambiental' ou quebra de segredo da Justiça, quando a violação ocorre nesses casos ou nos casos de interceptações sem a vênia judicial ou com objetivos não autorizados em Lei.

Apesar da previsão normativa, a questão técnico-procedimental e a territorialidade dos servidores das aplicações podem ser empecilhos para a execução de uma ordem judicial concedida no Brasil. São circunstâncias que necessitam, conforme o entrevistado 03BA, de treinamento e orientação, bem como de conhecimentos para além dos atores de investigação criminal cibernética, como o Ministério Público e Poder Judiciário (20RR). Ademais, a carência de softwares para a atividade também é relatada por entrevistados (21RN). Não basta, assim, a estruturação normativa, pois que há necessidade de conhecimentos técnicos, treinamento e capacitação, além de equipamentos e softwares para a execução da medida judicial, respeitando-se, igualmente, a cadeia de custódia da evidência digital.

4.2.2.2 Ritual processual em relação às violações dos direitos autorais e de programa de computador

Tendo sido apontado no tópico anterior as reconstruções da tipologia de violação de programa de computador e dos direitos autorais, embora não relevantemente destacadas pelos entrevistados, cumpre fazer anotações sumárias sobre a parte processual penal, pois a Lei nº

---

[182] "Art. 10-A. Realizar captação ambiental de sinais eletromagnéticos, ópticos ou acústicos para investigação ou instrução criminal sem autorização judicial, quando esta for exigida:
Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
§ 1º Não há crime se a captação é realizada por um dos interlocutores.
§ 2º A pena será aplicada em dobro ao funcionário público que descumprir determinação de sigilo das investigações que envolvam a captação ambiental ou revelar o conteúdo das gravações enquanto mantido o sigilo judicial".

10.695/2003, além de incrementar os verbos penais, punição e modalidade de ação penal relativos às violações dos direitos do autor, também estipulou regras procedimentais próprias em nove artigos inseridos no Código de Processo Penal.

As orientações normativas estipulam regras quanto (a) à apreensão de "bens ilicitamente produzidos ou reproduzidos, em sua totalidade, juntamente com os equipamentos, suportes e materiais que possibilitaram a sua existência" (art. 530-B e 530-C do CPP); (b) à realização de perícia (art. 530-D do CPP); (c) à designação de fiel depositário (art. 530-E do CPP); (d) à destruição da produção ou reprodução apreendida (art. 530-F e 530-G do CPP); (e) ao perdimento dos equipamentos apreendidos (art. 530-G do CPP); e (f) à assistência de acusação para o detentor dos direitos autorais (art. 530-H).

A Lei nº 9.609/1998, referente às violações de direitos sobre a programação de softwares de computadores/dispositivos, estabeleceu que a ação penal e as diligências preliminares de busca e apreensão devem ser precedidas de vistoria, podendo o juiz "ordenar a apreensão das cópias produzidas ou comercializadas com violação de direito de autor, suas versões e derivações, em poder do infrator ou de quem as esteja expondo, mantendo em depósito, reproduzindo ou comercializando" (art. 13). Ainda, o próprio detentor dos direitos sobre o software pode ajuizar ação "para proibir ao infrator a prática do ato incriminado, com cominação de pena pecuniária para o caso de transgressão do preceito" (art. 14, caput), possibilitando-lhe, também, cumular a ação de abstenção de prática de ato com perdas e danos (§ 1º do art. 14).

Tais procedimentos, tanto de uma lei quanto da outra, pressupõem então uma interação do detentor dos direitos autorais ou de programa de computador com a investigação criminal e/ou com o processo criminal[183], visando a produzir elementos que comprovem se tratar de violação total ou parcial dos direitos, bem como possibilitar a realização pericial e direcionar as apreensões e perícias necessárias, levando os dados necessários ao conjunto probatório e abrindo espaço ao contraditório.

4.2.2.3 Regras (estruturadas) para obtenção de dados telemáticos e informáticos

[183] Um exemplo desse trabalho relacional é a já referida Operação 404, deflagada sob coordenação do Ministério da Justiça de Segurança Pública, que, em uma das edições, "cumpriu 25 mandados de busca e apreensão e promoveu o bloqueio e suspensão de 252 sites e 65 aplicativos de *streaming*. Os *apps* eram dedicados à transmissão clandestina de filmes e séries. Além de atingir domínios brasileiros, a 404, desta vez, também derrubou 27 sites do Reino Unido e três dos EUA" (RIENTE, 2020).

A partir do uso da Internet, vários dados vão sendo gerados pela interação entre usuário e máquina. Ao utilizar um site, um aplicativo, uma rede social e/ou um comunicador instantâneo, os dados são gerados nas plataformas pelo simples cadastro e pela conexão e/ou sincronização constante: são os *logs* ou registros, tanto de cadastro quanto de conexão. Os provedores de conexão guardam esses dados justamente para identificar seu usuário e as suas conexões, havendo disparidade quanto à forma de guarda e repasse, em investigações, desses dados, o que já foi observado quando da análise das expectativas e frustrações dos entrevistados (especialmente o tópico 3.4.2).

No Brasil, pela Lei nº 12.965/2015, o Marco Civil da Internet[184] estabeleceu regras aos provedores de conexão e de aplicação (conteúdo) como forma de resguardar direitos e garantias de seus usuários. Surgiu, assim, o limite temporal de guarda de dados de conexão e de dados de aplicação, respectivamente por um ano (art. 13) e por seis meses (art. 15). Esse prazo poderá ser alongado a pedido da autoridade policial ou administrativa ou do Ministério Público (arts. 13, § 2º, e 15, § 2º).

Além disso, o Marco Civil da Internet estipulou como 'regra' do fornecimento de dados mediante ordem judicial, quando o "provedor responsável pela guarda" é obrigado a disponibilizar os registros de conexão e/ou de acesso a aplicações de internet, "de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal" (art. 10, caput, e § 1º). Também se resguardou à vênia judicial o "conteúdo das comunicações privadas" (art. 10, § 2º).

Se a regra é a ordem judicial para o fornecimento dos *logs* de cadastro e de conexão, a exceção, prevista no art. 10, § 3º, diz respeito tão-somente ao acesso aos dados cadastrais que "informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição", ou seja, não podem ser fornecidos, sem ordem judicial, outros dados que não os referidos. O Decreto nº 8.771/2016, que regulamentou o Marco Civil da Internet, estabeleceu o que são "dados cadastrais" no art. 11, § 2º:

> § 2º São considerados dados cadastrais:
> I - a filiação;
> II - o endereço; e
> III - a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário.

[184] O Marco Civil da Internet teve origem em discussão pública nacional e o PL nº 2.126/2011 foi discutido na Câmara por três anos e, sob o PLC nº 21/2014, aprovado no Senado Federal em 2014.

No entanto, eximiu os provedores que não coletarem os dados cadastrais de responsabilidade de repasse às autoridades, informando-as a respeito, conforme o § 1º do art. 11. A autoridade solicitante, igualmente, "deve especificar os indivíduos cujos dados estão sendo requeridos e as informações desejadas, sendo vedados pedidos coletivos que sejam genéricos ou inespecíficos", conforme § 3º do mesmo artigo.

Regras similares – para fornecimento de dados cadastrais sem ordem judicial – já haviam sido previstas em outras normativas e tiveram seguimento em aprovações legislativas sobre outros temas, especialmente lavagem de dinheiro, organizações criminosas e tráfico de pessoas. Vejamos:

- Lei nº 12.683/2012[185], que alterou a Lei nº 9.613/1998, quanto à persecução penal dos crimes de lavagem de dinheiro: previu no art. 17-B que as autoridades policiais e os membros do Ministério Público "terão acesso, exclusivamente, aos dados cadastrais do investigado que informam qualificação pessoal, filiação e endereço", sem necessidade de autorização judicial, mantidos (a) pela Justiça Eleitoral, (b) pelas empresas telefônicas, (c) pelas instituições financeiras, (d) pelos provedores de internet e (e) pelas administradoras de cartão de crédito.

- Lei nº 12.850/2013[186], Lei do Crime Organizado: o art. 15 definiu que tanto o delegado de polícia quanto o representante do Ministério Público podem ter acesso, "independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço", mantidos (a) pela Justiça Eleitoral, (b) empresas telefônicas, (c) instituições financeiras, (d) provedores de internet e (e) administradoras de cartão de crédito. Também, no art. 16, estipulou regra de resguardo de dados, por 5 anos, que as empresas de transporte devem ter sobre os passageiros, regra similar em relação às empresas de telefonia (art. 17).

A Lei do Crime Organizado trouxe um adendo à questão dos dados cadastrais e de sua eventual negativa: um tipo penal específico. Assim, pelo art. 21, estará sujeito a uma pena de 6 (seis) meses a 2 (dois) anos quem (a) recusar ou omitir "dados cadastrais, registros, documentos e informações requisitadas pelo juiz, Ministério Público ou delegado de polícia,

---

[185] A Lei nº 12.683/2012 teve suas discussões iniciadas no Senado Federal por meio do PLS nº 209/2003, passando à Câmara dos Deputados após 5 anos. O PL nº 3443/2008 foi aprovado em texto substitutivo, retornando ao Senado Federal para nova análise em 2011 e, após dois anos, foi aprovado.

[186] A Lei do Crime Organizado teve início de suas discussões no Senado Federal com o PLS nº 150/2006, sendo remetido à Câmara dos Deputados três anos depois. Um substitutivo ao PL nº 6.578/2009 foi aprovado em 2012 e devolvido ao Senado Federal, que, em sua reanálise, de dois anos, aprovou-o.

no curso de investigação ou do processo", e (b) de forma indevida, se apossa, propala, divulga ou faz uso dos dados cadastrais de que trata esta Lei.

Está em curso no Supremo Tribunal Federal a Ação Direta de Inconstitucionalidade 5.063[187], questionando a constitucionalidade e legalidade dos arts. 15, 17 e 21, sob alegação de "que há violação ao artigo 5º, inciso X, da Constituição, que trata da inviolabilidade do direito à intimidade do indivíduo", e, quanto ao art. 21, a proponente da ADI, Associação Nacional das Operadoras de Celulares (Acel), afirma que "a imposição de pena de seis meses a dois anos de reclusão mais multa pela omissão dos dados cadastrais fere o princípio constitucional da proporcionalidade" (OPERADORAS, 2013). Também, para a Acel,

> a norma, ao permitir que o delegado de polícia e o Ministério Público possam requisitar "quaisquer informações, documentos e dados pertinentes à investigação criminal, sem que haja ponderação judicial que determine esta medida", afronta o princípio constitucional de proteção à privacidade e ao sigilo das comunicações. (OPERADORAS, 2013).

Corroborando o posicionamento das operadoras, Moreira (2014) também entende pela violação das normas constitucionais e legais. Navas e Cambi (2018) discordam desse posicionamento e consideram que

> A fim de proteger o direito fundamental à segurança pública e como forma de concretização do princípio da proteção eficiente, deve ser considerada legítima a cessão de dados constantes na Justiça Eleitoral para as autoridades policiais, a exemplo do que já ocorre com membros do Poder Judiciário e do Ministério Público, sem autorização judicial, não apenas nas hipóteses das Leis nº 9.613/98 e nº 12.850/13, com a finalidade de agilizar as investigações criminais.

Verifica-se, de outro lado, que esses entendimentos doutrinários e judiciais sobre o que diz a legislação geram frustrações das expectativas cognitivas [nos atores de investigação cibernética] sobre procedimentos estruturados normativamente e que poderiam auxiliar na resolução dos casos em investigação.

- Lei nº 13.344/2016[188], prevenção e repressão ao tráfico interno e internacional de pessoas e sobre medidas de atenção às vítimas: a normativa inseriu o art. 13-A no Código de

---

[187] Consulta de acompanhamento no STF: http://portal.stf.jus.br/processos/detalhe.asp?incidente=4494216. Pesquisa realizada em 11 jan. 2023, os autos estavam conclusos ao relator.

[188] A Lei nº 13.344/2016 teve origem na Comissão Parlamentar de Inquérito (CPI) do Tráfico Nacional e Internacional de Pessoas no Brasil, que funcionou no Senado entre 2011 e 2012, que gerou o PLS nº 479/2012, remetido à Câmara dos Deputados dois anos depois e, sob o PL nº 7.370, discutido e aprovado em dois anos.

Processo Penal[189] e, diferente das duas legislações anteriores que estipularam o acesso aos dados cadastrais, sem vênia judicial, de determinados segmentos de empresas, houve a autorização de acesso, por parte do Ministério Público e do delegado de polícia, aos "dados e informações cadastrais da vítima ou de suspeitos" de "quaisquer órgãos do poder público ou de empresas da iniciativa privada", devendo o pedido, tratado como requisição, conter (a) o nome da autoridade requisitante, (b) o número do inquérito policial e (c) a identificação da unidade de polícia judiciária responsável pela investigação.

Se a Lei em questão não estipulou o rol de empresas, por outro lado indicou quais os delitos que permitem tal acesso independentemente de ordem judicial: sequestro e cárcere privado, redução à condição análoga à de escravo, tráfico de pessoas, extorsão, extorsão mediante sequestro e ato destinado ao envio de criança ou adolescente para o exterior. Também, é o único dispositivo procedimental que contempla prazo de resposta, pois a requisição deverá ser atendida em até 24 horas (art. 13-A, parágrafo único, do CPP).

A mesma lei acrescentou a possibilidade (art. 13-B do CPP), no caso dos crimes de tráfico de pessoas, que o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante ordem judicial, "às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso", definindo que "sinal" é o "posicionamento da estação de cobertura, setorização e intensidade de radiofrequência" (art. 13-B, § 1º, do CPP), porém (a) sem acesso ao conteúdo da comunicação, sempre dependente de ordem judicial, (b) limitado ao prazo de 30 dias, e (c) para prazos superiores apenas com ordem judicial.

A precaução da escrita normativa quanto à [necessidade da] ordem judicial em relação ao art. 13-B do CPP se justifica, pois que, conforme art. 13-B, § 4º, do CPP, em razão da urgência dos casos e do risco à vida dos envolvidos, uma vez não despachada a manifestação judicial em 12 horas, pode a autoridade competente na investigação requisitar

---

[189] Código de Processo Penal: "Art. 13-A. Nos crimes previstos nos arts. 148, 149 e 149-A, no § 3º do art. 158 e no art. 159 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e no art. 239 da Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), o membro do Ministério Público ou o delegado de polícia poderá requisitar, de quaisquer órgãos do poder público ou de empresas da iniciativa privada, dados e informações cadastrais da vítima ou de suspeitos.
Parágrafo único. A requisição, que será atendida no prazo de 24 (vinte e quatro) horas, conterá:
I - o nome da autoridade requisitante;
II - o número do inquérito policial; e
III - a identificação da unidade de polícia judiciária responsável pela investigação".

> às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso, com imediata comunicação ao juiz.

Às facilidades de interação das autoridades investigativas corresponde a responsabilidade na atuação, porquanto a cláusula da reserva judicial é estabelecedora da garantia do devido processo legal já desde a formatação da peça informativa, o inquérito policial, que deverá ser instaurado em até 72 horas após o registro da ocorrência (art. 13-B, § 3º, do CPP.

As normativas em questão podem auxiliar a agilidade dos processos investigativos e processuais, porém a principal crítica sobre eles é quanto à ausência de controle sobre o que se solicita e em relação ao que é vinculado, não sendo efetivo, assim, documento normativo regulatório, protocolo auxiliar do Poder Judiciário no controle sobre os fornecimentos de dados e ocorrência ou não de violações a direitos e garantias de dados e da comunicação.

O previsto no regulamento do Marco Civil da Internet, Decreto nº 8.771/2016, art. 12, pode ser aplicado como uma das formas de controle:

> Art. 12. A autoridade máxima de cada órgão da administração pública federal publicará anualmente em seu sítio na internet relatórios estatísticos de requisição de dados cadastrais, contendo:
> I - o número de pedidos realizados;
> II - a listagem dos provedores de conexão ou de acesso a aplicações aos quais os dados foram requeridos;
> III - o número de pedidos deferidos e indeferidos pelos provedores de conexão e de acesso a aplicações; e
> IV - o número de usuários afetados por tais solicitações.

No entanto, essa forma de controle é direcionada à Administração Pública e não ao Poder Judiciário. De outra parte, não contemplam as normativas citadas um prazo mínimo e máximo em que a resposta deve ser fornecida pelos provedores, ficando ao alvedrio do tempo e da estrutura de cada serviço. Esta é, sim, uma expectativa de mudança dos atores de investigação criminal, pois frustram-se com a demora na resposta e o alongamento da investigação cibernética.

Por outro lado, a redação do art. 13-B do CPP é um exemplo importante de condicionamento de ações e praticidade temporal e dinâmica da interação dos atores de investigação cibernética com os provedores, tudo pautado na estrutura normativa. Se é exemplo, uma vez estendido e readequado às demais situações, atenderia a grande parte das expectativas cognitivas dos atores de investigação cibernética sobre a estrutura normativo-procedimental.

4.2.2.4 Infiltração de agentes policiais na Internet

A criação e a evolução da Internet permitiram a interação entre pessoas em seus mais diversos níveis, sejam eles públicos ou mais restritos, sejam eles visíveis ou invisíveis. Essa possibilidade de usar o contexto do invisível da rede mundial de computadores e, também, de usar mecanismos aptos a anonimizar a comunicação propiciou também a sua exploração por autores de delitos dos mais diversos, dentre eles a *pedofilia*, o estelionato, a extorsão, a lavagem de dinheiro e o crime organizado, dentre tantos.

Acompanhar essa evolução no contexto de produção de provas e que (a) possam estar de acordo com as normas constitucionais e legais, (b) não serem violadoras de direitos humanos e fundamentais, e (c) respeitadoras dos direitos e garantias fundamentais é importante, não só para a garantia do investigado, mas também para o resguardo de quem realiza a investigação, o ator de investigação cibernética.

Assim, um dos temas que trouxe uma inovação procedimental, de investigação e processo penal, é a possibilidade de infiltração de agentes policiais na Internet. Nesse sentido, duas normativas surgiram a partir de uma discussão legislativa iniciada com o PLS nº 100/2010 no Senado Federal, na CPI da Pedofilia. A matéria teve sequência com a análise da Câmara dos Deputados do Projeto de Lei nº 1.404-B/2011, aprovado com quatro emendas em abril de 2015, sendo, após dois anos de discussão, gerada a Lei nº 13.441/2017.

As normativas até então vigentes[190] apenas se limitaram a citar o "instituto" da infiltração policial, "não o descrevendo em seus pontos e aspectos procedimentais necessários, o que foi feito pela Lei do Crime Organizado (Lei nº 12.850/2013) através dos artigos 3º, VII, e 10 a 14" (WENDT, 2017a, p. 149).

A Lei nº 13.441/2017 estabeleceu procedimentos relativos à infiltração policial de agentes para investigação de crimes contra a liberdade/dignidade sexual de crianças e adolescentes. Com a aprovação dos projetos e sua conversão na Lei nº 13.441/2017, foram acrescidos cinco artigos ao ECA[191], estabelecendo-se a possibilidade de autorização de infiltração de policiais na Internet em casos específicos previstos no caput do art. 190-A da

[190] A infiltração policial foi inicialmente normatizada através dos seguintes atos normativos: no art. 2º, V, da Lei nº 9.034/95; no art. 20 da Convenção das Nações Unidas contra o Crime Organizado Transnacional (Decreto nº 5.015/2004); no art. 50 da Convenção das Nações Unidas contra a Corrupção (Decreto nº 5.687/2006); e no art. 53, I, da Lei nº 11.343, de 23 de agosto de 2006, chamada de "Lei de Drogas".

[191] São os artigos 190-A, 190-B, 190-C, 190-D e 190-E, Lei nº 8.069/1990.

Lei nº 8.069/1990, ou seja, *numerus clausus*, não podendo ser ampliada por entendimento de delegado de polícia, membro do Ministério Público ou do magistrado.

Já a Lei nº 13.964/2019 inseriu na Lei do Crime Organizado os arts. 10-A, 10-B, 10-C e 10-D, permitindo a ação de "agentes de polícia infiltrados virtuais" na Internet, obedecidos os requisitos estipulados para o infiltração 'normal' prevista no art. 10, com o fim de investigar os crimes previstos na Lei nº 12.850/2013 e a eles conexos, 'praticados por organizações criminosas', desde que (a) demonstrada sua necessidade e (b) indicados o alcance das tarefas dos policiais, (c) os nomes ou apelidos das pessoas investigadas e, (d) quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas.

O parâmetro de normatização seguiu o da Lei já autorizativa para os casos de *pedofilia*, especialmente em razão dos requisitos para admissão, tempo de execução, forma de relatórios e resguardo do agente policial infiltrado 'virtualmente'.

Na concepção de Bini (2017, p. 108-109),

> a norma brasileira é clara quanto à preservação da identidade, imagem e voz do infiltrado, objetivando salvaguardar o agente, sua família, amigos e rede de relacionamentos, pois, caso contrário, dificilmente o infiltrado atuará em outras operações e isso pode desestimular voluntários para futuras operações.

Acompanha-se Bini (2017, p. 109) no argumento de que a "proporcionalidade deve ser a viga mestra já no pedido inicial da medida, sendo seguida na autorização judicial, bem como conduzindo a atuação do policial infiltrado".

Os limites da atuação e as principais regras da infiltração de agentes policiais na Internet foram estipulados nas normas citadas, devendo o procedimento ser utilizado quando os anteriores – investigação tradicional, interceptação telefônica, ótica ou acústica etc. –, já esgotados, não lograram efeito na consecução da prova. Os procedimentos e normas previstos são novidade (RESCHKE; WENDT; MATSUBAYACI, 2021) e, por isso, ainda serão analisados doutrinariamente e judicialmente sob vários aspectos, inclusive da legalidade e constitucionalidade.

No entanto, embora prevista normativamente, percebe-se uma ausência de utilização da ferramenta investigativa, pois, conforme alegado pelo entrevistado 02SE, "para isso tudo a delegacia não tem condições", havendo necessidade de conversar com o magistrado para explicar o procedimento (14PR). Há que se acrescentar que apenas dois entrevistados se referiram espontaneamente à ferramenta da infiltração de agentes policiais na Internet.

Não basta então a estruturação normativa do procedimento, mas também a estruturação administrativa e operacional do procedimento, incluindo treinamento, conhecimento e habilidades sobre ferramentas técnicas, especialmente a *deep* e a *dark web* (20RR cita a necessidade de aquisição de softwares e equipamentos; 07PB menciona treinamentos específicos; e 04RS menciona a necessidade de rede de Internet "boa" para ingressar nesses ambientes).

4.2.2.5 Competência para julgamento da fraude eletrônica [estelionato]

A Lei nº 14.155/2021 trouxe o apontamento de uma solução processual a uma regra, então vigente, que dificultava a atividade investigativa em face das constantes declarações de incompetência para a decisão, cautelar ou não, de entrega de dados telemáticos, informáticos, bancários etc., aptos a auxiliar a resolução de um delito de estelionato praticado com a utilização de engenharia social pela Internet.

Assim, o § 4º do art. 70 do Código de Processo Penal estipulou que nos crimes de estelionato, do art. 171 do Código Penal, "quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores", a definição da competência será tendo em vista o local do domicílio da vítima, e, "em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção".

Assim, evita-se o envio dos procedimentos policiais a locais que podem sequer ser o local final da competência, conforme regramento anterior, ou seja, do local do auferimento da vantagem indevida.

> RECURSO EM SENTIDO ESTRITO. CRIME DE ESTELIONATO. COMPETÊNCIA. 1. O núcleo do crime material previsto no artigo 171, caput, do Código Penal, é obter vantagem ilícita, razão pela qual a consumação se efetiva com a entrada do dinheiro na conta bancária do suposto estelionatário e não no momento da fraude, aplicando-se a regra de competência prevista no artigo 70, do CPP. 2. Recurso conhecido e provido. Competência do Juízo da Comarca de Goiânia. (GOIÁS, 2019).

Embora as decisões judiciais nesse sentido, importa referir que outras decisões já pontuavam a competência no local de residência da vítima:

> CONFLITO NEGATIVO DE JURISDIÇÃO. CRIME CONTRA O PATRIMÔNIO. ESTELIONATO. COMPETÊNCIA. A competência para processar e julgar o crime de estelionato, quando há transferência eletrônica de

> valores, é do juízo do local onde situada a agência da conta corrente das vítimas, ou seja, onde ocorreu o efetivo prejuízo aos ofendidos. Precedentes do STJ. (RIO GRANDE DO SUL, 2018).

Assim, a disposição processual definidora da competência para processamento e julgamento dos casos de estelionato acabou por ser mecanismo reconhecedor dos direitos da vítima e delimitador do processo de persecução criminal. No entanto, essa modificação ser benéfica ou não para a investigação não é consenso entre os entrevistados:

A favor da modificação realizada em 2021:

> Houve melhoramento, na minha visão, em relação ao crime ser apurado e a competência passar pro local da vítima, o local não mais do proveito do crime, pois é o ambiente que se reúne maior quantidade de provas, então foi benéfico pra investigação criminal. (03BA).
> temos muita dificuldade na questão da competência, em que o crime é plurilocal, então é comum a vítima estar no DF e o autor estar em outro Estado. Tivemos essa mudança recente do estelionato, isso resultou no aumento do nosso trabalho, pois é muito comum encaminhar as ocorrências para São Paulo, onde estão a maioria dos estelionatários e de repente temos que ir a São Paulo, foi uma alteração positiva, pois conseguimos ver o resultado final, mesmo tendo que viajar para outros Estados. (19DF).

Contra a modificação:

> Então, se pensarmos no Brasil, que tem vinte justiças estaduais e na maioria dos crimes, que investigamos no Estado do Piauí, vítimas num Estado e autores num Estado diverso, além da dificuldade operacional na realização dessa investigação, muitas vezes temos dificuldade a respeito da competência. O ponto legislativo que levou a essa situação foi a alteração do artigo 70 do CPP, que fixou uma competência territorial. Acredito que a lei não deveria fixar competência territorial, quando, dentre outras situações, o estelionato se consuma por meio de transferência bancária, fixaram competência ao local de residência da vítima, isso muitas vezes gera o travamento das investigações e encaminhamento do pedido de informações, consequentemente a não responsabilização dos autores. (12PI).
> não podemos investir tempo, também não teria atribuição para investir tempo e esforços em algo que não é competência da Comarca em que atuamos. Então, é um prejuízo quanto a esse ponto específico do artigo 70. Imagina que chega uma denúncia anônima, no site da Polícia Civil do Piauí, sobre organização criminosa que pratica crimes virtuais, clonagem de cartões de crédito e fraudes financeiras diversas, se conseguirmos identificar essas pessoas, identificar o patrimônio aparente, identificar duas/três fraudes financeiras cometidas por meio de transferência, se a residência da vítima é local diverso, deixamos de ter competência do Tribunal de Justiça local, assim deixamos de ter facilidade em nossa atribuição. (12PI).
> vou iniciar pela investigação por competência, cito o estelionato, pois causa maior prejuízo ao país. Começamos com problema na questão de competências, na qual teve alteração legislativa recente, em que os crimes de estelionato e furto mediante fraude são de competência do local (Estado) da vítima, porém o criminoso está em outro local (Estado), nesse sentido precisaremos da colaboração da Polícia Civil de outro Estado. Esses crimes são centenas, são diários, no mês, assim essa questão de competência (geográfica) dificulta o trabalho da polícia. (13AL).

> Sobre o crime de estelionato, na qual a competência do crime foi para o local de residência da vítima, essa situação foi terrível, nessa o legislador fez besteira. [...] Enfim, toda essa problemática, que se a competência fosse pelo local do criminoso isso seria resolvido, a própria notícia-crime teria chego (sic) aqui [...]. (14PR).

Aliás, a questão da competência para o processamento judicial dos casos de crimes cibernéticos – e correspondente atribuição de investigação – é um dos temas importantes que devem voltar a ser debatidos, não só pela adesão do Brasil à Convenção de Budapeste, mas também pelas expectativas e frustrações dos atores de investigação cibernética, consubstanciadas na observação dos entrevistados:

> Acredito que precisa de legislação no cibercrime disciplinando a atuação, crimes e competências, pois está muito dúbio (cada um tem um entendimento). (14PR)
> [...] a parte processual penal, a questão da competência, deveria ser melhor (sic) regulamentada. (19DF).
> Então, no Direito Processual Penal, são essas questões de competência, cito uns casos de fraudes bancárias, em que as pessoas não têm agências, pois são agências virtuais, assim os juízes querem mandar a investigação para a sede do banco, ou para o domicílio do réu, ou para o local da agência, nesse sentido o regramento processual não está bem definido. Percebemos que uma legislação mais clara, para tratar desses assuntos, tiraria as dúvidas dos juízes. Nota-se, na primeira instância, uma diversidade grande de entendimento relacionada a isso. (19DF).

Volta-se aqui a uma conclusão já delineada: a solução normativa quanto ao procedimento não corresponde necessariamente à solução procedimental prática. Para ajustar corretamente, o legislador precisa absorver as comunicações advindas dos sistemas psíquicos e organizacionais envolvidos na persecução da criminalidade cibernética.

4.2.2.6 Políticas procedimentais e processuais de remoção de conteúdo na Internet: a mitigação e redução dos danos na Internet

Embora já elencadas observações no decorrer desta tese sobre o tema da mitigação e redução de danos cibernéticos, cumpre condensar (a) as possibilidades procedimentais e processuais de remoção, retirada e/ou suspensão de conteúdo na Internet, bem como (b) a políticas públicas de prevenção aos crimes cibernéticos previstas normativamente, as quais denominaremos, simplesmente, ‘políticas de redução de danos cibernéticos’.

Nesse campo, seis textos normativos podem ser mencionados, sendo somente um deles possível sem a vênia judicial. Observa-se que, em não havendo regra específica, há que se buscar o fundamento para remoção de conteúdo no Marco Civil da Internet, principal referencial normativo e de âmbito geral no Brasil.

Quadro 11 - Linha do tempo da legislação com previsão de políticas públicas de redução de danos em relação à Internet e seu uso no Brasil – Parte 1

2010	**2012**	**2013**	**2014**
Lei nº 12.288	**Lei nº 12.735**	**Lei nº 12.891**	**Lei nº 12.965**
- Prevê a **interdição** das respectivas mensagens ou páginas de informação na rede mundial de computadores - Lei nº 7.716/1989, art. 20, § 3º, III	- Estruturação de órgãos de polícia judiciária – Art. 4º - **Remoção** de conteúdo racista – Lei nº 7.716/1989, art. 20, § 3º, II	Possibilidade de a Justiça Eleitoral determinar, por solicitação do ofendido, "a **retirada** de publicações que contenham agressões ou ataques a candidatos em sítios da internet, inclusive redes sociais" – § 3º no art. 57-D da Lei nº 9.504/1997	Marco Civil da Internet - **Remoção** de conteúdo íntimo – Art. 21 - Instituto da **remoção** do conteúdo perante os Juizados Especiais – Art. 19 § 3º - **Remoção** judicial a pedido da parte interessada – Art. 22 - Promoção da educação digital – Arts. 26 e 27

Fonte: Produzido pelo autor (2023).

Quadro 12 - Linha do tempo da legislação com previsão de políticas públicas de redução de danos em relação à Internet e seu uso no Brasil – Parte 2

2015		**2017**	**2018**	**2023**
Lei nº 13.185	**Lei nº 13.188**	**Lei nº 13.488**	**Lei nº 13.663**	**Lei nº 14.533**
Programa de Combate à Intimidação Sistemática (*bullying*): - Caracterização - Classificação - Objetivos	"**Direito de resposta**": quanto à resposta ou retificação do ofendido em matéria divulgada, publicada ou transmitida por veículo de comunicação social.	- Justiça Eleitoral poderá determinar, no âmbito e nos limites técnicos de cada aplicação de Internet, a **suspensão** do acesso a todo conteúdo veiculado que deixar de cumprir as disposições – Art. 57-I	Altera o art. 12, inc. IX e X, da Lei nº 9.394, de 20 de dezembro de 1996, para incluir a **promoção** de medidas de conscientização, de prevenção e de combate a todos os tipos de violência e a promoção da cultura de paz entre as incumbências dos estabelecimentos de ensino	Política Nacional de Educação Digital (PNED), em quatro eixos: "Inclusão Digital", "Educação Digital Escolar", "Capacitação e Especialização Digital" e "Pesquisa e Desenvolvimento (P&D) em Tecnologias da Informação e Comunicação (TICs)"

Fonte: Produzido pelo autor (2023).

Assim, a partir do quadro anterior, passa-se a uma análise dinâmica sobre as formas procedimentais e políticas de redução de danos cibernéticos.

I - Marco Civil da Internet (Lei nº 12.965/2014), que (a) em seu art. 21 estabeleceu a responsabilização do provedor de conteúdo/aplicação quando, uma vez notificado, não retirar

imagens, vídeos e outros materiais, contendo nus e atos sexuais. O expediente é direto, pela própria vítima e/ou seu representante legal, não sendo necessária ordem judicial.

E, (b), no art. 19, *caput*, e § 3º, quando o provedor de aplicações na Internet, "após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente", podendo essas causas, "que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na Internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de Internet", ser apresentadas perante os juizados especiais.

Ainda, (c) o art. 22 do MCI prevê que a parte interessada poderá, tendo em vista a formação de conjunto probatório em processos judiciais, cíveis ou penais, "em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de Internet". Ou seja, tem a possibilidade de a parte, independentemente de investigação criminal instaurada, provocar ao Judiciário para obtenção prévia dos dados, uma antecipação probatória de análise da situação e de encaminhamentos futuros, em processo penal ou civil. Para tanto, deve o requerente comprovar "fundados indícios da ocorrência do ilícito", ter "justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória" e, ainda, informar a qual período se referem os registros.

Ainda, no art. 26, o Marco Civil da Internet previu o dever constitucional do Estado na "prestação de educação, em todos os níveis de ensino" sobre o "uso seguro, consciente e responsável da Internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico", incluindo, no art. 27, iniciativas de fomento à cultura digital. Previu, então, o MCI medidas preventivas e reativas aos danos cibernéticos.

II – Lei nº 12.288/2010[192], o Estatuto da Igualdade Racial, que acrescentou o inciso III no § 3º do art. 20 da Lei nº 7.716/1989, que define os crimes resultantes de preconceito de raça ou de cor, dando ao juiz a possibilidade de determinar, "ouvido o Ministério Público ou a pedido deste, ainda antes do inquérito policial, sob pena de desobediência", a "interdição das respectivas mensagens ou páginas de informação na rede mundial de computadores".

[192] O Estatuto da Igualdade Racial teve sua origem no PLS nº 213/2003, passando pela Câmara dos Deputados sob o PL nº 6.264/2005, voltando ao Senado Federal para análise do substitutivo aprovado pelos deputados.

III - Lei nº 12.735/2012[193], que deu nova redação ao inciso II no § 3º do art. 20 da Lei nº 7.716/1989, que define os crimes resultantes de preconceito de raça ou de cor, dando ao juiz a possibilidade de determinar, "ouvido o Ministério Público ou a pedido deste, ainda antes do inquérito policial, sob pena de desobediência", a "cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio".

Até a aprovação da Lei nº 12.735/2012, o projeto que dela tratava, o PL nº 84/1999, teve vários percalços, com acréscimos, revisões, "sendo retalhado" (SYDOW, 2013, p. 273) até chegar na redação do PL nº 84-G/1999 (sétima versão). Segundo Sydow (2013, p. 276-277), o "único artigo com repercussão processual penal significativa e imediata" que sobrou dos retalhos feitos nos projetos e que gerou a Lei nº 12.735/2012 foi o art. 5º, o que alterou o inciso II no § 3º do art. 20 da Lei nº 7.716/1989, conforme antes exposto.

O autor, no entanto, desconsidera a importância do art. 4º da mesma Lei (SYDOW, 2013, p. 276), que estipula a necessidade de que os órgãos de polícia judiciária estruturem setores e equipes especializadas no combate à ação delituosa "em rede de computadores, dispositivo de comunicação ou em sistema informatizado".

IV - Lei nº 12.891/2013, que acrescentou o § 3º no art. 57-D da Lei nº 9.504/1997, estipulando a possibilidade de a Justiça Eleitoral determinar, por solicitação do ofendido, "a retirada de publicações que contenham agressões ou ataques a candidatos em sítios da Internet, inclusive redes sociais", ou seja, abarcando postagem em sites de notícias, blogs e mídias sociais de interação.

V – O "Direito de Resposta", regulado pela Lei nº 13.188/2015, quanto à resposta ou retificação do ofendido em matéria divulgada, publicada ou transmitida por 'veículo de comunicação social'.

VI - Lei nº 13.488/2017, que deu nova redação ao *caput* do art. 57-I da Lei nº 9.504/1997, possibilitando, a requerimento de candidato, partido ou coligação, à Justiça Eleitoral determinar, "no âmbito e nos limites técnicos de cada aplicação de Internet, a suspensão do acesso a todo conteúdo veiculado que deixar de cumprir as disposições" da Lei Eleitoral, "devendo o número de horas de suspensão ser definido proporcionalmente à gravidade da infração cometida em cada caso, observado o limite máximo de vinte e quatro horas", podendo ser dobrada em caso de reiteração (§ 1º do mesmo artigo).

VII - No que tange às políticas públicas e preventivas aos danos cibernéticos, cita-se:

---

[193] A Lei nº 12.735/2012 foi o que 'restou' do PL nº 84/1999, denominado 'Projeto de Lei Azeredo' e considerado o AI-5 Digital (WENDT, 2017b). O PL ficou em discussão por 4 anos na Câmara dos Deputados e 9 anos no Senado Federal, sob o PLC nº 89/2003.

- a previsão, na Lei nº 13.185/2015, do programa de ‘combate’ ao *bullying*, prática que pode e deve ser integrada à educação, conforme previsão no art. 26 do Marco Civil da Internet e no art. 12 da Lei nº 9.394/1996, modificado pela Lei nº 13.663/2018, para incluir a promoção de medidas de conscientização, de prevenção e de combate a todos os tipos de violência e a promoção da cultura de paz entre as incumbências dos estabelecimentos de ensino;

- a Lei nº 14.533/2023, que estrutura a Política Nacional de Educação Digital (PNED).

Portanto, o ideal é que a previsão normativa esteja acompanhada de medidas estruturantes da política pública e preventiva de redução de danos cibernéticos, sem as quais é ineficaz. A Lei nº 14.533/2023 tem uma estrutura de política preventiva composta por eixos, o que a deixa mais prática e tendente à eficácia (ver 4.3.3).

***

Uma análise, portanto, da estruturação da legislação processual no Brasil em relação à Internet, comparada à estruturação das normativas criminalizatórias, com novos tipos penais e aumento de penas, leva à conclusão de que o enfoque principal das legislações não parece voltado à parte procedimental, desde o contexto internacional até o campo interno dos países, com criação de mecanismos normativos para auxiliar na formação da prova e da coleta de evidências, ajudando, por um lado, a polícia judiciária e o Poder Judiciário na resolução da lide de maneira mais célere e, de outro lado, o investigado, pois poderá conhecer corretamente esses mecanismos que serão usados dentro da ótica de direitos humanos e fundamentais.

Mesmo as normativas referidas nos subtópicos anteriores carecem de maior clareza, direcionamento, objetividade e definições de temporalidade. A própria Lei nº 13.964/2019 (Pacote Anticrime), que tratou da preservação da cadeia de custódia nos arts. 158-A a 158-F, não tratou de discriminar o ritual procedimental em relação à cadeia de custódia da evidência digital.

A necessidade de melhoria desses mecanismos procedimentais reforça-se em razão de as dificuldades não se concentrarem na falta de legislação adequada na parte procedimental – embora as expectativas cognitivas e normativas dos atores possam ser encaminhadas nesse sentido –, mas em razão da investigação se prolongar no tempo e depender da obtenção dos dados frente aos provedores de conexão e de aplicação, além do fato de os integrantes do

sistema de persecução criminal desconhecerem termos técnicos, procedimentos e ações necessárias à obtenção dos dados voltados à apuração do delito e de sua autoria.

De acordo com os atores de investigação cibernética entrevistados, os demais atores [integrantes do Ministério Público e do Poder Judiciário] necessitam de uma maior qualificação e, consequentemente, compreensão dos termos atinentes ao cibersistema da Internet. Esta não é necessariamente uma visão dos aspectos atinentes à persecução da criminalidade cibernética no Brasil.

> Las discrepancias pueden causar dificultades para las investigaciones tanto a nivel nacional como internacional y, aunque la tipificación penal de estas actividades es esencial, pero la capacitación de los administradores de justicia es vital, para garantizar el éxito de los resultados de investigación punitiva, en la procura de acercarnos a los cambios que las tecnologías de información y comunicación han aportado en la aparición de estas nuevas conductas delictivas. (GARCÍA LUNA; PEÑA LABRIN, 2017, p. 16).

Aliado às observações postas, não há protocolo formal quanto à atuação procedimental das polícias judiciárias, do Ministério Público e do Poder Judiciário e, principalmente, quanto ao tratamento e à custódia de evidências digitais. Aliás, não há protocolo básico do atendimento de ocorrências em que os atos criminosos são cometidos com o uso da Internet, nem de como preservar essas evidências, carecendo a estrutura administrativa de uma padronização e uniformidade.

Então, complementar esses estudos e analisar as práticas procedimentais vigentes nos órgãos policiais e periciais [no âmbito dos Estados] é um caminho hábil ao debate público e estratégico na construção de um protocolo regulativo ideal, baseado na efetividade dos direitos e garantias dos usuários da Internet e dos investigados. O "Plano Tático de Combate a Crimes Cibernéticos" foi aprovado em 2022, no âmbito do Ministério da Justiça e Segurança Pública (MJSP)[194], tendo sido discutido e formatado no 1º Cibercap, já referido, plano que "prevê a criação de um banco de dados de ocorrências, que terá o amplo acesso das polícias judiciárias da União e dos estados. Dessa forma, os modelos de investigações e soluções de crimes poderão ser replicados de forma eficiente em todo o país" (BRASIL, 2022a).

Esse plano, gerado a partir de debates interdisciplinares e interorganizacionais,

[194] O Plano Tático de Combate a Crimes Cibernéticos do MJSP foi aprovado por Decisão do Ministro nº 54/2022 (BRASIL, 2022a).

> contém eixos temáticos que destacam a prevenção e a mitigação de ameaças cibernéticas; o gerenciamento de riscos e incidentes decorrentes da criminalidade cibernética; o aprimoramento de infraestruturas críticas para combate a crimes cibernéticos; o amparo legal e regulamentar; as parcerias nacionais e cooperação internacional; a padronização e a integração informacional; além de pesquisa, desenvolvimento, inovação e educação para o enfrentamento a crimes cibernéticos (BRASIL, 2022a).

A partir desse plano, foi criado um Grupo Técnico, incluindo o autor desta tese, pelas Portarias nº 418/2022 (BRASIL, 2022c – ANEXO I) e nº 463/2022 (BRASIL, 2022d – ANEXO II), esta de alteração e prorrogação da anterior, ambas da Secretaria Nacional de Segurança Pública do MJSP, com membros indicados pelo Conselho Nacional de Chefes de Polícia – CONCPC, "com a finalidade de subsidiar ações afetas à Secretaria Nacional de Segurança Pública – SENASP, instituídas no Plano Tático de Combate a Crimes Cibernéticos do Ministério da Justiça e Segurança Pública".

O referido GT, observando o referido Plano Tático quanto ao Eixo Temático E3 (Aprimoramento das infraestruturas críticas para combate a crimes cibernéticos) e ao Eixo E6-A1 (Estabelecimento de protocolos norteadores das polícias judiciárias), teve cinco reuniões no período de 2022, colocando como diretrizes o estabelecimento de, inicialmente, um Roteiro Nacional de Atendimento, Registro e Investigação de Crimes Cibernéticos, com três Estados enviando modelos locais de Procedimentos Operacionais Padrão (POPs): Mato Grosso[195], Distrito Federal[196] e Minas Gerais[197].

Não houve, porém, até o final de 2022, a consolidação de um modelo unificado para estabelecer, *ab initio*, um modelo padrão de atendimento de ocorrências e preservação de provas e evidências digitais. Também não se tem notícias sobre a análise e evolução de outros eixos previstos no referido Plano Tático, que também envolve outros órgãos e setores, incluindo a Polícia Federal, também participante do 1º Cibercap.

4.3 Projetos de lei relativos à Internet no Brasil e as realidades expectantes a serem estruturadas penalmente

As comunicações que partem dos sistemas psíquicos, sociais e organizacionais podem vir a ser também recepcionadas pelo sistema político em sua função legislativa, de produção

---

[195] Possui "CERTIDÃO SIMPLIFICADA DE IDENTIFICAÇÃO, COLETA, AQUISIÇÃO E PRESERVAÇÃO DE EVIDÊNCIAS DIGITAIS".

[196] Possui 27 POPs sobre o tema.

[197] Possui POP de "INVESTIGAÇÃO DE DELITOS NO MEIO CIBERNÉTICO", produzido em 2019, sendo que um novo POP estaria em fase de conclusão.

normativa. O sistema da Comunicação, com seu principal *médium*, os *mass media*, como visto durante este trabalho, tem sido um contributo bastante acentuado na construção da realidade normativa a partir do sistema legislativo brasileiro. Diferentemente, o contributo dos atores de investigação policial, especialmente a cibernética, não tem irritado o legislativo brasileiro a ponto de ser considerado em seus debates, exceto por eventuais participações nos debates, tal qual ocorreu nas audiências públicas da criminalização da fraude envolvendo os ativos digitais (ver 4.2.1.9).

Como abordado no tópico 3.2.3, de acordo com a expectativa dos atores de investigação criminal, haveria a tipificação como crime de novas condutas, sobre as quais o legislador brasileiro deveria se debruçar. Dentre essas estão as *fake news*, o *bullying*, a desconfiguração de páginas da Internet (*defacement*), o uso de *ransomwere* (encriptação de arquivos com uso de código malicioso e solicitação de resgate em criptoativos), perfil falso no âmbito da Internet (perfis de pessoas físicas ou jurídicas), estupro pela Internet, invasão e sequestro de contas de redes sociais e, também, lavagem de dinheiro com criptoativos. Houve, ainda, expectativa sobre a tipificação criminal dos atos preparatórios, publicados ou como vídeo ou como *e-commerce*, por exemplo, ensinando a montagem de explosivos ou demonstrando como aplicar um golpe ou uma fraude com sucesso.

Há que se destacar que muitos projetos estão em debate no Congresso Nacional e mereceriam uma análise acurada e, necessariamente, comparativa quanto aos seus intentos, sejam eles criminalizatórios ou processuais, incluindo as políticas de remoção de conteúdo (ver 4.4).

Para efeitos desta pesquisa e pela restrição de sua abrangência, no âmbito penal procurar-se-á delimitar a análise sobre dois temas contemporâneos: *bullying* (e *cyberbullying*) e as *fake news*.

4.3.1 *Timeline* da expectativa estruturante quanto ao *bullying* e ao *cyberbullying*

O *bullying* é uma denominação inglesa, surgida na década de 1970 na Noruega, adotada por países europeus e africanos e também pelo Brasil (ANTUNES; ZUIN, 2008), conceituado pelos autores como

> [...] um conjunto de comportamentos agressivos, físicos ou psicológicos, como chutar, empurrar, apelidar, discriminar e excluir, que ocorrem entre colegas sem motivação evidente, e repetidas vezes, sendo que um grupo de alunos ou um aluno

> com mais força, vitimiza um outro que não consegue encontrar um modo eficiente para se defender (ANTUNES; ZUIN, 2008, p. 34).

Os campos da psicologia comportamental, da antropologia e do direito têm estudado o tema, que não se trata somente de um problema do/no âmbito escolar e, sim, de uma questão de saúde pública (SILVA, 2010, p. 14). Essa discussão, tendo em vista a potencialização da "cultura" de *bullying* e *cyberbullying* nos ambientes, especialmente o escolar, ocasionou a remessa da discussão ao legislativo brasileiro.

A *timeline* da discussão normativa referente ao *bullying*, e, por consequência, ao *cyberbullying*, inicia sua trajetória na Câmara dos Deputados em 2009. Porém, antes de especificar os aspectos desse projeto inicial, sobre o tema – *bullying* e *cyberbullying* – tem-se de esclarecer a metodologia de coleta e análise dos dados (projetos discutidos, em discussão e normas sancionadas).

A pesquisa pelo tema no sítio da Câmara dos Deputados demonstra o extenso rol de projetos existentes e, por não estarem sistematizados, há necessidade de compreendê-los sob três finalidades principais: (a) estabelecimento de políticas públicas de prevenção e orientações (aos gestores públicos e ao setor privado); (b) criminalização de condutas; e (c) procedimentos administrativos e/ou processuais para o enfrentamento. Aliás, o entrevistado 03BA refere a necessidade de um amadurecimento por parte da Polícia Civil quanto ao tema e tratamento policial dos casos registrados.

4.3.1.1 Projetos e normativas de estabelecimento de políticas públicas de prevenção e orientações (aos gestores públicos e ao setor privado) no enfrentamento ao *bullying* e *cyberbullying*

O primeiro tópico das finalidades categorizadas – e pretendidas pelo legislador – entra na ótica de previsão de direitos e imposição de deveres ao poder público e ao(s) setor(es) privado(s) para enfrentar a demanda social por prevenção à conduta de *bullying* e *cyberbullying*, não só por mais esclarecimento, mas também quanto ao translado da letra fria da Lei, para o mundo real, de práticas reais de enfrentamento à intimidação sistemática, especialmente no ambiente escolar.

Neste tópico, então, tem-se o Projeto de Lei nº 5.369/2009, que foi proposto na Câmara dos Deputados com a finalidade de instituir o "Programa de Combate ao *Bullying*", trazendo em seu bojo o conceito, a amplitude, a classificação de condutas possíveis de enquadramento,

além dos objetivos do programa. No Senado Federal, sob a numeração de PLC nº 68/2013, o programa recebe o aval da Casa, conforme o parecer da senadora Kátia Abreu:

> O projeto não envereda pelo caminho mais polêmico do direito penal. Ele sabiamente insiste no caráter educativo para coibir comportamentos de intimidação sistemática. Desse modo, apenas se arrisca em conceituar práticas nocivas que, em algumas situações, podem ter limites tênues com atitudes efetivamente inócuas, fruto de brincadeiras inofensivas. (SENADO FEDERAL, 2014, p. 3).

A alteração que ocorre no Senado Federal é apenas quanto à nomenclatura do Programa, que passa a ser de combate à intimidação sistemática, incorporação ao vernáculo em português da expressão inglesa *bullying*.

Assim, surge a Lei nº 13.185/2015, que institui o 'Programa de Combate à Intimidação Sistemática' (*Bullying*), normatizando conceitos, caracterizações, abrangência e objetivos da 'política pública', também prevendo que estabelecimentos de ensino, clubes e agremiações recreativas assegurem medidas de conscientização, prevenção, diagnose e combate à violência e à intimidação sistemática. Convênios e relatórios bimestrais das ocorrências também foram previstos.

Nesse ínterim, entre 2009 e 2015, dois Projetos de Lei do Senado, de nº 228/2010 e nº 196/2011, trataram do mesmo objetivo: incluir, na Lei de Diretrizes e Bases da Educação Nacional (Lei nº 9.394/1996), entre as incumbências dos estabelecimentos de ensino, a promoção de ambiente escolar seguro e a adoção de estratégias de prevenção e combate ao *bullying*.

Aprovado no Senado Federal, o PLS nº 228/2010 teve curso à Câmara dos Deputados, transformando-se em PL nº 1.785/2011, enquanto o PLS nº 196/2011 foi arquivado, por tratar do mesmo assunto do anterior: acréscimo de um inciso no art. 12 da Lei nº 9.394/1996 (ver 4.2.2.6).

Na Câmara dos Deputados o PL nº 1.785/2011 teve apensados outros doze (12) Projetos de Lei[198], todos propostos entre os anos de 2010 e 2012, estando em discussão na Comissão de Finanças e Tributação[199]. Portanto, o acréscimo ao art. 12 da Lei nº 9.394/1996 ainda "penderia" de debate e decisão legislativa.

---

[198] Apensados ao PL nº 1.785/2011 (12): PL nº 7.457/2010 (10), PL nº 283/2011 (2), PL nº 350/2011, PL nº 1.841/2011, PL nº 908/2011, PL nº 1.226/2011, PL nº 1.633/2011 (1), PL nº 2.108/2011, PL nº 1.765/2011, PL nº 2.048/2011, PL nº 3.036/2011, PL nº 3.153/2012.

[199] A mesma situação de pendência desde o ano de 2019.

A adoção do termo “penderia” é proposital, pois o Projeto de Lei nº 5.826/2016 trouxe a proposta de incluir o combate a todas as formas de violência e a promoção da cultura de paz como incumbência dos estabelecimentos de ensino, com a inserção de dois incisos no art. 12 da Lei nº 9.394/1996.

No Senado Federal, esse projeto transformou-se em PLC nº 171/2017 e, após os trâmites, foi aprovada e sancionada a Lei nº 13.663/2018, inserindo no art. 12 da Lei de Diretrizes e Bases da Educação Nacional os incisos IX e X, respectivamente, para a adoção de medidas de enfrentamento à intimidação sistemática e ações de promoção da cultura de paz nas escolas.

Portanto, verifica-se que, quanto ao estabelecimento de políticas públicas de prevenção e orientações (aos gestores públicos da educação e ao setor privado da educação) em relação ao *bullying* e *cyberbullying*, o campo normativo brasileiro está ajustado.

Porém, a efetividade prática desses direitos e deveres instituídos depende de ações concretas por parte dos gestores públicos e privados da educação, conforme já ponderado quando se tratou dos direitos humanos e a relação com a Internet.

4.3.1.2 Projetos e normativas estabelecendo criminalização de condutas como mecanismo de enfrentamento ao *bullying* e *cyberbullying*

No quesito *criminalização de condutas* cumpre uma análise pormenorizada, não dos termos de cada Projeto de Lei, mas sim das finalidades de cada proposta, facilitando a compreensão da lógica dos debates e caminhos legislativos (possíveis).

A atual legislação penal brasileira permite o enquadramento da prática das condutas definidas como ‘intimidação vexatória’ (*bullying*), dependendo de como ocorreu o fato, tanto nos casos de delitos contra a honra (arts. 138 a 140 do Código Penal) – calúnia, difamação ou injúria – quanto nos casos de lesão corporal, reconhecida esta nas situações de violência física e/ou psicológica (art. 129 do Código Penal).

As discussões legislativas sobre a criminalização dos atos de violência física ou psicológica intencional e repetitiva, praticados com o objetivo de intimidação/agressão, provocando dor física e sofrimento psicológico (pela situação vexatória a que as vítimas são expostas), têm sido objeto de análise da Câmara dos Deputados desde 2011.

Somente naquele ano, os PLs nº 1.011/2011, nº 1.494/2011 e nº 1.573/2011 foram propostos, seguindo-se a eles uma plêiade de, ao todo, doze (12) projetos legislativos,

incluindo o PL nº 5.064/2019 e o PL nº 2.385/2021. Todos os projetos sobre o tema estão apensados ao PL nº 847/2019, sendo, portanto, atualmente, 18 projetos discutindo o tema[200].

Para a análise conjunta dos projetos, propõe-se um quadro dinâmico-temporal e analítico-conceitual, compondo o período da proposta e seus objetivos principais: criminalização (seja pela previsão de novo tipo penal, seja pela previsão de acréscimo de pena), política pública e de orientação ou imposição de cumprimento de pena/medida socioeducativa ou processos e procedimentos de redução de danos cibernéticos.

Percebe-se, desde já, que a maioria dos projetos legislativos não só busca a criminalização como também insere no debate referente ao *bullying* e *cyberbullying* os aspectos atinentes ao trote estudantil e o *cyberstalking*[201]. Vejamos:

Quadro 13: Projetos de Lei sobre *bullying* e *cyberbullying* na Câmara dos Deputados

Ano	**Número do PL**	**Criminalização das condutas**	**Política pública**	**Proposta de processos administrativos e/ou processuais alternativos**
2011	1011	Crime de intimidação escolar	Não	Não
	1494	Crimes de intimidação vexatória, intimidação vexatória qualificada e intimidação vexatória seguida de morte	Não	Não
	1573	Crime de *bullying*	Não	Alteração do ECA (art. 117-A) para aplicação da medida de prestação de serviços à comunidade para adolescentes
2014	7609	Crime de trote estudantil	Não	Não
	7946	Crime de trote estudantil	Imposição de indenização por despesas médicas e psicológicas decorrentes	Não
2015	3263	Não	Não	Retratação do agressor pelo mesmo meio do ato de agressão
	3686	Crime de intimidação sistemática e aumento de pena no caso de *cyberbullying*	Não	Não
2016	4805	Crime de perseguição sistemática digital (*ciberstalking*). Obs.: alteração na Lei nº 13.185/2015	Não	Não
	5382	Crime de trote estudantil	Proibição de trote estudantil	Imposição de e penalidades administrativas

[200] Pesquisa realizada no site da Câmara dos Deputados em 12 jan. 2023.

[201] O *cyberstalking*, no sentido de perseguição virtual, conforme visto no tópico 4.2.1.7, está enquadrado no tipo penal do art. 147-A do Código Penal.

2017	9243	Não	Responsabilização dos agressores e medidas para estabelecimentos de ensino – alteração na Lei nº 13.185/2015	Não
2019	847	Previsão de criação do tipo penal do art. 132-A do Código Penal, de "conduta cibernética prejudicial à saúde, à incolumidade física ou psíquica ou à vida de outrem"	Não	Não
	5064	Previsão de acréscimo de pena no caso de homicídio resultante de trote estudantil	Conceito e circunstâncias consideradas como trote	Sanções administrativas, julgamento e destinação do valor das multas
2021	2385	Previsão de criação do art. 145-A e acréscimo de §§ no art. 147-A no Código Penal	Não	Não
	2699	Previsão da criminalização da prática de *haters* na Internet.	Não	Sim, responsabilização pelos danos e remoção de conteúdo.
	2706	Altera a Lei nº 13.185/2015, que institui o Programa de Combate à Intimidação Sistemática (*bullying*). Prevê aumento de pena, embora não preveja alteração no Código Penal.	Sim	Sim (reparação dos danos a cargo do responsável pelo *bullying*).
	3402	Prevê a criminalização, pelo art. 140-A do Código Penal, do crime de *cyberbullying*.	Não	Prevê possibilidade de meios alternativos à pena privativa de liberdade (retratação do autor, uso de programa de rastreamento etc.).
	3744	Altera o art. 4º da Lei nº 13.185/2015, para dispor sobre os objetivos do Programa de Combate à Intimidação Sistemática (*bullying*).	Sim	Prevê prática de prevenção no âmbito das escolas.
2022	1926	Acréscimo do art. 7º-B na Lei de Diretrizes e Bases da Educação (Lei nº 9.394/1996) e do art. 146-A no Código Penal ("Trote abusivo em Instituição de Ensino").	Sim	Não

Fonte: Produzido pelo autor (2023).

Como se percebe, apenas quatro projetos – dos 18 PLs – não contemplam criminalização de condutas e/ou acréscimo de penas, com majorantes em caso de presentes determinadas circunstâncias que envolverem os casos de *bullying* e *cyberbullying*, escolar ou não. De outra parte, dez projetos não contemplam medidas alternativas de solução dos conflitos resultantes e/ou consubstanciais da prática da intimidação vexatória/sistemática. Da mesma forma, 11 projetos não contemplam orientações ao gestor público e ao privado, especialmente aos estabelecimentos de ensino, propiciando o tratamento não penal das condutas dos adolescentes. Ou seja, o foco do legislador brasileiro centrou-se na

criminalização e não em aspectos importantes de redução de danos, tanto por ausência de previsão de políticas públicas orientativas quanto por inexistência de medidas de remoção/retirada de conteúdo do âmbito da rede[202].

4.3.1.3 Previsão de procedimentos administrativos e/ou processuais para o enfrentamento ao *bullying* e *cyberbullying*

Conforme tópico anterior, dentre os Projetos de Lei que contemplam, em seu escopo inicial, previsão de procedimentos administrativos e/ou processuais (alternativos à imposição penal) para o enfrentamento ao *bullying* e *cyberbullying*, a minoria tem este caráter não-penal.

De outra parte, demonstrando um claro direcionamento à criminalização, poucos projetos têm previsão quanto a medidas alternativas de solução dos conflitos originários da prática de intimidação sistemática/vexatória, como a retratação e/ou uso de aplicativos de controle e rastreio, sendo que somente o PL nº 2.699/2021 estabelece medida para retirada de postagem, comentário, imagem ou vídeo referente ao *cyberbullying* do ambiente digital, o que, em não sendo aprovada esta parcela, permanece aplicável o regramento básico do Marco Civil da Internet – Lei nº 12.965/2014.

A previsão de tal medida de redução de danos cibernéticos, a remoção/retirada do conteúdo, seria importante e evitaria danos (psicológicos) ainda maiores às vítimas (WENDT; LISBOA, 2013; SCHREIBER; ANTUNES, 2015), tal qual ocorre com a possibilidade de retirada, por via 'administrativa', de cenas de caráter íntimo e/ou sexual, previsão esta do art. 21 do Marco Civil da Internet.

Na esteira dos projetos não criminalizatórios citados, em 2018 surgiu o PL nº 9.674/2018, que propôs a instituição da Semana Nacional de Conscientização, Prevenção e

---

[202] No parecer do Relator, Deputado Luiz Henrique Mandetta, na Comissão de Seguridade Social e Família (CSSF), no ano de 2018, a proposta de substitutivo apenas prevê três tópicos relativos à criminalização, que seriam (a) intimidação vexatória, (b) trote estudantil e (c) suicídio resultante de intimidação vexatória (tal reivindicação já se encontra abarcada com a edição da Lei nº 13.968/2019). No entanto, os demais aspectos foram suprimidos, restando, por esse substitutivo, apenas a obrigação do estabelecimento escolar em notificar o fato ao órgão responsável no Ministério da Educação (CÂMARA DOS DEPUTADOS, 2018a, p. 6-7). Porém, após um ano, na mesma Comissão de Seguridade Social e Família (CSSF), foi apresentado um novo Parecer, também pela aprovação do Projeto de Lei nº 1.011/2011 e seus apensos, porém com redução do escopo penal a uma inclusão no art. 140 do Código Penal, quando a injúria consistir em intimidação vexatória, passando a ter uma pena específica de um a três anos de reclusão (CÂMARA DOS DEPUTADOS, 2019, p. 8-9). Tal substitutivo, assim, não previu nenhuma política pública ou meio alternativo para resolução do conflito. O PL nº 1.011/2011 foi apensado, em 2021, ao PL nº 847/2019, que tem como principal foco a criminalização da conduta.

Combate a Intimidação Sistemática (*Bullying*) nas escolas públicas e privadas de ensino fundamental e médio em todo o território nacional. Outros cinco PLs com o mesmo enfoque foram propostos desde então, destacando-se os PLs nº 311/2019, nº 1.574/2019, nº 2.706/2021, nº 3.744/2021 e nº 1.926/2022 por acrescentarem dispositivos à Lei de Diretrizes e Bases da Educação para incluir no projeto pedagógico escolar medidas de conscientização, prevenção, diagnose e combate ao *bullying* no ensino fundamental.

4.3.2 *Timeline* de normatização e propostas legislativas estruturantes quanto às *fake news*

A temática das notícias falsas, falsas notícias ou *fake news*, tem sido motivo de preocupação do mundo todo, especialmente pela sua proliferação instantânea com o uso de aplicativos de mensageria[203] e redes sociais na Internet[204]. Cinco entrevistados mencionaram as *fake news*, tendo um destacado o porquê de sua expectativa:

> a DRCI tem enfrentado fortes ataques de crimes informáticos impróprios (*fake news*), assim **acredito que o legislador deveria ter criado tipo penal próprio para a divulgação de notícias falsas**, por meio de redes sociais, de sites, porque a lesão dessas condutas é grande. **Essa ausência de tipificação gera entrave na investigação**, pois temos que fazer as devidas adequações no âmbito dos crimes contra a honra. (17MT, destaques nossos).

Não só pela ausência de regulamentação normativa atualizada no Brasil, não só pelo conceito, mas também pela tradução do termo *fake news* para o português, o que pode levar a uma compreensão errônea de sua tipificação e enquadramento penal, seja na legislação atual, seja na legislação vindoura.

Paralelamente, outra preocupação é pela possibilidade de que tais *fake news* possam (ser usadas para) influenciar processos eleitorais, tal qual como teria ocorrido com o Brexit[205] e as eleições norte-americanas. Martins e Tateoki (2019) exploram o tema, juntamente com dois parâmetros muito importantes: a proteção de dados e a democracia. Ponderam eles que *fake news*

> São supostas notícias que tentam se passar por matérias jornalísticas dignas de confiança, mas que, em diversos graus, propagam informações inverídicas,

---

[203] WhatsApp, Facebook Messenger, Viber, Telegram, Signal, dentre outros.
[204] Facebook, Instagram, Twitter, dentre outras.
[205] O Brexit, que vem da contração das palavras inglesas *Britain*, de Grã-Bretanha, e *exit*, de saída, foi o movimento e consequente referendo do país europeu em que se decidia pela saída da União Europeia (BUENO, 2016; SOARES, 2019).

> distorcem fatos ocorridos ou mesmo opiniões emitidas por alguém. (MARTINS; TATEOKI, 2019, p. 141).

O caso *Cambridgne Analytica* teve repercussão internacional, pois a empresa teve acesso a milhões de contas de usuários de rede social, possibilitando, através da análise comportamental, por exemplo, por meio de curtidas, "identificar diversos parâmetros de personalidade existentes na imensa base de dados colhidos e, com isso, engendrou uma campanha publicitária específica para cada tipo de usuário" (MARTINS; TATEOKI, 2019, p. 144).

Voltando ao campo legislativo brasileiro, tamanha atenção o fenômeno comunicativo gerou a partir do tema *fake news* que, no Congresso Nacional, até o final de 2019, tramitavam vinte e nove (29) Projetos de Lei, sendo vinte e quatro (24) deles na Câmara dos Deputados e quatro (4) no Senado Federal[206]. Já em 2020, em razão da pandemia da Covid-19, outros 26 projetos normativos passaram a tramitar nas duas casas legislativas. A partir de 2021 o número de projetos cresceu, chegando a 87 propostas de regulamentação, resultado da operação de reflexividade da comunicação entre o cibersistema da Internet e os sistemas da Política, do Direito e da Comunicação.

Antes, porém, cumpre referir quanto ao primeiro projeto que teve trâmite sobre o tema, o PL nº 1.978/2011, pois ele visou à alteração do Código Penal, porém acabou por ser direcionado à modificação do Código Eleitoral[207], ao que passaria a tipificar o delito de denunciação caluniosa eleitoral. O projeto, aprovado na Câmara dos Deputados em 2014, foi enviado ao Senado Federal, casa legislativa no qual o PLC nº 43/2014 tramitou por cinco anos, indo à sanção presidencial e, em virtude de vetos, retornando ao Congresso Nacional, que os rejeitou.

A redação final da Lei nº 13.834/2019 trouxe, conforme análise na *timeline* da legislação eleitoral já realizada (ver 4.2.1.2), a inclusão do art. 326-A no Código Eleitoral, igualando quem deu causa à instauração de um processo ou investigação àquele que divulga ou propala, dolosamente, o fato que lhe foi falsamente atribuído[208]. Assim, percebe-se, um

---

[206] Antes das eleições de 2018 o número de projetos que visavam a criminalizar a propagação de *fake news* já era grande, com 20 propostas legislativas, inclusive algumas baseadas e fundamentadas com falsas notícias: PL nº 9.931/2018 e o PL nº 9.554/2018 (GRIGORI, 2018).

[207] Lei nº 4.737, de 15 de julho de 1965 – Código Eleitoral.

[208] "Art. 326-A. Dar causa à instauração de investigação policial, de processo judicial, de investigação administrativa, de inquérito civil ou ação de improbidade administrativa, atribuindo a alguém a prática de crime ou ato infracional de que o sabe inocente, com finalidade eleitoral:
Pena - reclusão, de 2 (dois) a 8 (oito) anos, e multa.
§ 1º A pena é aumentada de sexta parte, se o agente se serve do anonimato ou de nome suposto.

dos campos da ‘necessidade política’, e não necessariamente social, foi suprido, instituindo-se na legislação eleitoral mais um tipo penal. Nesse mesmo processo, de autoproteção do legislador, do político com mandato ou não, o estabelecimento de uma ‘política pública’, através de uma ferramenta no site da Câmara dos Deputados[209], o ‘Comprove’, para checagem de notícias falsas, com interação através de WhatsApp (VALENTE, 2019).

Também, cumpre referir que a Lei nº 5250/1967 previu o tipo penal relativo às notícias falsas:

> Art. 16 Publicar ou divulgar notícias falsas ou fatos verdadeiros truncados ou deturpados, que provoquem:
> I - perturbação da ordem pública ou alarma social;
> II - desconfiança no sistema bancário ou abalo de crédito de instituição financeira ou de qualquer empresa [sic], pessoa física ou jurídica;
> III - prejuízo ao crédito da União, do Estado, do Distrito Federal ou do Município;
> IV - sensível perturbação na cotação das mercadorias e dos títulos imobiliários no mercado financeiro.

O art. 16 e, também, o art. 18 da Lei nº 5.250/1967 tipificam, respectivamente, a publicação ou divulgação de “notícias falsas ou fatos verdadeiros truncados ou deturpados” e de obtenção, “para si ou para outrem, favor, dinheiro ou outra vantagem para não fazer ou impedir que se faça publicação, transmissão ou distribuição de notícias”, atentando-se, especificamente, ao § 1º do art. 18, que amplia a pena quando esta conduta seja realizada e tenha capacidade de “produzir resultados, fôr [sic] desabonadora da honra e da conduta de alguém”.

No entanto, por vários fatores, dentre eles a especificidade da norma penal citada, a pena branda, bem como a falta de sua efetividade, os projetos normativos começaram a surgir em razão e a partir do incremento da prática no ambiente virtual.

Tendo em vista a quantidade de projetos existentes sobre *fake news*[210], bem como os enfoques variados existentes (na Câmara dos Deputados existiam blocos principais de análise da temática), utilizar-se-á a mesma metodologia já empregada na análise dos projetos

---

§ 2º A pena é diminuída de metade, se a imputação é de prática de contravenção.
§ 3º (VETADO) (Promulgação partes vetadas)
§ 3º Incorrerá nas mesmas penas deste artigo quem, comprovadamente ciente da inocência do denunciado e com finalidade eleitoral, divulga ou propala, por qualquer meio ou forma, o ato ou fato que lhe foi falsamente atribuído”.

[209] https://www.camara.leg.br/comprove.

[210] Poder-se-ia trabalhar sob a ótica de que legislar sobre *fake news* pode ser tendente a controlar ou diminuir o número de notícias falsas, mas não é o objetivo central deste trabalho.

relativos ao *bullying* e *cyberbullying*, porém, acrescentando-se uma coluna com a indicação da legislação a incrementar/alterar[211].

Para a análise conjunta dos projetos, propõe-se novamente um quadro dinâmico-temporal e analítico-conceitual, compondo o período da proposta e seus objetivos principais e secundários: criminalização (seja pela previsão de novo tipo penal, seja pela previsão de acréscimo de pena), política pública e de orientação ou proposta alternativa (de pena, de medida administrativa ou de solução alternativa de conflitos), além da legislação a incrementar/alterar.

Quadro 14: Projetos de Lei sobre *fake news* no Congresso Nacional (até 2019)

CÂMARA DOS DEPUTADOS					
Projeto principal	**Número dos projetos apensados**	**Enfoque da proposta**	**Política pública e de orientação**	**Proposta alternativa de pena, medida administrativa ou de solução de conflito**	**Legislação a incrementar ou alterar**
PL nº 215/2015	215/2015	Criminalização, com previsão de aumento de pena (art. 141, CP)	Não	Não	DL nº 2.848/1940
	1.547/2015	Criminalização (com aumento de pena – art. 141, CP) e resguardo de evidências digitais (art. 6º, CPP)	Não	Não, somente procedimento de resguardo de evidências digitais: investigação.	DL nº 2.848/1940 e DL nº 3.689/1941
	1.589/2015	Criminalização, com aumento de pena e mudança na ação penal. Crime hediondo nos casos de resultado morte. Acréscimo no CPP (arts. 323 e 387)	Não	Sim, com alterações e acréscimos no Marco Civil da Internet, com possibilidades administrativas e processuais.	DL nº 2.848/1940, DL nº 3.689/1941, Lei nº 8.072/1990 e Lei nº 12.965/2014
	4.148/2015	Criminalização, com aumento de pena (art. 141, CP)	Não	Não	DL nº 2.848/1940
	7.537/2017	Criminalização, com aumento de pena (art. 141, CP, e art. 66 do CDC)	Não	Não	DL nº 2.848/1940 Lei nº 8.078/1990

[211] Tal metodologia foi utilizada pelo autor da Tese para apresentar, na CPMI das *Fake News*, no ano de 2019, um estudo prévio sobre as *fake news* e a falha normativa no que tange "às políticas públicas sobre *fake news*" [...] Então a lógica que eu tenho visto é de termos uma legislação que vise a pena e a punição. Temos aí nesse contexto o Marco Civil da Internet e a Lei Geral de Proteção de Dados que são extremamente importantes, traz direitos e também traz deveres aos provedores de aplicação e conexão. Mas o ponto de vista procedimental, de políticas públicas, ainda há necessidade de um reforço nesse contexto justamente para obrigar os gestores a adotarem o que eu chamei genericamente de políticas públicas" (KINUE, 2019).

	781/2019	Criminalização, com aumento de pena (art. 141, Parágrafo único, CP), incluindo o uso de perfil falso.	Não	Não	DL nº 2.848/1940
	4.301/2019	Criminalização, com alteração da redação dos crimes de calúnia, difamação e injúria, além de aumento de pena (art. 141, CP)	Não	Não	DL nº 2.848/1940
PL nº 6.812/2017 [212]	6.812/2017	Criminalização, com previsão de tipo novo, com pena restritiva de liberdade e de multa	Pode ser considerado	A multa seria revertida ao Fundo de Defesa dos Direitos Difusos – CFDD	Não especifica
	7.604/2017	Responsabilidades aos provedores	Pode ser considerado	Aplicação de multa pela não retirada de informações falsas e imposição de filtros e ferramentas	Não especifica
	8.592/2017	Criminalização, com criação do tipo "Divulgação de informação falsa" (art. 287-A, CP)	Não	Não	DL nº 2.848/1940
	9.533/2018	Criminalização, com duas causas de aumento de pena (arts. 21 e 23, LSN) e criação do art. 22-A	Não	Não	Lei nº 7.170/1983
	9.554/2018	Criminalização, com criação do tipo "Divulgação de informação ou notícia falsa" (art. 287-A, CP)	Não	Não	DL n° 2.848/1940
	9.647/2018	Responsabilidade civil dos provedores, processo no juizado especial e tutela antecipada	Não	Responsabilidade civil dos provedores, processo no juizado especial e tutela antecipada	Lei nº 12.965/2014
	9.761/2018	Criminalização, com criação do tipo "Divulgação de notícia falsa" (art. 139-A, CP)	Não	Não	DL nº 2.848/1940

[212] O PL nº 6812/2017 deve outros projetos apensados a ele após 2020, chegando ao número de 28 projetos reunidos antes do apensamento ao PL nº 2.630/2020: PL nº 7.604/2017 (4), PL nº 9.647/2018 (2), PL nº 2.601/2019, PL nº 2.602/2019, PL nº 2.516/2022, PL nº 8.592/2017, PL nº 9.533/2018, PL nº 9.554/2018, PL nº 9.761/2018, PL nº 9.838/2018, PL nº 9.884/2018, PL nº 9.931/2018 (1), PL nº 4.134/2021, PL nº 200/2019, PL nº 241/2019, PL nº 693/2020 (10), PL nº 705/2020 (1), PL nº 1.394/2020, PL nº 988/2020 (1), PL nº 1.923/2021, PL nº 1.258/2020.

	9.838/2018	Criminalização, com criação do tipo "Criação e divulgação de notícia falsa" (art. 139-A, CP)	Não	Não	DL nº 2.848/1940
	9.884/2018	Criminalização, com criação do tipo "Divulgação de informação falsa" (art. 308-A, CP)	Não	Não	DL nº 2.848/1940
	9.931/2018	Criminalização, com criação do tipo "Divulgação de notícia falsa" (art. 286-A, CP), alteração do CPP e do MCI	Não	Sim, com norma processual penal de remoção de conteúdo (art. 319, CPP) e correspondência no MCI (art. 21-A)	DL nº 2.848/1940 DL nº 3.689/1941 e Lei nº 12.965/2014
	200/2019	Criminalização, com previsão de tipo novo, com pena restritiva de liberdade e de multa	Pode ser considerado	A multa seria revertida ao Fundo de Defesa dos Direitos Difusos – CFDD	Não especifica
	241/2019	Criminalização, com criação do tipo "Criação e propagação de notícia inverídica" (art. 139-A, CP)	Não	Não	DL nº 2.848/1940
	2.601/2019	Criminalização, com criação do tipo "Divulgação de notícia falsa" (art. 139-A, CP) e responsabilidade solidária do provedor (art. 21-A, MCI)	Não	Responsabilidade solidária do provedor de conteúdo caso deixe de remover a notícia falsa quando notificado	DL nº 2.848/1940 e Lei nº 12.965/2014
	2.602/2019	Responsabilidade civil dos provedores	Não	Responsabilidade civil dos provedores, caso deixe de remover a notícia falsa quando notificado e com ciência do boletim de ocorrência	Lei nº 12.965/2014
PL nº 1.585/2019	1.585/2019	Proibição de divulgação de nomes, fotos e vídeos de autores de crimes	Política pública de preservação da imagem dos autores de crimes	Não.	DL nº 2.848/1940 Lei nº 12.965/2014
	1.797/2019	Criminalização da conduta e proibição de publicização de imagem de autor de crime de terrorismo e/ou de crimes que causem comoção ou repúdio públicos	Não	Não	Lei nº 13.260/2016

	2.285/2019	Proibição de publicização de imagem de autor de crime de terrorismo e/ou de crimes de massacres/ataques	Não	Previsão de multa pelo descumprimento da proibição	Lei nº 13.260/2016
	2.463/2019	Proibição de publicização de imagens e informações sobre ataques massivos a pessoas	Não	Previsão de multa pelo descumprimento da proibição, sendo maior no caso de meios de comunicação	Não especifica
SENADO FEDERAL					
Ano	**Número do projeto**	**Enfoque da proposta**	**Política pública e de orientação**	**Proposta alternativa de pena, medida administrativa ou de solução de conflito**	**Legislação a incrementar ou alterar**
2018	PLS nº 246	Incremento do Marco Civil da Internet, com inclusão de dois artigos (21-A e 21-B)	Não	Prevê multa diária em caso de descumprimento de ordem judicial que determinar a indisponibilização de conteúdo	Lei nº 12.965/2014
	PLS nº 478	Institui os crimes de criação ou divulgação de notícia falsa, de criação ou divulgação de notícia falsa para afetar indevidamente o processo eleitoral, define notícia falta para os efeitos da lei e dá outras providências.	Não	Prevê a responsabilidade do provedor de aplicações de Internet na remoção, pós notificação, de notícias falsas (art. 18-A)	DL nº 2.848 (CP), Lei nº 4.737/1965 e Lei nº 12.965/2014
	PLS nº 533[213]	Definição de infrações penal, eleitoral e civil de criar ou divulgar notícia falsa, e cominar as respectivas penas	Não	Previsão de orientações aos provedores de aplicação quanto ao controle e à remoção de conteúdo de notícias falsas.	DL nº 2.848 (CP), Lei nº 4.737/1965 e Lei nº 12.965/2014
2019	PL nº 4.975[214]	Previsão de adequação da pena prevista no art. 326-A do Código	Não	Não	Lei nº 4.737/1965 e Lei nº 13.834/2019

[213] Traz o conceito de notícia falsa como "texto não ficcional que, consideradas as características de sua veiculação, possua o potencial de ludibriar o receptor em relação à veracidade do fato" (art. 5º, inc. IX).

[214] A partir de 2019 os Projetos de Lei do Senado Federal têm a nomenclatura igual à da Câmara dos Deputados, ou seja, apenas "Projeto de Lei", excluindo o complemento "do Senado". No entanto, por uma questão de identificação, continuar-se-á a adotar do termo "PLS" (Projeto de Lei do Senado).

		Eleitoral, inserido pela Lei nº 13.834/2019			

Fonte: Produzido pelo autor (2023).

Notadamente como forma de autoproteção do legislador nacional, a avalanche de projetos começou, conforme demonstrado no quadro anterior, em 2015, acentuando-se sobremaneira em 2018 (pré-eleições) e, novamente, em 2019. Na Câmara dos Deputados, o PL nº 215/2015, ao qual estão apensados atualmente outros dez projetos legislativos[215], teve discussão bastante intensa, tendo enfocado seus substitutivos para alteração do Código Penal, do Código de Processo Penal e Marco Civil da Internet, ou seja, teve atenção também voltada à produção de prova, com sua obtenção, legitimação e registro no procedimento policial e no processo (CÂMARA DOS DEPUTADOS, 2015, p. 522-550). Após passar pela Comissão de Constituição e Justiça e de Cidadania (CCJC), desde 2015 encontra-se na Mesa Diretora da Câmara dos Deputados (MESA)[216], não tendo sido apensado ao PL nº 2.630/2020.

Dois projetos legislativos, apensados ao PL nº 215/2015, destacam-se: o PL nº 1.547 e o PL nº 1.589, ambos de 2015, pois as propostas neles contidas foram consideradas no compilado dos substitutivos apresentados, não só focando na criminalização, mas também no aspecto procedimental, seja ele 'administrativo' – ou seja, de a própria vítima de uma ofensa por notícia falsa efetivar a notificação do provedor e este retirar o conteúdo sem necessidade de uma ordem judicial –, ou processual, não só judicial, mas ainda na fase inquisitória, estabelecendo diretrizes na obtenção dos registros de acesso, fundamentais para a apuração da autoria delitiva nos casos de delitos cometidos com o uso da Internet.

No segundo bloco de Projetos de Lei na Câmara dos Deputados, tabulados anteriormente, o PL nº 6.812/2017 é o projeto 'base' de um total de vinte e oito propostas, encontrando-se em apensado ao PL nº 2.630/2020[217]. A grande maioria dos projetos tende à criminalização das condutas, ou de criação e/ou de divulgação de notícias falsas/inverídicas, criando um tipo penal novo (variam os contextos de onde encaixar o delito, tanto que três projetos sequer fazem referência à norma penal a incrementar/modificar). Duas propostas legislativas (PL nº 7.604/2017 e nº 2.602/2019) se destacam por contemplar medidas de remoção/retirada de conteúdo com notícias falsas e responsabilização pela não exclusão após

[215] Apensados ao PL nº 215/2015 (10): PL nº 1.547/2015, PL nº 1.589/2015, PL nº 4.148/2015, PL nº 7.537/2017, PL nº 781/2019, PL nº 4.301/2019, PL nº 629/2020, PL nº 4.046/2020, PL nº 4.096/2020, PL nº 278/2021.
[216] Pesquisa efetuada em 13 jan. 2023.
[217] Pesquisa atualizada em 13 jan. 2023.

a notificação. Também, apenas o PL nº 9.931/2018 prevê alteração do Código de Processo Penal, porém ali inserindo a providência judicial na notificação para fins de remoção do conteúdo, pelos provedores, contendo a falsidade informacional. Nenhum dos PLs estabelece uma política pública em relação ao tema.

Já o terceiro bloco de análise, cujos Projetos de Lei foram apresentados em 2019 e estão reunidos no PL nº 1.585/2019, contempla também a previsão de proibição de divulgação de imagens e/ou notícias referentes a autores, quanto ao fato em si, de atos terroristas ou de ataques massivos (massacres), tal qual ocorreu na Escola de Suzano[218], podendo-se inferir que esse foi o principal fato propulsor dos projetos. Apenas um dos projetos pretende criminalizar a conduta (PL nº 1.797/2019), sendo os demais com propostas de imposição de multas pecuniárias. Esse bloco, então, transparece destoar dos dois anteriores, bem como das três propostas em curso no Senado Federal. Coaduna-se, muito mais, com outra proposta legislativa em curso há mais de 20 anos na Câmara dos Deputados: o PL nº 1.820/1996, que trata "sobre a identificação criminal dos indiciados pela prática de crimes hediondos"[219].

No entanto, percebe-se que o legislador brasileiro não se ateve, necessariamente, ao bem jurídico a ser tutelado, focando no desvio, na ação desviante. A moldura dada pelas notícias envolvendo *fake news* é reafirmadora e construtora da realidade social sobre o tema e da construção social da criminalidade cibernética, comunicação que é recepcionada pelo sistema legislativo brasileiro (BUDÓ, 2008; 2012; 2013). Trabalha no estereótipo perfeito das vítimas, no caso os políticos e candidatos, e no perfil agressor do criminoso, do propagador de notícias falsas, do *hater*, separando o bem e o mal, os bons e os ruins. Deixou-se de lado, então, a definição do bem jurídico a ser penalmente tutelado, por exemplo, a honra das pessoas objeto da notícia, da imagem ou do vídeo falso, a partir do que se poderia partir para o contexto da finalidade a ser atingida com tal conduta: (a) influenciar no processo eleitoral, seja ele eleições regulamentares ou para cargos específicos (ex.: reitor de universidade, conselheiro tutelar etc.); e (b) causar transtorno, balbúrdia e desassossego social (ex.: exploração de supostos casos de massacres).

Ademais, quanto à finalidade de preservação das eleições, em face da já sancionada Lei nº 13.834/2019, não faz, nessa parte, sentido o PLS nº 471/2018, porquanto já abarcada tal finalidade. A gama de projetos tem, então, um centro principal, no qual se concentram as

---

[218] O tiroteio na Escola Estadual Professor Raul Brasil, na cidade de Suzano, em São Paulo, ocorreu em 13 de março de 2019, tendo repercussão nacional e internacional na mídia (FREITAS; GONÇALVES, 2020).

[219] O PL nº 1.820/1996 recebeu outros projetos apensos durante esses anos: PL nº 188/1999 (4), PL nº 4.335/2008 (3), PL nº 4.487/2008 (2), PL nº 2.371/2011, PL nº 2.624/2011 e PL nº 417/2003. Tais projetos restaram prejudicados em razão da aprovação da Lei nº 12.654/2012, que trata da coleta de perfil genético.

ideias de criminalização, seja pelo incremento da pena, seja pela criação de novos tipos penais. Ao entorno desse centro ‘criminalizante’ gravitam poucas propostas contendo (a) a coleta, legitimação e validação de evidências digitais (ou seja, relativas ao Código de Processo Penal), e (b) outras enfocando responsabilidades pela remoção de conteúdo sob pena de responsabilidade, com menor ou maior imposição de multas, especificando ou não um tempo para essa medida (ou seja, relativas à Lei nº 12.965/2014).

No entanto, outras propostas legislativas também são relacionadas ao Marco Civil da Internet, conforme análise no tópico sobre as propostas normativas de caráter processual penal. Dos blocos analisados, o do PL nº 6.812/2017 segue relacionado ao tema das *fake news* (CÂMARA DOS DEPUTADOS, 2018b), porém agregado ao bloco de discussão principal da Câmara dos Deputados, o PL nº 2.630/2020, o qual será objeto de observações a seguir.

4.3.2.1 Pandemia *fake news*: o incremento da discussão legislativa

A já existente legislação brasileira, comentada nos itens anteriores, seja relativa à tipificação penal já disponível, seja também sobre as possibilidades de remoção/suspensão de conteúdo, não impede, portanto, que o legislativo brasileiro analise outras possibilidades de inclusão nas normas, penais e processuais, respectivamente, de tipos penais e de procedimentos quanto à circulação de desinformação no Brasil. Assim, cumpre acrescentar à análise não só os aspectos atinentes à proposta da ‘Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet’, como também as propostas legislativas pós-pandemia que buscam a criminalização de condutas relativas à propagação das chamadas *fake news*.

Na direção de controle, de remoção e/ou de indisponibilização do conteúdo da rede mundial de computadores, pode-se citar o PL nº 1.429/2020, dos Deputados Felipe Rigoni (PSB/ES) e Tabata Amaral (PDT/SP), que propunha a instituição da ‘Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet’. O projeto, já arquivado e substituído por outro similar (PL nº 3.063/2020[220]), estabelece diretrizes de atuação para provedores de aplicação em relação a contas inautênticas, disseminação de desinformação, conteúdos, anúncios *on-line* e propagandas políticas patrocinadas no Brasil, determinando ações proativas por parte de provedores de aplicação para proteger seus serviços contra a

[220] Atualmente, este PL está apensado ao PL nº 2.630/2020 (pesquisa em 13 jan. 2023).

disseminação de desinformação através de medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso de boas práticas.

Ainda, a proposta legislativa contempla a possibilidade de que, uma vez identificado o conteúdo malicioso, devem os provedores de aplicação (a) providenciar ações como sua rotulação como desinformação, (b) desabilitar sua transmissão para mais de um usuário por vez, (c) mostrar o nome do criador original do conteúdo e (d) alterar o algoritmo de visualização para diminuir ou eliminar seu alcance.

Verifica-se e pontua-se que os projetos citados não tratam da exclusão de conteúdo, mas sim da correção da desinformação veiculada o mais rápido possível (pelo menos na mesma velocidade da sua disseminação), evitando, assim, o efeito da pós-verdade. Em sua justificativa, aponta que pesquisas realizadas na Universidade George Washington e na Universidade de Ohio indicaram que o fornecimento de correções, realizadas por verificadores, aos usuários de mídias sociais que viram informações falsas ou enganosas tem o potencial de diminuir a crença na desinformação em até 61%.

Por sua vez, sob a mesma ótica dos projetos anteriores citados (Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet[221]), o PL nº 2.630/2020, apresentado no Senado Federal pelo senador Alessandro Vieira, também propunha filtrar os provedores de aplicação que devem se submeter às regras pelo número de usuários (dois milhões de usuários registrados) e não pela receita bruta anual, como o PL nº 1.429/2020 (substituído pelo PL nº 3.063/2020).

O PL nº 2.630/2020, aprovado no Senado Federal e enviado à Câmara dos Deputados, também considera os princípios dispostos na Lei nº 12.965/2014 (Marco Civil da Internet), fornece conceitos, dever de transparência de provedores de aplicação e outros dispositivos para o combate à desinformação e para o aumento da transparência na Internet. Ressalta-se também o "combate" a contas inautênticas, aos disseminadores artificiais não rotulados (robôs), assim como contas patrocinadas não identificadas.

Vários pontos polêmicos nesse PL seguem em debate na Câmara dos Deputados. O PL não vislumbra, assim, a remoção do conteúdo malicioso, porém reforça medidas contra sua proliferação, como remoção de contas de aplicativos de mensageria privados em que o

[221] Dentre todos os projetos da referida Lei, encontra-se em fase mais adiantada o PL nº 2.630 de 2020, de autoria do senador Alessandro Vieira, que recebeu mais de 100 emendas e foi aprovado no Senado Federal – mesmo tendo uma enquete pública com mais votos contrários do que a favor – e encontra-se na Câmara dos Deputados para análise. Informação disponível em https://www25.senado.leg.br/web/atividade/materias/-/materia/141944, acesso em 13 janeiro 2023.

usuário não declarar o uso de disseminadores artificiais caso o volume de movimentação e número de postagens seja incompatível com o uso humano.

Ainda, estipula o uso de verificadores de fatos independentes, desabilitação de recursos de transmissão de conteúdo desinformativo, sendo este rotulado como tal, e a interrupção imediata da promoção paga ou da promoção gratuita artificial do conteúdo, seja por mecanismo de recomendação ou outros mecanismos de ampliação de alcance do conteúdo na plataforma.

Ao final, conforme o projeto inicial (art. 28) e o projeto aprovado (art. 31), prevê sanções a que se sujeitam os provedores de aplicação.

A proposta da 'Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet', que visa a interrupção de transmissão de conteúdo malicioso através de ações proativas de provedores de aplicação no combate à desinformação, contemplava quatro propostas sobre o mesmíssimo tema (três na Câmara dos Deputados e uma no Senado Federal):

Quadro 15: Projetos de Lei sobre a 'Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet'

Projeto	Data da apresentação	Objetivo	Parâmetros obrigacionais	Casa legislativa	Situação em 09/06/2020
PL Nº 1.429 de 2020	01/04/2020	Ações proativas de provedores de aplicação no combate à desinformação	Provedores de aplicação com receita bruta total no ano-calendário superior a R$ 78.000.000,00	Câmara dos Deputados	Retirado em 04/06/2020
PL nº 2.630 de 2020	13/05/2020	Ações proativas de provedores de aplicação no combate à desinformação	Provedores de aplicação com mais de 2 milhões de usuários registrados	Senado Federal	Aprovado no Senado Federal, tendo tido mais de 100 emendas. Chegou na Câmara dos Deputados em 03/07/2020. Tem apensados 72 PLs.
PL nº 2.927 de 2020	26/05/2020	Ações proativas de provedores de aplicação no combate à desinformação	Provedores de aplicação com mais de 2 milhões de usuários registrados	Câmara dos Deputados	Requerimento de retirada protocolado em 02/06/2020
PL nº 3.063 de 2020	02/06/2020	Ações proativas de provedores de aplicação no combate à desinformação	Provedores de aplicação com mais de 2 milhões de usuários registrados	Câmara dos Deputados	Reapresentado em 02/06/2020

Fonte: Produzido pelo autor (2023).

Percebe-se, então, que o objeto do PL nº 2.630/2020, que trata da 'Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet', é não penal, de controle das *fake news*, de controle da desinformação. Em janeiro de 2023 o PL referido já conta com 87 projetos de lei[222] agregados ao debate do constructo normativo[223], alguns deles direcionando, como visto pela construção inicial dos blocos de projetos (a partir do PL nº 6.812/2017), a criação de tipos penais.

4.3.2.2 *Fake news*: entre a cruz e a espada, qual a solução?

A análise dos projetos voltados ao tema das *fake news* é complexa, porém, em razão da proposta da presente pesquisa, cumpre tecer observações sobre projetos legislativos buscando a criminalização e/ou incremento da pena, bem como não descuidar da previsão ou não quanto à remoção e/ou indisponibilidade do conteúdo com desinformação, o que seria uma política adequada de redução e/ou mitigação dos danos cibernéticos daí derivados. Conforme apontado por Kinue (2019), retratando uma das audiências públicas da CPMI das *Fake News* (TV SENADO, 2019), a falha apontada para a legislação sobre *fake news* é quanto à ausência de políticas públicas[224].

---

[222] Projetos normativos apensados ao PL nº 2.630/2020 (87): PL nº 1.676/2015 (28), PL nº 2.712/2015 (23), PL nº 346/2019, PL nº 283/2020 (20), PL nº 2.854/2020 (1), PL nº 3.029/2020, PL nº 2.883/2020 (1), PL nº 649/2021, PL nº 3.119/2020 (3), PL nº 1.589/2021, PL nº 2.393/2021, PL nº 2.831/2021, PL nº 3.395/2020 (3), PL nº 291/2021, PL nº 449/2021, PL nº 3.700/2021, PL nº 3.573/2020 (3), PL nº 213/2021, PL nº 495/2021, PL nº 2.401/2021, PL nº 127/2021 (3), PL nº 246/2021 (1), PL nº 1.362/2021, PL nº 865/2021, PL nº 2.390/2021, PL nº 10.860/2018 (1), PL nº 5.776/2019, PL nº 475/2020, PL nº 4.418/2020, PL nº 6.812/2017 (28), PL nº 7.604/2017 (4), PL nº 9.647/2018 (2), PL nº 2.601/2019 , PL nº 2.602/2019, PL nº 2.516/2022, PL nº 8.592/2017, PL nº 9.533/2018, PL nº 9.554/2018, PL nº 9.761/2018, PL nº 9.838/2018, PL nº 9.884/2018, PL nº 9.931/2018 (1), PL nº 4.134/2021, PL nº 200/2019, PL nº 241/2019, PL nº 693/2020 (10), PL nº 705/2020 (1), PL nº 1.394/2020, PL nº 988/2020 (1), PL nº 1.923/2021, PL nº 1.258/2020, PL nº 1.941/2020, PL nº 2.389/2020 (1), PL nº 808/2020, PL nº 2.790/2020 (1), PL nº 1.001/2021, PL nº 2.196/2020, PL nº 3.307/2020, PL nº 1.974/2019, PL nº 3.389/2019 (10), PL nº 4.925/2019 (3), PL nº 5.260/2019, PL nº 437/2020, PL nº 2.284/2020, PL nº 6.351/2019 (4), PL nº 517/2020, PL nº 3.044/2020, PL nº 1.590/2021, PL nº 2.989/2021, PL nº 2.763/2020, PL nº 3.857/2019, PL nº 5.959/2019 (2), PL nº 1.772/2021 (1), PL nº 2.060/2021, PL nº 2.844/2020 (1), PL nº 3.222/2020, PL nº 3.063/2020 (1), PL nº 3.144/2020, PL nº 3.627/2020, PL nº 356/2021 (1), PL nº 388/2021, PL nº 1.743/2021, PL nº 1.897/2021, PL nº 3.366/2021, PL nº 143/2022, PL nº 714/2022, PL nº 836/2022. O número entre parênteses colocado após o número do PL corresponde ao número de projetos apensados a ele antes do apensamento ao PL nº 2.630/2020.

[223] Os debates se concentram também na realização de audiências públicas sobre o tema.

[224] A audiência do dia 19/11/2019 teve participação do autor da tese, quando foram apresentadas as primeiras análises sobre a legislação e os projetos existentes (KINUE, 2019). "Senadores e deputados da Comissão Parlamentar Mista de Inquérito – *Fake News* (CPMI das *Fake News*) ouvem especialistas em crimes cibernéticos e segurança digital. Estão convidados o delegado Emerson Wendt, o professor da FGV Pablo Cerdeira e o diretor do InternetLab, Francisco Brito Cruz. Publicado na internet em 19/11/2019" (TV SENADO, 2019).

Inicia-se, assim, pela citação dos PLs nº 808/2020 e nº 1.258/2020, ambos apensados ao PL nº 2.630/2020, que visam a inclusões/alterações no Marco Civil da Internet (artigo 19, § 3º) e Código Penal (artigo 122, § 8º), assim como inclusão do artigo 259-A também no Código Penal, respectivamente.

Ambos os projetos discorrem sobre a remoção da desinformação, porém também apenas sob mecanismos judiciais ou pelo próprio autor da 'falácia', entretanto apenas após seu indiciamento formal pelo Delegado de Polícia. Ou seja, enfocam na tipificação de conduta sem apresentar mecanismos objetivos e céleres para a remoção do conteúdo, não impedindo, assim, que a desinformação seja cada vez mais disseminada no meio digital. Esses destaques foram feitos em depoimento, em 2021, ao Grupo de Trabalho (GT-NET) na Câmara dos Deputados, "destinado a analisar e elaborar parecer ao Projeto de Lei nº 2.630, de 2020 e apensados, que visa ao aperfeiçoamento da legislação brasileira referente à liberdade, responsabilidade e transparência na Internet"[225].

Também, outros dois PLs, nº 705/2020 e nº 1.394/2020 (ambos apensados ao PL nº 693/2020), visam à criminalização de condutas ligadas à propagação de notícia sabidamente falsa envolvendo a saúde pública nacional e/ou durante tempos de pandemia. O primeiro deles sugere a inserção do artigo 339-A no Código Penal Brasileiro (TÍTULO XI – Dos Crimes Contra a Administração Pública, Capítulo III – Crimes Contra a Administração da Justiça) logo após o crime de denunciação caluniosa. Já o segundo sugeriu a inserção do artigo 287-A sob o nome de 'Criação ou propagação de informação falsa', no TÍTULO IX – Dos Crimes Contra a Paz Pública.

Já o PL nº 2.389/2020 visa à tipificação da conduta de criação, divulgação e disseminação de informações falsas sobre qualquer pandemia na rede mundial de computadores, provedores de aplicações de Internet, mídias sociais ou mensagens instantâneas. Tal projeto foi apensado ao PL nº 693/2020[226], pois se trata de circunstância voltada ao controle (na divulgação) e à disseminação (compartilhamento) de notícias falsas sobre a pandemia. Há que se destacar e dar atenção às penas sugeridas, pelo PL nº 2.389/2020, para o tipo penal criado no artigo 140-A (Crimes Contra a Honra) do Código

---

[225] O GT-NET foi criado em 21/06/2021 na Câmara dos Deputados. Em requerimento apresentado no dia 15/07/2021, o nome do autor da tese foi apresentado para ser ouvido em audiência pública, esta realizada em 23/09/202. O GT teve sua última reunião em 7/12/2021 e tem um relatório final com apresentação de substitutivo (CÂMARA, 2021).

[226] Estão apensados ao PL nº 693/2020 dez projetos legislativos: PL nº 705/2020 (1), PL nº 1.394/2020; PL nº 988/2020 (1), PL nº 1.923/2021; PL nº 1.258/2020; PL nº 1.941/2020; PL nº 2.389/2020 (1); PL nº 808/2020, PL nº 2.790/2020 (1), PL nº 1.001/2021.

Penal Brasileiro. Aquele que disseminar a desinformação acerca de qualquer pandemia através da Internet, redes sociais, aplicativos quaisquer ou redes sociais pode enfrentar pena de detenção de dois a quatro anos e multa ou reclusão de quatro a dez anos no caso de ser o agente líder ou coordenador do grupo de rede virtual ou social. Tal tipificação é similar à adotada no § 5º do art. 122 do CP. Cumpre referir que, mesmo com os debates já havidos, o PL nº 693/2020 foi apensado ao PL nº 2.630/2020.

O PL nº 1.416/2020, por sua vez, propõe o crime de responsabilidade a disseminação ou o compartilhamento por ocupante de cargo, função ou emprego público de informação falsa, sem fundamento ou difamatória[227].

Embora muito parecidos e com 'localização geográfica' diversa no diploma penal, a maioria dos projetos citados (e dos não citados) não trata de remoção de conteúdo, tendo o foco na simples e pura criminalização ou penalização da conduta de propagar informações sabiamente falsas. Esse apontamento foi feito em depoimento ao GT-NET:

> O Sr. Emerson Wendt, delegado de Polícia Civil, afirmou que o dano cibernético deve ser evitado antes da publicação. Abordou as várias leis que tentaram reduzir dados cibernéticos no Brasil. Disse que as plataformas são rápidas para atender seus próprios termos de uso, mas não tão rápidas para cumprir regras legais e que a suspensão do conteúdo deveria ser feita de forma cautelar se houvesse notícia falsa comprovada por mensagem. (CÂMARA, 2021, p. 24).

O panorama demonstrava uma divisão de intenções do legislador brasileiro em 2020, com 11 (onze) das propostas voltadas à criminalização e o incremento do Direito Penal e 11 (onze) propostas sem previsão de crime e com opções de remoção de conteúdo, enfrentamento à desinformação, bloqueio, desanonimização de postagens, responsabilidade (solidária) dos provedores e, inclusive, vedação de restrições para redução de alcance de usuários por motivos de convicção política e ideológica, ou seja, propugnando pela liberdade de expressão, corolário constitucional já vigente.

Esse panorama está mais complexo no início de 2023, com o sistema legislativo tendo de, com a estruturação normativa do tema, estruturar vários aspectos relacionados às *fake news* a partir do contexto da Internet e assim o fará a partir do projeto principal, o PL nº 2.630/2020, mais direcionado à regulação cível, e com propostas e discussões já relatadas, como o substitutivo apresentado pelo GT-NET em final de 2021 (CÂMARA, 2021).

---

[227] O PL nº 1.416/2020 tem um apensado: PL nº 4.329/2020.

4.3.3 Expectativas dos atores de investigação cibernética e incremento penal: outras observações

Destacou-se, no princípio do tópico sobre os projetos relativos à Internet no Brasil, que a expectativa dos atores de investigação cibernética estava voltada, também, à criação de tipos penais aptos a abarcar as condutas de (a) desconfiguração de páginas da Internet (*defacement*), (b) o uso de *ransomwere* (encriptação de arquivos com uso de código malicioso e solicitação de resgate em criptoativos), (c) perfil falso no âmbito da Internet (perfis de pessoas físicas ou jurídicas), (d) estupro pela Internet, (e) invasão e sequestro de contas de redes sociais e, também, (f) lavagem de dinheiro com criptoativos.

Quanto à lavagem de dinheiro com criptoativos, tal expectativa cognitiva dos atores de investigação cibernética [expectativa "f"] já foi suprida (ver 4.2.1.9), restando, pois, expectáveis as suas observações quanto à adequação prática dos tipos penais às situações do dia a dia.

Em relação ao *ransomwere* [expectativa "b"], o PL nº 2.232/2021[228] condensava a proposta de criação do crime de "extorsão cibernética", incluindo os §§ 4º e 5º no art. 158 do Código Penal. Esse projeto foi apensado ao PL nº 5.441/2020[229], que traz os conceitos, para fins de efeitos penais, de "sistema informatizado", "dados informatizados", "provedor de serviços", "dados de tráfego", "artefato malicioso" e "credencial de acesso", além de prever os crimes de "acesso indevido", "sabotagem informática", "dano a dados informatizados", "fraude informatizada", "obtenção indevida de credenciais de acesso" e "artefato malicioso".

O PLs nº 5.441/2020 e nº 2.232/2021 foram apensados ao PL nº 3.357/2015, que trata do projeto de criação do tipo penal específico de invadir dispositivo informático, sem a devida autorização, modificando conteúdo de sítio da Internet, ou seja, abarcando a expectativa "a", referida por um dos atores de investigação cibernética. No Senado Federal foi apresentado o PL nº 879/2022, que propõe integrar ao Código Penal o art. 154-C, de "Sequestro de dados informáticos", possibilitando o enquadramento conforme expectativa dos atores de investigação cibernética.

Outros PLs, que contemplam expectativas cognitivas dos atores de investigação cibernética, estão apensados ao PL nº 3.357/2015:

---

[228] Apensados ao PL nº 2.232/2021 (4): PL nº 2.971/2021 (3), PL nº 3.010/2021 (1), PL nº 970/2022, PL nº 4.072/2021.

[229] Apensados ao PL nº 5.441/2020 (5): PL nº 2.232/2021 (4), PL nº 2.971/2021 (3), PL nº 3.010/2021 (1), PL nº 970/2022, PL nº 4.072/2021.

- PL nº 2.233/2021: propõe a modificação da redação do art. 154-A, § 1º, para acrescentar a conduta típica de "usurpação ou acesso indevido de conta de usuário de aplicação de Internet ou qualquer meio digital (clonagem)" [expectativa "e"].

- Os PLs nº 2.545/2019, nº 5.261/2019, nº 310/2020, nº 5.265/2020, nº 5.506/2020, nº 5.278/2020, dentre outros apensados ao PL nº 3.357/2015, propõem a alteração do art. 154-A do Código Penal, tal qual é a expectativa dos entrevistados, inclusive quando ao aumento de pena (ver 3.2). Destaque para o PL nº 5.200/2016, cuja autoria é da Comissão Parlamentar de Inquérito Destinada a Investigar a Prática de Crimes Cibernéticos, cuja proposta também traz definições sobre "sistema informatizado", "dados informatizados" e "mecanismo de segurança", propondo a readequação do tipo penal do art. 154-A, substituindo "dispositivo informático" por "sistema informatizado", circunstância que retiraria da pauta a discussão da limitação do texto normativo atual.

A criminalização do uso de perfil falso na Internet [expectativa "c"] está contemplada no PL nº 781/2019, apensado ao PL nº 215/2015 (ver 4.3.2 e 3.2, este especialmente quanto às expectativas de aumento de penas nos casos de crimes contra a honra em redes sociais). Também, o PL nº 7.758/2014 propõe a alteração do art. 307 do Código Penal, incluindo a prática delitiva realizada pela rede de computadores. Além dos dois projetos mencionados, o PL nº 3.627/2020, apensado ao PL nº 2.630/2020, prevê "mecanismos de verificação de identidade dos perfis ativos em aplicações de Internet".

Já a criminalização do "estupro pela Internet" [expectativa "d"] tem um conjunto de 25 propostas vinculadas ao PL nº 1.213/2011[230], analisando aspectos do tipo penal estupro de vulnerável e aumento de pena, dentre os quais se destaca o PL nº 3.628/2020, que prevê a criação do tipo penal do art. 217-B, o "estupro virtual de vulnerável".

Percebe-se, por outra parte, que várias propostas atuais, de criminalização de condutas e aumento de penas relativas às condutas praticadas no âmbito da Internet, estão sendo anexadas ao PL nº 2.630/2020, o que torna ainda mais complexa a estruturação normativa, porém, ao mesmo tempo, não compartimenta conceitos, termos e definições em regulamentações futuras distintas.

---

[230] Apensados ao PL nº 1.213/2011 (25): PL nº 4.207/2012 (24), PL nº 8.037/2014 (11), PL nº 8.581/2017 (1), PL nº 4.183/2020, PL nº 8.937/2017, PL nº 4.071/2019 (3), PL nº 556/2020, PL nº 2.809/2021, PL nº 2.004/2022, PL nº 4.667/2019 (3), PL nº 4.285/2020, PL nº 5.102/2020, PL nº 3.485/2021, PL nº 4.731/2016 (1), PL nº 4.824/2020, PL nº 5.367/2019 (8), PL nº 5.642/2019, PL nº 4.245/2020 (4), PL nº 4.265/2020, PL nº 4.271/2020, PL nº 4.345/2020, PL nº 4.716/2020, PL nº 5.095/2020, PL nº 5.101/2020, PL nº 3.628/2020.

4.4 Propostas legislativas de caráter [estruturante] processual/procedimental penal

Em paralelo àquilo que já foi observado e se transformou em Lei, criminalizando condutas e/ou incrementando as penas, verificou-se, desde já, que três legislações trouxeram inovações importantes na seara da investigação e do processo penal: Lei nº 9.296/1996 (interceptação telefônica, telemática e de informática), Lei nº 13.441/2017 (infiltração de policiais na Internet nos casos de pedofilia) e Lei nº 13.964/2019 (infiltração de agentes de polícia nos casos de organizações criminosas e crimes correlatos).

A importância de tais normas processuais se expressa na usabilidade dos procedimentos em investigação criminal e no resguardo das atividades investigativas, tanto sob a ótica do investigado quanto sob o olhar do policial ator-investigador. A inovação está em estabelecer, em face das mudanças tecnológicas e ambientadas no cibersistema da Internet, a regulamentação correspondente à forma como se dá a comunicação e a interação no campo digital.

Assim, inovação e importância são pontos que convergem (a) à proteção normativa de impedimento de utilização do procedimento sem a vênia judicial e sob condições específicas, e (b) ao resguardo do ator-investigador, que possui como base de atuação e segurança, pessoal e funcional, o texto normativo.

Por outro lado, mesmo de 'conteúdo' cível, com direitos e deveres relativamente à Internet, seus usuários e provedores (de conteúdo e aplicação), a Lei nº 12.965/2014, o Marco Civil da Internet, estabeleceu limites (temporais) e garantias (jurídicas/judiciais) ao acesso aos dados cadastrais, de conexão e de acesso dos usuários (arts. 10 a 17)[231], embora não tenha prevista a temporalidade na resposta pelos provedores. Observa-se que, em relação às previsões normativas relativas à remoção/retirada, gerenciamento de conteúdo e de perfis do ambiente da web, seja por solicitação direta seja por determinação judicial, cujas situações possam ou não abarcar a ocorrência de um dano no contexto da Internet, tais temas serão delineados ou não com a regulamentação advinda do conjunto de projetos relacionados ao PL nº 2.630/2020.

Então, para efeitos desta pesquisa, no âmbito processual penal procurar-se-á delimitar a análise sobre as eventuais modificações sobre o Marco Civil da Internet à obtenção de

---

[231] No Brasil, optou-se pela regulamentação da Internet, dos direitos e deveres dos usuários, através do Marco Civil da Internet. Uma opção *tribalista* (própria do Brasil) que prevê, inclusive, a não responsabilização dos provedores quanto ao conteúdo de terceiros, numa clara e evidente violação constitucional. Não seria e não é uma solução completa, porquanto a sua análise comporta, necessariamente, também a análise da Lei Geral de Proteção de Dados (Lei nº 13.719/2018).

dados telemáticos e informáticos, registros e conteúdo, e a políticas públicas de educação digital.

4.4.1 Proposições de alterações do Marco Civil da Internet

Existem várias propostas normativas voltadas especialmente à alteração do Marco Civil da Internet, a Lei nº 12.965/2014. Porém, há que se destacar os projetos relativos ao foco do presente trabalho: política de redução de danos cibernéticos e [expectativas de] efetividade da investigação cibernética.

Como se observou, vários projetos que tratam também da alteração do MCI estão vinculados ao PL nº 2.630/2020. Dentre eles, destaca-se o PL nº 3.389/2019 e seus 10 apensos[232], que teria por objetivo "estabelecer a obrigatoriedade de fornecimento do número de inscrição no Cadastro de Pessoas Físicas (CPF) ou Cadastro Nacional de Pessoa Jurídica (CNPJ) para cadastro em aplicações de Internet", o que redundaria em um processo de controle direto sobre os acessos dos usuários, circunstância que, embora contemplando as expectativas dos atores de investigação criminal, foge da lógica regulativa da Internet[233].

Por outro lado, aponta-se o PL nº 9.808/2018[234], que pretende acrescentar os parágrafos 5° e 6º ao art. 10 da Lei nº 12.965, de 23 de abril de 2014, "para dispor sobre o acesso a dados de comunicação por meio de aplicativos de Internet para fins de persecução criminal, nos casos que especifica". O referido PL encontra-se apensado ao PL nº 6.960/2017, que possui outras propostas agregadas: PL nº 7.498/2017, PL nº 1.782/2019 e PL nº 4.442/2019. Este PL nº 4.442/2019 atenderia à expectativa dos entrevistados por prever a possibilidade de "a autoridade policial requisitar os dados".

Todos os projetos, segundo seus proponentes, visam a acrescer condições de instrumentalidade às investigações e processos judiciais, dando possibilidade de consecução mais célere da autoria delitiva e individualização da conduta, especialmente em casos de "situação flagrante de crimes definidos em lei como hediondo, de tráfico de drogas ou

---

[232] Apensados ao PL nº 3.389/2019 (10): PL nº 4.925/2019 (3), PL nº 5.260/2019, PL nº 437/2020, PL nº 2.284/2020, PL nº 6.351/2019 (4), PL nº 517/2020, PL nº 3.044/2020, PL nº 1.590/2021, PL nº 2.989/2021, PL nº 2.763/2020.

[233] O PL nº 1.585/2019 foi analisado quando das observações sobre as propostas normativas sobre *fake news*, porém também contempla modificação do Marco Civil da Internet (ver 4.3.2); o PL nº 215/2015 e seus apensos, já analisados, também têm previsão de alteração do Marco Civil da Internet (ver 4.3.2 e 4.3.3); os PLs nº 4.925/2019, nº 808/2020, nº 1.258/2020 e nº 3.389/2020, que foram apensados ao PL nº 2.630/2020, também preveem alteração no Marco Civil da Internet (ver 4.3.2).

[234] Apensados ao PL nº 9.808/2018 (2): PL nº 1.782/2019 e PL nº 4.442/2019.

terrorismo" (CÂMARA, 2017). Também, têm previsão para soluções técnicas como o fornecimento da chave criptográfica "que permita o acesso aos dados e conteúdos de comunicação privada de dispositivo móvel". As mutações citadas são sugeridas sobre o art. 10 do MCI, além das propostas de alteração e aumento do prazo de guarda de dados, a ser previsto nos arts. 13 e 15 do mesmo diploma. O bloco de projetos [PL nº 6.960/2017] teve parecer do relator na Comissão de Constituição e Justiça e de Cidadania (CCJC)[235], com apresentação de um substitutivo que reúne todas as propostas, condensando:

- inviolabilidade e sigilo de suas comunicações privadas e dos dados armazenados em terminal, salvo por ordem judicial (art. 7º, III, do MCI);

- praticidade na obtenção de dados pelos investigadores (modificação do § 1º do art. 10 do MCI, com acréscimo de dois parágrafos):

> Art.10.....
> § 1º Instaurado o procedimento investigatório, a autoridade policial ou membro do Ministério Público que presidi-lo poderá requisitar os registros referidos no caput, dispensada ordem judicial, ao provedor responsável pela guarda, que será obrigado a disponibilizá-los, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal.
> .....
> § 5º Encontrando-se o agente em situação flagrante de crimes definidos em lei como hediondo, de tráfico de drogas ou terrorismo, poderá a autoridade policial acessar, independente de autorização judicial, os dados de registro e conteúdos de comunicação privada de dispositivo móvel, quando necessário à investigação e/ou à interrupção da ação delitiva.
> § 6º No caso do parágrafo anterior, em se tratando de dados criptografados, poderá a autoridade policial requisitar, diretamente aos provedores de internet, provedores de conteúdo e autores de aplicativos de comunicação, o fornecimento de chave criptográfica que permita o acesso aos dados e conteúdos de comunicação privada de dispositivo móvel, sem prejuízo do desenvolvimento e emprego, pelas polícias judiciárias, de técnicas e ferramentas tecnológicas que atinjam esse fim específico, incluindo a utilização de dispositivos que possibilitem o acesso a conteúdo anterior à criptografia por meio de aplicativos, sistemas ou outras ferramentas".

- possibilidade de acesso aos eventos de conexão e de acesso pela autoridade policial (modificação de parágrafos dos arts. 13 e 15 do MCI):

> Art. 13. .....
> § 2º A autoridade policial poderá requisitar e a autoridade administrativa poderá requerer, cautelarmente, que os registros de conexão sejam guardados por prazo superior ao previsto no caput.
> § 3º Na hipótese do § 2º, a autoridade administrativa requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput.
> .....

[235] Pesquisa feita em 15 jan. 2023. O relator designado é o "Delegado Pablo", do Estado do Amazonas.

> § 5º Em qualquer hipótese, a disponibilização à autoridade administrativa requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.
> [...]
> Art. 15. .....
> § 1º Por ordem judicial ou por requisição da autoridade policial, os provedores de aplicações de internet que não estão sujeitos ao disposto no caput poderão ser obrigados a guardar, por certo tempo, registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.
> § 2º A autoridade policial poderá requisitar e a autoridade administrativa poderá requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado em relação à autoridade administrativa o disposto nos §§ 3º e 4º do art. 13.

Os destaques são importantes, até porque o enfoque das normas nacionais, atualmente em vigor, não parece voltado à parte procedimental, desde o contexto internacional até o campo interno dos países. Legislações voltadas a

> la solicitud de preservación y obtención de datos, la validez de la prueba obtenida en otro país, el registro de cosas físicas versus el registro de datos; la posibilidad de aplicar un software judicial a distancia, cuestiones de competencia, utilización de tecnología de cifrado. (GARCÍA LUNA; PEÑA LABRIN, 2017, p. 15).

Assim, as dificuldades não se concentram na falta de legislação adequada na parte procedimental, mas em razão da investigação ser longa e tediosa e dependente da obtenção dos dados frente aos provedores de conexão e de aplicação, além do fato de os integrantes do sistema de persecução criminal desconhecerem termos técnicos, procedimentos e ações necessárias à obtenção dos dados voltados à apuração do delito e de sua autoria.

Por outro lado, as discussões no Brasil também são relativas a um maior controle sobre a investigação criminal e atuação da segurança pública quando se trate de dados pessoais. Destacam Fernandes, Meggiolaro e Prates (2022, n.p.), que "a pretexto de se apurar a autoria de crimes, não faltam devassas de toda ordem nos sigilos telefônicos, telemáticos, de dados, bancários, compartilhamentos de informações sigilosas, tudo em prol do sucesso das investigações".

A LGPD, conhecida dos atores de investigação criminal cibernética, previu no art. 4º, caput, III, "a" e "d", c/c § 1º, necessidade de "lei específica que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular". Assim, desde 2020 foram discutidos os parâmetros de uma "LGPD Penal", cujo anteprojeto foi apresentado ao Congresso Nacional e contém 68 artigos.

Na Câmara dos Deputados, foi apresentado o PL nº 1.515/2022, contemplando proposta de "Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais", trazendo alterações nas Leis nº 12.850/2013, nº 12.965/2014; nº 9.613/1998 e nº 12.037/2009. O Anteprojeto da LGPD Penal e o PL nº 1.515/2022 são diferentes e, portanto, debates no entorno do tema serão intensos nos próximos encontros legislativos sobre o assunto. Há que se acompanhar e observar qual o caminho que o legislador brasileiro adotará para reduzir a complexidade sobre as expectativas cognitivas sociais e psíquicas, especialmente a dos envolvidos na persecução criminal.

4.4.2 Alterações previstas sobre procedimentos de obtenção de dados telemáticos (registros e conteúdo)

Independentemente do encaixe geoespacial da norma proposta sobre a obtenção de dados cadastrais e dados de acesso de um determinado perfil em aplicação da Internet utilizado em crime, a expectativa dos atores de investigação policial é por um acesso não burocratizado e, por outro lado, ágil, fazendo com que os provedores possam repassar a informação e, com isso, ser mais célere e efetiva a resposta da persecução criminal.

Em uma pesquisa no site da Câmara dos Deputados sobre o termo "telemática"[236], além de projetos de lei sobre a criminalização do estelionato eletrônico, houve retorno das seguintes propostas:

- PL nº 5.668/2019: a proposta visa a permitir que membros do Ministério Público ou os delegados de polícia "requisitem diretamente às empresas prestadoras de serviço de telecomunicações e/ou telemática os meios técnicos adequados para a localização da vítima ou dos suspeitos do delito em curso em determinados casos", propondo a alteração do art. 13-B do Código de Processo Penal. O PL nº 566/2019 foi apensado ao PL nº 8.045/2010, que trata do novo Código de Processo Penal e tem, em seus debates, 406 projetos normativos.

- PL nº 5388/2020: propõe a dispensa de autorização judicial para que "o membro do Ministério Público ou o delegado de polícia requisitem às empresas prestadoras de serviço de telecomunicações e/ou telemática os meios técnicos adequados para a localização da vítima ou dos suspeitos do delito em curso", também propondo a modificação do art. 13-B do Código de Processo Penal. Este PL foi apensado ao PL nº 5.668/2019;

---

[236] Pesquisa feita em 16 jan. 2023.

- PL nº 3.703/2015: proposta de regulamentação do "acesso a dados cadastrais e aos sinais de comunicação telefônica e/ou telemática que importem na investigação criminal e dá outras providências", estipulando regras de acesso aos dados, tipos penais relacionados às condutas divergentes quanto aos dados cadastrais, dentre outras vedações. O PL foi apensado ao PL nº 5.286/2009, que foi vinculado ao PL nº 1.258/1995;

- PL nº 1.258/1995: agrega um conjunto de 49 propostas normativas, com "critérios para realização de interceptação ou escuta telefônica ('grampo'), para fins de investigação criminal ou instrução processual", não sendo movimentada desde 2012, aguardando Comissão Especial para dar parecer sobre o tema[237].

Todas as pesquisas complementares, de outros projetos, ou direcionam para a proposta do novo Código de Processo Penal (PL nº 8.045/2010) ou da nova redação de Lei de Interceptação Telefônica (PL nº 1.258/1995). Assim o é em relação ao PL nº 5.223/2020, que trata de uma das expectativas dos atores de investigação cibernética, a de ajustes na competência para "o processamento e julgamento dos crimes cometidos por qualquer meio de comunicação ou por sistema de informática ou telemática". A referida proposta foi apensada ao PL nº 2.857/2020 (para inserir o domicílio do réu em ações de crimes contra a honra), que foi, por sua vez, apensada ao PL nº 8.045/2010.

Pesquisa complementares, no mesmo sítio legislativo, pelo termo "dados cadastrais"[238], ou retornam pesquisas não vinculadas ao tema da tese ou retornam informações sobre propostas vinculadas ao projeto do novo Código de Processo Penal ou incremento na Lei do Crime Organizado:

- PL nº 5.968/2019: proposta que visa a alterar o "Código de Processo Penal para determinar que os órgãos do poder público e as empresas da iniciativa privada simplifiquem o acesso aos dados cadastrais para as autoridades responsáveis pela investigação", instituindo uma modificação no art. 13-A do CPP atual. Tal proposta foi apensada ao PL nº 8.040/2014, com proposição semelhante, de acrescentar "o inciso V ao art. 13" do CPP vigente. Ambos os projetos estão apensos ao PL nº 8.045/2010.

- PL nº 1.395/2021: tem a proposição de acrescentar "o § 3º ao artigo 3º e os artigos 15-A, 21-A, 21-B, 25-A e 25-B" à Lei nº 12.850/2013, regulamentando a apreensão e análise de dispositivos móveis, a consulta à base de dados cadastrais (os quais procura definir), também estipulando normativa sobre a "escuta ambiental", esta já regulada sob o nome

[237] Pesquisa feita em 16 jan. 2023.
[238] Pesquisa feita em 16 jan. 2023.

jurídico “captação ambiental” pela Lei nº 9.296/1996, com os acréscimos da Lei nº 13.964/2019.

Pela complexidade envolvida nos temas, certamente as discussões legislativas terão sequência, podendo-se, inclusive, instar os atores de investigação cibernética a externalizar suas expectativas cognitivas em relação à estrutura normativa já existente, tornando-a prática e efetiva e, ao mesmo tempo, que possa ser delineada em respeito aos direitos e garantias fundamentais.

4.4.3 Propostas normativas sobre inclusão de políticas públicas de redução de danos

As observações dos atores de investigação criminal cibernética tendem a determinar como necessárias ações e políticas voltadas à segurança e educação digital (ver 3.4.1, 3.4.2.1 e 3.4.2.3). Tal expectativa de estruturação normativa e prática, embora estivesse sendo debatida há mais tempo no Congresso Nacional, foi contemplada com a Lei nº 14.533/2023, que implementa a

> Política Nacional de Educação Digital (PNED), estruturada a partir da articulação entre programas, projetos e ações de diferentes entes federados, áreas e setores governamentais, a fim de potencializar os padrões e incrementar os resultados das políticas públicas relacionadas ao acesso da população brasileira a recursos, ferramentas e práticas digitais, com prioridade para as populações mais vulneráveis. (BRASIL, 2023).

A lei estruturou a política em quatro eixos, “Inclusão Digital”, “Educação Digital Escolar”, “Capacitação e Especialização Digital” e “Pesquisa e Desenvolvimento (P&D) em Tecnologias da Informação e Comunicação (TICs)”. Acrescentou, assim, no art. 3º, a educação digital nas escolas, com estratégias prioritárias relacionadas ao “pensamento computacional”, “mundo digital”, “cultura digital”, “direitos digitais” e “tecnologia assistiva”.

A lei foi objeto de discussão em razão do PL nº 4.513/2020, que, após ir ao Senado Federal, voltou à Câmara dos Deputados em razão de um substitutivo aprovado, tendo passado em um dia só por várias comissões e aprovado, sendo enviado para sanção presidencial.

Outro projeto discutia tema semelhante, o PL nº 2.557/2022, sob o nome de “Política Nacional de Proteção Digital das Crianças e Adolescentes – PNPD”. Este projeto foi apensado ao PL nº 2.390/2015, que criaria o “Cadastro Nacional de Acesso à Internet, com

a finalidade de proibir o acesso de crianças e adolescentes a sítios eletrônicos com conteúdo inadequado", ou seja, um projeto relacionado a controles e não à prevenção propriamente dita. Esta pauta, que tem em seu bojo mais 11 projetos normativos[239], caso não seja considerada prejudicada em razão da Lei nº 14.533/2023, seguirá em debate e poderá vir a alterar o Estatuto da Criança e do Adolescente.

No bojo do PL nº 2.390/2015 foram acrescentadas duas propostas a destacar: o PL nº 3.993/2020, que discute a "obrigatoriedade de apresentação de documentos comprobatórios da idade para acesso às plataformas digitais", também uma forma de controle, porém, com o objetivo de alterar o Marco Civil da Internet; o PL nº 5.016/2016, no mesmo sentido, porém propondo a modificação do Estatuto da Criança e do Adolescente, "para obrigar as empresas que prestam serviços de telefonia móvel a implementarem bloqueio prévio ao acesso a determinados conteúdos da Internet ou aplicativos", referindo-se a "especialmente sites e aplicativos de relacionamento que contenham conteúdo pornográfico ou que instiguem a violência".

Os temas se cruzam – regras de controle sobre condutas e políticas públicas –, em vários projetos diferentes, demonstrando-se que em uma complexidade, inerente ao processo legislativo, há necessidade de redução dessa complexidade por meio de estruturação dos temas.

***

Finalizando, destaca-se que a análise realizada não é consolidadora de todos os projetos e normativas que tratam do tema, porém é direcionada aos aspectos principais da discussão legislativa e produção legislativa no que diz respeito aos aspectos (a) penal, (b) processual penal e (c) políticas públicas, incluindo-se normativas de (d) cunho cível com reflexos em outras searas do Direito.

Alguns aspectos que levaram à discussão e à produção normativa foram considerados, especialmente aqueles relacionados às expectativas observadas quando das entrevistas com os atores de investigação criminal. Embora já pontuado, ressalta-se o foco principal do legislador quanto à questão penal, com novos tipos ou incremento nas sanções. Mesmo no caso do PL nº 2.630/2020, que tem característica eminentemente regulatória, de cunho cível

[239] Apensados ao PL nº 2.390/2015 (11): PL nº 3.597/2015 (1), PL nº 2.617/2020, PL nº 5.016/2016 (3), PL nº 6,449/2016 (1), PL nº 5.191/2019, PL nº 7.689/2017, PL nº 5.096/2016, PL nº 8.461/2017 (1), PL nº 5.211/2019, PL nº 3.993/2020, PL nº 2.557/2022.

e administrativo, os PLs a ele agregados têm também propostas de criminalização, embora também tenham propostas de regulamentação sobre aspectos procedimentais.

Os caminhos dos debates legislativos, então, quanto às propostas normativas, poderiam ser assim condensados: (a) propostas de incremento dos tipos penais, especialmente de *fake news*, *bullying*, dentre outros tipos penais e aumento de sanções penais; (b) propostas relativas à regulamentação da transparência e 'controle' na Internet, vinculados ao PL nº 2.630/2020, incluindo discussões que visam a alterar o Marco Civil da Internet; (c) propostas de acesso a dados, pelo Ministério Público e pela Polícia Civil, com direcionamento ao novo Código de Processo Penal; (d) propostas de regulamentação do acesso ao conteúdo de comunicações telefônicas, telemáticas e informáticas, seja pretérito (quebra de sigilo) seja futuro (interceptação); e (e) propostas que tornem prática a prevenção e redução de danos na Internet.

No entanto, para que as expectativas cognitivas dos atores de investigação cibernética – não só os policiais civis, mas também os federais e membros do Ministério Público, estaduais e federais – sejam percepcionadas pelo sistema Político no Brasil, há necessidade de um remolde na segunda fase da comunicação luhmaniana: o modo de dar a conhecer. Justifica-se essa observação, pois comunicação que não chega ao destinatário não é comunicação, é apenas uma informação não recepcionada.

Ou seja, em outros termos, considerando que a operação básica dos sistemas psíquicos é a consciência, não basta a consciência para comunicar ao exterior, aos demais sistemas, havendo necessidade de operar a comunicação, operação de todos os sistemas sociais. Sendo sistemas de sentido, os sistemas psíquicos – dos atores de investigação criminal cibernética – necessitam, através do *médium*, criar e gerar seletivamente a informação apta a chegar ao entorno do sistema Político, sendo que esta distinção terá de ser talhada em sua atualidade x potencialidade, aqui condicionando os aspectos inerentes ao cibersistema da Internet e ao procedimento de persecução criminal, ou seja, uma interconexão e co-reflexividade comunicacional entre sistemas sociais e psíquicos.

Assim, pelas suas experiências, os atores de investigação criminal cibernética podem projetar novas possibilidades, potencializando suas experiências no processo investigativo. Por outro lado, o sistema Político [legislativo], que produz suas próprias operações, por meio da autopoiese pode conectar a variabilidade e os estímulos ambientais e estabelecer sua função, a de tomar decisões que vinculem a coletividade, leia-se, inclusive, os responsáveis pela persecução criminal [cibernética].

CONCLUSÃO

Esta tese tem como pressuposto que uma investigação científica na área do Direito deve considerar, desde seu início, a complexidade da sociedade. Assim, a pesquisa que norteou este trabalho considerou a existência da complexidade na ambiência do cibersistema da Internet, dos sistemas psíquicos, responsáveis pela investigação criminal cibernética, dos sistemas Político e do Direito. Aquele, pela sua organização, pela produção legislativa ou pela administração dos recursos aptos à persecução criminal; o segundo, em razão da estruturação das expectativas advindas e correlacionadas aos demais sistemas sociais.

O sistema do Direito não elimina as complexidades; organiza-as! O Direito torna gerais e congruentes as expectativas normativas. Isso não impede a projeção de novas possibilidades, a criação de expectativas reflexivas sobre vários aspectos da estrutura normativa já estabilizada. 'Organizar' as complexidades inerentes aos crimes cibernéticos também é uma das funções do Direito; expectar e projetar novas possibilidades normativas sobre crimes cibernéticos é função operativa dos demais sistemas, especialmente os psíquicos. Compreender o entorno, especialmente o cibersistema da Internet, faz parte do processo coevolutivo dos sistemas que recepcionam a comunicação advinda de dados e informações.

Os estudos realizados nesta pesquisa possibilitaram concluir que esse contexto precisa ser compreendido, então, sob o viés da cibersociologia, que contempla a prática de observação dessas relações no ciberespaço, especialmente abrangendo os estudos críticos para além do Direito, ou seja, nos âmbitos tecnológicos, culturais e políticos (administrativos). Tem-se, assim, a compreensão desse processo coevolutivo dos sistemas envolvidos e acoplados por determinadas e selecionadas comunicações, não se podendo observar, isoladamente, como se dá a produção legislativa e normativa, penal e processual penal em relação à Internet e ao ciberespaço no Brasil.

Essa comunicação, aliás, transformou-se coevolutivamente com o advento da interação digital por meio da rede [mundial] de computadores. O tempo teve sua noção ressignificada em razão da celeridade na transmissão de dados e informações, o tempo não-tempo, o tempo sem o controle de cronos, o tempo da presencialidade *on-line*; enquanto isso, o espaço foi ressignificado, com novas ferramentas tecnológicas, como o espaço digital, sem fronteiras físicas e de interação síncrona e assíncrona. A conectividade de redes físicas e lógicas se estendeu para as conexões humanas [psíquicas], expandindo possibilidades de autoconhecimentos. Permite que a informação chegue livremente, por exemplo, em países

onde restrições não são impostas aos cidadãos por regimes e sistemas totalitários. Por outro lado, essas redes também servem para direcionar e limitar o conteúdo informacional em espaços físico-territoriais nos quais há sistemas políticos autoritários instalados, mas, mesmo assim, possibilitam que comunicações sejam comunicadas. Essa circunstância subverte os controles estatais, sendo isso possível em razão das formas diferenciadas e complexas das aplicações e estruturas existentes nas camadas visíveis e invisíveis da Internet.

Partiu-se, nas observações e formação de autoconhecimento sobre o tema, da premissa em compreender como possível o cibersistema da Internet, já que construído e constituído [por] suas próprias estruturas de funcionamento e funcionalidade, com características autopoiéticas, de auto-organização, autorregulação e autodesenvolvimento. Sua característica principal é possibilitar a comunicação, advinda de dados e informações, que estão disponíveis e aptos a comunicar. Esse armazenamento, processamento e transmissão de dados e informações possui regras próprias e específicas, com o fechamento operacional do cibersistema, tendo em seu entorno os sistemas psíquicos [usuários] e demais sistemas sociais e organizacionais, com os quais mantém a comunicação, pela abertura cognitiva, para com eles interagir (Direito, Moral, Economia, Política etc.), irritando-os ou sendo irritado.

A partir da revisão bibliográfica, não só da Teoria Geral dos Sistemas Sociais, desenvolvida por Niklas Luhmann, mas também de seus observadores, juntamente com as observações sobre a complexidade inerente à estrutura da Internet, concluiu-se pela condição cibersistêmica da Internet, ou seja, de ser um subsistema do sistema da sociedade, tendo-se partido da análise das características de um sistema/subsistema, que contempla a sistematicidade autopoiética da rede [mundial] de computadores, correspondendo, ao mesmo tempo, a um sistema autopoiético basal, derivado e estaminal, possuindo um fechamento operativo singular em razão da linguagem computacional.

A diferenciação funcional do cibersistema da Internet é caracterizada, internamente, pela existência de múltiplos e específicos códigos binários, pois dependentes de sua especificidade digital, bem como pelo sentido, o limite da Internet, dado pela construção cultural dos observadores, porém, baseada totalmente em informação, ou seja, o sentido-informação ou a informação-sentido: ela é, a Internet, composta de uma estrutura que contém dados e informações e estes podem comunicar, tal qual o Direito contém as normas e estas também comunicam. Se a Internet contempla, internamente, múltiplos códigos, a programação é uma só, a programação binária da rede, em “0s” (zeros) e “1s” (uns) (0/1 – binariedade).

Neste contexto, observa-se que o sentido da Internet é informação em seu sentido mais puro, com possibilidade de conexão entre dados [dados + dados = informação], não necessariamente interpretados, reinterpretados, readaptados, percepcionados ou não, mas é só informação, a partir da qual o sistema se comunica [informação + informação + seleção do que informar + seleção do modo de compartilhar + recepção da informação = comunicação].

Por isso, diverge-se do entendimento mais simplista, do observador-usuário, com a noção de que a Internet é basicamente um *médium*, um meio de comunicação, pois as observações delineadas nesta tese importam em dizer que ela vai além disso, em razão do seu ambiente estrutural, da sua organização e composição, e da sua formação de autorregras (as autorregras das aplicações de Internet, como Facebook e Instagram, ou, também, as regras de recomendação sobre configuração de e-mails, ou, ainda, as recomendações internacionais aos referidos serviços ou a distribuição e recomendações sobre as configurações do Protocolo de Internet – IP). Seus algoritmos, compostos por dados e informações, carregados de memória sobre o que já foi realizado [armazenado e processado], por exemplo, por um outro sistema [usuário], conformam o próprio sentido do cibersistema: a partir da conexão, facilitar e ampliar evolutivamente também o espectro de outros sistemas.

A aplicação da TGSS à Internet não só é possível como necessária, dado o fluxo cognitivo atinente aos sistemas que são sensíveis aos processos de irritações que advêm de outras áreas de pesquisa e referentes aos demais sistemas. Também observa-se que a Internet, em razão de sua estrutura organizacional, sua auto-organização, autorreferencialidade, autodesenvolvimento, ou seja, suas características autopoiéticas, e por ter como seu sentido principal o dado e a informação capaz de gerar comunicação, possui campo de relações em todos os sistemas e subsistemas da sociedade contemporânea e possui, conectivamente, uma inter-relação e uma interdisciplinaridade inigualável à dos demais sistemas/subsistemas. A singularidade do fechamento operacional, referida anteriormente, não afeta a abertura cognitiva; ao contrário, amplia-a de maneira que a estrutura cibersistêmica da Internet possa ser considerada, em importância e tamanho, ao sistema da Economia, em face das integrações e interações para além de territórios e espaços delimitados.

A partir da teoria luhmaniana, buscou-se não necessariamente apresentar uma solução a algum problema, mas sim tecer observações aceitáveis sobre como é possível o cibersistema da Internet, ou seja, a Internet como um dos subsistemas do sistema social, desenvolvido a partir da coevolução tecnológica e baseado em dados e informações,

correspondentes a algoritmos, cujo código, responsável pela abertura e fechamento operativo, é *connect*/*disconnect* (conexão/desconexão).

A conexão ou não conexão a dados e informações é capaz de gerar conhecimento/autoconhecimento, de reduzir complexidades e de produzir complexidades. Um polo positivo – *connection* – e outro polo negativo – *disconnection* –, possibilitando a relação do sistema da Internet com seu entorno. Carrega, portanto, o *input* e o *output* da cibernética. Isso não lhe retira a característica de possuir, a depender da configuração na estrutura cibersistêmica [por exemplo, de aplicações e softwares específicos], códigos binários específicos.

Ao mesmo tempo em que se ampliou o espectro de atuação, interação e busca de dados e informações com o uso e expansão da Internet, há a sua exploração, considerada divergente – do ponto de vista moral, cultural e pelo Direito –, que pode produzir danos pessoais, sociais e às nações, como nos contextos de um enfrentamento cibernético em larga escala. Essa expectativa sobre as condutas divergentes é, assim, uma comunicação possível de ser absorvida pelo Direito, que a estrutura e estabiliza, no caso, tanto do ponto de vista penal-material quanto procedimental-subjetivo.

Para a realização da coleta dos dados e informações sobre as condutas divergentes, estabilizadas estruturalmente no Direito Penal, o sistema organizacional processual de persecução criminal contempla a estruturação de organizações [Polícia Judiciária, Ministério Público e Justiça] e atores [policiais, promotores e juízes], estes responsáveis pelas funções específicas previstas, no caso, no Código de Processo Penal e em legislações esparsas, conforme analisado [item 4.2.2]. Na presente pesquisa, com a utilização de metodologia empírica de entrevistas, o foco das observações foi sobre um dos atores envolvidos na persecução criminal: o policial responsável pela investigação policial dos crimes praticados pela Internet, ou seja, os crimes cibernéticos.

Objetivou-se, então, responder quais são e como repercutem comunicativamente as expectativas cognitivas e normativas dos atores de investigação policial ante a legislação penal e processual penal existente relativamente à Internet no Brasil e em relação à estrutura de enfrentamento aos crimes cibernéticos, centrando-se o Capítulo 3 na análise empírica do conteúdo obtido nas entrevistas. As 24 entrevistas realizadas foram importantes para compreender como observam e percepcionam esses atores as estruturas normativas (penal e processual penal) e administrativas de enfrentamento à criminalidade cibernética. Mesmo sem a realização da entrevista em relação a um Estado no qual já há uma estrutura de

investigação de crimes cibernéticos, os resultados foram satisfatórios e o conteúdo advindo dos questionamentos foi importante para as conclusões.

Assim, a partir da análise empírica do conteúdo das entrevistas, foram obtidas respostas quanto à questão-problema, pois se conseguiu delinear as expectativas cognitivas e normativas dos policiais com atuação na área ciber, bem como percepcionar que, embora desapontados nas suas expectativas, estas não são comunicadas efetivamente ao ou aos sistemas sociais, que poderiam, com a comunicação do seu entorno, analisar e incorporar estruturalmente a referida expectativa.

Os entrevistados, em suma, entendem a importância dos protocolos de atuação dos setores policiais, tal qual a padronização no desenvolvimento das atividades dos setores especializados na investigação cibernética, embora não tenham autoconhecimento padronizado sobre as legislações envolvidas, inclusive a de estruturação dos órgãos policiais responsáveis pelas investigações dos crimes perpetrados na rede de computadores (art. 4º da Lei nº 12.737/2012). Aliás, essa estruturação dos órgãos estaduais de enfrentamento à criminalidade cibernética, no âmbito das Polícias Civis, já ocorre antes da referida norma federal, e não é necessariamente a falta de um setor estruturado o problema da efetividade na investigação cibernética e sim um conjunto complexo de deficiências que deveriam, aos olhos dos policiais, ser tratadas conjuntamente: capacitação, qualificação, recursos materiais, softwares e hardwares, instalações etc.

Já em relação à legislação penal, além de se frustrarem com a legislação que não atende(ria) a todas as circunstâncias fáticas, contemplam a necessidade expectante de novos tipos penais ou um incremento nas sanções, para que sejam mais severas e rigorosas, possibilitando a prisão dos autores, sendo esta circunstância, por sua vez, elencada pelos entrevistados como um elemento circunstancial e ‘forte’ da efetividade da Lei penal. Não há incoerência nas suas expectativas, mas centrá-las em um momento findo da investigação criminal não necessariamente é compreender que o elemento principal, o objetivo principal, da investigação criminal é a apuração da autoria e da materialidade, sendo a efetivação da denúncia, das medidas cautelares de restrição de direitos e liberdades, e, também, da condenação, uma função a cargo de outros atores da persecução criminal.

A aplicação prática da norma aos casos concretos também elenca essa disparidade entre frustrações e expectativas normativas, porquanto as diferenças podem ser compreendidas tendo em vista as esferas geral e local de aplicação da legislação penal, bem como a análise dela em abstrato em contraposição à aplicação aos casos concretos. Pelos entrevistados, em suma, quando o *locus* é abstrato e está distante, avaliam [a maioria dos policiais

entrevistados] pela não suficiência da norma penal; porém, quando o *locus* é a prática aplicada e cotidiana, avaliam a legislação penal como suficiente. Na prática da aplicação da lei penal, ou seja, no dia a dia da análise dos fatos e do enquadramento deles às situações abstratamente previstas na legislação penal, há consideração pela suficiência da norma, embora se tenha, por outro lado, o reclame voluntário e acentuado quanto à pena.

Não obstante as referências à legislação penal, há desapontamentos também em relação à legislação processual, considerada inadequada e condicionante à atividade policial, inclusive pela falta de normativa quanto a prazos em que uma requisição ou determinação judicial deva ser cumprida. Embora o condicionamento procedimental seja evidente, a não delimitação de determinadas regras processuais torna o procedimento lento, bem como não há padronização na prestação das respostas às solicitações, judiciais ou não, pelos provedores de conexão e de aplicação da Internet.

Verificou-se, também pelas entrevistas, que entre a expectabilidade cognitiva dos atores de investigação [que corresponde a uma frustração seja pela demora ou tempo de resposta dos provedores, seja pela ausência de padronização ou, ainda, seja pelo baixo poder requisitório do delegado de polícia] e a possibilidade de câmbio da norma [que reestruturaria as regras de acordo com as várias expectativas organizacionais envolvidas, dos provedores, do Judiciário etc.], há uma lacuna muito grande, sobre a qual esses policiais, enquanto atores de investigação criminal cibernética, parecem não atuar, não se aprofundar, porquanto a imensa maioria deles desconhece projetos de lei que visem a melhorar e atender a essas expectativas sobre as expectativas normativas.

Assim, essas expectativas cognitivas dos atores de investigação criminal não se tornam comunicação hábil e não chegam diretamente ao sistema legislativo, e, por isso, não o irrita e não é capaz de produzir heterorreferência evolutiva na persecução criminal. O que não há é comunicação apta dessas frustrações: a seleção das expectativas, a seleção dos desapontamentos, assim como a forma de repasse dessas informações, precisa ser explícita para que estas possam ser conhecidas e, eventualmente, absorvidas pelos demais sistemas de acordo com sua função e código, inclusive os sistemas organizacionais. Em não saindo do espectro da consciência dos atores de investigação cibernética e/ou até mesmo do âmbito das organizações a que pertencem, essas comunicações não têm capacidade de irritar os demais sistemas sociais envolvidos, especialmente o legislativo [brasileiro].

Conforme apontado no decorrer da tese, confirma-se, portanto, a primeira hipótese do projeto de pesquisa, de que as frustrações e os desapontamentos em relação às estruturas administrativas e normativas relacionadas aos crimes cibernéticos são mais latentes do que

as expectativas, cognitivas e/ou normativas, e a comunicação destas [pelos atores de investigação cibernética] não informa os demais sistemas sociais, especialmente o Político, sendo apenas ruido comunicacional, quando não apenas um reclame da própria consciência. Esses subsistemas sociais, a Política (Legislativo e Executivo) e o Direito, não conseguem, portanto, recepcionar uma comunicação não feita pelas consciências dos atores de investigação cibernética ou, até mesmo, uma comunicação feita apenas dentro da organização policial. Há, assim, um *gap* na comunicação, que a torna inefetiva, tornando as frustrações e desapontamentos mais latentes.

De outra parte, percebe-se como possível a estruturação das expectativas dos entrevistados quanto à estrutura administrativa envolvida no enfrentamento aos crimes cibernéticos, especialmente quando se parte do interesse pessoal para o institucional, em um processo de convencimento, realizado ou a ser realizado, por parte dos atores de investigação criminal cibernética em relação aos gestores institucionais. Assim, é possível delinear como uma perspectiva, ou local e/ou nacional, a adequação da estrutura normativo-institucional para atender aos casos de crimes praticados no âmbito da Internet. Essa readequação local deve atender aos parâmetros da realidade local, do Estado e, por que não dizer, não se limitar somente à realidade da capital, onde as 'delegacias ciber' estão localizadas, mas sim correlacionar à realidade de toda a unidade federativa.

Assim, tem coerência essa redefinição de atribuição com um processo macro, de orientação e auxílio interno aos demais órgãos não especializados na área, seja pela existência de um laboratório de operações ou inteligência cibernética (os Ciber-Labs), seja pela existência da função relacionada à delegacia, ao departamento, à divisão, à diretoria ou à coordenadoria. Esse processo evolutivo e constante nas perspectivas dos atores de investigação criminal é fundamental para o desenvolvimento hábil e efetivo no atendimento às situações de investigação em relação aos crimes cibernéticos.

Em suma, há uma co-reflexividade de expectativas dos atores de investigação cibernética em relação às estruturas federais e estaduais, responsáveis por definir as políticas administrativas capazes de enfrentar efetivamente a criminalidade praticada no contexto da rede [mundial] de computadores. Essas expectativas, em regra frustradas em razão da inexistência de uma política contínua de formação e preparo dos atores de investigação criminal cibernética, acabam por refletir no contexto da sociedade, que se vê desamparada em razão da ineficiência [declarada pelos entrevistados] do sistema policial para atender a todas as demandas. Essas expectativas são, portanto, complexificadas por serem pautadas sobre recursos humanos e materiais, aqueles qualificados e em constante autoaprendizado, e

estes últimos com hardwares, softwares e equipamentos capazes de auxiliar a atuação policial em dar efetividade à apuração da autoria e materialidade dos crimes cibernéticos.

Porém, afirma-se que não apenas o sistema policial investigativo está carente dessas políticas administrativas locais e nacionais, sejam (a) *estruturais* – em termos de recursos materiais e humanos –, sejam (b) *procedimentais* – em termos de atuação uniforme e padronizada –, ou (c) *educacionais* – em termos de capacitação básica ou avançada, com qualificação contínua. Outros atores envolvidos na persecução da criminalidade cibernética, como integrantes do Ministério Público e do Poder Judiciário, entendidas sistematicamente como estruturas diversas da policial, estão mais atrasadas nesse processo evolutivo de atenção à especialização no contexto cibernético, embora já possuam sistemas processuais que atendam às suas situações protocolares. A coevolução das organizações e de todos os atores envolvidos na persecução da criminalidade cibernética é essencial para o incremento da efetividade, seja em termos de qualidade procedimental, seja em termos de aumento do número de identificações de autores, dentre outras consequências possíveis de uma interação interinstitucional desejada como perfeita.

Confirma-se então, durante observações realizadas na pesquisa empírica, outra hipótese delineada, de que o quadro estrutural atual das Polícias Civis brasileiras não comporta unicidade, padronicidade ou uniformidade, sendo fundamental o estabelecimento de uma diretiva única e protocolos uniformizados e padronizados no enfrentamento à criminalidade em rede de computadores, dispositivos de comunicação ou sistemas informatizados [criminalidade cibernética], sem os quais torna-se difícil aprimorar a investigação criminal cibernética, já que a organização administrativa é local nas unidades federativas e as decisões nesse âmbito não são uniformizadas, gerando também frustrações e desapontamentos quanto à efetividade da resposta procedimental. Embora se tenha um embrião formado de uma política de segurança pública voltada ao enfrentamento da criminalidade cibernética no Brasil, a partir do 1º Ciber Cap, há muito para ser implementado.

O impacto do avanço da tecnologia e da ampliação da rede de computadores pelo mundo não foi só na atividade policial. Outros setores foram atingidos, mas as demandas relacionadas à investigação no âmbito cibernético foram antecedentes às mutações no sistema do Direito. Não se poderia deixar, então, de analisar essa coevolução no sistema do Direito e, por isso, no quarto e último Capítulo desta tese buscou-se, a partir da análise de documentos normativos e projetos legislativos, analisar a linha do tempo da mudança da legislação brasileira e o processo histórico-normativo a partir do maior uso e da proliferação

da Internet no Brasil, contextualizando com as expectativas cognitivas e normativas dos atores de investigação cibernética.

Num primeiro momento, analisou-se criticamente como se deu a construção da estruturação da realidade normativa em face da Internet nos âmbitos penal e processual penal, não se olvidando de temas considerados importantes na preservação de direitos e garantias fundamentais: criança e adolescente e defesa do consumidor e correspondentes alterações. Também adentrou-se nas mudanças significativas na legislação eleitoral, porquanto o uso da Internet tanto para o exercício do voto quanto para a influência em relação a ele são os principais objetos de atenção e discussão, especialmente após o advento de análises de dados pessoais, de redes sociais, com o foco na estratégia e disseminação de informações capazes de direcionar qualquer pleito eleitoral (as *fake news*, ou seja, a desinformação).

Enfocou-se, em momentos distintos, como a mídia ajuda no processo de construção de uma realidade social 'provocadora' de modificações normativas em virtude da irritação que causa no sistema político-legislativo, com a proliferação e ampliação dos projetos de lei voltados à criminalização, especialmente. Assim, a construção, a produção e a reprodução da realidade social pela mídia, tradicional e digital, acabam por reafirmar o sistema hegemônico vigente, voltado à área penal e à produção de sanções, não necessariamente à redução sistemática de danos no ambiente cibernético.

Com essas observações, confirmou-se a segunda afirmativa, elencada na tese, de pontuar que o legislador brasileiro possui, sim, um foco direcionado à área penal, à produção de direito material penal, circunstância que reflete sobre o sistema de persecução criminal, com medidas limitadas na área processual penal, seja para ampliar a efetividade da investigação criminal cibernética, seja para reduzir ou mitigar os danos e riscos no ambiente cibernético. Em verdade, o legislador brasileiro atua em reflexo não só da construção da realidade pelos veículos de comunicação, mas também, indiretamente, dos atores envolvidos na persecução criminal. Estes, é necessário dizer, são a principal fonte de informação utilizada pelos veículos de comunicação, os *mass media*, e, mesmo não comunicando diretamente ao sistema legislativo suas expectativas e frustrações, acabam por fazê-lo por meio da imprensa, porém esta acaba realizando uma seleção no que comunicar, especialmente para validar a linha editorial.

Ainda no quarto capítulo, com o mesmo viés historiográfico, procurou-se produzir e expor pesquisa empírica [documental] sobre os principais projetos legislativos atinentes a temas de exploração pela mídia e redes sociais brasileiras: *bullying*/*cyberbullying* e notícias falsas/desinformação, as *fake news*. Nessa abordagem crítica, procurou-se demonstrar não só

a quantidade de projetos normativos no Congresso Nacional, mas também quais os ‘direcionamentos’ envolvidos e possíveis, observando-se que o enfoque na criminalização é o que tem dominado os debates em detrimento dos aspectos procedimentais e de políticas públicas preventivas, e, mesmo quando estas são aprovadas e sancionadas, não contêm, no texto normativo, nenhum comando com imposição e controle de efetividade.

Percebeu-se, pela análise dos atos normativos consolidados e/ou em discussão, que o esforço das legislações está voltado para considerar crime informático aquelas atividades que causem danos e afetem ou pessoas em funções específicas (a exemplo do art. 154-A do Código Penal) ou atividades econômicas de empresas de grande valor comercial, pois as vítimas de delitos econômicos são agentes de uma significativa influência política (a exemplo dos arts. 155, § 4º-B, e 171, § 2º-A, ambos do Código Penal), porquanto a maior parte afeta o sistema financeiro brasileiro.

Um dos exemplos analisados foi em relação à criminalização do induzimento, da instigação ou do auxílio a automutilação, com base na Lei nº 13.968/2019, pois sofreu influência da realidade construída a partir das notícias sobre o jogo ‘baleia azul’ e não sobre estudos técnicos e científicos de quais fatores levavam crianças e adolescentes à prática de automutilação. Aliás, outros estudos podem ser levados em conta em outras situações, como a da exploração indevida das imagens íntimas de pessoas, estando o *sexting* (envio e recebimento de imagens e vídeos de conteúdo íntimo) entre as práticas rotineiras entre jovens, assim dependente de processos orientativos e não necessariamente de um tipo penal. Com outro viés, de proteção da intimidade e repulso às violências não físicas, outras criminalizações foram adicionadas na legislação penal, como as de 2018 e 2021, respectivamente sobre o registro e a divulgação não consentida da intimidade e o *stalking*, sendo estas pautas do movimento feminista.

Assim, é complexo compreender o que faz um determinado país a encaminhar-se à constante criminalização de condutas usando argumentos e análises diferenciadas. Em regra, na maioria dos casos, conforme visto na análise da estruturação das Leis e dos respectivos projetos, a emergência ‘se justifica’ em razão do contexto de (a) ‘mais controle’ (vejam-se as normas e os projetos de caráter eleitoral), (b) ‘mais segurança’ (vejam-se as normas relativas aos bancos de dados das administrações públicas), (c) ‘assegurar direitos’ (vejam-se as normativas e os projetos relativos à proteção da intimidade), (d) ‘mais proteção’ (veja-se a previsão do tipo penal de ‘invasão de dispositivo informático’) e (e) ‘atender a uma demanda emergente social’ (veja-se a criação do tipo penal de estelionato eletrônico [fraude eletrônica]), dentre tantas justificativas legislativas.

As expectativas dos sistemas sociais e dos sistemas psíquicos, em razão da sua complexidade, acabam reproduzindo no legislador uma necessidade de estruturação dessas expectativas e, por isso, uma utilização maior do Direito como mecanismo de contingenciamento e de redução de complexidades. Assim, após normatizada penalmente a previsão sobre a conduta (cibernética), acaba-se por gerar as correspondentes expectativas normativas, tanto pelos sujeitos usuários da Internet quanto pelos operadores [atores] da investigação criminal, que têm a função de investigar e formar o molde de enquadramento do fato, da conduta, à norma penal. Essas expectativas normativas tendem a resistir à frustração, pois a norma persiste embora frustrada a expectativa. Por certo, não é o que ocorre no caso das comunicações não selecionadas e normatizadas pelo legislador, pois as expectativas nesse caso são frustradas e assimiladas, possibilitando, ao menos, processos de aprendizado.

A dizer que, sim, os atores de investigação policial cibernética possuem consenso [selecionar] quanto às necessidades de normatividade de medidas procedimentais, embora nem todos tenham a mesma avaliação sobre os mecanismos efetivos na redução/mitigação dos danos cibernéticos, ou seja, o foco não está necessariamente na mitigação do dano, mas concentrado na identificação de quem o causou. Especialmente quanto à desejada melhoria dos procedimentos auxiliares à investigação, a correspondência do ideário da comunicação deveria ser a produção da comunicação [compartilhar] do consenso ao sistema produtor-legislativo.

Por outro lado, a solução normativa adotada pelo sistema político-legislativo [compreender] quanto ao procedimento pode não corresponder, necessariamente, à solução procedimental prática, aquela vivenciada no dia a dia, seja no enquadramento da conduta incriminadora à situação fática, seja quanto aos procedimentos aptos à apuração da autoria e da materialidade. Para ajustar a norma à realidade, o legislador necessita(ria) conhecer e absorver – com maior frequência – as comunicações advindas dos sistemas psíquicos e organizacionais envolvidos na persecução da criminalidade cibernética, não indiretamente, mas diretamente.

Essa estruturação da legislação processual no Brasil, quando tem em vista a coleta e busca de evidências no contexto da Internet, uma vez comparada à estruturação das normativas criminalizatórias, com novos tipos penais e aumento de penas, leva à conclusão de que o enfoque principal das legislações não parece voltado à parte procedimental, com criação de mecanismos normativos para a formação da prova, a fim de resolver a lide de maneira mais célere.

Além disso, outras regras e políticas deixam de ser o foco e se tornam acessórias e/ou desconsideráveis, especialmente aquelas que preconizem, de maneira mais célere, a redução ou mitigação de danos cibernéticos às vítimas dos crimes praticados no âmbito da Internet. Os próprios atores de investigação cibernética não os conhecem e preconizam seu uso, quando existentes, por ser seu enfoque principal a apuração da autoria e materialidade. Portanto, tais normas mereceriam uma categorização e adaptação à realidade no âmbito cibernético, adaptação capaz de mitigar efetivamente um dano cibernético e evitar e revitimização.

Por outro lado, para que as expectativas cognitivas dos atores de investigação cibernética – não só os policiais civis, mas também os federais e membros do Ministério Público, estaduais e federais – sejam percepcionadas pelo sistema Político [legislativo] no Brasil há necessidade de um remolde na segunda fase da comunicação luhmaniana: o modo de dar a conhecer. As frustrações e desapontamentos em relação às estruturas normativas e administrativas, elencadas pelos entrevistados, necessitam ser ‘apresentadas’ – no formato de expectativas – ao sistema Político, irritando-o e possibilitando a sua seleção, mesmo que parcial.

A comunicação que não chega ao destinatário não é comunicação, é apenas uma informação não recepcionada, é apenas uma análise estrutural da informação em nível de consciência ou, quando muito, uma abordagem comunicacional interna das organizações. Esse foi o principal enfoque nesta tese, de procurar conhecer quais são e como comunicam as expectativas dos atores de investigação cibernética, restando claro que há uma lacuna, um vazio, um *gap* comunicacional entre a realidade da investigação cibernética e a estrutura normativa. Por outro lado, apontou-se e reforça-se a necessidade de uma maior abertura cognitiva do sistema Político em relação ao seu entorno, possibilitando conhecer e recepcionar expectativas reflexivas dos sistemas sociais e psíquicos, especialmente às relativas à persecução da criminalidade cibernética no Brasil.

REFERÊNCIAS

ABNT. Sobre a normalização. **Associação Brasileira de Normas Técnicas**. 2022. Disponível em: https://www.abnt.org.br/normalizacao/sobre. Acesso em: 2 set. 2022.

ALVES, Emylly. STJ: foto de biquíni e sem mostrar rosto também configura pornografia de vingança. **Jota**, 26 jun. 2020. Disponível em: https://www.jota.info/coberturas-especiais/liberdade-de-expressao/stj-foto-de-biquini-e-sem-mostrar-rosto-tambem-configura-pornografia-de-vinganca-26062020. Acesso em: 16 fev. 2021.

AMARO, Lorena. Polícia Civil recebe capacitação internacional sobre criptomoedas. **Criptofacil**, 29/11/2020. Disponível em: https://www.criptofacil.com/policia-civil-recebe-capacitacao-internacional-sobre-criptomoedas/. Acesso em: 11 jan. 2023.

ANTUNES, Deborah Christina; ZUIN, Antônio Álvaro Soares. Do bullying ao preconceito: os desafios da barbárie à educação. **Psicologia & Sociedade**, v. 20, n. 1, p. 33-41, 2008.

ARBULU, Rafael. Prejuízo global do cibercrime passa de US$ 1 trilhão, diz McAfee. **Olhar Digital**, 07/12/2020. Disponível em: https://olhardigital.com.br/2020/12/07/seguranca/prejuizo-global-do-cibercrime-passa-de-us-1-trilhao-diz-mcafee/. Acesso em: 14 jul. 2021.

AUGSTEN, Patrícia; WENDT, Emerson. Não existem mais palavras inocentes: a construção social da realidade a partir de divulgações oficiais. *In:* [Anais do] III **Congresso Internacional de Diálogos Interdisciplinares**: comunicação digital e futuros possíveis. Coordenação Mary Sandra Guerra Ashton [recurso eletrônico]. Novo Hamburgo: Editora Feevale, p. 1535-1541, 2021.

BALEIA Azul. **Google Trends**. Disponível em: https://trends.google.com.br/trends/explore?date=all&geo=BR&q=%2Fg%2F11c7190bky. Acesso em: 09 jan. 2023.

BARDIN, Laurence. **Análise de conteúdo.** Edições 70: Lisboa. 1977.

BARRETO, Alesandro Gonçalves. Teredo IPV6–Procedimentos a Serem Adotados Durante a Investigação Policial para Evitar Falsos Positivos. **Revista Eletrônica Direito & TI**, v. 1, n. 8, p. 3-3, 2017.

BARRETO JUNIOR, Irineu Francisco; LIMA, Marco Antonio. Suicídio e o jogo da baleia azul analisados na perspectiva de anomia de Émile Durkheim. **Revista de Sociologia, Antropologia e Cultura Jurídica**, v. 3, n. 1, p. 121-136, 2017.

BECKER, Howard S. **Outsiders:** estudos de sociologia do desvio. Rio de Janeiro: Zahar, 2008.

BERTALANFFY, Ludwig Von. **Teoria geral dos sistemas:** Fundamentos, desenvolvimento e aplicações. 4ª Ed. Petrópolis: Vozes, 2009.

BERTOLUCCI, Gustavo. Polícia Civil coloca criptomoedas como aprendizado obrigatório de novos agentes em MT. **Livecoins**, 20/12/2022. Disponível em: https://livecoins.com.br/policia-civil-coloca-criptomoedas-como-aprendizado-obrigatorio-de-novos-agentes-em-mt/. Acesso em: 11 jan. 2023.

BINI, Adriano Krul. **O agente infiltrado:** perspectivas para a investigação criminal na contemporaneidade. Dissertação de Mestrado. Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna – ISCPS, 2017.

BLOISE, Juliana; RUBIM, Karen L. B.; WENDT, Emerson; COSTA, Renata Almeida da. A Deep Web, Cibersistema(s) e Direito: qual é o código? **Pesquisas na pós-graduação em tempos de pandemia**, p. 29, 2021.

BÔAS FILHO, Orlando Villas; GONÇALVES, Guilherme Leite. **Teoria dos sistemas sociais**. São Paulo: Saraiva, 2013.

BRASIL. **Decreto nº 7.962, de 15 de março de 2013**. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D7962.htm. Acesso em: 17 nov. 2022.

BRASIL. **Decreto nº 8.771, de 11 de maio de 2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em: 11 jan. 2023.

BRASIL. **Decreto Legislativo nº 37, de 16 de dezembro de 2021**. Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-legislativo-368859089. Acesso em: 06 jan. 2023.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 09 jan. 2023.

BRASIL FIGURA como um dos países com mais ameaças cibernéticas do mundo em 2020. **Infor Channel**, 18/12/2020. Disponível em: https://inforchannel.com.br/2020/12/18/brasil-figura-como-um-dos-paises-com-mais-ameacas-ciberneticas-do-mundo-em-2020/. Acesso em: 14 jul. 2022.

BRASIL. Governo Federal lança Plano Tático de Combate a Crimes Cibernéticos. **Ministério da Justiça e Segurança Pública**, 23/03/2022a. Disponível em:

https://www.gov.br/pt-br/noticias/justica-e-seguranca/2022/03/governo-federal-lanca-plano-tatico-de-combate-a-crimes-ciberneticos. Acesso em: 11 jan. 2023.

BRASIL. Grotius: Programa Nacional de Difusão de Cooperação Jurídica Internacional – Grotius Brasil. **Ministério da Justiça e Segurança Pública**, 25/11/2022b. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-protecao/lavagem-de-dinheiro/institucional-2/capacitacao/grotius. Acesso em: 11 de jan. 2023.

BRASIL. **Lei nº 4.737, de 15 de julho de 1965**. Institui o Código Eleitoral. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L4737compilado.htm. Acesso em: 06 fev. 2023.

BRASIL. **Lei nº 7.646, de 18 de dezembro de 1987**. Dispõe quanto à proteção da propriedade intelectual sobre programas de computador e sua comercialização no País e dá outras providências. Revogada. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L7646.htm. Acesso em: 17 nov. 2022.

BRASIL. **Lei nº 7.716, de 05 de janeiro de 1989**. Define os crimes resultantes de preconceito de raça ou de cor. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L7716compilado.htm. Acesso em: 10 fev. 2023.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 17 nov. 2022.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8069compilado.htm. Acesso em: 17 nov. 2022.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do Art. 5° da Constituição Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 09 fev. 2023.

BRASIL. **Lei nº 9.394, de 20 de dezembro de 1996**. Estabelece as diretrizes e bases da educação nacional. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9394.htm. Acesso em: 17 nov. 2022.

BRASIL. **Lei nº 9.504, de 30 de setembro de 1997**. Estabelece normas para as eleições. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9504compilado.htm. Acesso em: 06 fev. 2023.

BRASIL. **Lei nº 9.609, de 19 de fevereiro de 1998**. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9609.htm. Acesso em: 17 nov. 2022.

BRASIL. **Lei nº 9.983, de 14 de julho de 2000**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9983.htm. Acesso em: 7 fev. 2023.

BRASIL. **Lei nº 10.695, de 1º de julho de 2003**. Altera e acresce parágrafo ao Art. 184 e dá nova redação ao Art. 186 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 – Código Penal, alterado pelas Leis nos 6.895, de 17 de dezembro de 1980, e 8.635, de 16 de março de 1993, revoga o Art. 185 do Decreto-Lei no 2.848, de 1940, e acrescenta dispositivos ao Decreto-Lei no 3.689, de 3 de outubro de 1941 – Código de Processo Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/2003/L10.695.htm. Acesso em: 5 fev. 2023.

BRASIL. **Lei nº 11.079, de 30 de dezembro de 2004**. Institui normas gerais para licitação e contratação de parceria público-privada no âmbito da administração pública. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/lei/L11079compilado.htm. Acesso em: 4 jan. 2023.

BRASIL. **Lei nº 11.343, de 23 de agosto de 2006**. Institui o Sistema Nacional de Políticas Públicas sobre Drogas - Sisnad; prescreve medidas para prevenção do uso indevido, atenção e reinserção social de usuários e dependentes de drogas; estabelece normas para repressão à produção não autorizada e ao tráfico ilícito de drogas; define crimes e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11343.htm. Acesso em: 4 set. 2022.

BRASIL. **Lei nº 11.829, de 25 de novembro de 2008**. Altera a Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11829.htm. Acesso em: 17 nov. 2022.

BRASIL. **Lei nº 12.034, de 29 de setembro de 2009**. Altera as Leis nos 9.096, de 19 de setembro de 1995 - Lei dos Partidos Políticos, 9.504, de 30 de setembro de 1997, que estabelece normas para as eleições, e 4.737, de 15 de julho de 1965 - Código Eleitoral. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2009/Lei/L12034.htm. Acesso em: 15 jan. 2023.

BRASIL. **Lei nº 12.037, de 1º de outubro de 2009**. Dispõe sobre a identificação criminal do civilmente identificado, regulamentando o art. 5º, inciso LVIII, da Constituição Federal. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l12037.htm. Acesso em: 15 jan. 2023.

BRASIL. **Lei nº 12.288, de 20 de julho de 2010**. Institui o Estatuto da Igualdade Racial; altera as Leis nos 7.716, de 5 de janeiro de 1989, 9.029, de 13 de abril de 1995, 7.347, de 24 de julho de 1985, e 10.778, de 24 de novembro de 2003. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2010/Lei/L12288.htm. Acesso em: 16 fev. 2023.

BRASIL. **Lei nº 12.683, de 09 de julho de 2012**. Altera a Lei nº 9.613, de 3 de março de 1998, para tornar mais eficiente a persecução penal dos crimes de lavagem de dinheiro. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12683.htm. Acesso em: 10 fev. 2023.

BRASIL. **Lei nº 12.735, de 30 de novembro de 2012**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm. Acesso em: 28 nov. 2022.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 7 fev. 2023.

BRASIL. **Lei nº 12.830, de 20 de junho de 2013**. Dispõe sobre a investigação criminal conduzida pelo delegado de polícia. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12830.htm. Acesso em: 2 set. 2022.

BRASIL. **Lei nº 12.850, de 02 de agosto de 2013**. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 15 fev. 2023.

BRASIL. **Lei nº 12.891, de 11 de dezembro de 2013**. Altera as Leis nºs 4.737, de 15 de julho de 1965, 9.096, de 19 de setembro de 1995, e 9.504, de 30 de setembro de 1997, para diminuir o custo das campanhas eleitorais, e revoga dispositivos das Leis nºs 4.737, de 15 de julho de 1965, e 9.504, de 30 de setembro de 1997. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Lei/L12891.htm. Acesso em: 06 fev. 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 27 nov. 2022.

BRASIL. **Lei nº 13.165, de 29 de setembro de 2015**. Altera as Leis nº 9.504, de 30 de setembro de 1997, 9.096, de 19 de setembro de 1995, e 4.737, de 15 de julho de 1965 - Código Eleitoral, para reduzir os custos das campanhas eleitorais, simplificar a administração dos Partidos Políticos e incentivar a participação feminina. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Lei/L13165.htm. Acesso em: 06 fev. 2023.

BRASIL. **Lei nº 13.185, de 6 de novembro de 2015**. Institui o Programa de Combate à Intimidação Sistemática (Bullying). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13185.htm. Acesso em: 3 nov. 2022.

BRASIL. **Lei nº 13.188, de 11 de novembro de 2015**. Dispõe sobre o direito de resposta ou retificação do ofendido em matéria divulgada, publicada ou transmitida por veículo de comunicação social. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13188.htm. Acesso em: 3 nov. 2022.

BRASIL. **Lei nº 13.344, de 06 de outubro de 2016**. Dispõe sobre prevenção e repressão ao tráfico interno e internacional de pessoas e sobre medidas de atenção às vítimas; altera a Lei nº 6.815, de 19 de agosto de 1980, o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); e revoga dispositivos do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/L13344.htm. Acesso em: 10 jan. 2023.

BRASIL. **Lei nº 13.441, de 08 de maio de 2017**. Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13441.htm. Acesso em: 17 nov. 2022.

BRASIL. **Lei nº 13.488, de 06 de outubro de 2017**. Altera as Leis nº 9.504, de 30 de setembro de 1997 (Lei das Eleições), 9.096, de 19 de setembro de 1995, e 4.737, de 15 de julho de 1965 (Código Eleitoral), e revoga dispositivos da Lei nº 13.165, de 29 de setembro de 2015 (Minirreforma Eleitoral de 2015), com o fim de promover reforma no ordenamento político-eleitoral. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13488.htm. Acesso em: 06 fev. 2023.

BRASIL. **Lei nº 13.663, de 14 de maio de 2018**. Altera o Art. 12 da Lei nº 9.394, de 20 de dezembro de 1996, para incluir a promoção de medidas de conscientização, de prevenção e de combate a todos os tipos de violência e a promoção da cultura de paz entre as incumbências dos estabelecimentos de ensino. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13663.htm. Acesso em: 28 nov. 2022.

BRASIL. **Lei nº 13.675, de 11 de junho de 2018**. Disciplina a organização e o funcionamento dos órgãos responsáveis pela segurança pública, nos termos do § 7º do art. 144 da Constituição Federal; cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS); institui o Sistema Único de Segurança Pública (Susp); altera a Lei Complementar nº 79, de 7 de janeiro de 1994, a Lei nº 10.201, de 14 de fevereiro de 2001, e a Lei nº 11.530, de 24 de outubro de 2007; e revoga dispositivos da Lei nº 12.681, de 4 de julho de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13675.htm. Acesso em: 01 set. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 mai. 2023.

BRASIL. **Lei nº 13.718, de 24 de setembro de 2018**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar os crimes de importunação sexual e de divulgação de cena de estupro, tornar pública incondicionada a natureza da ação penal dos crimes contra a liberdade sexual e dos crimes sexuais contra vulnerável, estabelecer causas

de aumento de pena para esses crimes e definir como causas de aumento de pena o estupro coletivo e o estupro corretivo; e revoga dispositivo do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13718.htm. Acesso em: 07 fev. 2023.

BRASIL. **Lei nº 13.772, de 19 de dezembro de 2018**. Altera a Lei nº 11.340, de 7 de agosto de 2006 (Lei Maria da Penha), e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para reconhecer que a violação da intimidade da mulher configura violência doméstica e familiar e para criminalizar o registro não autorizado de conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13772.htm. Acesso em: 07 fev. 2023.

BRASIL. **Lei nº 13.834, de 04 de junho de 2019**. Altera a Lei nº 4.737, de 15 de julho de 1965 - Código Eleitoral, para tipificar o crime de denunciação caluniosa com finalidade eleitoral. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13834.htm. Acesso em: 17 nov. 2022.

BRASIL. **Lei nº 13.869, de 05 de setembro de 2019**. Dispõe sobre os crimes de abuso de autoridade; altera a Lei nº 7.960, de 21 de dezembro de 1989, a Lei nº 9.296, de 24 de julho de 1996, a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 8.906, de 4 de julho de 1994; e revoga a Lei nº 4.898, de 9 de dezembro de 1965, e dispositivos do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13869.htm. Acesso em: 09 fev. 2023.

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm. Acesso em: 05 fev. 2023.

BRASIL. **Lei nº 13.968, de 26 de dezembro de 2019**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para modificar o crime de incitação ao suicídio e incluir as condutas de induzir ou instigar a automutilação, bem como a de prestar auxílio a quem a pratique. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13968.htm. Acesso em: 05 fev. 2023.

BRASIL. **Lei nº 14.132, de 31 de março de 2021a**. Acrescenta o Art. 147-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de perseguição; e revoga o Art. 65 do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14132.htm. Acesso em: 21 maio. 2022.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021b**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm. Acesso em: 09 jan. 2023.

BRASIL. **Lei nº 14.197, de 1º de setembro de 2021**. Acrescenta o Título XII na Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), relativo aos crimes contra o Estado Democrático de Direito; e revoga a Lei nº 7.170, de 14 de dezembro de 1983 (Lei de Segurança Nacional), e dispositivo do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14197.htm. Acesso em: 09 jan. 2023.

BRASIL. **Lei nº 14.478, de 21 de dezembro de 2022**. Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros; e altera a Lei nº 7.492, de 16 de junho de 1986, que define crimes contra o sistema financeiro nacional, e a Lei nº 9.613, de 3 de março de 1998, que dispõe sobre lavagem de dinheiro, para incluir as prestadoras de serviços de ativos virtuais no rol de suas disposições. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Lei/L14478.htm. Acesso em: 03 jan. 2023.

BRASIL. **Lei nº 14.532, de 11 de janeiro de 2023**. Altera a Lei nº 7.716, de 5 de janeiro de 1989 (Lei do Crime Racial), e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar como crime de racismo a injúria racial, prever pena de suspensão de direito em caso de racismo praticado no contexto de atividade esportiva ou artística e prever pena para o racismo religioso e recreativo e para o praticado por funcionário público. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Lei/L14532.htm. Acesso em: 12 jan. 2023.

BRASIL. **Lei nº 14.533, de 11 de janeiro de 2023**. Institui a Política Nacional de Educação Digital e altera as Leis nºs 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional), 9.448, de 14 de março de 1997, 10.260, de 12 de julho de 2001, e 10.753, de 30 de outubro de 2003. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Lei/L14533.htm. Acesso em: 15 jan. 2023.

BRASIL. **Medida Provisória nº 869, de 27 de dezembro de 2018**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Mpv/mpv869.htm. Acesso em: 28 nov. 2022.

BRASIL. Portaria SENASP/MJSP nº 418, de 11 de maio de 2022. Designa os integrantes de Grupo Técnico, indicados pelo Conselho Nacional de Chefes de Polícia Civil, com a finalidade de subsidiar ações afetas à SENASP instituídas no Plano Tático de Combate a Crimes Cibernéticos Do MJSP. **Ministério da Justiça e Segurança Pública**, Boletim de Serviço, em 12/05/2022. Disponível em: https://sei.mj.gov.br/sei/publicacoes/controlador_publicacoes.php?acao=publicacao_visualizar&id_documento=21068389&id_orgao_publicacao=0. Acesso em: 11 jan. 2023.

BRASIL. Portaria SENASP/MJSP nº 563, de 26 de setembro de 2022. ALTERAÇÃO e PRORROGAÇÃO da Portaria SENASP/MJSP Nº 418, DE 11 DE MAIO DE 2022 (18003710) para a conclusão das atividades do Grupo Técnico, indicado pelo Conselho Nacional de Chefes da Polícia Civil, com a finalidade de subsidiar ações afetas à SENASP, instituídas no Plano Tático de Combate a Crimes Cibernéticos do MJSP. **Ministério da Justiça e Segurança Pública**, Boletim de Serviço, em 26/09/2022. Disponível em: https://sei.mj.gov.br/sei/publicacoes/controlador_publicacoes.php?acao=publicacao_visualizar&id_documento=23102176&id_orgao_publicacao=0. Acesso em: 11 jan. 2023.

BRASIL. **Resolução nº 738, de 21 de dezembro de 2020.** Altera o Regulamento dos Serviços de Telecomunicações para incluir disposições sobre sigilo, prevenção à fraude e ações de apoio à segurança pública, e dá outras providências. Ministério das Comunicações, Agência Nacional de Telecomunicações, Conselho Diretor. Disponível em: https://www.in.gov.br/web/dou/-/resolucao-n-738-de-21-de-dezembro-de-2020-296152700. Acesso em: 11 jan. 2023.

BRASIL. **TRF-4 - CC: 16796 PR 2007.04.00.016796-0**. TRANSFERÊNCIA BANCÁRIA FRAUDULENTA VIA INTERNET. FURTO QUALIFICADO. COMPETÊNCIA - LOCAL DA CONSUMAÇÃO. Relator: AMAURY CHAVES DE ATHAYDE, Data de Julgamento: 24/09/2007, QUARTA SEÇÃO, Data de Publicação: D.E. 10/10/2007. Disponível em: https://trf-4.jusbrasil.com.br/jurisprudencia/1261176/conflito-de-competencia-cc-16796. Acesso em: 3 jun. 2022.

BRASIL. **TRF-4 - ACR: 14815 PR 2002.70.00.014815-4**: FURTO QUALIFICADO (FRAUDE). ART. 155, § 4º, II, DO CP. TRANSFERÊNCIA BANCÁRIA FRAUDULENTA VIA INTERNET. Relator: ARTUR CÉSAR DE SOUZA, Data de Julgamento: 30/07/2008, OITAVA TURMA, Data de Publicação: D.E. 13/08/2008. Disponível em: https://trf-4.jusbrasil.com.br/jurisprudencia/1311220/apelacao-criminal-acr-14815. Acesso em: 3 jun. 2022.

BUDÓ, Marília De Nardin. **Da Construção Social da Criminalidade à Reprodução da Violência Estrutural**: os conflitos agrários no jornal. Dissertação de Mestrado em Direito, UFSC, Florianópolis, 2008.

BUDÓ, Marília de Nardin. Newsmaking criminology: o papel dos intelectuais na construção de um novo discurso sobre o crime nos *media*. **Comunicação & Cultura**, v. 14, p. 107-123, 2012.

BUDÓ, Marília de Nardin. **Mídias e discursos do poder:** a legitimação discursiva do processo de encarceramento da juventude pobre no Brasil. 2013. Tese de Doutorado. Tese (Doutorado em Direito) – Curso de Pós-Graduação em Direito, Universidade Federal do Paraná, Curitiba.

BUENO, Chris. Brexit e o novo momento para a Europa. **Ciência e Cultura**, v. 68, n. 4, p. 14-16, 2016.

BUENO, Samira; LIMA, Renato Sérgio de Lima. Anuário Brasileiro de Segurança Pública 2022. **Fórum Brasileiro de Segurança Pública**, ano 16, 2022. ISSN 1983-7364. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2022/06/anuario-2022.pdf?v=5. Acesso em: 2 set. 2022.

BUZZI, Vitória de Macedo. **Pornografia de vingança**: contexto histórico-social e abordagem no direito brasileiro. Florianópolis: Empório do Direito, 2015.

CABRAL, Isabela. A História dos domínios de Internet. **TechTudo**. 7 jul. 2018. Disponível em: https://www.techtudo.com.br/noticias/2018/07/a-historia-dos-dominios-de-internet.ghtml. Acesso em: 15 dez. 2022.

CAGNINI, Henry *et al.* Mundo virtual minecraft: uma experiência no ensino de circuitos digitais. *In:* **Anais do XXIII Workshop sobre Educação em Computação**. SBC, p. 206-215, 2015.

CÂMARA DOS DEPUTADOS. **APERFEIÇOAMENTO DA LEGISLAÇÃO BRASILEIRA - INTERNET**. GT - Aperfeiçoamento da Legislação Brasileira sobre Internet. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/aperfeicoamento-da-legislacao-brasileira-internet. Acesso em: 19 jan. 2023.

CÂMARA DOS DEPUTADOS. **Comprove**: combate às notícias falsas. Disponível em: https://www.camara.leg.br/comprove. Acesso em: 19 jan. 2023.

CÂMARA DOS DEPUTADOS. **Diário da Câmara dos Deputados**: 14 de outubro de 2015, p. 522-550. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1434573&filename=Tramitacao-PL+215/2015. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. Parecer do Relator, Dep. Mandetta (DEM-MS), pela aprovação deste, e dos PLs nºs 1.494/2011, 1.573/2011, 7.609/2014, 3.263/2015, 3.686/2015, 4.805/2016, 7.946/2014, 5.382/2016, e 9.243/2017, apensados, com substitutivo. 2018a. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1657451&filename=Tramitacao-PL+1011/2011. Acesso em: 17 nov. 2022.

CÂMARA DOS DEPUTADOS. Parecer do Relator, Dep. Celso Pansera (PT-RJ), pela rejeição deste, e dos de nºs 7.604/2017, 8.592/2017, 9.533/2018, 9.554/2018, 9.761/2018, 9.838/2018, 9.884/2018, 9.931/2018, e 9.647/2018, apensados. **2018b**. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1694884&filename=Tramitacao-PL+6812/2017. Acesso em: 17 nov. 2022.

CÂMARA DOS DEPUTADOS. Parecer da Relatora, Dep. Flordelis (PSD-RJ), pela aprovação do PL 1011/2011, do PL 1494/2011, do PL 1573/2011, do PL 7609/2014, do PL 3263/2015, do PL 3686/2015, do PL 4805/2016, do PL 7946/2014, do PL 5382/2016, do PL 9243/2017, e do PL 5064/2019, apensados, com substitutivo. 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1827842&filename=Tramitacao-PL+1011/2011. Acesso em: 17 nov. 2022.

CÂMARA DOS DEPUTADOS. **PAUTA DE REUNIÃO EXTRAORDINÁRIA AUDIÊNCIA PÚBLICA DIA 23/09/2021**. GRUPO DE TRABALHO DESTINADO A ANALISAR E ELABORAR PARECER AO PROJETO DE LEI Nº 2630, DE 2020, E APENSADOS, QUE VISA AO APERFEIÇOAMENTO DA LEGISLAÇÃO

BRASILEIRA REFERENTE À LIBERDADE, RESPONSABILIDADE E TRANSPARÊNCIA NA INTERNET, 23/09/2021. Disponível em: https://www.camara.leg.br/internet/ordemdodia/integras/2076866.htm. Acesso em: 19 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Decreto Legislativo 255/2021**. Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2287513. Acesso em: 27 jul. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 8.551/1987**. Dispõe quanto à proteção da propriedade intelectual sobre programas para computadores e sua comercialização no país, e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=233097. Acesso em: 17 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 5.172/1990**. Dispõe sobre o Estatuto da Criança e do Adolescente, e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=226513. Acesso em: 17 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 3.683/1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=214992. Acesso em: 17 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 2.462/1991**. Define os crimes contra o Estado Democrático de Direito e a Humanidade. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=18156. Acesso em: 09 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 4.102/1993**. Regula a garantia constitucional da inviolabilidade de dados; define crimes praticados por meio de computador; altera a Lei nº 7.646, de 18 de dezembro de 1987, que "dispõe sobre a proteção da propriedade intelectual de programas de computador e sua comercialização no País, e dá outras providências". Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=20670. Acesso em: 5 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 200/1995**. Dispõe sobre a proteção da propriedade intelectual de programas de computador, sua comercialização no país, e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=173046. Acesso em: 17 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 1.156/1995**. Regulamenta o inciso XII, parte final, do artigo quinto da Constituição Federal. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=188225. Acesso em: 09 fev. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 1.258/1995**. Disciplina o inciso XII do art. 5º da Constituição Federal e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=16481. Acesso em: 16 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 2.681/1996**. Dá nova redação aos §§ 1º e 3º do Art. 184 e ao Art. 186 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, e acrescenta parágrafos ao Art. 525 do Decreto-Lei nº 3.689, de 3 de outubro de 1941 – Código de Processo Penal. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=18480. Acesso em: 5 fev. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 2.695/1997**. Estabelece normas para as eleições de 03 de outubro de 1998 e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=205889. Acesso em: 7 fev. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 84/1999**. Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=15028. Acesso em: 10 fev. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 933/1999**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, mediante a tipificação de condutas que constituem crimes contra a previdência social, e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=25156. Acesso em: 7 fev. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 6.264/2005**. Institui o Estatuto da Igualdade Racial. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=307731. Acesso em: 10 fev. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 3.443/2008**. Dá nova redação a dispositivos da Lei nº 9.613, de 3 de março de 1998, objetivando tornar mais eficiente a persecução penal dos crimes de lavagem de dinheiro. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=395834. Acesso em: 10 fev. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 3.773/2008**. Altera a Lei nº 8.069, de 13 de julho de 1990 – Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na Internet. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=405465. Acesso em: 17 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 5.286/2009**. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Disponível em:

https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=436097. Acesso em: 16 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 5.369/2009**. Institui o Programa de Combate ao "Bullying". Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=437390. Acesso em: 17 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 5.409/2009**. Acrescenta o Art. 146-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, dispondo sobre o crime de perseguição "stalking". Disponível em: https://www.camara.leg.br/propostas-legislativas/438638. Acesso em: 23 mai. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 5.498/2009**. Altera a Lei nº 9.096, de 19 de setembro de 1995 (Lei dos Partidos Políticos) e a Lei nº 9.504, de 30 de setembro de 1997, que "estabelece normas para as eleições". Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=440269. Acesso em: 07 fev. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 6.578/2009**. Dispõe sobre as organizações criminosas, os meios de obtenção da prova, o procedimento criminal e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=463455. Acesso em: 10 fev. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 8.045/2010**. Código de Processo Penal. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=490263. Acesso em: 16 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 1.011/2011**. Define o crime de Intimidação escolar no Código Penal Brasileiro e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=498107. Acesso em: 17 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 1.213/2011**. Altera o § 1º do art. 217-A do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=500200. Acesso em: 13 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 1.404/2011**. Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes da polícia na internet com o fim de investigar crimes contra a liberdade sexual de criança ou adolescente. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=503024. Acesso em: 17 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 1.494/2011**. Dispõe sobre o crime de intimidação vexatória. Disponível em:

https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=505174. Acesso em: 17 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 1.573/2011**. Acrescenta o Art. 140-A ao Decreto-lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, e o Art. 117-A à Lei nº 8.069, de 13 de julho de 1990, que "dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências", a fim de tipificar o crime de "bullying". Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=508898. Acesso em: 17 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 1.785/2011**. Acrescenta inciso IX ao art. 12 da Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional), para incluir entre as incumbências dos estabelecimentos de ensino a promoção de ambiente escolar seguro e a adoção de estratégias de prevenção e combate ao *bullying*. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=511619. Acesso em: 17 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 1.978/2011**. Altera a Lei nº 4.737, de 15 de julho de 1965 – Código Eleitoral, para tipificar o crime de denunciação caluniosa com finalidade eleitoral. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=514939. Acesso em: 17 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 2.126/2011**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=517255. Acesso em: 10 fev. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 2.793/2011**. Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=529011. Acesso em: 07 fev. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 4.060, de 2012**. Dispõe sobre o tratamento de dados pessoais e dá outras providências. Disponível em: https://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066. Acesso em: 28 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 5.555/2013**. Altera a Lei nº 11.340, de 7 de agosto de 2006 – Lei Maria da Penha – criando mecanismos para o combate a condutas ofensivas contra a mulher na Internet ou em outros meios de propagação da informação. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=576366. Acesso em: 07 fev. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 5.735/2013**. Altera dispositivos da Lei nº 4.737, de 15 de julho de 1965 (Código Eleitoral), da Lei nº 9.096, de 19 de setembro de 1995 (Lei dos Partidos Políticos) e da Lei nº 9.504, de 30 de setembro de 1997 (Lei das Eleições). Disponível em:

https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=580148. Acesso em: 07 fev. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 6.397/2013**. Altera as Leis nºs 4.737, de 15 de julho de 1965, 9.096, de 19 de setembro de 1995, e 9.504, de 30 de setembro de 1997, para diminuir o custo das campanhas eleitorais, e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=592935. Acesso em: 07 fev. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 6.630/2013**. Acrescenta artigo ao Código Penal, tipificando a conduta de divulgar fotos ou vídeos com cena de nudez ou ato sexual sem autorização da vítima e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=598038. Acesso em: 29 fev. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 7.370/2014**. Dispõe sobre prevenção e repressão ao tráfico interno e internacional de pessoas e sobre medidas de atenção às vítimas; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e as Leis nºs 6.815, de 19 de agosto de 1980, e 7.998, de 11 de janeiro de 1990; e revoga dispositivos do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal). Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=611445. Acesso em: 10 fev. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 7.609/2014**. Acrescenta artigo ao Código Penal, tipificando a conduta de constranger alguém a participar de trote estudantil. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=617184. Acesso em: 17 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 7.758/2014**. Modifica o disposto no art. 307 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=619448. Acesso em: 13 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 7.946/2014**. Acrescenta parágrafo ao artigo 146 do Código Penal, tipificando a conduta de realizar trote estudantil. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=622151. Acesso em: 17 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 8.040/2014**. Altera o Código de Processo Penal para determinar que os órgãos do poder público e as empresas da iniciativa privada simplifiquem o acesso aos dados cadastrais para as autoridades responsáveis pela investigação. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2229416. Acesso em: 16 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 215/2015**. Acrescenta inciso V ao Art. 141 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=946034&ord=1. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 1.547/2015**. Institui nova causa de aumento de pena aos crimes contra a honra, em sítios ou por meio de mensagens eletrônicas difundidas pela Internet, e determina à Autoridade Policial que promova, mediante requerimento de quem tem qualidade para intentar a respectiva ação penal, o acesso ao sítio indicado e respectiva impressão do material ofensivo, lavrando-se o competente termo. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=1278965. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 1.589/2015**. Torna mais rigorosa a punição dos crimes contra a honra cometidos mediantes disponibilização de conteúdo na internet ou que ensejarem a prática de atos que causem a morte da vítima. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=1279451. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 1.676/2015**. Tipifica o ato de fotografar, filmar ou captar a voz de pessoa, sem autorização ou sem fins lícitos, prevendo qualificadoras para as diversas formas de sua divulgação, e dispõe sobre a garantia de desvinculação do nome, imagem e demais aspectos da personalidade, publicados na rede mundial de computadores, internet, relativos a fatos que não possuem, ou não possuem mais, interesse público. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=1295741. Acesso em: 29 fev. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 2.390/2015**. Altera a Lei nº 8.069, de 12 de julho de 1990, criando o Cadastro Nacional de Acesso à Internet, com a finalidade de proibir o acesso de crianças e adolescentes a sítios eletrônicos com conteúdo inadequado. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=1584972. Acesso em: 15 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 3.263/2015**. Dispõe sobre o direito da criança e do adolescente à retratação, pelo mesmo meio, em caso de "bullying" virtual. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2017174. Acesso em: 17 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 3.357/2015**. Dispõe sobre o crime de invadir dispositivo informático, sem a devida autorização, modificando conteúdo de sítio da internet. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2024070. Acesso em: 13 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 3.686/2015**. Tipifica o crime de intimidação sistemática (*Bullying*), prevendo causa de aumento se a conduta for realizada por meio da internet (*Cyberbullying*). Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2055840. Acesso em: 17 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 3.703/2015**. Regula o acesso a dados cadastrais e aos sinais de comunicação telefônica e/ou telemática que importem na investigação criminal e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2055957. Acesso em: 16 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 4.148/2015**. Altera o inciso III do Art. 141 do dec-lei 2.848, de 7 de dezembro de 1940 e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2075795. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 4.805/2016**. Trata da perseguição sistemática digital (*cyberstalking*), que consiste no uso das ferramentas tecnológicas com intuito de perseguir, controlar ou ameaçar de modo continuado uma pessoa. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2080265. Acesso em: 17 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 5.016/2016**. Altera a Lei nº 8.609, de 13 de julho de 1990, para obrigar as empresas que prestam serviços de telefonia móvel a implementarem bloqueio prévio ao acesso a determinados conteúdos da Internet ou aplicativos, especialmente sites e aplicativos de relacionamento que contenham conteúdo pornográfico ou que instiguem a violência. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2082037. Acesso em: 13 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 5.200/2016**. Altera a redação do art. 154-A do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, para ampliar a abrangência do crime de invasão de dispositivo informático. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2083668. Acesso em: 13 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 5.382/2016**. Proíbe a realização de trote em estabelecimentos educacionais de ensino superior; acrescenta o Art. 146-A ao Código Penal para tipificar o trote como crime, além de estabelecer causa de aumento de pena se do trote resultar morte. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2085580. Acesso em: 17 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 5.452/2016**. Acrescenta os arts. 218-C e 225-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar o crime de divulgação de cena de estupro e prever causa de aumento de pena para o crime de estupro cometido por duas ou mais pessoas. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2086414. Acesso em: 07 fev. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 5.826/2016**. Acrescenta incisos IX e X ao Art. 12 da Lei nº 9.394, de 20 de dezembro de 1996, para incluir o combate a todas as formas de violência e a promoção de cultura de paz entre as incumbências dos estabelecimentos de ensino. Disponível em:

https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2091857. Acesso em: 17 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 6.812/2017**. Dispõe sobre a tipificação criminal da divulgação ou compartilhamento de informação falsa ou incompleta na rede mundial de computadores e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2122678. Acesso em: 13 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 6.960/2017**. Alterar a Lei nº 12.965 de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, alterando o art 5º, inciso II e o art 7º, inciso III. Disponível em: https://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2124030&ord=1. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 6.989/2017**. Altera o Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014, para incluir procedimento de retirada de conteúdos que induzam, instiguem ou auxiliem a suicídio de aplicações de internet. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2124329. Acesso em: 08 fev. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 7.537/2017**. Institui causa de aumento de pena àqueles que se utilizam de dispositivos de transmissão de dados que potencializam a divulgação de informações nos crimes contra a honra e no tipo penal de que trata o Art. 66 do Código de Defesa do Consumidor. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2132797. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 7.596/2017**. Dispõe sobre os crimes de abuso de autoridade e altera a Lei nº 7.960, de 21 de dezembro de 1989, a Lei nº 9.296, de 24 de julho de 1996, a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 8.906, de 4 de julho de 1994. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2136580. Acesso em: 09 fev. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 7.604/2017**. Dispõe sobre a aplicação de multa pela divulgação de informações falsas pela rede social e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2136633. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 8.612/2017**. Altera a Lei nº 9.096, de 19 de setembro de 1995 (Lei dos Partidos Políticos), a Lei nº 9.504, de 30 de setembro de 1997 (Lei das Eleições), a Lei nº 4.737, de 15 de julho de 1965 (Código Eleitoral), a Lei nº 13.165, de 29 de setembro de 2015 (Minirreforma Eleitoral de 2015), e a Lei nº 5.768, de 20 de dezembro de 1971, com o fim de promover ampla reforma no ordenamento político-eleitoral. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2151995. Acesso em: 07 fev. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 8.592/2017**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, para tipificar a divulgação de informação falsa ou prejudicialmente incompleta. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2151560. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 8.833/2017**. Acrescenta Art. 244-C à Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para tipificar o crime de induzimento, instigação ou auxílio à automutilação de criança ou adolescente. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2155635. Acesso em: 08 fev. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 9.243/2017**. Altera a redação da Lei nº 13.185, de 6 de novembro de 2015, que institui o Programa de Combate à Intimidação Sistemática (*Bullying*), para prever medidas coercitivas a quem pratica violência contra crianças e adolescentes no ambiente escolar. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2164055. Acesso em: 17 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 9.533/2018**. Altera a Lei nº 7.170, de 14 de dezembro de 1983, que define os crimes contra a segurança nacional, a ordem política e social, estabelece seu processo e julgamento e dá outras providências, para dispor sobre o incitamento através das redes sociais. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2167860. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 9.554/2018**. Acrescenta artigo ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, para tipificar o crime de divulgação de informação falsa – *fake news*. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2167903. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 9.647/2018**. Dispõe sobre alteração na Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2168550. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 9.674/2018**. Institui a Semana Nacional de Conscientização, Prevenção e Combate a Intimidação Sistemática (*Bullying*) nas escolas públicas e privadas de ensino fundamental e médio em todo o território nacional e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2168640&ord=1. Acesso em: 16 fev. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 9.761/2018**. Tipifica criminalmente a conduta de quem cria, veicula, compartilha, ou não remove, em meios eletrônicos, notícias ou informações que sabe ser falsas. Disponível em:

https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2169225. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 9.808/2018**. Acrescenta os parágrafos 5° e 6º ao Art. 10 da Lei nº 12.965, de 23 de abril de 2014, para dispor sobre o acesso a dados de comunicação por meio de aplicativos de internet para fins de persecução criminal, nos casos que especifica. Disponível em: https://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2169629. Acesso em: 15 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 9.838/2018**. Tipifica criminalmente a conduta de quem oferece, publica, distribui, difunde notícia ou informação que sabe ser falsa em meios eletrônicos ou impressos. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2169820. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 9.884/2018**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, para tipificar a divulgação de informação falsa. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2170450. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 9.931/2018**. Tipifica o crime de divulgação de notícias ou informações falsas: Altera o Decreto-lei nº 2.848, de 1940; a Lei nº 12.965, de 2014 e o Decreto-lei nº 3.689, de 1941. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2170681. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 10.372/2018**. Introduz modificações na legislação penal e processual penal para aperfeiçoar o combate ao crime organizado, aos delitos de tráfico de drogas, tráfico de armas e milícia privada, aos crimes cometidos com violência ou grave ameaça e crimes hediondos, bem como para agilizar e modernizar a investigação criminal e a persecução penal. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2178170. Acesso em: 09 fev. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 200/2019**. Dispõe sobre a tipificação criminal da divulgação ou compartilhamento de informação falsa ou incompleta na rede mundial de computadores e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2190714. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 241/2019**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, para tipificar o crime de criação e propagação de notícia inverídica. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2190763. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 781/2019**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, para prever aplicação da pena em dobro

aos crimes contra honra cometidos mediante o uso perfil falso de redes sociais na internet. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2192022. Acesso em: 13 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 847/2019**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar o crime de conduta cibernética prejudicial à saúde, à incolumidade física ou psíquica ou à vida de outrem. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2229552. Acesso em: 12 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 1.369/2019**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal, tipificando o crime de perseguição e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2229558. Acesso em: 23 mai. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 1.585/2019**. Altera o Decreto Lei nº 2.848, de 20 de dezembro de 1940, altera a Lei nº 12.965, de 23 de abril de 2014, e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2194556. Acesso em: 15 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 1.797/2019**. Altera a Lei nº 13.260, de 16 de março de 2016, para proibir a conduta de disponibilizar, transmitir, distribuir, publicar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, mensagem escrita ou de áudio, vídeo ou outro registro que contenha, conforme suas características, nome ou imagem de autor de ataque terrorista ou de crimes que causem comoção ou repúdio nacional. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2195647. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 2.285/2019**. Veda a divulgação de imagens, nomes e conteúdos que identifiquem os autores de ataques, massacres e atos terroristas ocorridos em território brasileiro. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2198028. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 2.463/2019**. Dispõe sobre a limitação de divulgação de imagens e informações em veículos de mídia e redes sociais em situações de ataque massivo a pessoas. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2198978. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 2.601/2019**. Altera a Lei nº 12.965, de 23 de abril de 2014, para criar obrigação de indisponibilização de notícias falsas por provedores de aplicações de internet e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2199770. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 2.602/2019**. Altera o Art. 19 da Lei nº 12.965, de 23 de abril de 2014, para estabelecer a obrigação de indisponibilidade de conteúdo apontado como infringente em boletim de ocorrência policial. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2199771. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 3.389/2019**. Acrescenta os §§ 5º e 6º ao art. 10 da Lei nº 12.965, de 23 de abril de 2014, para estabelecer a obrigatoriedade de fornecimento do número de inscrição no Cadastro de Pessoas Físicas (CPF) ou Cadastro Nacional de Pessoa Jurídica (CNPJ) para cadastro em aplicações de internet. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2207075. Acesso em: 15 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 3.545/2019**. Aumenta a pena do crime de invasão de dispositivo informático alheio, tanto na sua forma simples como qualificada, previsto no art. 154-A, caput, e § 3º, do Código Penal. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2208102. Acesso em: 13 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 4.301/2019**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, para dispor sobre os crimes de calúnia, difamação e injúria praticados na rede mundial de computadores e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2214005. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 4.442/2019**. Altera a Lei nº 12.965, de 23 de abril de 2014, para estabelecer a autoridade policial a requisição de dados. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2214922. Acesso em: 15 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 5.064/2019**. Proíbe a realização de trote nos estabelecimentos educacionais públicos e privados e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2220216. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 5.261/2019**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, para inserir nova modalidade de invasão de dispositivo informático. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2222079. Acesso em: 13 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 5.419/2019**. Altera a Lei nº 11.340, de 7 de agosto de 2006 (Lei Maria da Penha) e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), a fim de aprimorar a legislação pátria quanto à violência patrimonial contra a mulher. Disponível em:

https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2224318. Acesso em: 14 jul. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 5.668/2019**. Permite que o membro do Ministério Público ou o delegado de polícia requisitem diretamente às empresas prestadoras de serviço de telecomunicações e/ou telemática os meios técnicos adequados para a localização da vítima ou dos suspeitos do delito em curso em determinados casos. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2226834. Acesso em: 16 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 5.968/2019**. Acrescenta o inciso V ao art. 13 do Decreto-Lei nº 3.689, de 3 de outubro de 1941. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=623798. Acesso em: 16 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 310/2020**. Altera o art. 154-A, constante do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, que dispõe sobre Invasão de dispositivo informático. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2237311. Acesso em: 13 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 693, de 2020**. Dispõe sobre a responsabilidade sanitária da conduta das autoridades públicas, tipifica o crime de divulgação ou compartilhamento de informação falsas que atentem contra a segurança sanitária e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2239459. Acesso em: 13 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 705, de 2020**. Insere o art. 339-A ao Decreto-Lei nº 2.848, de 7 de fevereiro de 1940, tipificando a conduta propagação de informações sabidamente falsas em relação a epidemias e pandemias que acometam a saúde pública nacional. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2239478. Acesso em: 21 mai. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 808, de 2020**. Altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet) e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para inibir práticas que induzam, instiguem ou auxiliem alguém à autolesão, à automutilação, ao suicídio, à exposição a situação de risco de vida, ou à exposição a situação de risco de contaminação por moléstia contagiosa. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2241665. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 1.258, de 2020**. Tipifica a divulgação de notícias falsas durante o período de calamidade pública, estado de defesa, estado de sítio ou intervenção, tratando ainda do indiciamento e da indenização em tais casos, alterando o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2242374 . Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 1.394, de 2020.** Tipifica, no Art. 287-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), a criação e a propagação, por qualquer meio, de informação falsa referente à saúde pública ou à segurança pública. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2242661. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 1.416, de 2020.** Tipifica como crime de responsabilidade a disseminação ou compartilhamento por ocupante de cargo, função ou emprego público de informação falsa, sem fundamento ou difamatória. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2242694. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 1.429, de 2020**. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2242713. Acesso em: 09 mai. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 2.389, de 2020.** Dispõe sobre a tipificação do crime de criação e divulgação de notícias falsas – *Fake News* sobre a pandemia do Coronavírus - Covid-19 acrescentando o art. 140-A ao do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2251491 . Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 2.630, de 2020**. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735. Acesso em: 13 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 2.857/2020**. Altera o artigo 69 do Decreto Lei nº 3.689/1941, Código de Processo Penal, para inserir o domicílio do réu em ações de crime contra a honra. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2253611. Acesso em: 16 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 3.063, de 2020.** Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2254270. Acesso em: 10 jun. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 3.627, de 2020**. Altera a Lei nº 12.965, de 23 de abril de 2014, para criar mecanismos de verificação de identidade dos perfis ativos em aplicações de internet que atuem como redes sociais e plataforma de registro de ocorrência policial na hipótese de crimes contra a honra cometidos ou divulgados em quaisquer modalidades das redes sociais da rede mundial de computadores e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256710. Acesso em: 13 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 3.628/2020**. Aumenta as penas do crime de estupro de vulnerável e tipifica a conduta de estupro virtual de vulnerável. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256711. Acesso em: 13 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 3.993/2020**. Dispõe sobre a obrigatoriedade de apresentação de documentos comprobatórios da idade para acesso às plataformas digitais. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2258897. Acesso em: 15 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 4.513/2020**. Institui a Política Nacional de Educação Digital e insere dispositivos no art. 4º da Lei nº 9.394, de 1996, de diretrizes e bases da educação nacional. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2262422. Acesso em: 15 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 4.554, de 2020.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet, e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2266148. Acesso em: 3 jun. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 5.223/2020**. Fixa a competência para o processamento e julgamento dos crimes cometidos por qualquer meio de comunicação ou por sistema de informática ou telemática. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2265478. Acesso em: 16 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 5.265/2020**. Modifica o art. 154-A do Decreto-Lei nº 2.848, de 07 de dezembro de 1940 – Código Penal Brasileiro, para alterar as penas de crimes por fraude cometida através de dispositivo eletrônico ou informático; e o art. 70 do Decreto-Lei nº 3.689 para prever a competência do foro do domicílio da vítima. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2265593. Acesso em: 13 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 5.278/2020**. Altera o art.154–A do Código Penal. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2265625. Acesso em: 13 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 5.388/2020**. Dispensa a autorização judicial para que o membro do Ministério Público ou o delegado de polícia requisitem às empresas prestadoras de serviço de telecomunicações e/ou telemática os meios técnicos adequados para a localização da vítima ou dos suspeitos do delito em curso em

determinados casos. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2266106. Acesso em: 16 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 5.441, de 2020.** Define os crimes cibernéticos e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2266423. Acesso em: 13 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 5.505/2020**. Altera o art. 154-A do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, para aumentar a pena máxima do crime de invasão de dispositivo informático. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2266993. Acesso em: 13 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 1.395/2021**. Acrescenta o § 3º ao artigo 3º e os artigos 15-A, 21-A, 21-B, 25-A e 25-B à lei nº 12.850 de 2 de agosto de 2013 (Lei de Combate às Organizações Criminosas). Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2278012. Acesso em: 18 nov. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 2.232, de 2021.** Altera o art. 158 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever a qualificadora da extorsão cibernética. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2287526. Acesso em: 13 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 2.233, de 2021.** Tipifica a usurpação ou acesso indevido de conta de usuário de aplicação de internet ou qualquer meio digital (clonagem). Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2287527. Acesso em: 13 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 2.385, de 2021.** Modifica o Decreto-Lei n° 2.848, de 7 de dezembro de 1940 – Código Penal, que "dispõe sobre a intimidação sistemática verbal, moral, sexual, social, psicológica, físico, material ou virtual". Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=498107. Acesso em: 12 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 2.699, de 2021.** Dispõe sobre a criminalização da prática de *haters* na rede mundial de computadores e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2292364. Acesso em: 12 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 2.706, de 2021.** Torna puníveis as postagens nas redes sociais de intimidação sistemática na rede mundial de computadores com o intuito de criar meios de constrangimento psicossocial (*cyberbullying*). Disponível

em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2292456. Acesso em: 12 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 3.402, de 2021.** Acrescenta o art. 140-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de *cyberbullying*. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2301264. Acesso em: 12 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 3.744, de 2021.** Altera o art. 4º da Lei nº 13.185, de 6 de novembro de 2015, para dispor sobre os objetivos do Programa de Combate à Intimidação Sistemática (*Bullying*), e o art. 1º da Lei nº 13.935, de 11 de dezembro de 2019, para dispor sobre a prevenção à intimidação sistemática no âmbito escolar. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2304288. Acesso em: 12 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 4.401, de 2021 (nº anterior: PL 2.303/2015)**. Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros; e altera a Lei nº 7.492, de 16 de junho de 1986, que define crimes contra o sistema financeiro nacional, e a Lei nº 9.613, de 3 de março de 1998, que dispõe sobre lavagem de dinheiro, para incluir as prestadoras de serviços de ativos virtuais no rol de suas disposições. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=1555470. Acesso em: 10 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 4.566, de 2021 (nº anterior: PL 1.749/2015)**. Tipifica o crime de injúria racial coletiva e torna pública incondicionada a respectiva ação penal. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=1301128. Acesso em: 12 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 1.515, de 2022a**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Disponível em: https://www.camara.leg.br/propostas-legislativas/2326300. Acesso em: 22 dez. 2022.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 1.926, de 2022b**. Dispõe sobre o trote em instituições de ensino, alterando a Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação), e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal). Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2331649. Acesso em: 12 jan. 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 2.557/2022c**. Institui a Política Nacional de Proteção Digital das Crianças e Adolescentes – PNPD. Disponível em:

https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2335259. Acesso em: 15 jan. 2023.

CÂMARA DOS DEPUTADOS. **Proposta de Emenda à Constituição nº 17, de 2019**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757. Acesso em: 25 nov. 2019.

CÂMARA DOS DEPUTADOS. **RELATÓRIO DO GRUPO DE TRABALHO APERFEIÇOAMENTO DA LEGISLAÇÃO BRASILEIRA – INTERNET**. GRUPO DE TRABALHO DESTINADO A ANALISAR E ELABORAR PARECER AO PROJETO DE LEI Nº 2630, DE 2020, E APENSADOS, QUE VISA AO APERFEIÇOAMENTO DA LEGISLAÇÃO BRASILEIRA REFERENTE À LIBERDADE, RESPONSABILIDADE E TRANSPARÊNCIA NA INTERNET, 07/12/2021. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/aperfeicoamento-da-legislacao-brasileira-internet/documentos/outros-documentos/relatorio-adotado-do-grupo-de-trabalho. Acesso em: 19 jan. 2023.

CALDERON, Barbara. **Deep & Dark Web**. Rio de Janeiro: Alta Books, 2017.

CARDOSO, André Tavares; FALCKE, Denise; MOSMANN, Clarisse Pereira. Sexting: percepções de adolescentes sobre o fenômeno e acerca do papel das relações familiares. **Estudos e Pesquisas em Psicologia**, v. 19, n. 3, p. 665-685, 2019.

CARONE, Carlos. Estelionato na internet cresceu mais de 1.200% no DF durante pandemia. **Metrópoles**, 12/04/2021. Disponível em: https://www.metropoles.com/distrito-federal/estelionato-na-internet-cresceu-mais-de-1-200-no-df-durante-pandemia. Acesso em: 14 jul. 2022.

CARONE, Carlos; PINHEIRO, Mirelle. Operação Brick: polícia faz ação contra pirataria de videogames. **Metrópoles**, 10/11/2021. Disponível em: https://www.metropoles.com/distrito-federal/na-mira/operacao-brick-policia-faz-acao-contra-pirataria-de-videogames. Acesso em: 09 jan. 2023.

CASTELLS, Manuel. **A sociedade em rede**. A era da Informação: Economia, Sociedade e Cultura, v. 1, 4ª edição. São Paulo: Paz e Terra, 1999.

CASTELLS, Manuel. **Redes de Indignação e Esperança**. Movimentos Sociais na era da internet. Rio de Janeiro: Zahar, 2013.

COLUCCI, Cláudia. Criminosos aproveitam pandemia de Covid-19 para aplicar golpes virtuais. **Folha de São Paulo**, 04/06/2020. Disponível em: https://www1.folha.uol.com.br/cotidiano/2020/06/criminosos-aproveitam-pandemia-de-covid-19-para-aplicar-golpes-virtuais.shtml. Acesso em: 14 jul. 2022.

COMITÊ GESTOR DA INTERNET NO BRASIL – CGI.br. **Portaria Interministerial nº 147, de 31 de maio de 1995**. Dispõe sobre a criação e gestão do Comitê Gestor da Internet

no Brasil – CGI.br. Disponível em: https://cgi.br/portarias/numero/147. Acesso em: 18 nov. 2022.

COMITÊ GESTOR DA INTERNET NO BRASIL – CGI.br. **Decreto nº 4.829, de 3 de setembro de 2003**. Dispõe sobre a criação do Comitê Gestor da Internet no Brasil – CGI.br, sobre o modelo de governança na Internet no Brasil, e dá outras providências. Disponível em: http://cgi.br/pagina/decretos/108. Acesso em: 18 nov. 2022.

CONGRESSO NACIONAL. **Decreto Legislativo nº 37, de 16 de dezembro de 2021**. Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-legislativo-368859089. Acesso em: 4 set. 2022.

COUNCIL OF EUROPE. **Consultations with civil society, data protection authorities and industry on the 2nd Additional Protocol to the Budapest Convention on Cybercrime**. 2021. Disponível em: https://www.coe.int/en/web/cybercrime/protocol-consultations. Acesso em: 25 jan. 2023.

COSTA, Mári Cibele Cosentino da; WENDT, Emerson. Nova metodologia da inquirição de crianças e adolescentes: avanços, limites e desafios à investigação criminal. *In:* WENDT, Emerson; LEITÃO JUNIOR, Joaquim; WENDT, Valquiria P. C. (org.). **Direito Policial:** na raiz dos problemas. Rio de Janeiro: Brasport, p. 142-157, 2022.

COSTA, Adriano Sousa; WENDT, Emerson; CAMPELO, Francisco Enaldo Sales. O conceito de redes sociais nos crimes cibernéticos. **Consultor Jurídico**, 27/09/2022. Disponível em: https://www.conjur.com.br/2022-set-27/academia-policia-terminologia-conceito-redes-sociais-crimes-ciberneticos. Acesso em: 11 jan. 2023.

COVARRUBIAS, Jersain Llamas. El estatus de México y el Convenio sobre la Ciberdelincuencia de Budapest. Foro Juridico, 14 set. 2020. Disponível em: https://forojuridico.mx/el-estatus-de-mexico-y-el-convenio-sobre-la-ciberdelincuencia-de-budapest/. Acesso em: 2 out. 2020.

CRIMES CIBERNÉTICOS contra mulheres aumentam durante pandemia. **Metro Jornal**, 12/04/2021. Disponível em: https://www.band.uol.com.br/noticias/bora-sp/ultimas/crimes-ciberneticos-contra-mulheres-aumentam-durante-pandemia-16344446. Acesso em: 14 jul. 2022.

CRUZ, Bruna Souza. PL das fake news: aprovado no Senado, entenda o que pode mudar. **Uol Tilt São Paulo**, 1º jul. 2020, às 21h41. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/06/30/com-44-votos-senado-aprova-pl-das-fake-news.htm. Acesso em: 27 jul. 2022.

CRUZ, Francisco Carvalho de Brito. **Direito, democracia e cultura digital:** a experiência de elaboração legislativa do Marco Civil da Internet. 2015. Tese de Doutorado. Universidade de São Paulo.

CULTURA DIGITAL. **Debate Público**: Proteção de Dados Pessoais. 2010. Disponível em: http://culturadigital.br/dadospessoais/. Acesso em: 28 nov. 2022.

DIAS, Natália; ROSALEN, Marilena. Minecraft: aprendendo mais com blocos. **Cadernos de Educação**, v. 13, n. 27, p. 158-170, 2014.

DIOGO, Darcianne. Com 17.843 ocorrências, crimes cometidos pela internet sobem 87,1% em 2020. **Correio Braziliense**, 13/02/2021. Disponível em: https://www.correiobraziliense.com.br/cidades-df/2021/02/4906387-com-17-843-ocorrencias-crimes-cometidos-pela-internet-sobem-871--em-2020.html. Acesso em: 18 nov. 2022.

DUTRA, Daniele. Homem faz Pix para ex com ameaças em Goiás: "Vou te matar". **Metrópoles**, 19/06/2022. Disponível em: https://www.metropoles.com/brasil/policia-de-go-prende-homem-acusado-de-fazer-pix-para-ex-com-ameacas. Acesso em: 09 jan. 2023.

EMPRESÁRIO é condenado por publicar fotos de Rose Leonel. **Maringa.com**, 18/08/2011. Disponível em: https://noticias.maringa.com/9647/empresario-e-condenado-por-publicar-fotos-de-rose-leonel. Acesso em: 18 nov. 2022.

EPSTEIN, Isaac. **Cibernética**. São Paulo: Ática, 2000.

EWALLY. P2P: O Que É, Como Funciona E Principais Aplicações. 2021. Disponível em: https://www.ewally.com.br/blog/falando-de-negocios/inovacao/p2p/. Acesso em: 4 set. 2022.

ENCONTRO: Rose Leonel fala sobre a luta contra a difamação na internet. **RPC TV**, 25/09/2014. Disponível em: http://redeglobo.globo.com/rpctv/noticia/2014/09/encontro-rose-leonel-fala-sobre-luta-contra-difamacao-na-internet.html. Acesso em: 18 nov. 2022.

EXPRESSO DAS ILHAS. **Representantes da Justiça da CPLP terminam jornadas com recomendações alinhadas de combate ao cibercrime**. 21/11/2019. Disponível em: https://expressodasilhas.cv/pais/2019/11/21/representantes-da-justica-da-cplp-terminam-jornadas-com-recomendacoes-alinhadas-de-combate-ao-cibercrime/66721. Acesso em: 18 nov. 2022.

FAKE news e ataques ao STF: oito ministros votam pela legalidade da abertura do inquérito. **Notícias STF**, 17 jun. 2020, 20h25. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=445764&ori=1. Acesso em: 05 ago. 2022.

FARÍAS, Raúl Zamorano. DERECHO Y DEMOCRACIA EN LA PERIFERIA DE LA SOCIEDAD MODERNA. ESTRUCTURAS, SEMÁNTICAS Y EXPECTATIVAS. **Revista de Direito Brasileira**, v. 32, n. 12, p. 17-34, 2023.

FERNANDES, Maíra; MEGGIOLARO, Daniella; PRATES, Fernanda. Lei de Proteção de Dados para segurança pública e persecução penal. **Consultor Jurídico**, 28/10/2022. Disponível em: https://www.conjur.com.br/2022-out-28/escritos-mulher-lei-protecao-dados-seguranca-publica-persecucao-penal. Acesso em: 15 jan. 2023.

FINCO, Matteo; MARTINI, Sandra Regina. Direitos do futuro e futuro dos direitos: existem normas indispensáveis? *In*: FEBRAJO, Alberto; LIMA, Fernando Rister de Sousa; BÔAS FILHO, Orlando Villas; BARROS, Marco Antonio Loschiavo Leme de (orgs.)

Sociologia Jurídica: Novas observações sobre problemas fundamentais. Curitiba: Juruá, p. 43-53, 2022.

FLÁVIO, Lúcio. **Policiais do DF no combate à violência virtual contra crianças**. Agência Brasília. Disponível em: https://www.agenciabrasilia.df.gov.br/2019/10/09/policiais-do-df-no-combate-a-violencia-virtual-contra-criancas/. Acesso em: 18 nov. 2022.

FOLETTO, Leonardo. Proteção de dados pessoais ganha plataforma de debate público na rede. **Cultura Digital**, 2010. Disponível em: http://culturadigital.br/blog/2010/12/10/protecao-de-dados-pessoais-ganha-plataforma-de-debate-publico-na-rede/. Acesso em: 23 jan. 2023.

FREITAS, Mariana Müller de; GONÇALVES, Camila dos Santos. Violência e Representações Sociais: Discursos Jornalísticos sobre Tiroteio em Escola. **PSI UNISC**, v. 4, n. 2, p. 99-113, 2020.

FURNALETO NETO, Mário; SANTOS, José Eduardo Lourenço dos. APONTAMENTOS SOBRE A CADEIA DE CUSTÓDIA DA PROVA DIGITAL NO BRASIL. **Revista Em Tempo**, [S.l.], v. 20, n. 1, nov. 2020. ISSN 1984-7858. Disponível em: https://revista.univem.edu.br/emtempo/article/view/3130. Acesso em: 02 set. 2022. doi: https://doi.org/10.26729/et.v20i1.3130.

GARCÍA LUNA, Julio César; PEÑA LABRIN, Daniel Ernesto. **Cibercriminalidad & postmodernidad**: la cibercriminología como respuesta al escenario contemporáneo. 2017. Disponível em: http://www.pensamientopenal.com.ar/doctrina/44898-cibercriminalidad-y-posmodernidad-cibercriminologia-respuesta-al-escenario. Acesso em: 18 nov. 2022.

GOIÁS. TJ-GO – **Recurso em Sentido Estrito nº 818265520188090175.** RECURSO EM SENTIDO ESTRITO. CRIME DE ESTELIONATO. COMPETÊNCIA. 1. O núcleo do crime material previsto no artigo 171, *caput*, do Código Penal, é obter vantagem ilícita, razão pela qual a consumação se efetiva com a entrada do dinheiro na conta do suposto estelionatário e não no momento da fraude [...]. Relator: Des. J. Paganucci Jr., Data de Julgamento: 04/04/2019, 1ª Câmara Criminal, Data de Publicação: DJ 2730 de 22/04/2019. Disponível em: https://tj-go.jusbrasil.com.br/jurisprudencia/712851653/recurso-em-sentido-estrito-rse-818265520188090175. Acesso em: 3 jun. 2022.

GOUSSINSKY, Eugenio. Crimes digitais têm forte alta em vários estados; saiba como prevenir. **R7 Tecnologia e Ciência**, 05/05/2021. Disponível em: https://noticias.r7.com/tecnologia-e-ciencia/crimes-digitais-tem-forte-alta-em-varios-estados-saiba-como-prevenir-05052021. Acesso em: 18 nov. 2022.

GRIGORI, Pedro. 20 projetos de leis no Congresso pretendem criminalizar fake news. **Pública**: Agência de jornalismo investigativo. Disponível em: https://apublica.org/2018/05/20-projetos-de-lei-no-congresso-pretendem-criminalizar-fake-news/. Acesso em: 18 nov. 2022.

GUADIX, Manuel Gámez *et al*. Autolesiones online entre adolescentes españoles: análisis de la prevalencia y de las motivaciones. **Revista de Psicología Clínica con Niños y Adolescentes**, v. 7, n. 1, p. 9-15, 2020.

GUIBENTIF, Pierre. Os direitos subjetivos na teoria dos sistemas de Niklas Luhmann. *In*: SCHWARTZ, Germano. Organizador. **Juridicização das Esferas Sociais e Fragmentação do Direito na Sociedade Contemporânea**. Porto Alegre: Livraria do Advogado, p. 171-198, 2012.

GUILLEN, Fábio. Condenado por postar fotos íntimas da ex-namorada na web. **Gazeta do Povo**, 17/08/2011. Disponível em: https://www.gazetadopovo.com.br/vida-e-cidadania/condenado-por-postar-fotos-intimas-da-ex-namorada-na-web-bjzp6gdfa3cf1fqylbf7mkzm6. Acesso em: 18 nov. 2022.

GUILHERI, Juliana; ANDRONIKOF, Anne; YAZIGI, Latife. Brincadeira do desmaio": uma nova moda mortal entre crianças e adolescentes. Características psicofisiológicas, comportamentais e epidemiologia dos 'jogos de asfixia. **Ciência & Saúde Coletiva**, v. 22, p. 867-878, 2017.

GUIMARÃES, Arthur. PL das criptomoedas divide especialistas acerca de impacto sobre setor. **Jota**, 13/01/2022. Disponível em: https://www.jota.info/legislativo/pl-criptomoedas-divide-especialistas-13012022. Acesso em: 10 jan. 2023.

HERRERA FLORES, Joaquín. **A (re)invenção dos direitos humanos**. Florianópolis: Fundação Boiteux, 2009.

HOMMERDING, Adalberto Narciso. **A quinta fase da Sociologia do Direito**: o cruzamento da Teoria Comunicativa de Jürgen Habermas com a Teoria Sistêmica de Niklas Luhmann. São Paulo: Tirant lo Blanch, 2020.

IMENES, Martha. País tem aumento de crimes virtuais durante a pandemia. **O Dia**, 06/09/2020. Disponível em: https://odia.ig.com.br/economia/2020/09/5982325-alerta-de-crimes-ciberneticos.html. Acesso em: 18 nov. 2022.

JÚNIOR, Janary. Projeto aprova adesão do Brasil à convenção europeia sobre crime cibernético. **Agência Câmara de Notícias**, 26/07/2021. Disponível em: https://www.camara.leg.br/noticias/779447-projeto-aprova-adesao-do-brasil-a-convencao-europeia-sobre-crime-cibernetico/. Acesso em: 27 jul. 2022.

KINUE, Lara. CPMI das Fake News ouve especialistas em crimes cibernéticos e segurança digital. **Rádio Senado**, 19/11/2019. Disponível em: https://www12.senado.leg.br/radio/1/noticia/2019/11/19/cpmi-das-fake-news-ouve-especialistas-em-crimes-ciberneticos-e-seguranca-digital. Acesso em: 19 jan. 2023.

KISHIMOTO, André. Inteligência artificial em jogos eletrônicos. *In*: **Academic research about Artificial Intelligence for games**, 2004. Disponível em: http://www.karenreis.com.br/pdf/andre_kishimoto.pdf. Acesso em: 19 jan. 2023.

LE COADIC, Yves-François. **A ciência da informação**. Brasília/DF: Briquet de lemos Livros, 1996.

LINS, Bernardo Felipe Estellita. A evolução da Internet: uma perspectiva histórica. **Cadernos Aslegis**, v. 48, p. 11-45, 2013.

LOSANO, Mario Giuseppe. Os sistemas cibernéticos do direito. *In:* **Sistema e estrutura no Direito**: volume 3, do século XX a pós-modernidade. São Paulo: WMF Martins Fontes, 2019, p. 1-141.

LUHMANN, Niklas. **Legitimação pelo procedimento**. Brasília: Universidade de Brasília, 1980.

LUHMANN, Niklas. **Sociologia do direito I**. Rio de Janeiro: Tempo Brasileiro, 1983.

LUHMANN, Niklas. **Sociologia do direito II**. Rio de Janeiro: Tempo Brasileiro, 1985.

LUHMANN, Niklas. **Sistemas sociales**: lineamentos para una teoría general. Barcelona/México DF/Santa Fé de Bogotá: Anthropos/Universidade Iberoamericana/Pontifica Universidad Javeriana, 1998.

LUHMANN, Niklas. **A realidade dos meios de comunicação**. São Paulo: Paulus, 2005.

LUHMANN, Niklas. **A improbabilidade da comunicação**. Lisboa: Vega, 2006.

LUHMANN, Niklas. **La sociedad de la sociedad**. México/Barcelona: Universidad Iberoamericana/Herder, 2007. 1357 p.

LUHMANN, Niklas. **O direito da sociedade**. São Paulo: Martins Fontes, 2016.

MANSILLA, Darío Rodriguez. II. La sociologia y la teoria de la sociedad. *In:* LUHMANN, Niklas. **La sociedad de la sociedad**. México/Barcelona: Universidad Iberoamericana/Herder, 2007.

MANSUR, Rafaela. Ameaças cibernéticas crescem 394% durante a pandemia. **O Tempo**, 13/01/2021. Disponível em: https://www.otempo.com.br/economia/ameacas-ciberneticas-crescem-394-durante-a-pandemia-1.2434524. Acesso em: 18 nov. 2022.

MARANHÃO, Juliano; CAMPOS, Ricardo. Fake news e autorregulação regulada das redes sociais no Brasil: fundamentos constitucionais. **Fake news e Regulação.** Coordenadores: Georges Abboud; Nelson Nery Jr. e Ricardo Campos. São Paulo: Thomson Reuters Brasil, 2018.

MARTINS, Marcelo Guerra; TATEOKI, Victor Augusto. Proteção de dados pessoais e democracia: fake news, manipulação do eleitor e o caso da Cambridge Analytica. **Revista Eletrônica Direito e Sociedade-REDES**, v. 7, n. 3, p. 135-148, 2019.

MATURANA, Humberto; VARELA, Francisco. **A árvore do conhecimento**. Campinas: Psy, 1995.

MELLO JR., John P. How cybercriminals turn ‘harmless’ stolen or leaked data into dollars. **CSO United States**, 1/06/2021. Disponível em: https://www.csoonline.com/article/3619510/how-cybercriminals-turn-harmless-stolen-or-leaked-data-into-dollars.html. Acesso em: 03 jun. 2022.

MINISTÉRIO DA JUSTIÇA. Proteção de Dados Pessoais. **Pensando o Direito**. 2015a. Disponível em: http://pensando.mj.gov.br/dadospessoais/. Acesso em: 28 nov. 2022.

MINISTÉRIO DA JUSTIÇA. Proteção de Dados Pessoais Pelo Mundo. **Pensando o Direito**. 2015b. Disponível em: http://pensando.mj.gov.br/dadospessoais/2015/04/protecao-de-dados-pessoais-pelo-mundo/. Acesso em: 28 nov. 2022.

MINISTÉRIO DAS RELAÇÕES EXTERIORES. **Nota 309**: Processo de adesão à Convenção de Budapeste – Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública. 11 dez 2019. Disponível em: http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/21146-processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica. Acesso em: 15 dez 2022.

MOREIRA, Eduardo. Microsoft facilita as denúncias ao ‘revenge porn’. **TargetHD**, Florianópolis, Blog, 23 jul. 2015. Disponível em: http://www.targethd.net/microsoft-facilita-as-denuncias-ao-revenge-porn/. Acesso: 08 fev. 2023.

MOREIRA, Rômulo de Andrade. A Lei nº 12.850/13 e a quebra de dados cadastrais e dos registros das ligações telefônicas. **Direito UNIFACS – Debate Virtual**, n. 173, 2014.

MURILO, José. Ministério da Justiça quer ouvir a sociedade sobre Marco Civil da Internet e Proteção de Dados Pessoais. **Cultura Digital**, 2015. Disponível em: http://culturadigital.br/blog/2015/01/27/ministerio-da-justica-quer-ouvir-a-sociedade-sobre-marco-civil-da-internet-e-protecao-de-dados-pessoais/. Acesso em: 23 jan. 2023.

NAVAS, Ana Paula Pavanini; CAMBI, Eduardo. Acesso aos dados cadastrais da Justiça Eleitoral pela autoridade policial sem autorização judicial. **Ius gentium**, v. 9, n. 1, p. 6-24, 2018.

NEVES, Kelli Angelini. **Nomes de domínio na internet**: Aplicação do sistema de solução de conflitos. São Paulo: Novatec Editora, 2015.

NOBRE, Noéli. Sancionadas quatro novas leis de proteção à mulher. **Câmara dos Deputados**. 19 dez. 2018. Disponível em: https://www.camara.leg.br/noticias/550089-sancionadas-quatro-novas-leis-de-protecao-a-mulher/. Acesso em: 07 fev. 2023.

OPERAÇÃO 404 chega a 4ª edição com buscas no metaverso, suspensão de 4 canais e 90 vídeos retirados do ar. Ministério da Justiça e Segurança Pública, 21/06/2022. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/operacao-404-chega-a-4a-edicao-com-buscas-no-metaverso-suspensao-de-4-canais-e-90-videos-retirados-do-ar. Acesso em: 09 jan. 2023.

PARETO, Vilfredo. **Trattato di sociologia generale**.Primary source edition, v. I.USA: Nabu Press, 2014.

PARETO, Vilfredo. **A Transformação da Democracia**. São Paulo: Leya, 2019.

PARSONS, Talcott. **O sistema das sociedades modernas**. Fortaleza: Pioneira, 1974.

PEDUZZI, Pedro. Foco da Operação 404 são sites piratas, e não consumidores. **Agência Brasil**, 01/11/2019. Disponível em: https://agenciabrasil.ebc.com.br/justica/noticia/2019-11/foco-da-operacao-404-sao-sites-piratas-e-nao-consumidores. Acesso em: 09 jan. 2023.

PF ALERTA para aumento nos crimes cibernéticos durante a pandemia. **CBN Curitiba**, 08/04/2020. Disponível em: https://cbncuritiba.com/pf-alerta-para-aumento-nos-crimes-ciberneticos-durante-a-pandemia/. Acesso em: 18 nov. 2022.

PIRATARIA de livros é alvo de operação em quatro estados. **Agência Brasil**, 30/11/2022. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2022-11/pirataria-de-livros-e-alvo-de-operacao-em-quatro-estados. Acesso em: 09 jan. 2023.

PIRES, Sara A.; SANI, Ana Isabel; SOEIRO, Cristina. Stalking e ciberstalking em estudantes universitários: Uma revisão sistemática. **Revista Portuguesa de Investigação Comportamental E Social**, 4(2), 60-75, 2018.

REMUS, Vivian do Nascimento; WENDT, Emerson. A prova testemunhal na investigação dos crimes de homicídio relacionado ao tráfico de drogas. *In:* WENDT, Emerson; LEITÃO JUNIOR, Joaquim; WENDT, Valquiria P. C. (org.). **Direito Policial:** na raiz dos problemas. Rio de Janeiro: Brasport, p. 126-141, 2022.

REPRESSÃO a crimes cibernéticos é tema de seminário do Ministério da Justiça e Segurança Pública. **Ministério da Justiça e Segurança Pública**. 29/10/2021a. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/repressao-a-crimes-ciberneticos-e-tema-de-seminario-do-ministerio-da-justica-e-seguranca-publica. Acesso em: 15 fev. 2023.

REPRESSÃO a crimes cibernéticos é tema de seminário do Ministério da Justiça e Segurança Pública. **Relator Policial**: Portal de segurança pública e privada. 09/11/2021b. Disponível em: https://relatorpolicial.com.br/noticia/441/repressao-a-crimes-ciberneticos-e-tema-de-seminario-do-ministerio-da-justica-e-seguranca-publica. Acesso em: 15 fev. 2023.

RESCHKE, Cristiano de Castro; WENDT, Emerson; MATSUBAYACI, Mayumi Bezerra. **Infiltração Policial**: da tradicional à virtual. Rio de Janeiro: Brasport, 2021.

REVENGE Porn; PORNOGRAFIA de vingança. **Google Trends**. Disponível em: https://trends.google.com.br/trends/explore?date=all&geo=BR&q=pornografia%20de%20vingan%C3%A7a,revenge%20porn. Acesso em: 09 jan. 2023.

RIBEIRO, Diógenes V. Hassan; RIBEIRO, Douglas Cunha. Inclusão e exclusão: acesso aos direitos sociais nos países periféricos. **Revista de Informação Legislativa**, v. 53, n. 210, p. 117-134, 2016.

RIENTE, Letícia. Operação 404 atinge mais de 26 milhões de usuários de IPTV no Brasil. **Olhar Digital**, 19/11/2020. Disponível em: https://olhardigital.com.br/2020/11/19/noticias/operacao-404-atingiu-mais-de-26-milhoes-de-usuarios-de-iptv-no-brasil/. Acesso em: 03 jun. 2020.

RIO GRANDE DO SUL. TJ-RS – **CONFLITO DE JURISDIÇÃO Nº 70078211596**. CONFLITO DE COMPETÊNCIA NEGATIVO. CRIME CONTRA O PATRIMÔNIO. ESTELIONATO. COMPETÊNCIA. A competência para processar e julgar o crime de

estelionato, quando há transferência de valores, é do juízo do local [...]. Relatora Lizete Andreis Sebben, Data de Julgamento 29/08/2018. Quinta Câmara Criminal, Data da Publicação, Diário Oficial De Justiça do dia 11/09/2018. Disponível em: https://tj-rs.jusbrasil.com.br/jurisprudencia/625213720/conflito-de-jurisdicao-cj-70078211596-rs/inteiro-teor-625213739. Acesso em: 3 jun. 2023.

ROCHA, Leonel Severo; KING, Michael; SCHWARTZ, Germano. **A verdade sobre a autopoiese no Direito**. Porto Alegre: Livraria do Advogado, 2009.

ROCHA, Leonel Severo; SCHWARTZ, Germano; CLAM, Jean. **Introdução à teoria do sistema autopoiético do Direito**. 2.ed. Porto Alegre: Livraria do Advogado, 2013.

RODAS, Sérgio. Autoridades podem solicitar dados diretamente aos provedores no exterior. **Consultor Jurídico**, 23/02/2023. Disponível em: https://www.conjur.com.br/2023-fev-23/autoridades-podem-pedir-dados-provedores-exterior-stf. Acesso em: 23 fev. 2023.

RODRIGUES, Léo Peixoto; NEVES, Fabrício Monteiro. **A sociologia de Niklas Luhmann**. Petrópolis: Vozes, 2017.

RODRIGUES, Léo Peixoto. Autopoiésis: aula proferida na disciplina Sociedade, Sistemas e Direito do Doutorado em Direito. **PPGD da Universidade La Salle – Canoas/RS**, em 27 mai. 2020. Canoas: Universidade La Salle, 2020.

ROLFINI, Fabiana. Cibercrime: ataques no Brasil aumentam mais de 300% com a pandemia. **Olhar Digital**, 03/07/2020. Disponível em: https://olhardigital.com.br/2020/07/03/seguranca/cibercrime-ataques-no-brasil-aumentam-mais-de-300-com-a-pandemia/. Acesso em: 18 nov. 2022.

SAADI, Ricardo Andrade. CARTILHA COOPERAÇÃO JURÍDICA INTERNACIONAL EM MATÉRIA PENAL. **Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional, Secretaria Nacional de Justiça, Ministério da Justiça**. 2014. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-protecao/lavagem-de-dinheiro/institucional-2/publicacoes/manuais/cooperacao-juridica-internacional-em-materia-penal/cartilha-penal-09-10-14-1.pdf. Acesso em: 4 set. 2022.

SALES, Renata Celeste; ELIHIMAS, Beatriz Izabelli Zumba; ELIHIMAS, Monique Dayane Zumba. Revenge porn, dispositivo de poder e violência de gênero: uma abordagem crítica à ordem penal vigente. **Revista da Faculdade de Direito da Universidade São Judas Tadeu**, v. 6, p. 103-116, 2018.

SANDRE, Leonardo. Homem é preso após enviar diversos PIX ameaçando ex-namorada. **Gazeta de São Paulo**, 20/06/2022. Disponível em: https://www.gazetasp.com.br/brasil/homem-e-preso-apos-enviar-diversos-pix-ameacando-ex-namorada/1111317/. Acesso em: 09 jan. 2023.

SANTARÉM, Paulo Renã da Silva. **O direito achado na rede**: a emergência do acesso à Internet como direito fundamental no Brasil. Dissertação de Mestrado: UNB, 2010.

SANTINO, Renato. A pandemia de cibercrime: por que os ataques de ransomware estão disparando? **Olhar Digital**, 21/08/2020. Disponível em: https://olhardigital.com.br/2020/08/21/seguranca/a-pandemia-de-cibercrime-por-que-os-ataques-de-ransomware-estao-disparando/. Acesso em: 18 nov. 2022.

SCHREIBER, Anderson. PEC 17/19: Uma Análise Crítica. **Carta Forense**. Colunas. 2019. Disponível em: http://www.cartaforense.com.br/conteudo/colunas/pec-1719-uma-analise-critica/18345. Acesso em: 28 nov. 2022.

SCHREIBER, Fernando Cesar de Castro; ANTUNES, Maria Cristina. Cyberbullying: do virtual ao psicológico. **Boletim-Academia Paulista de Psicologia**, v. 35, n. 88, p. 109-125, 2015. Disponível em: http://pepsic.bvsalud.org/pdf/bapp/v35n88/v35n88a08.pdf. Acesso em: 17 fev. 2022.

SCHWARTZ, Germano; PRIBÁN, Jirí; ROCHA, Leonel Severo. **Sociologia sistêmico-autopoiética das constituições**. Porto Alegre: Livraria do Advogado, 2015.

SCHWARTZ, Germano. **As Constituições estão mortas?** Movimentos constituintes e comunicações constitucionalizantes dos Novos Movimentos Sociais do Século XXI. 2.ed. Rio de Janeiro: Lumen Juris, 2020.

SCHWARTZ, Germano André Doederlein; RIBEIRO, Diógenes V. Hassan; RIBEIRO, Douglas Cunha. Direita (o) volver? Os sistemas do direito, da política e da educação no Brasil contemporâneo. **Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito (RECHTD)**, v. 12, n. 3, p. 461-480, 2020.

SENADO FEDERAL. **Projeto de Lei do Senado nº 152, de 1991**. Define os crimes de uso indevido de computador e dá outras providências. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/1463. Acesso em: 5 jan. 2023.

SENADO FEDERAL. **Projeto de Lei da Câmara nº 4, de 1996**. Regulamenta o inciso XII, parte final, do artigo quinto da Constituição Federal (Interceptação de comunicação telefônica, para prova em investigação criminal e em instrução processual penal). Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/19073. Acesso em: 9 fev. 2023.

SENADO FEDERAL. **Projeto de Lei da Câmara nº 37, de 1997**. Estabelece normas para as eleições. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/20122. Acesso em: 9 fev. 2023.

SENADO FEDERAL. **Projeto de Lei da Câmara nº 23, de 2000**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências (mediante a tipificação de condutas que constituem crimes contra a Previdência Social). Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/44229. Acesso em: 9 fev. 2023.

SENADO FEDERAL. **Projeto de Lei do Senado nº 11, de 2003**. Altera e acresce parágrafos ao artigo 184 e dá nova redação ao artigo 186 do Decreto-Lei nº 2848, de 7 de dezembro de 1940 – Código Penal, alterado pela Lei nº 8635, de 16 de março de 1993, e

acrescenta dispositivos ao Decreto-Lei nº 3689, de 3 de outubro de 1941 – Código de Processo Penal. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/56028. Acesso em: 9 fev. 2023.

SENADO FEDERAL. **Projeto de Lei da Câmara nº 89, de 2003**. Altera o Decreto-Lei nº 2848, de 07 de dezembro de 1940 – Código Penal, e a Lei nº 9296, de 24 de julho de 1996, e dá outras providências. (Dispõe sobre os crimes cometidos na área de informática, e suas penalidades, dispondo que o acesso de terceiros, não autorizados pelos respectivos interessados, a informações privadas mantidas em redes de computadores, dependerá de prévia autorização judicial). Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/63967. Acesso em: 10 fev. 2023.

SENADO FEDERAL. **Projeto de Lei do Senado nº 209, de 2003**. Dá nova redação a dispositivos da Lei nº 9613, de 3 de março de 1998, objetivando tornar mais eficiente a perseguição penal dos crimes de lavagem de dinheiro. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/58211. Acesso em: 10 fev. 2023.

SENADO FEDERAL. **Projeto de Lei do Senado nº 213, de 2003**. Institui o Estatuto da Igualdade Racial. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/58268. Acesso em: 10 fev. 2023.

SENADO FEDERAL. **Projeto de Lei do Senado nº 150, de 2006**. Dispõe sobre a repressão ao crime organizado e dá outras providências. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/77859. Acesso em: 10 fev. 2023.

SENADO FEDERAL. **Projeto de Lei do Senado nº 250, de 2008**. Altera o Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/86025. Acesso em: 10 fev. 2023.

SENADO FEDERAL. **Projeto de Lei da Câmara nº 141, de 2009**. Altera as Leis nºs 9.096, de 19 de setembro de 1995 – Lei dos Partidos Políticos, 9.504, de 30 de setembro de 1997, que estabelece normas para as eleições, e 4.737, de 15 de julho de 1965 – Código Eleitoral. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/92221. Acesso em: 9 fev. 2023.

SENADO FEDERAL. **Projeto de Lei do Senado nº 100, de 2010**. Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes da polícia na Internet com o fim de investigar crimes contra a liberdade sexual de criança ou adolescente. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/96360. Acesso em: 10 fev. 2023.

SENADO FEDERAL. **Projeto de Lei do Senado nº 228, de 2010**. Altera a Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da educação nacional), para incluir

entre as incumbências dos estabelecimentos de ensino a promoção de ambiente escolar seguro e a adoção de estratégias de prevenção e combate ao bullying. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/97988. Acesso em: 18 nov. 2022.

SENADO FEDERAL. **Projeto de Lei do Senado nº 196, de 2011**. Acrescenta inciso ao Art.12 da Lei nº 9.394, de 20 de dezembro de 1996, para dispor sobre o combate ao *bullying* nas escolas. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/100018. Acesso em: 18 nov. 2022.

SENADO FEDERAL. **Projeto de Lei da Câmara nº 35, de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/105612. Acesso em: 09 fev. 2023.

SENADO FEDERAL. **Projeto de Lei do Senado nº 441, de 2012**. Altera a redação dos Art. 8º, 11, 16, 17-A, 26, 28, 36, 37, 38, 45, 47, 52, 57-A e 77, da Lei nº 9.504, de 30 de setembro de 1997, que estabelece normas para eleições para reduzir o tempo e diminuir o custo das campanhas eleitorais e dá outras providências. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/109427. Acesso em: 09 fev. 2023.

SENADO FEDERAL. **Projeto de Lei do Senado nº 479, de 2012**. Dispõe sobre prevenção e punição ao tráfico interno e internacional de pessoas, bem como sobre medidas de proteção às vítimas. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/110044. Acesso em: 10 fev. 2023.

SENADO FEDERAL. **Projeto de Lei da Câmara nº 68, de 2013**. Institui o Programa de Combate à Intimidação Sistemática (*Bullying*). Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/114433. Acesso em: 18 nov. 2022.

SENADO FEDERAL. **Projeto de Lei da Câmara nº 21, de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/116682. Acesso em: 10 fev. 2023.

SENADO FEDERAL. **Projeto de Lei da Câmara nº 43, de 2014**. Altera a Lei nº 4.737, de 15 de julho de 1965 – Código Eleitoral, para tipificar o crime de denunciação caluniosa com finalidade eleitoral. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/117592. Acesso em: 09 fev. 2023.

SENADO FEDERAL. **Projeto de Lei da Câmara nº 75, de 2015**. Altera as Leis nºs 9.504, de 30 de setembro de 1997, 9.096, de 19 de setembro de 1995, e 4.737, de 15 de julho de 1965 – Código Eleitoral, alterando as instituições político-eleitorais. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/122392. Acesso em: 09 fev. 2023.

SENADO FEDERAL. **Projeto de Lei do Senado nº 618, de 2015**. Acrescenta o Art. 225-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, para prever causa de aumento de pena para o crime de estupro cometido por duas ou mais pessoas. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/123183. Acesso em: 09 fev. 2023.

SENADO FEDERAL. **Projeto de Lei do Senado nº 664, de 2015**. Inclui o Art. 244-C na Lei nº 8.069, de 13 de julho de 1990 – Estatuto da Criança e do Adolescente, para tipificar o crime de induzimento, instigação ou auxílio à automutilação de criança ou adolescente. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/123447. Acesso em: 10 fev. 2023.

SENADO FEDERAL. **Projeto de Lei da Câmara nº 18, de 2017** – Projeto de Lei Rose Leonel. Inclui a comunicação no rol de direitos assegurados à mulher pela Lei Maria da Penha, bem como reconhece que a violação da sua intimidade consiste em uma das formas de violência doméstica e familiar; tipifica a exposição pública da intimidade sexual; e altera a Lei nº 11.340 de 7 de agosto de 2006 (Lei Maria da Penha), e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal). Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/128223. Acesso em: 09 fev. 2023.

SENADO FEDERAL. **Projeto de Lei do Senado nº 85, de 2017**. Define os crimes de abuso de autoridade e dá outras providências. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/128545. Acesso em: 09 fev. 2023.

SENADO FEDERAL. **Projeto de Lei da Câmara nº 110, de 2017**. Altera as Leis nºs 9.504, de 30 de setembro de 1997 (Lei das Eleições), 9.096, de 19 de setembro de 1995, e 4.737, de 15 de julho de 1965 (Código Eleitoral), e revoga dispositivos da Lei nº 13.165, de 29 de setembro de 2015 (Minirreforma Eleitoral de 2015), com o fim de promover reforma no ordenamento político-eleitoral. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/131127. Acesso em: 09 fev. 2023.

SENADO FEDERAL. **Projeto de Lei da Câmara nº 171, de 2017**. Altera o Art. 12 da Lei nº 9.394, de 20 de dezembro de 1996, para incluir a promoção de medidas de conscientização, de prevenção e de combate a todos os tipos de violência e a promoção da cultura de paz entre as incumbências dos estabelecimentos de ensino. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/131995. Acesso em: 18 nov. 2022.

SENADO FEDERAL. **Projeto de Lei do Senado nº 246, de 2018**. Acrescenta dispositivos à Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, para dispor sobre medidas de combate à divulgação de conteúdos falsos (*fake news*) ou ofensivos em aplicações de internet. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/133353. Acesso em: 18 nov. 2022.

SENADO FEDERAL. **Projeto de Lei do Senado nº 471, de 2018**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, a Lei nº 4.737, de 15 de julho de 1965, e a Lei nº 12.965,

de 23 de abril de 2014, para dispor sobre a definição das infrações penal, eleitoral e civil de criar ou divulgar notícia falsa, e cominar as respectivas penas. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/134781. Acesso em: 18 nov. 2022.

SENADO FEDERAL. **Projeto de Lei do Senado nº 533, de 2018**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), a Lei nº 4.737, de 15 de julho de 1965 (Código Eleitoral), e a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), para dispor sobre a definição das infrações penal, eleitoral e civil de criar ou divulgar notícia falsa, e cominar as respectivas penas. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/134952. Acesso em: 15 dez. 2022.

SENADO FEDERAL. **Projeto de Lei nº 1.369, de 2019 (Substitutivo da Câmara dos Deputados)**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para incluir o Art. 147-A, que dispõe sobre o crime de perseguição obsessiva. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/146091. Acesso em: 18 nov. 2022.

SENADO FEDERAL. **Projeto de Lei nº 4.975, de 2019**. Altera da Lei nº 4.737, de 15 de julho de 1965 – Código Eleitoral, para redimensionar a pena do crime previsto no § 3º do Art. 326-A. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/138675. Acesso em: 24 nov. 2019.

SENADO FEDERAL. **Projeto de Lei nº 6.341, de 2019**. Aperfeiçoa a legislação penal e processual penal. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/140099. Acesso: em 09 fev. 2023.

SENADO FEDERAL. **Projeto de Lei nº 6.389, de 2019** (Substitutivo da Câmara dos Deputados ao Projeto de Lei do Senado nº 664, de 2015). Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para modificar o crime de incitação ao suicídio e incluir as condutas de induzir ou instigar a automutilação, bem como a de prestar auxílio a quem a pratique. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/140121. Acesso em: 10 fev. 2023.

SENADO FEDERAL. **Projeto de Lei nº 2.630, de 2020**. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/141944. Acesso em: 13 jan. 2023.

SENADO FEDERAL. **Projeto de Lei nº 4.554, de 2020**. Combate a prática de fraude eletrônica, modifica o Art. 155 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, e apresenta hipóteses agravantes. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/144667. Acesso em: 03 jun. 2022.

SENADO FEDERAL. **Projeto de Lei nº 4.554, de 2020 (Substitutivo da Câmara dos Deputados)**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet, e o Decreto-Lei nº 3.689, de 3 de outubro

de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/148159. Acesso em: 03 jun. 2022.

SENADO FEDERAL. **Projeto de Lei nº 2.108, de 2021**. Acrescenta o Título XII na Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), relativo aos crimes contra o Estado Democrático de Direito; e revoga a Lei nº 7.170, de 14 de dezembro de 1983 (Lei de Segurança Nacional), e dispositivo do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/148741. Acesso em: 09 jan. 2023.

SENADO FEDERAL. **Projeto de Lei nº 4.401, de 2021**. Dispõe sobre a prestadora de serviços de ativos virtuais; e altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e as Leis nºs 7.492, de 16 de junho de 1986, e 9.613, de 3 de março de 1998, para incluir a prestadora de serviços de ativos virtuais no rol de instituições sujeitas às suas disposições. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/151264. Acesso em: 10 jan. 2023.

SENADO FEDERAL. **Projeto de Lei nº 4.566, de 2021**. Altera a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar a conduta de injúria racial em local público ou privado aberto ao público de uso coletivo. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/151397. Acesso em: 12 jan. 2023.

SENADO FEDERAL. **Projeto de Lei nº 879, de 2022**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, para qualificar o crime de invasão de dispositivo informático quando houver a obtenção de dados pessoais e criar o crime de sequestro de dados informáticos. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/152669. Acesso em: 22 jan. 2023.

SENADO FEDERAL. **Relatório Final da Comissão Parlamentar de Inquérito**. Criada por meio do Requerimento nº 2, de 2005-CN, "com o objetivo de investigar e apurar a utilização da Internet para a prática de crimes de 'pedofilia', bem como a relação desses crimes com o crime organizado". Disponível em: http://www.senado.gov.br/noticias/agencia/pdfs/RELATORIOFinalCPIPEDOFILIA.pdf. Acesso em: 18 nov. 2022.

SENADO FEDERAL. **Relatório legislativo**. Devolvido pela relatora, Senadora Kátia Abreu, com relatório favorável ao presente projeto, estando em condições de ser incluído em pauta. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=4324504&ts=1567524255968&disposition=inline. Acesso em: 18 nov. 2022.

SENADO FEDERAL. **Substitutivo da Câmara dos Deputados nº 209, de 2003, ao Projeto de Lei do Senado nº 209, de 2003.** Altera a Lei nº 9.613, de 3 de março de 1998, objetivando tornar mais eficiente a persecução penal dos crimes de lavagem de dinheiro. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/103258. Acesso em: 10 fev. 2023.

SENADO FEDERAL. **Substitutivo da Câmara dos Deputados nº 213, de 2003, ao Projeto de Lei do Senado nº 213, de 2003 – ESTATUTO DA IGUALDADE RACIAL**. Institui o Estatuto da Igualdade Racial; altera as Leis nºs 7.716, de 5 de janeiro de 1989; 9.029, de 13 de abril de 1995, 7.347, de 24 de julho de 1985, 10.778, de 24 de novembro de 2003, e 9.504, de 30 de setembro de 1997, e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal (estabelece critérios para o combate à discriminação racial de afro-brasileiros; igualdade de oportunidades; defesa dos direitos étnico-raciais individuais, coletivos e difusos). Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/94019. Acesso em: 10 fev. 2023.

SENADO FEDERAL. **Substitutivo da Câmara dos Deputados nº 150, de 2006, ao Projeto de Lei do Senado nº 150, de 2006**. Dispõe sobre as organizações criminosas, os meios de obtenção da prova, o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/109765. Acesso em: 10 fev. 2023.

SENADO FEDERAL. **Substitutivo da Câmara dos Deputados nº 441, de 2012, ao Projeto de Lei do Senado nº 441, de 2012**. Altera as Leis nºs 4.737, de 15 de julho de 1965, 9.096, de 19 de setembro de 1995, e 9.504, de 30 de setembro de 1997, para diminuir o custo das campanhas eleitorais. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/114961. Acesso em: 09 fev. 2023.

SENADO FEDERAL. **Substitutivo da Câmara dos Deputados nº 2, de 2018, ao Projeto de Lei do Senado nº 618, de 2015**. Tipifica os crimes de importunação sexual e de divulgação de cena de estupro; altera para pública incondicionada a natureza da ação penal dos crimes contra a dignidade sexual; estabelece causas de aumento de pena para esses crimes; cria formas qualificadas dos crimes de incitação ao crime e de apologia de crime ou criminoso; e revoga dispositivo do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/132479. Acesso em: 09 fev. 2023.

SENADO FEDERAL. Pacheco destaca esforço do Congresso para diminuir desigualdade de gênero. **Agência Senado**, 08/03/2021. 2021a. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/03/08/pacheco-destaca-esforco-do-congresso-para-diminuir-desigualdade-de-genero. Acesso em: 21 maio 2022.

SENADO FEDERAL. Representação e combate à violência: Senado aprova projetos da pauta feminina. **Agência Senado**, 09/03/2021. 2021a. Disponível em: https://www12.senado.leg.br/noticias/videos/2021/03/representacao-e-combate-a-violencia-senado-aprova-projetos-da-pauta-feminina. Acesso em: 21 maio 2022.

SETE anos depois, jornalista que foi exposta por ex como prostituta na web ainda tenta se recuperar. **R7**, 25/10/2013. Disponível em: http://noticias.r7.com/cidades/fotos/sete-anos-depois-jornalista-que-foi-exposta-por-ex-como-prostituta-na-web-ainda-tenta-se-recuperar-25102013#!/foto/1. Acesso em: 18 nov. 2022.

SILVA, Ana Beatriz Barbosa. **Mentes perigosas nas escolas**: bullying. Rio de Janeiro: Objetiva, 2010.

SILVA, Artur Stamford da. **10 lições sobre Luhmann**. Petrópolis: Vozes, 2016.

SILVA, Artur Stamford da. Niklas Luhmann: 20 anos do Sociedade da Sociedade. O lugar do ao mesmo tempo na teoria do direito. **Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito (RECHTD)**, v. 10. janeiro-abril, p. 27 a 40 2018.

SOARES, António Goucha. Brexit: O referendo de 2016. **Relações Internacionais (R: I)**, n. 61, p. 63-75, 2019.

SOARES, Marcos Antônio Striquer. Sistema Jurídico e Teoria Geral dos Sistemas — Aulas do professor Tercio Sampaio Ferraz Júnior nos dias 12, 14 e 16/03/73 — Apostila do "Curso de Extensão Universitária" da Associação dos Advogados de São Paulo. **Revista Jurídica da UniFil**, [S.l.], v. 1, n. 1, p. 207-2015, set. 2018. ISSN 2674-7251. Disponível em: http://periodicos.unifil.br/index.php/rev-juridica/article/view/550. Acesso em: 16 nov. 2023.

SORO, Emilio Sáez. **Acción comunicativa en el Ciberespacio**: el análisis de las páginas web personales. 2006. Disponível em: http://bocc.ubi.pt/pag/saez-soro-emilio-ciberespacio.pdf. Acesso em: 05 dez. 2022.

SOUZA, Luciana Coutinho Pagliarini de; CANIELLO, Angelica. O potencial significativo de games da educação: análise do Minecraft. **Comunicação & Educação**, v. 20, n. 2, p. 37-46, 2015.

STOCKINGER, Gottfried. A interação em ciberambientes e sistemas sociais. *In:* LEMOS, André; PALACIOS, Marcos. **As janelas do ciberespaço**, v. 2, p. 106-127, 2001.

STOCKINGER, Gottfried. **A sociedade da comunicação**: o contributo de Niklas Luhmann. Rio de Janeiro: Papel Virtual, 2003

SUPREMO TRIBUNAL FEDERAL. **ADI 5063**. Relator: MIN. GILMAR MENDES. Acompanhamento processual. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=4494216. Acesso em: 19 fev. 2023.

SUPREMO TRIBUNAL FEDERAL. Operadoras de celular questionam norma sobre fornecimento de dados de clientes. **STF Notícias**: 22 nov. 2013. Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=254181. Acesso em: 19 fev. 2023.

SVANTESSON, Dan Jerker B. **Internet & jurisdição**: relatório de status global 2019. Núcleo de Informação e Coordenação do Ponto BR. Trad. Ana Zuleika Pinheiro Machado. São Paulo: Comitê Gestor da Internet no Brasil, 2020.

SYDOW, Spencer Toth. **Crimes Informáticos e Suas Vítimas**. São Paulo: Saraiva, 2013.

SYDOW, Spencer Toth. Escravidão Digital e o Problema da Conduta Vitimal. **Revista Consulex**. Ano XX, n. 474, p. 18-25, 15 de outubro de 2016.

TONDO, Stephanie. A pandemia de golpes digitais no Brasil. **O Globo**, 07/05/2021. Disponível em: https://oglobo.globo.com/epoca/sociedade/a-pandemia-de-golpes-digitais-no-brasil-1-25007188. Acesso em: 22 fev. 2023.

TONET, Fernando. **Entre Cila e Caríbdis**: o árduo caminho do constitucionalismo sistêmico. São Leopoldo: Editora Unisinos, 2019.

TORRES, Jhonny Bezerra. **A Ciberguerra**: Uma nova forma de confronto entre os Estados. 2015. Tese de Doutorado. Universidade de São Paulo.

TV SENADO. CPMI Fake News – Oitivas – 19/11/2019. Disponível em: https://www.youtube.com/watch?v=CL6Itj2Wboc&t. Acesso em: 19 jan. 2023.

VALENTE, Jonas. Câmara lança ferramenta para checagem de notícias falsas. **Agência Brasil**, 25/09/2019. Disponível em: http://agenciabrasil.ebc.com.br/geral/noticia/2019-09/camara-lanca-ferramenta-para-checagem-de-noticias-falsas. Acesso em: 18 nov. 2022.

VASCONCELOS, Fernando Antônio de; BRANDÃO, Fernanda Holanda Vasconcelos. As redes sociais e a evolução da informação no século XXI. **Direito e Desenvolvimento**, v. 4, n. 7, p. 125-144, 2013.

VIANNA, Túlio Lima. A ideologia da propriedade intelectual: a inconstitucionalidade da tutela penal dos direitos patrimoniais de autor. **Anuario de Derecho Constitucional Latinoamericano**, v. 2, p. 933-948, 2006.

VITTA, Lucas de. Interpol alerta para crescimento de crimes virtuais durante a pandemia. **Valor Econômico**, 04/08/2020. Disponível em: https://valor.globo.com/mundo/noticia/2020/08/04/interpol-alerta-para-crescimento-de-crimes-virtuais-durante-a-pandemia.ghtml. Acesso em: 18 nov. 2022.

WEISHEIMER, Evandro; MORENO, Márcio de Abreu; SILVA, Márcio Niederauer Nunes da; ZUMAS, Vytautas Fabiano Silva. **Criptolavagem e Compliance**. São Paulo: Rideel, 2022.

WENDT, Emerson. Morocha Virtual: alguns aspectos da violência de gênero na Internet. **REVISTA ELETRÔNICA DIREITO & TI**, v. 1, p. 1-5, 2015a.

WENDT, Emerson. Morocha Virtual: revenge porn e o Direito Penal brasileiro. **REVISTA ELETRÔNICA DIREITO & TI**, v. 1, p. 1-5, 2015b.

WENDT, Emerson. **A internet e a fragmentação do direito penal no reforço da cultura do medo no Brasil:** percepção social e perspectiva legislativa. Dissertação de Mestrado. Canoas: Universidade La Salle, 2016.

WENDT, Emerson. Infiltração de agentes policiais na Internet nos casos de "pedofilia": limites e perspectivas investigativas. *In*: Clayton da Silva Bezerra; Giovani Celso Agnoletto. (Org.). **Pedofilia**: Repressão aos Crimes de Violência Sexual Contra Crianças e Adolescentes. Rio de Janeiro: Mallet Editora, v. 1, p. 147-162, 2017a.

WENDT, Emerson. **Internet & Direito Penal:** risco e cultura do medo. Porto Alegre: Livraria do Advogado, 2017b.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos**: ameaças e procedimentos de investigação. 3.ed. Rio de Janeiro: Brasport, 2021.

WENDT, Emerson; WENDT, Luiz Augusto. Jogos eletrônicos, comportamentos virtuais e o Direito. **Revista Eletrônica Direito & TI**, v. 1, p. 1-5, 2015.

WENDT, Emerson; ZUMAS, Vytautas Fabiano Silva. Caiu na rede é peixe: *sextortion* baseado no anonimato dos criptoativos. *In* **Relatos sobre a investigação de crimes cibernéticos**. Org. Higor Vinicius Nogueira Jorge e Gaetano Vergine. São Paulo: Editora JusPodivm, p. 19-34. 2022.

WENDT, Guilherme Welter; LISBOA, Carolina Saraiva de Macedo. Agressão entre pares no espaço virtual: definições, impactos e desafios do cyberbullying. **Psicologia Clínica**, v. 25, n. 1, p. 73-87, 2013. Disponível em: http://pepsic.bvsalud.org/pdf/pc/v25n1/05.pdf. Acesso em: 12 fev. 2023.

WIENER, Norbert. **Cibernética e sociedade**: o uso humano de seres humanos. São Paulo: Cultrix, 1970.

ZIEMER, Christine J. *et al*. Estimating distance in real and virtual environments: Does order make a difference? **Attention, Perception, & Psychophysics**, v. 71, n. 5, p. 1095-1106, 2009.

APÊNCICE A - TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Convidamos o (a) Sr.(a) para participar da Pesquisa: "AS EXPECTATIVAS COGNITIVAS E NORMATIVAS DOS ATORES DE INVESTIGAÇÃO POLICIAL EM FACE DOS CRIMES CIBERNÉTICOS.**"**, sob a responsabilidade do pesquisador Emerson Wendt, doutorando ligado ao Programa de Pós-Graduação em Direito da UNIVERSIDADE LA SALLE – Canoas (sob a orientação da Prof.ª Dr.ª Renata Almeida da Costa).

A pesquisa se propõe a examinar as normas penais e processuais penais atinentes aos crimes cibernéticos no Brasil e as expectativas normativas por elas geradas nos atores de investigação policial em relação aos crimes cibernéticos.

Sua participação é voluntária e se dará por entrevista, realizada de forma remota, via Google Meet, gravada com sua autorização. A duração da entrevista será de 45 a 60 minutos, quando, após seu consentimento, o roteiro de perguntas será compartilhado com o participante. Sobre qualquer pergunta efetuada o (a) Sr.(a) poderá realizar questionamentos e/ou justificativas para esclarecê-la, podendo não a responder, desistir e/ou continuar a responder às demais. Estes dados ficarão sob responsabilidade do pesquisador.

Nesse estudo, pautado nos preceitos éticos e fundamentados pela Res. CNS 466/12, entende-se que os riscos existentes serão mínimos, relacionados ao eventual constrangimento e desconforto com os questionamentos. O (a) Sr.(a), ainda, em caso de desconforto e mesmo depois de consentir com a participação, tem o direito de desistir e interromper o processo de resposta do instrumento de pesquisa a qualquer momento e, caso desejar, ser excluído da pesquisa, assim, esse risco será minimizado ou excluído com a interrupção e/ou suspensão da entrevista e exclusão dela do rol de entrevistas. Também serão minimizados os riscos para o entrevistado na realização de pesquisa on-line, pois os contatos prévios, de interlocução e encaminhamento da aceitação da participação na entrevista, conterão os meios e formas de realização dela, ou seja, por um sistema seguro de ponta a ponta, desde o entrevistador até o participante, não sendo transmitida e/ou publicada, apenas armazenada, em ambiente privado, para fins da

pesquisa. Após a entrevista, a gravação será baixada em local seguro com o pesquisador, não permanecendo em ambiente na nuvem, e o(a) Sr.(a) poderá solicitar uma cópia.

Se você aceitar participar, o benefício será grande ao lhe apresentar, ao participante, um espaço de autorreflexão sobre as necessidades normativas e/ou estruturais para a melhora nos resultados das investigações dos crimes cibernéticos.

Se depois de consentir em sua participação o(a) Sr.(a) desistir de continuar participando, tem o direito e a liberdade de retirar seu consentimento em qualquer fase da pesquisa, simplesmente parando de responder às perguntas, independentemente do motivo e sem nenhum prejuízo a sua pessoa. O (a) Sr.(a) não terá nenhuma despesa e não receberá nenhuma remuneração. Os resultados da pesquisa serão analisados e publicados junto com a tese de doutoramento, mas sua identidade não será divulgada, sendo guardada em sigilo. Para qualquer outra informação, o(a) Sr.(a) poderá entrar em contato com o pesquisador pelo telefone (51) 982010431, ou poderá entrar em contato com o Comitê de Ética em Pesquisa – CEP/UNILASALLE, que aprovou a presente pesquisa, no endereço: 3º andar do Prédio 6, conforme horários constantes no sítio específico (Segunda-feira: 14h às 18h; Terça-feira: 14h às 20h; Quarta-feira: 10h às 12h – 14h às 18h; Quinta-feira: 14h às 20h; Sexta-feira: 14h às 19h), telefone: (51) 3476.8452. E-mail: cep.unilasalle@unilasalle.edu.br. Site CEP/UNILASALLE: https://www.unilasalle.edu.br/canoas/mais/comite-de-etica-em-pesquisa.

Ainda, importante esclarecer que a participação é restrita a pessoas com mais de 18 anos, servidores públicos policiais, não envolvendo interação com criança ou adolescente.

Consentimento Pós–Informação

Assim, fui devidamente informado(a) sobre o que o pesquisador quer fazer e por que precisa da minha colaboração, e entendi a explicação, bem como que a entrevista será gravada. Por isso, em responder ao e-mail com este anexo, com o “De acordo”, eu concordo em participar do projeto, sabendo que não vou ganhar nada e que posso desistir quando quiser, mesmo após ter iniciado a responder os questionamentos.

O resultado da pesquisa será divulgado após a defesa da tese, quando os entrevistados poderão acessar o conteúdo disponibilizado pelo pesquisador.

Sugere-se que uma cópia desse documento e/ou do e-mail seja devidamente arquivado/guardado com o(a) Sr.(a).

Emerson Wendt, Pesquisador Responsável, (e-mail: emersonwendt@gmail.com; 51-982010431), Lattes http://lattes.cnpq.br/9475388941521093

Renata Almeida da Costa, Orientadora (e-mail: renata.costa@unilasalle.edu.br), Lattes http://lattes.cnpq.br/8431378002523967

Entrevistado – Aceite por e-mail

APÊNDICE B - QUESTIONAMENTOS E METODOLOGIA DA ENTREVISTA – TESE DE DOUTORADO - DOUTORANDO EMERSON WENDT

Objeto da entrevista: titular/integrante da Delegacia especializada de cada Estado

Tempo de duração: aproximadamente 1 hora

Apresentação inicial: Emerson Wendt, tema de pesquisa e dados do TCLE: Agradeço por participar da Pesquisa "AS EXPECTATIVAS COGNITIVAS E NORMATIVAS DOS ATORES DE INVESTIGAÇÃO POLICIAL EM FACE DOS CRIMES CIBERNÉTICOS", sob a minha responsabilidade, objeto do Doutoramento ligado à Instituição UNIVERSIDADE LA SALLE – Canoas, sob a orientação da Prof.ª Dr.ª Renata Almeida da Costa.

A pesquisa, relacionada a esta entrevista, propõe-se a examinar as normas penais e processuais penais atinentes aos crimes cibernéticos no Brasil e as expectativas normativas (das expectativas) por elas geradas nos atores de investigação policial em relação aos crimes cibernéticos.

Sua participação é voluntária e se dará por meio desta entrevista, gravada com sua autorização, podendo a qualquer momento interromper o procedimento e referir eventual desconforto em responder aos questionamentos, podendo informar o desejo de ser excluído da pesquisa.

Entende-se que não haverá desconfortos ou riscos ao sujeito de pesquisa (a quem responder a pesquisa). Caso existam, serão minimizados em relação aos benefícios advindos dos resultados da pesquisa (geral). Se você aceitar participar, o benefício será grande ao lhe apresentar, ao final da pesquisa, soluções para o delineamento de políticas públicas de enfrentamento à criminalidade cibernética no Brasil.

Se depois de consentir em sua participação o (a) Sr.(a) desistir de continuar participando, tem o direito e a liberdade de retirar seu consentimento em qualquer fase da pesquisa, simplesmente parando de responder às perguntas, independentemente do motivo e sem nenhum prejuízo a sua pessoa. O (a) Sr.(a) não terá nenhuma despesa e não receberá nenhuma remuneração.

Assim, sendo devidamente informado(a) sobre o que o pesquisador quer fazer e por que precisa da sua colaboração e entendeu a explicação, aceita prosseguir?

Roteiro da entrevista:

Conhecendo o entrevistado e sua carreira na investigação criminal:

O que aconteceu na sua carreira para você chegar na posição atual, de investigação de crimes cibernéticos? Fale um pouco sobre você e sua relação com o tema investigação x crimes pela/na Internet.

1 – Quanto às expectativas cognitivas e normativas:

Perguntas prévias:

Quais as normativas que você mais domina sobre os crimes cibernéticos?

(dependendo da resposta, poderão ser feitos os seguintes questionamentos mais diretos)

Conhece a Lei Geral de Proteção de Dados?

Conhece o Marco Civil da Internet?

Conhece a Lei nº 12.735/2012?

(Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.)

Quanto ao Direito Penal, objetiva-se buscar o entendimento do entrevistado sobre:

Pela sua experiência, os tipos penais existentes são suficientes para o enquadramento às situações fáticas que ocorrem na Internet (geral, no Estado)?

- Os tipos penais existentes são suficientes para o enquadramento aos fatos de maior incidência no âmbito da sua delegacia?

- Você entende que há necessidade de outras tipificações?

- Você entente que há necessidade de incremento das penas existentes (e em qual delito)?

Quanto ao Direito Processual Penal existente, você entende que:

Pela sua experiência, as normas de caráter procedimental são adequadas à realidade das investigações dos crimes praticados com uso e por meio da Internet?

- A legislação (processual penal) existente condiciona a rotina procedimental do órgão?

- Como é a coleta/busca de evidências e provas (o que é trazido pela vítima e o que é buscado pela polícia)?

- Como é a relação com provedores de conexão e de aplicação? Plataformas (*law enforcement*) facilitam a interação? Quais são as plataformas mais utilizadas atualmente?

- Você já experienciou, em algum caso, a utilização do procedimento de cooperação penal policial (com polícias judiciárias do Brasil e/ou polícias judiciárias de fora do Brasil)?

- Você já experienciou, em algum caso, a utilização do procedimento de cooperação penal internacional (via MJSP/DRCI)?

Se sim, explicar como aconteceu.

Se não, nunca houve demanda ou é procedimento complexo?

- No dia a dia da sua atividade, qual o tempo médio de um procedimento policial da área de investigação cibernética (desde a ocorrência até o envio ao PJ)?

- Em relação às regras processuais penais, você entende que existem carências normativas?

Se sim, qual aspecto?

Sabe de algum projeto importante em andamento no Congresso Nacional?

2 – Quanto às expectativas cognitivas e normativas em relação à estrutura administrativa e aspectos procedimentais:

Há quanto tempo a delegacia existe?

Há quanto tempo você está atuando na delegacia?

Como é que o público chega à delegacia? O público sabe que ela existe e qual a função da especializada?

E sobre estrutura existente para investigação de crimes cibernéticos, como você percebe ela e qual a experiência?

O local é próprio, locado ou cedido gratuitamente? Como são as instalações?

O pessoal (efetivo policial) possui conhecimento prévio e há corpo técnico especializado para as investigações?

Os equipamentos e softwares são adequados às necessidades investigativas?

Você tem alguma sugestão/proposta de melhoria?

<u>Sobre os investimentos na investigação criminal dos crimes cibernéticos:</u>

O que você acha dos investimentos na investigação de crimes cibernéticos?

- O órgão recebeu verbas e investimentos estaduais?

- O órgão recebeu verbas e investimentos federais?

(dependendo do contexto, pode-se pedir para limitar o tempo de análise na resposta)

- O órgão recebeu recursos de doação e apoio de empresas e pessoas privadas nos últimos três anos?

- Quer acrescentar algo sobre os investimentos? Qual é a necessidade e/ou expectativa de investimentos que deveriam ser feitos?

3 – Quanto ao foco de atuação do órgão policial em que está lotado:

Vocês têm algum foco principal de atuação na delegacia? Como funciona?

- Você diria que vocês têm algum foco principal (em relação aos crimes cibernéticos)? Se sim, por quê? Se não, por quê?

- Qual o foco acessório de vocês (em relação aos crimes cibernéticos)?

- Existem atos normativos estaduais delimitando a atuação?

- A atribuição do órgão, no âmbito estadual, está adequada à realidade?

- Como é a relação com a Polícia Federal, nas trocas de informações e conhecimentos das práticas investigativas cibernéticas?

- Como é a relação com o Ministério da Justiça e Segurança Pública com relação aos treinamentos e às orientações?

- Como é a relação com MP e PJ? A estrutura desses órgãos é voltada para o cibercrime ou é normal, que atende a todos os delitos?

- Como dar efetividade à Lei nº 12.735/2012? (questionamento limitado ao conhecimento da norma).

4 - Quanto ao treinamento para investigação de crimes cibernéticos:

O que você diz sobre a qualificação profissional dos servidores policiais lotados no órgão onde está lotado?

- Os servidores policiais do órgão receberam treinamento da academia de polícia correspondente nos últimos três anos?

- Os servidores policiais do órgão receberam treinamento de órgão/instituição federal nos últimos três anos?

- Os servidores policiais do órgão realizaram treinamento mediante custeio próprio nos últimos três anos?

5 - Quanto à mitigação/redução de danos na Internet:

- Você já teve experiência com usos de mecanismos de mitigação/redução de danos na Internet?

- Você conhece atos normativos que ajudem a mitigar/reduzir danos na Internet? Se sim, quais?

- Você entende que a investigação criminal é meio hábil para mitigar/reduzir danos na Internet? Se sim, quais as condições para fazê-lo?

- Finalmente, qual o caminho ideal para melhorar a persecução da criminalidade no âmbito da Internet?

Você se incomodaria de preencher um formulário com os dados de criação do órgão e informação sobre os atos normativos correspondentes?

Obs.: itens numerados em tópicos são apenas orientativos ao pesquisador.

ANEXO I - PORTARIA SENASP/MJSP Nº 418, DE 11 DE MAIO DE 2022

PORTARIA SENASP/MJSP Nº 418, DE 11 DE MAIO DE 2022[240]

Designa os integrantes de Grupo Técnico, indicados pelo Conselho Nacional de Chefes de Polícia Civil, com a finalidade de subsidiar ações afetas à SENASP instituídas no Plano Tático de Combate a Crimes Cibernéticos Do MJSP.

O SECRETÁRIO NACIONAL DE SEGURANÇA PÚBLICA, no uso das atribuições que lhe foram conferidas pela Portaria nº 77, de 17 de janeiro de 2020, publicada no DOU nº 13, Seção 1, Página 70, de 20/01/2020, combinado com o art. 74, VIII, do Regimento Interno da Secretaria Nacional de Segurança Pública, aprovado pela Portaria nº 151, de 26 de setembro de 2018, do Ministro de Estado da Justiça, publicada no DOU nº 200, Seção 1, Páginas 45-51, de 17/10/2018, e tendo em vista o disposto na Lei 13.709, de 14 de agosto de 2018; na Lei nº 13.675, de 11 de junho de 2018; no Decreto 9.489, de 30 de agosto de 2018; e no Decreto nº 9.876, de 17 de junho de 2019.

CONSIDERANDO a Lei 13.675 de 11 de junho de 2018, que cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS) e tem como um dos seus objetivos fortalecer as ações de prevenção e repressão aos crimes cibernéticos;

CONSIDERANDO o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

CONSIDERANDO o Decreto 10.222, de 5 de fevereiro de 2020 que aprova a Estratégia Nacional de Segurança Cibernética;

CONSIDERANDO o Plano Tático de Combate a Crimes Cibernéticos do MJSP aprovado por Decisão do Ministro nº 54/2022;

CAPÍTULO I

[240] Publicada no Boletim de Serviço em 12/05/2022 (BRASIL, 2022c).

NATUREZA E FINALIDADE

RESOLVE:

Art. 1º Designar os integrantes do Grupo de Técnico- GT, indicados no âmbito desta Secretaria pelo Conselho Nacional dos Chefes de Polícia - CONCPC, com a finalidade de subsidiar ações afetas à Secretaria Nacional de Segurança Pública - SENASP, instituídas no Plano Tático de Combate a Crimes Cibernéticos do Ministério da Justiça e Segurança Pública- MJSP.

Art. 2º Na concepção do Grupo Técnico, deve ser observado o Eixo Temático E3 (Aprimoramento das infraestruturas críticas para combate a crimes cibernéticos) e Eixo E6-A1 (Estabelecimento de protocolos norteadores das polícias judiciárias) do referido Plano Tático.

Art. 3º As ações do Grupo Técnico deverão atender, no que couber, à Metodologia de Gerenciamento de Programas e Projetos Institucionais da SENASP, instituída através da Portaria nº 290, de 18 de junho de 2021.

CAPÍTULO II

DA COMPOSIÇÃO

Art. 4º O Grupo de Técnico será composto pelos seguintes profissionais:

I. Indicado pela Polícia Civil do Estado do Mato Grosso, Delegado RUY GUILHERME PERAL DA SILVA
II. Indicado pela Polícia Civil do Estado de Santa Catarina, Delegado LUIZ FELIPE VALLES ROSADO
III. Indicada pela Polícia Civil do Estado de São Paulo, Delegada NAYARA CAETANO BORLINA DUQUE

IV. Indicado pela Polícia Civil do Estado do Goiás, Delegado DANIEL JOSÉ DA SILVA OLIVEIRA

V. Indicado pela Polícia Civil do Estado de Pernambuco, Agente de Polícia Civil PAULO ROBERTO MEDEIROS VIANA

VI. Indicado pela Polícia Civil do Estado do Rio Grande do Sul, Delegado ANDRÉ LOBO ANICET

VII. Indicada pela Polícia Civil do Estado do Pará, Delegada THICIANE PANTOJA MAIA

VIII. Indicado pela Polícia Civil do Estado de Minas Gerais, Delegado RENATO NUNES GUIMARÃES

§ 1º A coordenação do presente GT será exercida pela Delegada de Polícia Civil, Ana Cristina Braga de Sousa tendo como suplente o Comissário de Polícia Civil, Kelson Rodrigues de Melo, ambos servidores mobilizados da SENASP.

§ 2º A Coordenação Geral de Políticas para as Instituições de Segurança Pública - CGISP/DPSP proporcionará o apoio metodológico e técnico ao desenvolvimento das atividades do GT.

CAPÍTULO I

DAS ATRIBUIÇÕES DOS MEMBROS

Art. 5º Compete ao Coordenador:

I. coordenar a equipe técnica e as atividades do Projeto;

II. gerenciar os recursos disponibilizados para estruturação e realização do projeto;

III. movimentar o processo e juntar documentos e instrumentos produzidos;

IV. requerer a convocação de servidores para auxiliarem nos trabalhos;

V. providenciar a elaboração de todos os artefatos e documentos necessários para operacionalizar a implementação do projeto;

VI. convocar e realizar reuniões de acompanhamento conforme previamente programado;

VII. submeter as entregas definidas nesta portaria à validação do demandante, patrocinador e coordenador;

VIII. exercer as demais funções definidas, no que couber, na Metodologia de Gerenciamento de Projetos da DPSP/SENASP.

Art. 6º Compete ao coordenador-adjunto, além de outras atividades necessárias:

I. substituir e representar o coordenador em sua ausência, impedimento e/ou quando designado,
II. assessorar o coordenador na realização de todas as atividades do projeto, conforme cronograma;
III. auxiliar na movimentação do processo e na juntada de documentos e instrumentos produzidos;
IV. reportar o andamento dos trabalhos ao Coordenador do Projeto;
V. propor, apresentar e definir alterações e revisões necessárias do Projeto; e
VI. exercer as demais funções definidas, no que couber, na Metodologia de Gerenciamento de Projetos da DPSP/SENASP.

Art. 6º Compete aos demais membros do Grupo Técnico:

I. participar das reuniões, bem como tomar parte dos demais atos necessários ao funcionamento do GT;
II. auxiliar na elaboração de documentos técnicos como, Termos de Referência, Estudo Técnico Preliminar e demais artefatos relacionados a processos de contratações de acordo com o que preceitua as ações das atividades de Crimes cibernético;
III. elaboração de diagnóstico visando a instrução dos processos de contratações, quanto a real necessidade da compra de tais equipamentos, bem como o quantitativo específico dos mesmos.

Art. 8º As reuniões do Grupo Técnico ocorrerão, inicialmente, de forma remota e preferencialmente por meio da plataforma Microsoft Teams, podendo ser realizadas de maneira presencial na Secretaria Nacional de Segurança Pública em Brasília-DF, que arcará com as despesas provenientes de diárias e passagens conforme a legislação vigente.

Art. 9º O Grupo de Técnico terá o prazo de 60 (sessenta) dias para conclusão de suas atividades, contados do início das atividades do grupo, podendo ser prorrogável.

Parágrafo único. O coordenador do Grupo Técnico deverá apresentar em 30 (trinta) dias após publicação desse instrumento, plano de trabalho contendo cronogramas de atividades, objetivando monitoramento das ações empreendidas pelo Grupo Técnico.

Art. 10º A participação dos integrantes no Grupo de Técnico será considerada prestação de serviço público relevante, não remunerada.

Parágrafo único. O Plano de Trabalho deverá conter cronogramas de atividades, linhas de ação em consonância com os parâmetros estabelecidos no Art. 3º desta Portaria no que couber, bem como artefatos relativos as necessidades de contratação, critérios de priorização de aquisições, treinamento e capacitação na área de crimes cibernéticos e estimativas de custo.

Art. 11º Esta Portaria revoga a PORTARIA SENASP/MJSP Nº 407, DE 12 DE ABRIL DE 2022 (17769990), e entra em vigor na data de sua publicação.

CARLOS RENATO MACHADO PAIM

ANEXO II - PORTARIA SENASP/MJSP Nº 463, DE 26 DE SETEMBRO DE 2022

PORTARIA SENASP/MJSP Nº 463, DE 26 DE SETEMBRO DE 2022

ALTERAÇÃO e PRORROGAÇÃO da Portaria SENASP/MJSP Nº 418, DE 11 DE MAIO DE 2022 (18003710) para a conclusão das atividades do Grupo Técnico, indicado pelo Conselho Nacional de Chefes da Polícia Civil, com a finalidade de subsidiar ações afetas à SENASP, instituídas no Plano Tático de Combate a Crimes Cibernéticos do MJSP.

O SECRETÁRIO NACIONAL DE SEGURANÇA PÚBLICA, no uso das atribuições que lhe foram conferidas pela Portaria nº 77, de 17 de janeiro de 2020, publicada no DOU nº 13, Seção 1, Página 70, de 20/01/2020, combinado com o art. 74, VIII, do Regimento Interno da Secretaria Nacional de Segurança Pública, aprovado pela Portaria nº 151, de 26 de setembro de 2018, do Ministro de Estado da Justiça, publicada no DOU nº 200, Seção 1, Páginas 45-51, de 17/10/2018, e tendo em vista o disposto na Lei 13.709, de 14 de agosto de 2018; na Lei nº 13.675, de 11 de junho de 2018; no Decreto 9.489, de 30 de agosto de 2018; e no Decreto nº 9.876, de 17 de junho de 2019, e:

CONSIDERANDO a Lei 13.675 de 11 de junho de 2018, que cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS) e tem como um dos seus objetivos fortalecer as ações de prevenção e repressão aos crimes cibernéticos;

CONSIDERANDO o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

CONSIDERANDO o Decreto 10.222, de 5 de fevereiro de 2020 que aprova a Estratégia Nacional de Segurança Cibernética;

CONSIDERANDO o Plano Tático de Combate a Crimes Cibernéticos do MJSP aprovado por Decisão do Ministro nº 54/2022;

CONSIDERANDO o teor do Ofício (17553594), no qual o Conselho Nacional dos Chefes de Polícia Civil - CONCPC, apresenta as indicações de representantes técnicos da Polícia Civil para composição de Grupo de Trabalho;

CONSIDERANDO a necessidade de dilação de prazo para o cumprimento das atividades elencadas no Plano de Trabalho (18417333);

CONSIDERANDO as novas indicações de representantes técnicos da Polícia Civil pelo Conselho Nacional de Chefes da Polícia Civil (19740980);

RESOLVE:

Art. 1º A Portaria SENASP/MJSP Nº 418, DE 11 DE MAIO DE 2022 (18003710) passa a vigorar com a seguinte alteração:

Art. 4º O Grupo Técnico será composto pelos seguintes profissionais:

I - Delegado RUY GUILHERME PERAL DA SILVA - Polícia Civil do estado do Mato Grosso;

II - Delegado LUIZ FELIPE VALLES ROSADO - Polícia Civil do estado de Santa Catarina;

III - Delegada NAYARA CAETANO BORLINA DUQUE - Polícia Civil do estado de São Paulo;

IV -Delegado DANIEL JOSÉ DA SILVA OLIVEIRA - Polícia Civil do estado do Goiás;

V - Agente de Polícia Civil PAULO ROBERTO MEDEIROS VIANA - Polícia Civil do estado de Pernambuco;

VI - Delegado ANDRÉ LOBO ANICET - Polícia Civil do estado do Rio Grande do Sul;

VII - Delegada THICIANE PANTOJA MAIA - Polícia Civil do estado do Pará;

VIII - Delegado RENATO NUNES GUIMARÃES - Polícia Civil do estado de Minas Gerais;

IX - Delegado ALESANDRO GONÇALVES BARRETO - Polícia Civil do estado do Piauí;

X - Delegado EMERSON WENDT - Polícia Civil do estado do Rio Grande do Sul;

XI - Delegado JOSÉ ANCHIETA NERY NETO - Polícia Civil do estado do Piauí; e

XII - Agente de Polícia - MARCELINO DE ANDRADE AMARAL - Polícia civil do Distrito Federal.

§ 1º A coordenação do presente GT será exercida pela Delegada de Polícia Civil, Ana Cristina Braga de Sousa tendo como suplente o Investigador de Polícia Civil, Roberto Wagner Oliveira Teixeira, ambos servidores mobilizados da SENASP.

Art. 2º Prorrogar, por mais 60 (sessenta) dias, o prazo para conclusão das atividades do Grupo Técnico- GT, indicados no âmbito desta Secretaria e pelo Conselho Nacional dos Chefes de Polícia - CONCPC, com a finalidade de subsidiar ações afetas à Secretaria Nacional de Segurança Pública - SENASP, instituídas no Plano Tático de Combate a Crimes Cibernéticos do Ministério da Justiça e Segurança Pública- MJSP.

Art. 3º Esta Portaria entrará em vigor a partir do primeiro dia, após o vencimento do prazo da Portaria SENASP/MJSP Nº 441, DE 29 DE JULHO DE 2022 (18783209), publicando-se no Boletim de Serviço Eletrônico.

CARLOS RENATO MACHADO PAIM

ANEXO III - ESTRUTURA POLÍTICO-ADMINISTRATIVA DOS ÓRGÃOS INTEGRANTES DAS POLÍCAIS CIVIS ESPECIALIZADOS NO ENFRENTAMENTO AOS CRIMES CIBERNÉTICOS NO BRASIL

ESTRUTURA POLÍTICO-ADMINISTRATIVA DOS ÓRGÃOS INTEGRANTES DAS POLÍCAIS CIVIS ESPECIALIZADOS NO ENFRENTAMENTO AOS CRIMES CIBERNÉTICOS NO BRASIL

Estado	Ato(s) Normativo(s) de Previsão (atual)[241]	Observações a partir do entrevistado
AC	- Portaria Regulamentar nº 16, de 07/12/2021, instituindo o Núcleo Especializado de Apoio a Investigações de Crimes Cibernéticos – NECIBER. - Decreto nº 11.096, de 29/07/2022, cria a Delegacia de Repressão a Crimes Cibernéticos – DRCC.	Tem Neciber previsto desde 2021, não ativo. Decreto criou delegacia em 2022, não ativa.
AL	- Portaria nº 407, de 14/03/2016, prevendo a investigação de crimes cometidos pela rede mundial de computadores pela Seção Antissequestro e Crimes Cibernéticos.	Tem uma seção antissequestro e de crimes cibernéticos, prevista por Portaria – 2016.
AM	- Portaria Normativa nº 10, de 05/07/2021, previu a Delegacia Especializada em Repressão a Crimes Cibernéticos – DERCC.	Portaria previu – 2021
AP	- Lei nº 2.507, de 13/08/2020, prevendo a Delegacia de Repressão aos Crimes Cibernéticos – DR-CCIBER, dentre outros órgãos	Lei previu Delegacia – 2020. Atividade, no

[241] Estes dados ou foram enviados pelos entrevistados ou coletados na Internet.

		entanto, vem desde setembro de 2021.
BA	- Portaria de nº 139, de 04/05/2012, criou o Grupo Especializado de Repressão aos Crimes por Meios Eletrônicos – GME. - Instrução Normativa nº 01, de 10/09/2021, previu o Laboratório de Inteligência Cibernética – CIBER-LAB. - Em 2022, foi criada a Delegacia de Repressão aos Crimes de Estelionato por Meio Eletrônico (DreofCiber), pela Portaria nº 379, de 05/08/2022.	Não tem delegacia. Tem laboratório, previsto por IN, desde 2021. Delegacia, desde agosto 2022, após entrevista.
CE	- Lei nº 17.305, de 25/09/2020, previu a Delegacia de Repressão aos Crimes Cibernéticos – DRCC.	
DF	- Decreto nº 38.098, de 30/03/2017, previu a Delegacia Especial de Repressão aos Crimes Cibernéticos.	Decreto previu em 2017.
ES	- Instrução de Serviço nº 214, de 18/03/2019, definiu atribuições da especializada, criada pela Lei Complementar nº 892, de 08/06/2018, regulamentada pelo decreto nº 4277-R, de 05/07/2018, que criou a Delegacia Especializada de Repressão aos Crimes Cibernéticos – DRCC.	Criação em 2018 e regulamentação de atribuição em 2019.
GO	- Lei nº 19.907, de 14/12/2017, previu as atribuições da Delegacia Estadual de Repressão a Crimes Cibernéticos – DERCC. - Portaria nº 007, de 13/03/2018, regulamentou atividades da DERCC.	Criação da especializada, por Lei, em 2017. Regulamentação das atribuições em 2018.
MA	- Instrução Normativa nº 004, de 20/08/2016, previu o Departamento de Combate a Crimes Tecnológicos – DCCT.	Órgão existente desde 2011. Em 2016 houve a modificação.
MG	- Resolução nº 8004, de 14/03/2018. Previu a Divisão Especializada de Investigação aos Crimes Cibernéticos e Defesa do Consumidor: a) Delegacia Especializada em Defesa do Consumidor; b) Delegacia Especializada em	Tem uma divisão e duas delegacias (2018). Existência

	Investigação de Crime Cibernético; c) Laboratório de Crimes Cibernéticos	de especializada desde 2006.
MT	Lei Complementar Estadual nº 694/2020, regulamentada pela Resolução nº 067, de 10/12/2020.	Criação em 2020.
MS	Não tem órgão.	
PA	Decreto nº 690, de 16/04/2020, previu a Diretoria Estadual de Combate a Crimes Cibernéticos (Deccc), com três divisões: - Divisão de Combate a Crimes contra Direitos Individuais Praticados por Meios Cibernéticos - Divisão de Combate a Crimes Econômicos e Patrimoniais Praticados por Meios Cibernéticos - Divisão de Combate a Crimes contra Grupos Vulneráveis Praticados por Meios Cibernéticos - Cada divisão tem três delegacias, ou seja, nove delegacias ao todo.	Delegacia desde 2005. Atualmente, tem Diretoria, prevista em 2020, com três divisões e 9 delegacias (três instaladas).
PB	- Portaria nº 272, de 17/05/2022, previu a Delegacia Especializada de Crimes Cibernéticos – DECC e outros órgãos.	Previsão por Portaria, desde 2022.
PE	- Lei nº 15.026, de 20/06/2013, previu a Delegacia de Polícia de Repressão aos Crimes Cibernéticos – DPCRIC. - Portaria nº 050, de 15/02/2017, estabelece atribuições.	Desde 2013, por Lei, com regulamentação em 2017.
PI	- Portaria nº 002, de 11/01/2017, previu a Delegacia de Repressão aos Crimes de Informática e definiu atribuições atuais.	Previsão por Portaria, desde 2017.
PR	- Resolução nº 293, de 18/11/2005, previu o Núcleo de Combate aos Cibercrimes – NuCiber.	Previsão por Resolução, desde 2005.
RJ	- Decreto nº 26.209, de 19/04/2000, previu a Delegacia de Repressão aos Crimes de Informática – DRCI.	Desde 2000. Não participaram da pesquisa.

RN	- Decreto nº 31.169, de 08/12/2021, previu a Delegacia Especializada Repressão em Crimes Cibernéticos (DERCC).	Tem delegacia prevista, não instalada.
RO	- Lei nº 4.630, de 31/10/2019, previu Laboratório de Tecnologia de combate a Crimes Cibernéticos – CIBER-LAB (dentro da Inteligência). - Delegacia Especializada em Repressão às Fraudes é criada pela Resolução nº 10, de 25/05/2022.	Não tem delegacia específica. Tem Delegacia focada em fraudes. Existe Ciber-Lab, com um servidor.
RR	- Decreto nº 29.637-E, de 03/12/2020, previu o Distrito Estadual de Repressão a Crimes Cibernéticos. - Resolução nº 002, de 21/04/2021, regulamentou atribuições.	Previsão por Decreto, desde 2020. Resolução, em 2021, regulamentou o órgão.
RS	- Decreto nº 54.406, de 2018, com alteração pelo Decreto nº 55.627, de 08/12/2020, Delegacia de Polícia de Repressão aos Crimes Informáticos e de Defraudações – DRCID	Previsão desde 2006. Instalação em 2010. Reestruturação em 2018 e 2020.
SC	- Decreto nº 1.820, de 24/03/2022, previu a Delegacia de Repressão aos Crimes de Informática (DRCI) e o Laboratório de Tecnologia Cibernética (CIBER-LAB), regulamentado pela Resolução nº 013, de 06/05/2022.	Desde 2017, tem delegacia e laboratório. Reestruturação por Decreto, em 2022.
SE	- Portaria nº 11, de 19/08/2016, previu a Delegacia Especial de Repressão a Crimes Cibernéticos.	Existência desde 2014, com regulamentação em 2016.
SP	- Decreto nº 65.241, de 13/10/2020, previu a Divisão de Crimes Cibernéticos – DCCIBER, com: II - 1ª Delegacia de Polícia sobre Fraudes contra Instituições Financeiras praticadas por Meios Eletrônicos;	Existência desde 2001, com alterações em 2013 e 2020, quando

	III - 2ª Delegacia de Polícia sobre Fraudes contra Instituições de Comércio Eletrônico praticadas por Meios Eletrônicos; IV- 3ª Delegacia de Polícia sobre Violação de Dispositivos Eletrônicos e Redes de Dados; V- 4ª Delegacia de Polícia de Lavagem e Ocultação de Ativos Ilícitos por Meios Eletrônicos; VI- Centro de Inteligência Cibernética - CIC; VII- Laboratório Técnico de Análises Cibernéticas - Lab-TAC.	previu uma divisão vinculada ao DEIC.
TO	- Decreto nº 5.979, de 12/08/2019, previu a Divisão Especializada de Repressão a Crimes Cibernéticos (DRCC)	Prevista por Decreto, desde 2019.