CRIMES CIBERNÉTICOS: INVESTIGAÇÃO E PREVENÇÃO

CYBER CRIMES: INVESTIGATION AND PREVENTION

Samuel Xavier Deolindo Júnior[1]
Michael Welter Jaime [2]

RESUMO

Este trabalho apresenta o conceito de Crimes Cibernéticos e a legislação que tipifica tais crimes. O foco do trabalho se estende aos aspectos de investigação e prevenção de casos invasivos de privacidade, exposição de dados confidenciais, bem como aponta caminhos para a segurança familiar no âmbito digital. Para exemplificar, o presente artigo expõe investigação que teve êxito na aplicação legal pátria, quando da apuração de fatos criminosos no âmbito digital.

Palavras-chave: Crime cibernético; Legislação; Investigação; Prevenção.

ABSTRACT

This work presents a concept of Cybercrimes and the legislation that describe those crimes. The focus of this article extends to inquiry aspects and prevention of privacy hacking cases, confidential data exposition as well as presenting ways toward security family in the digital environment. To Illustrate, this article exposes investigation that had success in the native legal application, when investigating criminal facts in digital environment.

KEYWORDS: Cybercrimes; Legislation; Inquiry; Prevention

INTRODUÇÃO

> *O que segue a justiça e a bondade achará a vida, a justiça e a honra*.
> Provérbios 21:21

Para tratar de um tema tão novo e presente nas vidas da maioria das pessoas da atualidade, como a tecnologia digital, é preciso ter como ponto de partida a concepção do que é a *cybercultura*. Pierre Lévy (1999) considera já desde o início dois pontos essenciais da *cybercultura*: um grupo, em especial jovens, à procura de experiências coletivas em uma plataforma diferente das convencionais; além de um

[1] Estudante do Curso de Direito na Faculdade Evangélica Raízes. Anápolis, Goiás, Brasil. E-mail:
[2]Professor Universitário. Bacharel em Direito. Dupla licenciatura em Língua Portuguesa e Língua Inglesa pela Universidade Estadual de Goiás. Especialista em Direção do Sistema de Execuções Penais pelo Centro Universitário UniEvangélica.. Mestre Multidisciplinar em Sociedade, Tecnologia e Meio Ambiente pelo Centro Universitário UniEvangélica. Cursando Doutorado em Direito Penal na Universidade Federal de Buenos Aires - Argentina.

novo espaço de comunicação que se abre no plano econômico, cultural, cultural e humano. É neste viés que esta pesquisa vem esclarecer pontos importantes dessa nova cultura digital.

Este trabalho, a partir da concepção da cybercultura explorou a positivação do Direito brasileiro, diante da plataforma digital de comunicação, inicialmente com base no marco regulatório da Lei Nº 12.965, DE 23 DE ABRIL DE 2014, chamada de Marco Civil da Internet. A lei que estabelece as diretrizes e bases do funcionamento da rede internacional no Brasil, nos dizeres da lei, apresenta os "princípios, garantias, direitos e deveres para o uso da Internet no Brasil".

A pesquisa apresentou a lei que, dois anos antes da sanção da lei do Marco Civil da Internet, havia sido aprovada e se tornou a Lei Nº 12.737, de 30 de novembro de 2012, apelidada de lei Carolina Dieckmann, pelo fato da atriz ter fotos e vídeo íntimos publicados pela rede mundial de computadores; a citada norma legal apresenta a "tipificação criminal de delitos informáticos", inserindo os artigos 154-A e 154-B e dando nova redação aos artigos 266 e 298 do Código Penal Brasileiro. Complementada pelo dispositivo legal da Lei Nº 12.735/2012, que institui delegacias especializadas para investigar tais crimes digitais.

Expõe-se a análise das definições trazidas pela lei Nº 13.709, de 14 de agosto de 2018, que trouxe ao ordenamento jurídico brasileiro o direito expresso de se manifestar pelos meios virtuais, bem como fortalecer o direito à intimidade e ao sigilo de informações.

Outro aspecto tratado neste artigo é a estratégia investigativa permitida em lei, cujo objetivo é o de desvendar e levar a julgamento criminosos cibernéticos e os demais que exploram os meios digitais para a continuidade de práticas delitivas.

Por fim, são apresentadas possíveis estratégias de segurança que os usuários da internet dispõem, sem expor a risco seus dados, ou até mesmo, a vida de seus entes queridos, em especial as crianças.

1. A *Cybercultura* na perspectiva de Pierre Lévy

Na constância da atualização da sociedade, os meios eletrônicos assumiram lugar de destaque nas relações sociais, trabalho, contato e comunicação, pode-se assim dizer, na humanidade em seu sentido lato.

O filósofo, sociólogo e pesquisador da Ciência da Informação, Pierre Lévy, faz uma análise abrangente do resultado das relações mencionadas, pela perspectiva da tecnologia.

Lévy sustenta que é imprescindível a abertura para a nova cultura, buscando compreendê-la como algo já presente, que se transforma e age por força da própria sociedade, não sendo ainda um organismo, mas ferramenta de exploração de outras áreas, como se vê

> ...tentemos compreendê-la, pois a verdadeira questão não é ser contra ou a favor, mas sim reconhecer as mudanças qualitativas na ecologia dos signos, o ambiente inédito que resulta da extensão das redes de comunicação para a vida social e cultural. Apenas dessa forma seremos capazes de desenvolver estas novas tecnologias dentre de uma perspectiva humanista. (LÉVY,1999,12).

Outro aspecto que encaixa na análise de Lévy é a perspectiva representativa que o mundo virtual mantém com o mundo real, Chomsky fortalece essa visão, quando explica as relações representativas que a sociedade cria com a palavra, trazendo um histórico desde Aristóteles, com a dicotomia entre forma e matéria, até nos dias atuais, diz “E agora – por estes dias – estamos de volta a um tipo de concepção neoescolástica das relações palavra-coisa” (CHOMSKY, 2014).

EM artigo publicado em 2015, Wendt e Meineiro, no livro intitulado “Ciberdireito e Democracia”, apresentam que a sociedade foi apresentada a um novo universo, que possibilitou mudanças significativas e estruturantes, já que não há volta para as relações como fora no passado. Trazem os autores que

> Desde a criação da Internet, na década de 1960, e com a interação gerada após a criação da web (rede “WWW”), as relações interpessoais foram drasticamente alteradas. A proximidade virtual entre os indivíduos reduziu as distâncias e favoreceu a comunicação. Aliás, estamos, segundo Castells (2008), na era da “rede das redes”. Essa comunicação aproxima culturas e até mesmo as cria dentro do ambiente virtual. As comunidades virtuais, por assim entendidas, podem avizinhar indivíduos de crenças diferentes, raças e nacionalidades, mas que em uma rede de relacionamento encontram aspectos em comum a ponto de aculturarem-se. (WENDT e MEINERO, 2015)

Na visão dos estudiosos da cultura cibernética, a cultura se fundiu ao cotidiano dos indivíduos, desde o conhecimento dos “três WWW”, da web, como se

por simbiose, utilizando uma linguagem das ciências biológicas, que quer dizer “interação entre duas espécies que vivem juntas”, como se percebe, são duas espécies distintas que se coadunam naturalmente. Ao passo que, se tornou difícil voltar a viver sem a internet.

Coube aos pesquisadores revelarem, por suas habilidades, o que seja compreensível quanto à dimensão do impacto real das relações virtuais, passando pelas ações lícitas ou ilícitas, bem como o que há de legal produzido para controlar os aspectos de trocas de dados, manutenção e proteção de dados, no Brasil, o Marco Regulatório, as leis penais e o princípio da Liberdade cristalizado na Carta Magna, fazem parte desse rol de seguranças e garantias.

1.1 . Forma e matéria da Cybercultura

A necessidade de se entender a Cybercultura e seus impactos na realidade visa iniciar a discussão de como é transposto o comportamento da sociedade aos meios digitais, mormente, no caso em discussão, aos crimes, à investigação e prevenção.

Não apenas por sua novidade ou complexidade, a Cybercultura - ou de forma aportuguesada, cultura cibernética - tem relevância quanto ao modo que é utilizada, quais as finalidades objetivadas e o prejuízo que pode acarretar na má utilização do sistema.

Todo indivíduo exterioriza à sociedade, seus anseios e sentimentos, no ambiente digital essa manifestação torna-se o reflexo da sociedade. É um local de criação de ícones, representações da realidade; vejam-se os perfis das redes sociais, exemplo claro do que as pessoas querem ser ou, querem que as pessoas vejam de si.

A internet em si foi se consolidando como uma aliada à comunicação, tornando-se a plataforma mais utilizada entre as pessoas da pós-modernidade, tendo em vista seu imediatismo, praticidade, além da preservação do meio ambiente, por não ser mais utilizado o papel, o qual ao seu tempo revolucionou o comportamento global.

O homem passou a perceber o meio digital não mais como uma ferramenta inerte em seu funcionamento, mas uma extensão do seu mundo; real-digital passou a

se fundir em uma práxis natural. Esse é o sentimento interpretado pela ansiedade causada pelo simples esquecimento do objetivo chamado celular, em casa.

Justamente essa extensão da práxis cotidiana, que chama a atenção ao estudo proposto, visto que, as práticas criminosas enxergaram na tecnologia um aliado de última hora. Não há que se falar que é apenas uma arma a tecnologia, mas um campo passível das mais diversas atividades do cotidiano, da mais complexa à elementar, como uma cirurgia robótica ao pedido de uma comida para o almoço.

A mudança social pelo advento de um sistema virtual possibilitou a formação de comunidades, cujo interesse mútuo, pensamentos convergentes até gostos, Wendt e Meineiro explicam que essa é uma característica inerente ao processo de estruturação da própria internet, como se vê

> A Internet, no seu contexto de auto-organização e estruturação atual (WENDT, no prelo), baseada na interação através de aplicativos13, favorece a comunicação através de comunidades virtuais, não no sentido de grupos específicos, mas de aproximações geradas/consequentes do mesmo pensar/manifestar, do mesmo agir, do mesmo gostar/odiar, ou seja, dos mesmos interesses e/ou oportunidades. São seus vários códigos binários, dialógicos, pois um não necessariamente exclui o outro. (WENDT e MEINERO, 2015)

A interação entre indivíduos e a criação de uma teia social se evoluiu de modo acelerado, embora de recém-introdução no cenário brasileiro, há geração que já nasceu conhecendo em funcionamento o sistema digital, há ainda aqueles que nunca tiveram acesso direto ao sistema. Esses podem ser motivos relevantes para explicar a lentidão de processo de regulamentação desse espaço.

No Brasil, por se uma plataforma de uso muito recente, a rede web passou anos sem ter controle legal do ambiente, também foi forçado pela área econômica para garantir a segurança de dados, o que favoreceu também o combate à criminalidade e a prevenção de danos aos usuários.

2. A Legislação brasileira em busca de controle da Internet: o Marco Regulatório

Antes de conhecermos a realidade no Brasil, é interessante fazer um histórico geral da criação e expansão da rede mundial de computadores.

Pela explanação de Fabiano R. Kummer (2017) a internet passou a fazer parte da realidade tecnológica em um ambiente de experimento com financiamentos

do governo norte-americano, através do Departamento de Defesa dos Estados Unidos, no período da Guerra Fria, pelos idos da década de 1960.

Naquele período, foi o primeiro mecanismo de comunicação eletrônica fazendo ligações entre computadores, com o intuito de transmitir informações militares que permanecessem difundidas em rede como forma de proteção a bombardeios. Na pesquisa de Kummer, o primeiro período foi fundamental para a estruturação da rede, Kummer manifesta que

> Teve papel fundamental nessa criação, Paul Baran, que em 1964 idealizou uma rede híbrida, na forma de uma malha, na qual os dados se deslocariam de forma dinâmica, usando o caminho menos sobrecarregado (metodologia conhecida como “packetswitching”). O experimento conduzido pela ARPA – uma rede de computadores interligados denominada ARPANET - teve início no ambiente universitário, na Califórnia, EUA, interligando os centros universitários do Stanford Institute, da Universidade da Califórnia em Los Angeles, da Universidade da Califórnia em Santa Bárbara e da Universidade de Utah, e se notabilizou por ter sido a rede precursora da Internet. (KUMMER, 2017, posição 121, Kindle)

Após todos os aprimoramentos, a tecnologia pode ser vista como algo acadêmico e científico, o próximo passo foi a expansão comercial do dispositivo digital, cujo marco foi o ano de 1997, nos Estados Unidos.

Logo em seguida, no ano de 1990 a World Wide Web (WWW) se consolidou. Kummer (2017) escreve que o passo seguinte à criação do WWW foi o estabelecimento do protocolo HTTP (HyperText Transfer Protocol), “pelo físico inglês Tim Berners-Lee, que também criou a linguagem HTML (HyperText Markup Language)”, esse protocolo que possibilitou a simplificação da programação no ambiente da Internet.

Ainda segundo estudo de Kummer (2017), foi no ano de 1994, que ocorreu mais um aprimoramento na rede, veio a ser utilizado um novo protocolo apresentado pela empresa norte-americana Netscape, o protocolo HTTPS (HyperText Transfer Protocol Secure). A partir desse novo protocolo, as mensagens transferidas teriam garantia segurança, através do envio de dados criptografados, em especial para as transações comerciais pela internet.

O protocolo da empresa Netscap, “permitia a verificação de autenticidade, tanto do servidor, quanto do cliente, por meio do uso de certificados digitais, tornando então essas transações comerciais mais seguras" (Kummer, 2017).

Tais observações são úteis para compreender a formatação do processo de criação do dispositivo digital disponíveis aos usuários a partir dos anos 90, até que se estabelecessem parâmetros legais para a utilização.

Por muito tempo a internet ficou sem uma regulação no Brasil, após sua primeira conexão em setembro 1988. Guizzo (1999), em seu livro “Internet: O que é, o que oferece, como conectar-se” faz um retrato da história da Internet, a partir de seu primeiro passo, como experimentos acadêmicos, aperfeiçoamento, utilização pelas Organizações não governamentais (ONGs), em seguida pelo sistema governamental, até que chegasse ao meio doméstico.

Guizzo (1999) em seu profícuo relato histórico aponta que a comunicação de forma digital em seu início deu o primeiro passo cirando uma comunicação, via e-mail entre as ONGs, tal comunicação servia de fato como um correio eletrônico. No Brasil, a partir do ano de 1994 o Ministério de Ciência e Tecnologia e do Ministério das Comunicações anunciaram o investimento na nova tecnologia, institucionalizando a Embratel como o propulsor do evento tecnológico em solo brasileiro.

Nota-se que, ao longo de vinte e quatro anos não houve se quer uma lei que abrangesse tal questão, regulamentando de fato o sistema digital. O país viveu uma época de “silêncio legal”, quanto ao tema.

Nesse tempo, apenas as legislações já existentes sustentavam a aplicação de penalidades, tal legislação era utilizada subsidiariamente, com abrangência de forma parcial as condutas delituosas que se fizessem saltar ao âmbito do direito.

No ano de 2014, após alguns fatos largamente divulgados pela mídia, como o fato da publicação na rede mundial de computadores por hackers, de vídeos íntimos da atriz Carolina Dieckmann, foi o poder legislativo provocado de forma mais veemente, afim de que se criassem no Brasil regras mais direcionadas ao tema. Naquele ano, no dia 30 de novembro foi sancionada a lei 12.965, pela então presidente Dilma Rousseff.

2.1. A regulamentação legal da internet brasileira

No tempo em que não havia nenhuma legislação produzida que regulasse o uso das redes sociais, pela internet, apenas as legislações já existentes embasavam a aplicação de penalidades, tais legislações eram utilizadas subsidiariamente, com

abrangência de forma parcial as condutas delituosas que se fizessem saltar ao âmbito do direito.

Gonçalves (2017) defende que há uma necessidade premente de se regulamentar as manifestações no campo da internet, pois essas encontram ressonância e perpetuidade, já que todas as manifestações se espalham de forma rápida e alcança os mais altos patamares de receptores; também se perpetuam, pois não são rastros apagáveis, mas gravados em arquivos eletrônicos.

Como uma tentativa de controlar o ambiente virtual, no ano de 2014 foi sancionada pela presidente Dilma Roussef a lei de número 12.965 em 23 de abril, com objetivo de estabelecer os princípios, as garantias, os direitos e deveres para o uso da Internet no Brasil.

A lei que contém trinta e dois artigos manifesta a tentativa de apresentar um controle do Estado sobre as ações individuais em relação à utilização do meio de transmissão e manutenção de dados.

Como se percebe da leitura dos primeiros cinco artigos, há uma condensação dos princípios constitucionais, dos objetivos e as garantias que assiste a todos os cidadãos. Vê-se nesse aspecto a extensão da vida cotidiana ao meio digital como já expresso anteriormente.

Não há facilidade em dissociar a vida real com a vida virtual que impera nos dias atuais, visto que, é válida a manifestação digital como se real fosse, havendo implicações civis e penais, no âmbito da atual legislação brasileira.

No artigo 2º da referida lei do Marco Civil da Internet lê-se

> Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
> I - o reconhecimento da escala mundial da rede;
> II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
> III - a pluralidade e a diversidade;
> IV - a abertura e a colaboração;
> V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VI - a finalidade social da rede.

Há aqui a explanação dos fundamentos, o arcabouço basilar da lei. Depreende-se do exposto que há a condensação dos conceitos constitucionais fundamentais, vistos nos incisos do parágrafo 1º da Constituição Federal de 1988, como direito à cidadania, a dignidade da pessoa humana; os valores sociais do trabalho e da livre iniciativa; bem como a pluralidade de pensamentos.

Críticas são descritas também por Gonçalves, que aponta

> O Marco Civil é uma legislação que repete muitos preceitos constitucionais sem contextualizá-los a uma ideia do que seria essa construção do ser humano no século XXI. Não a construção de um ser humano universal e igual em qualquer lugar. Partindo do conceito de que a tecnologia, por ser transformadora, equaliza a todos, o que é incorreto. Ela potencializa as diversidades, eliminando barreiras exclusivas e impedimentos para a conquista de direitos (GONÇALVES, 2017, p.06).

Em sua visão, não há função específicas do retorno aos princípios constitucionais expressos e garantidos, visto que a função da lei não é mais de orientação normativa, mas de regulamentação. Também não vê como característica comum de todos os usuários da rede, já que há características próprias em cada cultura.

Rogério Sanches Cunha também tece críticas à tímida legislação penal brasileira “Apesar de a sociedade estar cada vez mais inserida no mundo da informática, percebe-se que o Direito (em especial, o Direito Penal) não acompanha, como deveria a evolução que movimenta o setor cibernético” (CUNHA, 2018, p.267).

Mesmo com as críticas, o ato regulatório apresenta de forma didática e prática o que se espera de um bom comportamento dos usuários da rede, em sentido lato.

O terceiro parágrafo tem por objeto destacar o direito do indivíduo como pessoa, com garante a Constituição Federal apresenta, os direitos de manutenção do uso da rede com segurança de continuidade, ou seja, permanência do canal em funcionamento, a responsabilidade do indivíduo nos termos da lei (infere-se que se refere à responsabilidade civil ou penal do usuário).

Com naturalidade o especialista jurídico percebe as diretrizes cunhadas no marco regulatório da internet nas vertentes civis, penais, além da consumerista, como uma prestação de serviço a ser garantida.

Como forma taxativa, o artigo quinto da lei em estampa, apresenta os termos que serão considerados para a devida interpretação da legislação penal e civil, a partir desse momento. A exemplo está o termo internet, conexão à internet entre outros.

As expressões que são acolhidas pela lei, ainda são insuficientes para abranger a complexa rede, a qual se tem como rede mundial de computadores. Essa é uma característica de conhecimento limita acerca do tema, por parte do legislador.

A lei reserva o capítulo três para dar direitos expressos aos usuários como consumidor, tornando regulamentada a continuidade de execução de um serviço, com transparência, eficiência, voltando-se sempre ao direito ao sigilo de informações.

Mais adiante, volta a garantir o direito ao sigilo de informações, do artigo 10 ao 11, deixando a disciplina, em casos de descumprimento do exposto nos artigos anteriores, para o artigo 12, que não descarta a responsabilização penal e civil da empresa fornecedora do serviço, bem como a aplicação de multas.

A lei expressou, como se estivesse ensaiando, uma regulamentação; deixou expressas as possiblidades de obtenção de informações sigilosas, pelas autoridades investigativas e processantes. É o que se vê nos artigos 18 ao 23.

Nos artigos finais da lei do Marco Civil Regulatório apresenta a função fomentadora do Estado em relação à democratização da rede.

Tal análise é feita constantemente pelos aplicadores do direito ao atuarem em causas que envolvam questões civis, mais constantemente quando se trata de questões eleitorais, um ambiente que apresenta uma farta seara de elementos a serem contestados, bem como em questões políticas.

2.2. A tipificação penal brasileira e sua implicação

Michel Foucault aponta a penalidade como um caminho para a mudança não só de hábito, mas do trabalho de aperfeiçoamento da moralidade, combatente à permanência do indivíduo na conduta delituosa, neste sentido escreve

> Não é, portanto, um respeito exterior pela lei ou apenas o receio da punição que vai agir sobre o detento, mas o próprio trabalho de sua consciência. Antes uma submissão profunda que um treinamento superficial; uma mudança de “moralidade” e não de atitude. (FOUCAULT, 2014, p.231)

Neste pensamento a legislação brasileira caminha em formalizar as condutas que manifestam a prática delitiva, efetuadas em ambiente virtual, nota se o esforço do legislador em consolidar cada comportamento, mesmo que de forma ainda tímida.

Em breve análise, leva-se em consideração a exposição do que seja *cracker*. Sanches também expõe o estudo de Luiz Regis Prado que considera como *cracker* para o direito penal brasileiro. Expõe PRADO

> ...Cracker é... o sujeito que 'invade sistemas de computadores de outra pessoa, frequentemente em uma rede, supera senhas ou licenças em programas de computadores ou de outras formas intencionalmente quebra a segurança de computadores. Um cracker pode fazer isso visando lucro, maliciosamente ou para alguma finalidade ou causa altruísta, ou porque o desafio está lá. Algumas invasões têm sido realizadas para demonstrar pontos fracos no sistema de segurança de um site'. (PRADO apud CUNHA, 2018, p.268)

Prado (apud CUNHA, 2018) também explica o termo *hacker*, que nem sempre deverá ser uma pessoa má intencionada. Para Prado, o termo serve para se referir a alguém que seja expert em informática, ou ainda, alguém cujo conhecimento da linguagem de programação seja profundo, cujo objeto de estudo seja a parte mais ínfima dos "sistemas operacionais", bem como trabalha para descobrir caminhos por "códigos de acesso a outros computadores".

Os crimes contra a honra são os mais comuns na plataforma digital são três: Calúnia art. 138, Difamação art. 139 e Injúria art. 140. A Lei nº 12.737/2012, que dispõe sobre a tipificação criminal de delitos informáticos, é uma espécie de primeiro instante da consagração da tipificação do delito no meio virtual. O diploma acrescentou ao Código Penal de 1940 os Arts. 154-A e 154-B, também trouxe nova redação dos artigos 266 e 298 do mesmo Código.

A nova redação dos artigos atentou para a segurança dos sigilos, como trata a Seção IV, do Capítulo VI dos Crimes Contra a Liberdade Individual, mais especificamente dos crimes contra a inviolabilidade dos segredos.

Foi inserido o título sobre a Invasão de dispositivo informático, artigo 154-A, onde se lê nos seus preceitos primário e secundário

> 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: (Incluído pela Lei nº 12.737, de 2012) Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. (CÓDIGO PENAL, 1940)

A norma incriminadora descreve como fato criminoso invadir dispositivo “informático” como computador, celular ou outro dispositivo conectado à rede mundial de computadores ou não, com o intuito de obter, modificar maldosamente ou destruir dados ou qualquer tipo de informação, sem qualquer autorização do titular dos dados. Também tornou crime a prática de instalação de aplicativo que torne vulnerável a segurança dos dados contidos no aparelho. Neste aspecto ficou em aberta a questão dos arquivos chamados de nuvens, já que, interpretativamente, os dados não necessariamente estariam em um dispositivo físico, mas em uma central de informações, essa sim física, distante do usuário.

A norma legal também disciplinou a forma de representação da ação penal, que antes poderia ser por qualquer pessoa, agora se torna personalíssima a ação penal, em seu estágio inicial, com tratamento diferenciado para os crimes contra a Administração Pública, a qual não precisa de representação.

A lei também trouxe de forma análogo ao documento particular o cartão de crédito ou débito, para os devidos fins legais de proteção de dados.

Para CUNHA (2018) o crime nos casos cibernéticos tem como objeto jurídico, ou bem a ser tutelado, a privacidade individual, seja profissional ou não, que esteja mantida em dispositivo informático, como o próprio penalista assevera, a defesa do bem tutelado em expresso na lei, tem cunho Constitucional, com fulcro no art. 5º, X, CF/88, ao rezar que “são invioláveis a intimidade a vida, privada, a honra e a imagem das pessoas, assegurando o direito de indenização pelo dano material ou moral decorrente de sua violação”.

Cunha ecoa o pensamento do penalista Guilherme Nucci, quando expõe a larga utilização dos meios cibernéticos como forma de comunicação, presente na sociedade moderna. Nas palavras de Nucci

> Sabe-se, por certo, constituir a comunicação telemática o atual meio mais difundido de transmissão de mensagens de toda a ordem entre as pessoas físicas e jurídicas. O e-mail tornou-se uma forma padrão de enviar informes e mensagens profissionais das mais diversas possíveis. As redes sociais criaram, também, mecanismos de comunicação, com dispositivos próprios de transmissão de mensagens. Tonar-se cada vez mais rara a utilização de cartas e outras bases físicas, suportando escritos, para a comunicação de dados e informes. Diante disso, criou-se novel figura típica incriminadora, buscando punir quem viole não apenas a comunicação telemática, mas também os dispositivos informáticos, que mantém

> dados relevantes do seu proprietário. (NUCCI apud CUNHA, 2018, p.268)

Acompanhando o raciocínio de Nucci, há que se destacar sempre a relevância do tema cibernético, haja vista a substituição aos poucos de meios físicos de expressão de pensamento, opiniões, dados, em fim, de todo conteúdo de comunicação, esse é o real motivo da segurança revelada na legislação.

A lei chamada de Antiterrorismo, sancionada em 2016, de número 13.260 também tratou da questão de sigilo, bem como sua pesada penalidade em casos de desobediência legal. Assim ensina Rogério Sanches Cunha,

> ... o art. 2º, §1º, inciso IV, da Lei nº 13.260/16 pune com reclusão de doze a trinta anos a conduta de sabotar o funcionamento ou apoderar-se, com violência, grave ameaça a pessoa ou servindo-se de mecanismos cibernéticos (grifo nosso), do controle total ou parcial, ainda que de modo temporários , de meio de comunicação se o fato é cometido por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, com a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública. (CUNHA, 2018, p. 258)

O exposto por Cunha explicita a severidade do ato delituoso, de sorte que, os meios cibernéticos também são locais de produção de crimes hediondos, visto que o terrorismo tem esse teor. O legislador, portanto, traz a prática delitiva para o campo cibernético para inibir a conexão de casos criminosos ou sua extensão para esse ambiente.

O crime citado por Cunha tem conexão com o crime tipificado no Art. 151 do Código Penal, já que ambos tratam da inviolabilidade da correspondência, no primeiro momento da lei, a correspondência física, agora, por meio virtual.

Cunha (2018) esboça crítica ao dispositivo legal, quando trata da invasão, tipificando como crime, mas fica em silêncio quanto ao conteúdo da informação. Para ele, apenas a conduta descrita é a invasão, e não o fato do conhecimento das informações. Para ele “O ideal seria, diante da possibilidade de que mais de um indivíduo utilize o dispositivo informático, que a tutela recaísse expressamente no titular das informações armazenadas” (CUNHA, 2018).

O crime cibernético é analisado, de acordo com a legislação na modalidade consumada ou na tentativa, já que é um delito plurissubsistente (aquele que pode ser fragmentado em diversas condutas); por ser um crime formal, ocorre com a comissão

do agente, no momento da invasão da segurança imposta pelo sistema ou na instalação de mecanismo virtual que gere prejuízo ao mantenedor dos dados, como adulteração de dados, destruição desses, ou ainda a obtenção de informações pessoas da vítima para fins ilícitos.

Em 2018 foi sancionada pelo ex-presidente Michel Temer a Lei que posteriormente foi oficializada como a Lei Geral de Proteção de Dados Pessoais (LGPD), em 2019, pela Lei de nº 13.709, de 14 de agosto de 2018.

Segundo Pinheiro (2018) o modelo seguiu as regulamentações, principalmente, "pelo regulamento Europeu de Proteção de Dados Pessoais, também conhecido como GDPR (PINHEIRO, 2018, p,04).

O princípio dos debates sobre a proteção de dados, segundo Pinheiro (2018), se deu na União Europeia (UE), se tornou consolidada com a promulgação do documento chamado Regulamento Geral de Proteção de Dados Pessoais n.679, assevera a especialista,

> ...aprovado em 27 de abril de 2016 (GDPR) com o objetivo d abordar a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoas à livre circulação desses dados, conhecido pela expressão "free data flow". O Regulamento trouxe a previsão de dois anos de prazo de adequação, até 25 de maio de 2018, quando se iniciou a aplicação das penalidades. (PINHEIRO, 2018, p.12)

Ao passo que a proteção passou a ser regra na União Europeia, as empresas que têm acordos comerciais com os países do bloco, pressionaram os seus países para que houvesse a aprovação de lei com o mesmo teor, em caso de falta desse dispositivo, tais empresas encontrariam abarreiras econômicas. Esse fato ocasionou uma corrida para a implantação de legislação correspondente, de proteção de dados.

A referida norma regulamentou o que são considerados, para todas as normas, os dados pessoais, visto que, para todas as movimentações por meio eletrônico há que se fornecerem dados específicos.

O diploma legal também estabeleceu os cuidados que as empresas de manutenção de dados devem manter quanto ao seu arquivo digital, bem como as penalidades em casos de quebra das regras legais nacionais.

Pinheiro (2018) também faz uma análise dos pontos fundamentais da Lei Geral de Proteção de Dados, segundo ela, os pontos se encontram em dois locais da determinada Lei, como descreve

> Segundo o preâmbulo (2) e (13) do GDPR, o regulamento tem como objetivo: a) contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união econômica, para o progresso econômico e social, a consolidação e a convergência das economias no nível do mercado interno e para o bem-estar das pessoas físicas; b) assegurar um nível coerente de proteção das pessoas físicas no âmbito da União e evitar que as divergências constituam um obstáculo à livre circulação de dados pessoais no mercado interno; c) garantir a segurança jurídica e a transparência aos envolvidos no tratamento de dados pessoais, aos órgãos públicos e à sociedade como um todo; d) impor obrigações e responsabilidades iguais aos controladores e processadores, que assegurem um controle coerente do tratamento dos dados pessoais; e) possibilitar uma cooperação efetiva entre as autoridades de controle dos diferentes Estados-Membros. (PINHEIRO, 2019, p,15)

Depreende-se do exposto que a maior intenção é a de preservar a condição econômica, o livre comércio, a segurança dos dados como garantia da movimentação financeira entre os parceiros. Mesmo assim alcança o indivíduo comum em suas relações sociais. Pinheiro deixa expressos os três efeitos imediatos da legislação

> Os efeitos do GDPR são principalmente econômicos, sociais e políticos. Trata-se de apenas uma das muitas regulamentações que vão surgir nessa linha, em que se busca trazer mecanismos de controle para equilibrar as relações em um cenário de negócios digitais sem fronteiras. (PINHEIRO, 2019, p,23).

Foi criado, ao tempo da modificação da lei original número 13.709 pela Lei nº 13.853, de 2019, um órgão oficial para o acompanhamento e fiscalização do cumprimento legal, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República.

Tal órgão tem como função principal o acompanhamento de todas as regras legais, pelas empresas de armazenamento de dados. O intuito é coibir as invasões de aparelhos e sistemas de telecomunicações e via internet por “*Crackers*”, pessoas com avançado grau de conhecimento na área de programação, que trabalham para “derrubar” serviços de vigilância virtuais de grandes corporações, governos, ou apenas clonar cartões para fins ilícitos.

3. Resultados de investigações a partir da nova legislação digital

Poderiam ser utilizadas nesta pesquisa as mais variadas produções investigas, incluindo a mais famosa do Brasil, que se tornou na chamada Operação Lava Jato, todavia, foi escolhida a produção didática e publicada da operação desenvolvida pelos Procuradores da República integrantes do Grupo de Trabalho de Combate aos Crimes Cibernéticos.

No estudo sobre as investigações de crimes cibernéticos, os procuradores analisaram três fatores intrínsecos ao uso da tecnologia nas práticas criminosas, quanto aos instrumentos como o computador ou outros meios tecnológicos de armazenamento ou transmissão de dados, “que pode ser o alvo direto do criminoso; pode ser o instrumento fundamental para efetivação do ato criminoso; pode ser um valioso repositório de evidências para a investigação” (MPF, 2016, 09).

Tais informações são a base para a investigação em defesa dos interesses coletivos e/ou difusos, pois os crimes praticados são os mais variados, desde a extorsão, ao desvio bilionário de recursos públicos para empresas Off Shores.

Por serem os crimes os mais variados praticados pela Internet, o que resta ao estudo é demonstra alguns cuidados que as famílias, em especial, tenham a inserirem seus entes queridos neste universo de informações, como se verá a seguir.

No estudo produzido pelos membros do Ministério Público Federal, são expostas as condutas criminosas praticas pelos agentes contra crianças, baseada na taxonomia (natureza) dos tipos de pornografia infantil, estabelecida a partir do nível 1: o Indicativo; nível 2: Nudismo; e sucessivamente, Erotismo; Pose; Pose Erótica; Pose Erótica Explícita; Atividade Sexual Explícita; Estupro; Estupro Grotesco; Sadismo/Bestialidade (MPF, 2016, p147).

Observa-se o estágio avançado das pesquisas propostas neste viés cientifico, para determinar, no caso específico, todas as condutas ilícitas dos agentes. O estudo é baseado na visão de TAYLOR (TAYLOR, 2003 apud MPF, 2018), em estudo específico da pornografia infantil, assim traz o estudo

> Cyberbullying. O National Crime Prevention Council define cyberbullying "como quando a Internet, telefones celulares ou outros dispositivos são utilizados para enviar textos ou imagens com a intenção de ferir ou constranger outra pessoa". Abuso e exploração sexual infanto-juvenil. Este tipo de crime envolve uma série de

> condutas, demandando portanto variados (e por vezes complexos) meios de enfrentamento e prevenção, onde os resultados dependem da cooperação entre setores da sociedade civil, indústria e governos. Em [Taylor 2003] os autores sugerem uma classificação dos "tipos de pornografia infantil", partindo do grau de severidade do conteúdo publicado na rede. Reproduzimos esta classificação na tabela 2.6, com pequenas adaptações, de forma a oferecer ao leitor uma ideia do problema em questão. Jogos com conteúdo inadequado. Segundo [Kurbalija 2010, pág. 151], a lista dos 10 jogos de video-game mais populares nos principais consoles tem sido dominada por temas de violência. Nota-se de fato a popularidade de tais jogos ao se consultar fontes especializadas na Internet, como a CNET, que lista os 10 melhores / mais populares jogos nos últimos 10 anos, onde 8 envolvem violência133. Surgem ainda novos temas na indústria de jogos, explorando terrorismo, uso de drogas, sexo, roubos, assassinatos em cenas cada vez mais realistas. O impacto destes jogos no comportamento de crianças e adolescentes tem sido largamente debatido. (MPF, 2016, p.147-178)

Os comportamentos ou condutas descritas por Taylor (2003) ofereceram subsídios aos investigadores para poderem montar um arcabouço de informações, que posteriormente foram analisadas de acordo com a legislação brasileira.

As técnicas investigativas também fazem parte da produção do MPF, consta dos caminhos percorridos pelos agentes, dentro da rede mundial de computadores, anotando passa a passo as condutas de um agente que permanece no mesmo local, produzindo, mantendo ou divulgando conteúdos ilícitos.

O estudo apresenta um quadro explicativo do que é a criptografia e a estenografia, como métodos de investigação.

Essa é uma das etapas capazes de obter informações sem que os agentes percebam a infiltração de um agente, como se esses agissem disfarçados digitalmente.

Tal estudo em tela apresenta uma profundidade técnica da área da informática bastante densa, por este motivo não se encaixaria nesta análise jurídica, todavia, vê-se que, a partir da legislação brasileira vigente, seja através do Marco Civil da Internet, ou pelas novas legislações penais, os investigadores conseguem chegar ao seu destino, que é o agente criminoso.

Nos Brasil, em matéria publicada pelo site de notícias G1 (GLOBO), no dia 05 de abril de 2019, a polícia conseguiu trazer à alça da lei, 546 pessoas de todo o país, após quatro fases da ação intitulada 'Luz na Infância', após realizarem mais de mil buscas. A operação investigou casos de armazenamento, compartilhamento e produção de pornografia infantil.

É uma quantidade alarmante para todos, visto que, há pessoas de vários níveis de educação, inclusive médicos pediatras, capazes de desejarem a criança ao nascer, fato que aos olhos do homem comum, como a ciência trata, seria algo de

Tabela 3.2: Criptografia e Esteganografia

Criptografia	Esteganografia
No instante em que se tem ciência da existência da mensagem pode-se tomar a ação de interceptá-la e evitar que esta alcance o destino pretendido pelo remetente. Mesmo diante da impossibilidade de conhecer o seu conteúdo consuma-se com relativa facilidade o prejuízo da comunicação entre as partes.	A mensagem pega carona em outra completa- mente desassociada, não gera suspeita e portanto não há interceptação.

extremo desvio moral.

A matéria traz em números as prisões nas quatro fases:

> Luz na Infância 1 - Realizada em 20 de outubro de 2017, cumpriu 157 mandados de busca e apreensão. Foram presas 108 pessoas.
> Luz na Infância 2 - Realizada em 17 de maio de 2018, cumpriu 579 mandados de busca e apreensão. Foram presas 251 pessoas.
> Luz na Infância 3 - Realizada em 22 de novembro de 2018, cumpriu 110 mandados de busca e apreensão no Brasil e na Argentina. Foram presas 46 pessoas pela Polícia Civil.
> Luz na Infância 4 - Realizada em 28 de março de 2019, cumpriu 266 mandados de busca e apreensão. Foram presas 141 pessoas.(G1, 2019).

A divulgação de casos mostra a celeridade em que a tecnologia criminal/investigativa alcança na segurança pública do país. Mesmo assim, ainda há preocupação dos casos que se escodem na chamada *deepweb* (plataforma digital profunda), tais casos já é sabido que, sãos os mais aterrorizantes, visto ser um ambiente com facilidades para desfazer rastros, caminhos e esconder informações.

Todos precisam se atentar para a segurança em especial, da família e seus membros que estão expostos a este ambiente digital, como já dito em alguns momentos da pesquisa.

3.1. Mecanismos minimizadores de impactos negativos no uso da internet

Após serem concluídas as investigações, os procuradores federais tornam públicas as informações de quantas pessoas são presas, na tentativa de alertar a sociedade para o perigo ao qual está exposta. Dessa forma, são expostas várias formas de auxiliar na prevenção contra crimes virtuais.

A par das combinações legais expostas, é imprescindível que os pais ou responsáveis por crianças, até mesmo idosos, se habilitem no cuidado de informações disponibilizadas na plataforma digital.

Para a segurança de todos, há sites que trazem um rol de orientações que devem ser consideradas, neste ambiente. A primeira delas é aprender sobre o universo virtual. É nesse universo que ocorrem todas as formas de interação virtual, sejam transferências financeiras, comunicação via e-mail, site de compras está na plataforma, bem como outras atividades que dependam de um suporte para a comunicação.

Outro importante cuidado a ser tomado é acerca das senhas. Este dispositivo de segurança não deve ser compartilhado, nem permanecer sem ser trocado durante muito tempo. Visto que, os *crackers* desenvolvem mecanismos

atualizados em todo o momento, capaz de colher essas informações dos aparelhos conectados à rede.

A instalação de Softwares desconhecidos ou de fonte não segura, também é um ponto forte para os mal-intencionados usuários da rede, pois esses dispositivos podem trazer acoplado outro software capaz de “sugar” informações e enviá-las para quem as criou, ou ainda, facilitar a entrada de outros “vírus” que farão esse serviço.

A orientação é sempre para se manter alertar sobre links desconhecidos, superpromoções na internet, que podem trazer vários *malwares*, que são os que abrem a porta digital para outros vírus entrarem em seu aparelho. A atualização de antivírus é uma importante arma contra invasões, já que, todos os invasores concorrem para estarem no computador e observar a conduta do usuário, além de dados sigilosos.

Hoje é possível verificar a segurança do site que está em acesso, a empresa Google fornece a possibilidade de certificação de segurança aos sites., funciona desta forma, no momento em que o próprio servidor, percebe o perigo no acesso a determinado site, o site indica uma informação de perigo, no mesmo momento, o antivírus instalado dá um sinal de alerta ao usuário do sistema.

Os especialistas em segurança apontam que os sites apresentam um ícone com a figura de cadeado, para indicar que aquele site utilizado é seguro e não trará problema.

Para utilizar o sistema, é recomendado aos pais, instalarem aplicativos que limitam o acesso às informações buscadas, tais aplicativos são oferecidos de forma gratuita ou vendidos nas plataformas digitais.

Outros aplicativos avisam os responsáveis sobre a busca de sites perigosos, o que dá tempo de prevenir os ataques de *crackers*.

Esses são alguns dos itens de segurança oferecidos pelos especialistas, para uso doméstico da rede digital.

CONCLUSÃO

Por fim, este trabalho segue a linha da necessidade da discussão permanente sobre o reflexo social nas redes sociais, tanto nas práticas comuns, como na manifestação criminosa, bem como sua reprimenda penal.

Este artigo demonstrou que existe uma esteira de análises da sociedade, cuja prática de relacionamento se vê imersa na *cybercultura*, mesmo que, ainda no primeiro estágio, aficionada ao novo, ao moderno, assim, notou-se que há um campo muito extenso para se analisar, desde as relações sociais impostas pela nova regra social, o que não foi o objeto de estudo, mesmo assim, houve a necessidade de avaliar pelo menos em termos gerais.

No primeiro momento se apontou como a sociedade se vê diante da extensão de suas atividades relacionais para um meio digital, qual o reflexo que se percebe nas redes sociais, a facilidade de transmissão de dados, bem como o encontro de grupos semelhantes em ideias, ideais, gostos, opiniões ou até mesmo divergências.

Em seguida, foi explorado o contexto histórico da criação da internet, com suas primeiras funções, cujo aspecto de transmissão segura de dados foi o primeiro ideal no universo militar. Logo após se estende para o mundo acadêmico, instante em que se conectaram computadores de ONGs, no experimento, fato que marcou a participação do Brasil.

Ao “desembarcar” no Brasil, viu-se que a rede mundial de computadores foi explorada largamente sem qualquer tipo de controle, tanto ético, moral ou penal. Vindo o marco Civil Regulatório no ano de 2012, o legislador formalizou os parâmetros que seriam a partir daquele momento, analisados no âmbito do mundo digital.

Com a quantidade de casos de exposição de intimidade nos meios digitais, houvesse a necessidade de se incluir no Código Penal condutas que passariam a ser tipificadas como criminosas, o que ocorreu em 2014.

Logo a seguir, o país foi impulsionado pelas potências econômicas mundiais, a enrijecer as regras em relação aos dados transmitidos em relações comerciais. Com a Lei Geral de Proteção de Dados Pessoais, sancionada em 2018 e modificada em 2019, tal legislação reflete as exigências de proteção para a continuidade do comércio entre o país e a União Europeia, por exemplo.

Na prática, a legislação brasileira favoreceu a investigação de diversos crimes cibernéticos, um deles serviu para exposição deste artigo, contribuindo para o arcabouço teórico. A produção do material pelo Ministério Público Federal de São Paulo, mostra como é possível o acompanhamento dos crimes cibernéticos, mesmo que sejam utilizados dispositivos avançados de camuflagem.

Neste aspecto, foi demonstrado o avanço dos aparatos técnicos para as investigações criminais no país, sem colocar em risco à intimidade da vítima ou de dados essenciais de segurança nacional.

Percebeu-se ao longo de toda a pesquisa, a que há uma falsa ideia de manutenção de sigilo entre as pessoas comuns, ao acessarem um computador ou um aparelho conectado ou não ao sistema mundial de computadores.

Nesse aspecto a pesquisa pode oferecer caminhos de segurança práticos, os quais podem ser utilizados pelas pessoas com poucos conhecimentos de informática. Tal informação se tornou imprescindível para todos os usuários da internet.

Restou demonstrado que, por consequência à falta de observância nos preceitos mais elementares de segurança em uma pesquisa virtual, as pessoas podem sofrer severos ataques de *crackers*, tendo suas senhas furtadas, além de dados bancários expostos e de fácil acesso aos maus intencionados. Não são poucos os casos em que a vítima perde sua capacidade de estorno de valores, por causa de compras que efetuaram em seu nome, com a senha inclusive, ou apenas pelo código de segurança que está no verso do cartão de crédito ou débito.

O crime praticado através de um computador é plenamente passível de se resolver, tornou o trabalho investigativo, menos físico e mais virtual, interpretativo e consequentemente, mais profícuo, já que as provas já estão disponíveis e ao seu alcance.

Infere-se das propostas legais que, o Brasil está no caminho para a consolidação de uma legislação eficiente, mesmo assim, falta um longo percurso para alcançar a diminuição da criminalidade pelos meios digitais.

Há ainda poucas leis, mesmo que eficientes até agora, para conter a propagação de graves crimes como o da pedofilia, extorsão e ainda mais, de lavagem de dinheiro. O que não foi objeto dessa análise, mas que está inteiramente ligado ao processo criminoso, a utilização de mecanismos de criptomoedas, para lavarem o dinheiro ilícito, é um dos graves problemas que a legislação brasileira enfrentará. O trabalho percorreu o caminho da legislação nacional produzida para demonstrar os subsídios jurídicos existentes.

Concluiu-se que as famílias estão com uma arma de destruição de grande proporção nas mãos, que tanto podem ser utilizadas para atacar os inimigos externos,

quanto para aproximá-los de seus entes queridos. Por isso tão importante quanto falar sobre o reflexo social nas páginas da internet, quanto à legislação regulamentadora desse uso e as investigações de crimes virtuais, é a preparação de uma sociedade capaz de distinguir o lugar onde avança.

Por último, o mais importante deste artigo foi tentar desvendar a realidade por trás do mundo virtual, para proteção da sociedade.

REFERÊNCIAS

ASSIS, Camilla de. **Confira 10 importantes dicas de segurança na internet**. Disponível em: <https://www.uninassau.edu.br/noticias/confira-10-importantes-dicas-de-seguranca-na-internet>. Acesso em: 20 mar. 2020.

BRASIL. Conselho Nacional de Justiça. **Crimes digitais: o que são, como denunciar e quais leis tipificam como crime?** Disponível em:<https://www.cnj.jus.br/crimes-digitais-o-que-sao-como-denunciar-e-quais-leis-tipificam-como-crime/> Acesso em: 23 mar. 2020

_____. 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. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 30 nov 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 15 fev. 2020.

_____. Lei nº 13.441, de 8 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: 15 fev. 2020.

_____. Lei Nº 13.709, DE 14 DE AGOSTO DE 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei nº 13.853, de 2019) Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm#art60>. Acesso em: 21 mar. 2020.

_____. Ministério Público Federal. **Roteiro de atuação: crimes cibernéticos / 2. Câmara de coordenação e revisão**. – 3.ed. rev. e ampl. – Brasília: MPF, 2016. Disponível em: < http://www.mpsp.mp.br/portal/page/portal/Escola_Superior/Biblioteca/Biblioteca_Virtual/Livros_Digitais/MPF%203186_Crimes_Ciberneticos_2016.pdf>. Acesso em: 15 fev. 2020.

CHOMSKY, Noam. **A ciência da linguagem:** conversas com James McGilvray. 1ª ed.. São Paulo: Editora Unesp, 2014.

CUNHA, Rogério Sanches. **Manual de Direito Penal**: parte especial. 10ª ed., rev., ampl. e atual. Salvador: JUSPODIVM, 2018.

FORTES, Vinícius Borges ; BOLESINA, Iuri (Org.) ; CELLA, J. R. (Org.). **Ciberdireito e democracia:** perspectivas contemporâneas do ciberespaço, da privacidade e da surveillance. 1. ed. Erechim: Deviant, 2015. v. 1.

FOUCAULT, Michel. Vigiar e Punir: Nascimento da prisão. 42 ed: Petrópolis, RJ: Vozes, 2014.

GLOBO, **Em três anos, operação contra pedofilia no Brasil prende mais de 500 pessoas** Disponível em: < https://g1.globo.com/politica/noticia/2019/04/05/em-tres-anos-operacao-contra-pedofilia-no-brasil-prende-mais-de-500-pessoas.ghtml >. Acesso em: 01 abr. 2020.

GONÇALVES, Victor Hugo Pereira. Marco civil da internet comentado. 1. ed.: São Paulo: Atlas, 2017.

GUIZZO, Érico Marui: Internet, o que é, o que oferece, como conectar-se. 1ª ed.: São Paulo: Editora Ática, 1999.

KUMMER, Fabiano R. **Direito Penal na Sociedade da Informação**, 1ª ed.: Paraná: Edição do Autor, 2017. Dispositivo KINDLE.

LÉVY, Pierre. **Cibercultura.** Tradução: Carlos Irineu da Costa. 1°. Ed. São Paulo:Editora 34. 1999. Disponível em: < https://books.google.com.br/books?hl=ptBR&lr=&id=7L29Np0d2YcC&oi=fnd&pg=PA11&dq=Cibercultura+LEVY+PIERRE&ots=gjXzAAXDdm&sig=xcokI0qZWDI3qbd7CDL6hswEmBA#v=onepage&q=Cibercultura%20LEVY%20PIERRE&f=false>. Acesso em: 20 mar. 2020.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais:** comentários à Lei n.13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.