THIAGO LEITE COSTA FARIAS

VIOLAÇÃO DE PRIVACIDADE DIGITAL:

O DIREITO À PRIVACIDADE E A TECNOLOGIA

São Paulo - SP
2022

THIAGO LEITE COSTA FARIAS

VIOLAÇÃO DE PRIVACIDADE DIGITAL:

O DIREITO À PRIVACIDADE E A TECNOLOGIA

Trabalho de conclusão de curso apresentado a Universidade Anhanguera; Unidade Belenzinho São Paulo – SP, como requisito parcial para a obtenção do título de graduado em Direito

Orientação: Carina Kamei

São Paulo
2022

THIAGO LEITE COSTA FARIAS

VIOLAÇÃO DE PRIVACIDADE DIGITAL:
O DIREITO À PRIVACIDADE E A TECNOLOGIA

Trabalho de Conclusão de Curso apresentado à Universidade Anhanguera, como requisito parcial para a obtenção do título de graduado em Direito

BANCA EXAMINADORA

Prof(a). Titulação Nome do Professor(a)

Prof(a). Titulação Nome do Professor(a)

Prof(a). Titulação Nome do Professor(a)

São Paulo, 05 junho de 2022

Dedico este trabalho de conclusão a minha tão saudosa e amada avó Maria Leite da Costa, sei que aí do céu deve estar orgulhosa!...

AGRADECIMENTOS

Agradeço a minha mãe, sem ela nada seria possível; ao meu tão presente e atencioso pai: Saudades meu velho.

Ao meu tio André por todos aqueles cursinhos e passagens de ônibus que você pagou pra mim, jamais serão esquecidos, fora o mega tio que você é! E a Deus, sem Ele, não há nada, tudo é dEle.

A justiça não consiste em ser neutro entre o certo e o errado, mas em descobrir o certo e sustentá-lo, onde quer que ele se encontre, contra o errado.

Theodore Roosevelt

FARIAS, Thiago Leite Costa Farias. **Violação de privacidade digital:** O direito à privacidade e a tecnologia. 2022. 35 folhas. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Anhanguera, São Paulo, 2022.

RESUMO

A tecnologia passou nas últimas décadas da imagem de futuro para uma realidade cada vez mais presente. O que se vê nas ruas constantemente são pessoas falando ao telefone, enviando mensagens, tirando fotos, ou até assistindo a filmes, de uma maneira tão natural como qualquer outra atividade do ser humano. Essa facilidade, no entanto, também se tornou uma porta aberta para os chamados crimes virtuais, sem que a legislação brasileira esteja completamente pronta e adaptada a esta nova realidade. O presente trabalho traz as nuances sobre o tema de crimes virtuais, dando enfoque especial à corrida paralela da legislação para alcançar a evolução da tecnologia. A questão problema analisada busca investigar quais os procedimentos legais para impedir a violação de privacidade digital, através do objetivo geral de analisar, sob a luz do Direito, quais as proteções à privacidade da pessoa humana. Para compor os capítulos partiu-se dos objetivos específicos, sendo que no primeiro capitulo buscou-se analisar as mudanças na sociedade aliadas à tecnologia que possibilitaram a problemática da violação de privacidade digital; no segundo capitulo buscou-se compreender o conceito de privacidade e intimidade, assim como os dispositivos que os protegem; e no terceiro capitulo buscou-se explorar os instrumentos legais que classificam tais violações como crimes virtuais. Embora a velocidade da tecnologia e do Direito ainda seja um verdadeiro abismo, o ordenamento já conta com matérias específicas, além de complementos no Código Penal, tipificando os crimes virtuais.

Palavras-chave: Crimes Virtuais; Crimes Cibernéticos; Violação da Privacidade; Direito à Privacidade; Direito à Intimidade.

FARIAS, Thiago Leite Costa Farias. **Digital privacy breach:** The right to privacy and technology. 2022. 35 folhas. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Anhanguera, São Paulo, 2022.

ABSTRACT

In recent decades, technology has moved from an image of the future to an increasingly present reality. What you see on the streets constantly are people talking on the phone, sending messages, taking pictures, or even watching movies, in a way as natural as any other human activity. This facility, however, has also become an open door for the so-called virtual crimes, without the Brazilian legislation being completely ready and adapted to this new reality. The present work brings the nuances on the topic of cyber crimes, giving special focus to the parallel race of legislation to achieve the evolution of technology. The problem question analyzed seeks to investigate which legal procedures to prevent the violation of digital privacy, through the general objective of analyzing, under the light of law, which are the protections for the privacy of the human person. In order to compose the chapters, it started with the specific objectives, and in the first chapter we sought to analyze the changes in society allied to technology that made possible the problem of violation of digital privacy; the second chapter sought to understand the concept of privacy and intimacy, as well as the devices that protect them; and the third chapter sought to explore the legal instruments that classify such violations as virtual crimes. Although the speed of technology and law is still a real abyss, the legal system already has specific matters, in addition to complements in the Penal Code, typifying virtual crimes.

Keywords**:** Virtual Crimes; Cyber Crimes; Breach of Privacy; Right to Privacy; Right to Intimacy.

LISTA DE ABREVIATURAS E SIGLAS

LGPD	Lei Geral de Proteção de Dados Pessoais
WWW	World Wide Web

SUMÁRIO

1. INTRODUÇÃO

A tecnologia passou nas últimas décadas da imagem de futuro para uma realidade cada vez mais presente. O que se vê nas ruas constantemente são pessoas falando ao telefone, enviando mensagens, tirando fotos, ou até assistindo a filmes, de uma maneira tão natural como qualquer outra atividade do ser humano. Essa facilidade, no entanto, também se tornou uma porta aberta para os chamados crimes virtuais, sem que a legislação brasileira esteja completamente pronta e adaptada a esta nova realidade.

É cada vez mais vulnerável o conceito de privacidade. O que até algumas décadas demandaria certo trabalho para descobrir, com relação à vida pessoal de alguém, na atualidade ocorre em segundos, e, de certa forma, com uma autorização implícita, já que o próprio sujeito posta, abertamente, detalhes de sua vida privada nas redes sociais.

Isso, no entanto, tem trazido aos Tribunais do país diversos trâmites processuais, especialmente pelo uso indevido de terceiros das informações publicadas online, o que fere o direito à intimidade do indivíduo.

O direito à privacidade, e mais especificamente, o direito à intimidade, alude à proteção da esfera privada ou íntima de uma pessoa, sendo esta abrigada contra ingerências externas, alheias e não requisitadas, e tutelada na medida em que não se permite, sem autorização do titular da informação ou dado, a sua divulgação no meio social.

Desta forma, a questão problema analisada busca investigar quais os procedimentos legais para impedir a violação de privacidade digital? Para obter a resposta, foi considerado como objetivo geral o de analisar sob a luz do Direito quais as proteções à privacidade da pessoa humana.

Para compor os capítulos partiu-se dos objetivos específicos a seguir descritos. No primeiro capitulo buscou-se analisar as mudanças na sociedade aliadas à tecnologia que possibilitaram a problemática da violação de privacidade digital; No segundo capitulo o objetivo foi o de compreender o conceito de privacidade e intimidade, assim como os dispositivos que os protegem; Já no terceiro capitulo foi o de explorar os instrumentos legais que classificam tais violações como crimes virtuais.

Utilizando a metodologia de pesquisa qualitativa, com caráter descritivo, o presente projeto se baseou nos resultados encontrados em artigos acadêmicos, documentos oficiais, jurisprudência e obras literárias, retiradas de bases de dados como SciElo, Lilacs, Jusbrasil, entre outras, com os descritores: violação de privacidade; privacidade digital; direito à intimidade, além de suas combinações. A construção do texto se deu através do método dedutivo, onde as informações são trazidas de forma a conduzir o leitor a tirar suas próprias conclusões. O tema é de relevância, atual e urgente, já que a cada dia mais crimes cibernéticos são cometidos.

2. SOCIEDADE MODERNA E A VIOLAÇÃO DE PRIVACIDADE

A tecnologia passou a ser uma constante na vida da sociedade moderna, como uma importante aliada para a interação entre os seres humanos. Seja com a finalidade de agilizar o mundo dos negócios ou de unir as famílias, independente da distância geográfica, a informática se tornou parte do cotidiano de toda a humanidade, que leva, literalmente, a tecnologia na palma da mão.

No entanto, essa mesma tecnologia sempre esteve sob o constante risco das invasões, através da figura dos hackers. Essas figuras, que sempre tem origem na interferência do homem sobre a máquina, encontraram na internet o canal perfeito para o acesso a informações antes restritas, e, portanto, mais seguras. Os ataques envolvem o roubo de senhas, assumir o controle de determinado sistema (principalmente das grandes empresas), o acesso à intimidade das pessoas e, em casos mais graves, esses ataques se transformam em um risco à vida e à intimidade, seja pela ameaça ou pela chantagem (CALHEIROS, 2015).

Para que seja possível construir o raciocínio que este texto propõe, é preciso compreender qual a dependência da sociedade a respeito da tecnologia e, até que ponto, o próprio indivíduo se torna uma presa fácil para pessoas mal intencionadas.

2.1. A VULNERABILIDADE DA INFORMAÇÃO

Enquanto o mundo via cada vez mais computadores assumirem funções antes exclusivamente humanas, o Brasil teve contato com a informática (informação automática) somente na década de 1970, com o especial trabalho desenvolvido nas universidades. A USP (Universidade de São Paulo) criou em 1972 o primeiro computador nacional, apelidado de ‘Patinho Feio’ (PCS, s/d), sendo seguida pela PUC (Pontifícia Universidade Católica) do Rio de Janeiro, onde, já sob encomenda, iniciou o desenvolvimento de sistemas para a Marinha de Guerra, que buscava automatizar seu sistema de nacionalização de eletrônica de bordo.

Apesar de iniciar sua jornada no Brasil de forma tímida, na década seguinte (anos 80) a informática já atingia crescimento de 30% ao ano, multiplicando-se, e, principalmente, saindo das empresas, iniciando sua incursão também nas residências.

Limitada a uns poucos que podiam investir valores altos nos equipamentos, que tinham poucas funções para sua utilização residencial, a informática exigiu, então, mais de seus desenvolvedores. Qual seria o objetivo de ter um equipamento em casa que fosse caro, pesado e limitado em suas funções.

Em resposta a essa demanda, algumas importantes empresas voltaram seus olhos à informática, incluindo as famosas Xerox, Hewlett-Packard, Microsoft, IBM e Apple. Essas empresas foram responsáveis pela criação de sistemas amigáveis ao ser humano, que já utilizavam interfaces gráficas, teclado, mouse, e, posteriormente, cores e movimentos (ZAMBARDA, 2013).

Na metade da década de 1980 veio o maior passo no sentido de tornar o computador, e seus sucessores, o sucesso de tecnologia que se acompanha na atualidade. É criada a World Wide Web (www), que garantiria a conectividade dos computadores, dando sentido às máquinas que até então funcionavam de forma isolada, sem acesso entre um equipamento e outro.

A década de 1990 foi marcada pela então chamada *internet*, que garantia ao usuário de computadores pessoais e às empresas as mesmas possibilidades no que se referia à pesquisas, acesso à informação, conectividade com o restante do mundo e, mesmo sem ter ideia do risco, disponibilização de dados e informações pessoais na rede.

Os *chats* se tornaram famosos nessa época, por possibilitar as conversas em ambiente virtual, além dos e-mails, sites de busca (Cade.com e Google.com são exemplos), além de download de arquivos disponibilizados pelos usuários e empresas.

Estava aberto o precedente que iria culminar nos riscos de acesso à privacidade visto na década atual. Nas palavras de Lins (2013):

> É comum ver pessoas teclando, tirando selfies ou falando ao telefone em público, sem qualquer cuidado com a privacidade. Abrigam-se em uma suposta redoma de cristal vinda do telefone, que as protegeria de qualquer indiscrição. Pura ilusão (LINS, 2013, p. 21).

O maior destaque no que diz respeito à disponibilização de informações é, sem dúvida, o Google, que conseguiu nas últimas décadas unificar informações e dados coletados dos usuários em uma plataforma única, que tinha como ideia inicial a de tornar fácil e acessível qualquer tipo de informação por parte do usuário. No entanto, essa mesma facilidade se estende continuamente aos chamados *hackers*,

que conseguem através de acessos burlados, acessar às informações pessoais dos usuários, não só da plataforma da Google, mas como de qualquer outra.

Para o campo do Direito, toda essa evolução ainda era uma realidade muito distante, não existindo até duas décadas atrás nenhum modelo de dispositivo que garantisse ao usuário o direito de não ter suas informações invadidas, furtadas ou utilizadas por terceiros.

Atualmente ainda existe o processo de 'correr atrás da solução' na relação entre a inovação tecnológica e o Direito. Nas palavras de Rodotà apud Doneda (2000, p. 120):

> Tem-se a sensação que cresce a distância entre o mundo velocíssimo da inovação tecnológicas e o mundo lentíssimo da proteção sócio constitucional. Quase a todo momento percebe-se a rápida obsolescência das soluções reguladoras de um determinado fenômeno técnico, destinadas à solução de um problema apenas (RODOTÀ apud DONEDA, 2000, p. 120).

Não se pretende, aqui, incutir a culpabilidade dos crimes na internet. Tem-se total ciência de que crimes como a pedofilia, o racismo, o abuso sexual e tantos outros encontravam meios para se reproduzir em uma sociedade 'analógica', por assim dizer. No entanto, essa evolução no que diz respeito ao acesso de informações alheias veio somente para facilitar esse tipo de ilegalidade.

A chegada das redes sociais trouxe à sociedade um fenômeno identificado como uma invisibilidade fictícia. Tanto quem disponibiliza a informação como quem recebe, tem a falsa sensação de que determinada informação ou não é importante ao ponto de ser utilizada como arma, ou que ninguém realmente faria isso. No entanto, isso ocorre, e é caracterizado no Direito como cibercrime.

Especificamente no Brasil, os crimes virtuais mais cometidos são aqueles que, especialmente, extraem informações do usuário, ou utilizam a própria imagem desse usuário para expô-lo. Segundo Pozzebom (2015), esses crimes incluem calúnia e difamação, insultos, divulgação de material íntimo com acréscimo de chantagem, clonagem de cartões, além dos tão vistos crimes de ódio contra negros, mulheres, população LGBT e, recentemente, escolha política (MOGNON, 2016).

É importante aqui traçar uma linha que, mesmo tênue, é relevante ao que se propõe. Diferente dos vírus, que acessavam (e ainda o fazem) os computadores dos usuários para roubar informações bancárias e dados pessoais, a facilidade da tecnologia na atualidade, com os smartphones, vê um diferencial importante: em muitos casos, os usuários inserem em redes sociais fotos pessoais, opiniões

pessoais e outros fatos individuais. Ou seja, o que antes era trabalhoso para qualquer hacker conseguir, hoje está à mão de quem quiser utilizar. No caminho oposto da prevenção, usuários facilitam o ataque à sua privacidade.

É, portanto, de se esperar que as figuras públicas tenham uma maior visibilidade no que se refere à sua imagem, que realmente é seu objetivo. No entanto, a visibilidade dessas figuras associada à facilidade do acesso às informações por pessoas mal-intencionadas, tem gerado inúmeros processos judiciais, mas somente quando o autor do crime pode ser identificado.

Impressionante, mas até o ano de 2012, o ato de invadir computadores e retirar informações pessoais de outros usuários, não era considerado um crime pelo Código Penal brasileiro. A alteração, vinda em grande parte pelo apelo da mídia, aconteceu após o caso ocorrido em 2011 com a atriz Carolina Dieckmann, que teve seu computador invadido após clicar em um e-mail falso. Esse clique possibilitou aos invasores a cópia de fotos íntimas da atriz. A partir de então, o contato feito com Carolina exigia o pagamento de dez mil reais, como forma de não ter suas fotos íntimas divulgadas. A atriz imediatamente procurou pela polícia, realizando a denúncia, e expondo um problema que não era exclusivo às celebridades, mas que só teve voz na política nacional a partir da denúncia de uma atriz global.

2.2. CRIMES CIBERNÉTICOS

A evolução tecnológica é o fenômeno que alcança todos com quem convive. Cada ser humano se adapta às inovações digitais, de tal forma, que atualmente é difícil encontrar alguém que não tenha na bolsa um smartphone conectado à internet, que não realize pesquisa, acesse mapas ou tire fotos enquanto caminha nas ruas.

Segundo Talamone (2017):

> Estar conectado à internet é uma necessidade para a maioria das pessoas na sociedade atual. A tecnologia influencia tantos aspectos da vida cotidiana que chega até mesmo a alterar a forma como o ser humano se relaciona (TALAMONE, 2017, n.p.).

Essa necessidade de acesso constante, gerou uma adaptação na vida das pessoas, o que ocorre também com o mundo do crime. A evolução dos criminosos

nas últimas décadas se voltou às informações disponibilizadas em rede, e ganharam uma nova roupagem, extrapolando o que ocorria nas décadas passadas, especialmente a espionagem e sabotagem de sistemas comerciais, para uma aplicação mais focada, atingindo usuários comuns através do roubo de senhas, pornografia, inclusive infantil, crimes de ódio, como racismo e discriminação sexual, abuso sexual e muitos outros. A estes crimes, especialmente cometidos de forma remota (através da internet) é dado o nome de Crimes Virtuais ou Crimes Cibernéticos (RODRIGUES, 2017).

Para uma melhor compreensão, serão utilizadas as palavras de Carvalho (2015):

> [...] para compreender a expressão “crime cibernético” (lato senso) temos que remeter aos conceitos da doutrina tradicional e ter em mente a acepção de crime como o fato típico, antijurídico e culpável, que pode ser analisado (...) sob os aspectos: material, como todo fato humano que, propositada ou descuidadamente, lesa ou expõe a perigo bens jurídicos considerados fundamentais para a existência da coletividade da paz social. E, formal, onde o crime resulta da mera subsunção da conduta ao tipo legal e, portanto, considera-se infração penal tudo aquilo que o legislador descrever como tal, pouco importando o seu conteúdo (CARVALHO, 2015, n.p.).

O autor ainda aponta para uma definição mais simplória, quando remete “toda conduta humana ilícita, de acordo com o ordenamento jurídico de um estado, realizada por meio ou contra um recurso tecnológico” (CARVALHO, 2015, n.p.).

A definição da terminologia, tão importante para o meio jurídico, envolve a conduta inapropriada, que cause malefício a alguém, desde que, para tanto, sejam utilizados meios tecnológicos no processo. Essa abrangência da terminologia é, ao mesmo tempo, uma vantagem e uma desvantagem. Se apresenta como vantagem por aceitar múltiplas interpretações, exata razão pela qual também é desvantagem.

Os crimes cibernéticos ou crimes virtuais trazem em sua característica uma especificidade, que é a invasão/violação da privacidade e intimidade do indivíduo, o que é garantido pelo ordenamento pátrio. Essa invasão se dá, tanto na retirada ou cópia das informações do usuário, quanto na divulgação realizada (transmissão de informação a terceiros) desse material. Essa violação também se dá quando os dados acessados são de alguma forma destruídos, o que acarreta prejuízo moral e material à vítima do crime virtual (SOUZA, 2015).

Otoboni e Almeida também contribuem com sua definição, mais ampla, dos crimes virtuais:

> Crimes Cibernéticos, também conhecidos como ciber crimes, crimes eletrônicos, crimes informáticos, etc., são aquelas condutas ilegais praticadas por criminosos através de qualquer equipamento eletrônico (computador, celular, notebook, etc.) com o intuito de produzir, oferecer, distribuir, vender ou difundir dispositivo ou programa de computador com o intuito de permitir a prática da conduta criminosa citada, como previsto no § 1º do Art. 154-A do Código Penal Brasileiro. Isto é, qualquer obtenção, adulteração ou destruição das informações pessoais dos usuários sem o seu livre consentimento, enseja sobre o cometimento do principal propósito desses criminosos (OTOBONI; ALMEIDA, 2019, n.p.).

Entende-se, portanto, que a própria definição do crime ainda é algo vago para o Direito Brasileiro, carecendo de maior experiência (vivência) para a correta classificação, tipificação e posterior julgamento. O que existe na atualidade são casos isolados de denúncias, geralmente relacionadas à prejuízos financeiros, quando é possível identificar o autor, que são tratados pelo magistrado como caso único, individual, como é possível exemplificar pela decisão do Desembargador Federal Néviton Guedes:

> PENAL. FURTO QUALIFICADO. FRAUDE NA INTERNET. CRIME VIRTUAL. TRANSFERÊNCIA BANCÁRIA ELETRÔNICA. CLIENTE DA CEF. SAQUE DO PRODUTO DO FURTO POR MEIO DE CONTA DE TERCEIROS. MATERIALIDADE COMPROVADA. AUTORIA NÃO COMPROVADA DE FORMA CABAL. SENTENÇA ABSOLUTÓRIA MANTIDA. 1. O Ministério Público Federal interpôs apelação contra sentença que absolveu o réu da imputação do crime tipificado no art. 155, § 4º, II e IV, c/c art. 29 do Código Penal, sob o fundamento de ausência de prova de que réu seja o autor do crime de furto (CPP, art. 386, V) por meio de fraude na Internet. 2. Está comprovada nos autos a materialidade do delito de furto qualificado por meio da comunicação feita pela Caixa Econômica Federal à Polícia Federal de transferência eletrônica fraudulenta de valores subtraídos da conta bancária da vítima, cliente do banco, creditados na conta de outra cliente, que denunciou a fraude à Polícia Federal, bem como pelo Auto de Apresentação e Apreensão de R$ 1.000,00 (um mil reais) em espécie e um comprovante de depósito em dinheiro feito em nome do cunhado do réu no valor de R$ 600,00 (seiscentos reais), que foram encontrados em poder de coautor (Gleydson) na ocasião de sua prisão em flagrante ocorrida em 31.3.2005. 3. Não há provas da autoria do réu Roney. O réu Gleydson (que teve o processo originário desmembrado) prestou depoimento perante a autoridade policial, ratificado judicialmente, no sentido de que o apelado Roney, instrutor de informática do Serviço Nacional de Aprendizagem Industrial - SENAI em Araguaína/TO (individualização precisa) o convidou para praticar a conduta delituosa e ofereceu parte dos valores que seriam furtados, indicando, inclusive, o número de conta bancária do cunhado para receber o depósito da parte que lhe cabia. 4. O depoimento, por si só, não é suficiente para amparar a condenação do apelado, porque não foi produzida nenhuma outra prova de que Roney tenha praticado a conduta delituosa que lhe é imputada e o depósito efetivado na conta de seu cunhado (que sequer foi chamado a depor) foi justificado pelo apelante. 5. Segundo dispõe o art. 158 do Código de Processo Penal, "[q]uando a infração deixar vestígios, será indispensável o exame de corpo de delito, não podendo supri-lo a confissão do acusado." 6. No caso, tratando-se de subtração de valores da conta bancária da vítima (cliente da Caixa) por meio de fraude na Internet, conduta imputada ao réu Roney, caberia ao órgão acusador a produção de

> prova para identificação de que teria partido de seu computador o comando para transferência bancária de saldo a débito da conta da vítima e a crédito da conta de pessoa interposta, "laranja", pessoa essa que era aliciada por Gleydson apenas para fornecer a conta para receber valores e efetuar o saque, entregando o produto do crime a este último, a fim de comprovar a participação do réu Roney na prática delituosa, nos termos do art. 158 do CPP. 7. Não tendo sido produzida qualquer prova pericial que ligasse os computadores, vê-se que o depoimento do corréu Gleydson não é suficiente para amparar a condenação de Roney, quando inexiste outra prova nos autos do processo a corroborá-la, devendo ser mantida a sentença absolutória. 8. Apelação desprovida.
> (TRF-1 - APR: 00015490820054014300 0001549-08.2005.4.01.4300, Relator: DESEMBARGADOR FEDERAL NÉVITON GUEDES, Data de Julgamento: 26/09/2017, QUARTA TURMA, Data de Publicação: 13/10/2017 e-DJF1)

Nota-se, portanto, que os crimes virtuais, muito diferente do que se imagina, não são somente cometidos através de computadores pessoais, mas através de sistemas inteiros, inclusive bancários.

Nos ataques pessoais, que tem como foco afetar a honra do indivíduo, o foco não necessariamente recai sobre o fator financeiro, a menos que seja por chantagem qualificada. Para exemplificação, traz-se a decisão do Ministro Rogerio Schietti Cruz:

> CONFLITO NEGATIVO DE COMPETÊNCIA. JUÍZO ESTADUAL X JUÍZO FEDERAL. AMEAÇAS DE EX-NAMORADO A MULHER VIA FACEBOOK. MEDIDAS PROTETIVAS DE URGÊNCIA. BOLETIM DE OCORRÊNCIA PERANTE AUTORIDADE POLICIAL BRASILEIRA. PEDIDO DE MEDIDAS PROTETIVAS DE URGÊNCIA AO PODER JUDICIÁRIO BRASILEIRO. REPRESENTAÇÃO DA OFENDIDA QUE DISPENSA FORMALIDADES. AMEAÇAS REALIZADAS EM SÍTIO VIRTUAL DE FÁCIL ACESSO. SUPOSTO AUTOR DAS AMEAÇAS RESIDENTE NOS ESTADOS UNIDOS DA AMÉRICA. CRIME À DISTÂNCIA. FACEBOOK. SÍTIO VIRTUAL DE FÁCIL ACESSO. INTERNACIONALIDADE CONFIGURADA. O BRASIL É SIGNATÁRIO DE CONVENÇÕES INTERNACIONAIS DE PROTEÇÃO À MULHER. A LEI MARIA DA PENHA DÁ CONCRETUDE ÀS CONVENÇÕES INTERNACIONAIS FIRMADAS PELO BRASIL. COMPETÊNCIA DA JUSTIÇA FEDERAL. [...] 2. Segundo o art. 109, V, da Constituição Federal - CF, compete aos juízes federais processar e julgar "os crimes previstos em tratado ou convenção internacional, quando iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente." Encontrando-se o suposto autor das ameaças em território estrangeiro, uma vez que não se tem notícia do seu ingresso no país, tem-se um possível crime à distância, tendo em vista que as ameaças foram praticadas nos EUA, mas a suposta vítima teria tomado conhecimento do seu teor no Brasil. [...] 4. No caso concreto é evidente a internacionalidade das ameaças que tiveram início nos EUA e, segundo relatado, tais ameaças foram direcionadas à suposta vítima e seus amigos, por meio da rede social de grande alcance, qual seja, o Facebook. 5. Conflito conhecido, para declarar a competência do o Juízo Federal da 1ª Vara de São José dos Campos - SJ/SP, o suscitado. (CC n. 150.712/SP, Rel. Ministro JOEL ILAN PACIORNIK, 3ª S., DJe 19/10/2018, destaquei). Em termos análogos, por ocasião do julgamento do CC n. 136.700/SP, de minha relatoria, teci os seguintes comentários, em relação à competência para processar e julgar delitos cometidos na internet, verbis: Tratando-se,

> pois, de crimes contra a honra praticados pela internet, a competência deve se firmar de acordo com a regra do art. 70 do Código de Processo Penal, segundo o qual "A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução". Isso porque constituem-se crimes formais e, portanto, consumam-se no momento de sua prática, independentemente da ocorrência de resultado naturalístico (BITENCOURT, Cezar Roberto. Código Penal comentado. São Paulo: Saraiva, 2002). Assim, a simples divulgação do conteúdo supostamente ofensivo na internet já é suficiente para delimitação da competência. No caso, conforme bem destacado pela Corte estadual, a vítima forneceu o endereço residencial da Comarca de São Miguel do Oeste como sendo o local dos fatos. O fato de haver endereço comprovado, posteriormente (2019), em localidade diversa não é capaz de infirmar os danos fornecidos à época (agosto de 2017) e a conclusão em sentido diverso demandaria dilação probatória, o que é vedado em habeas corpus. No mesmo sentido, o parecer do Ministério Público Federal: Destarte, in casu, não se verifica nenhum constrangimento ilegal, pois, ao contrário do que alega a Defesa, a vítima residia em São Miguel do Oeste/SC na época em que tomou conhecimento das ameaças contra ela perpetradas para a obtenção de vantagem indevida por meio do aplicativo de troca de mensagens WhatsApp, razão pela qual não há falar em relaxamento da prisão do recorrente e em nulidade de atos decisórios por incompetência do Juízo (fl. 555, grifei). Por fim, cumpre registrar que, de acordo com as informações prestadas pelo Juízo de primeiro grau, foi proferida sentença, que condenou o ora recorrente à pena de 8 anos e 5 meses de reclusão, em regime fechado, mais multa, pela prática dos delitos descritos nos arts. 158, caput, 158, caput, c/c o art. 14, II, ambos do Código Penal. A defesa interpôs recurso de apelação e o réu ainda não foi intimado, pois estaria, supostamente encarcerado em presídio da Comarca de Lagoa Vermelha - RS. À vista do exposto, nego provimento ao recurso. Publique-se e intimem-se. Brasília (DF), 13 de abril de 2020. Ministro ROGERIO SCHIETTI CRUZ
>
> (STJ - RHC: 114556 SC 2019/0181543-1, Relator: Ministro ROGERIO SCHIETTI CRUZ, Data de Publicação: DJ 15/04/2020)

A variedade de decisões a respeito dos crimes virtuais é ampla no magistrado, mas ainda vaga e adaptada para casos específicos, geralmente considerando aspectos alheios ao Crime Virtual. Para que se compreenda a real intencionalidade, as próximas laudas explanarão a respeito do Direito à Privacidade e Intimidade, e a forma como o magistrado normalmente julga, seja em crimes virtuais ou não.

3. DIREITO À PRIVACIDADE E À INTIMIDADE

O termo direito à intimidade é considerado como tipificação dos chamados “direitos da personalidade”, que são inerentes ao próprio homem e têm por objetivo resguardar a dignidade da pessoa humana. Surgem como uma reação à teoria estatal sobre o indivíduo e encontram guarida em documentos como a Declaração dos Direitos do Homem e do Cidadão, de 1789, a Declaração Universal dos Direitos do Homem, de 1948, a 9ª Conferência Internacional Americana de 1948, a Convenção Europeia dos Direitos do Homem de 1950, a Convenção Pan-americana dos Direitos do Homem de 1959, a Conferência Nórdica sobre o Direito à Intimidade, de 1967, além de outros documentos internacionais. Esta matéria é objeto tanto da Constituição Federal de 1988 quanto do Código Civil brasileiro de 2002, o que provocou o seu tratamento mais aprofundado e amplo pela doutrina nacional.

3.1. A ESFERA PRIVADA NO ORDENAMENTO PÁTRIO

No ordenamento brasileiro, o artigo 5º, X e XII da Constituição Federal, e o artigo 21, do Código Civil, fundamentam a proteção da esfera privada de uma pessoa, referindo-se tanto à vida privada, quando à intimidade da pessoa humana. O direito à privacidade, e mais especificamente, o direito à intimidade, alude à proteção da esfera privada ou íntima de uma pessoa, sendo esta abrigada contra ingerências externas, alheias e não requisitadas, e tutelada na medida em que não se permite, sem autorização do titular da informação ou dado, a sua divulgação no meio social.

Apesar de não ter sua redação expressa na Constituição Federal, o termo “Privacidade” se encaixa como implícito no que se refere o Art. 5º, inciso X, que garante da inviolabilidade da honra, imagem, intimidade e vida privada, o que remete à privacidade em si, conforme versa:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”. (BRASIL, 1988)

A garantia supracitada é de caráter individual, sendo ampla ao exercício pelo titular, não sendo condicionado a interesse difuso. Esse direito se estende às comunicações, inclusive correspondências, conforme ressalta o inciso XII do mesmo artigo:

> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal. (BRASIL, 1988).

O impasse que possa existir a respeito da privacidade é o quanto de propriedade existe sobre a coisa. Até que ponto é coisa privada e a partir de quando passa a ser coisa pública. Há que se analisar os diversos tipos e classificações a respeito da privacidade. Dimitri Dimoulis (2014) aponta em sua obra essa necessidade de verificação:

> O seguinte questionamento revela a necessidade de verificar a eventual incontrolabilidade que impõe o exercício do dever estatal de promover a segurança: Quem levantou os dados pessoais? Para quem os passou? Quais combinações de dados estão sendo feitas? Com que objetivo? O titular do direito à intimidade, nesses casos, não pode sequer reagir, pois reagiria contra quem? Quem sabe o que sobre ele? Quando determinadas autoridades e terceiros podem prever os passos da pessoa, o direito fundamental à intimidade torna-se obsoleto. Para evitar isso, o Estado deve cumprir com seu dever de tutela por meio de legislação sobre dados pessoais. (DIMOULIS, 2014, p. 57)

Fica expressa, portanto, a gravidade a respeito do tema. Especialmente por alguns pontos prementes: a invasão de privacidade, no que se refere à internet, por exemplo, raramente vem junto à identificação do autor. Nesses casos, como se defender se, sequer existe a identificação do agressor? Ainda há que se considerar a possibilidade de, estando em posse de alguns dados, como compreender quais dados foram realmente usurpados. Para exemplificar: um hacker invade o computador de uma jovem, através de software que copia números de contas e dá acesso à páginas de bancos. Com essa informação, consegue realizar transações em seu favor. Assim que identifica o ataque, a vítima tende a procurar ajuda, no entanto, em seu computador também haviam imagens íntimas.

Como saber até que ponto, realmente, a vítima já foi prejudicada ou ainda pode ser? Nessa esteira, a legislação nacional passou a contar, a partir do ano de 2018, com a conhecida LGPD (Lei Geral de Proteção de Dados Pessoais). Já no início de sua redação, em seu art. 1º, a lei especifica:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

O documento vem, portanto, de encontro à necessidade da sociedade brasileira, mas não caminha sozinho. No ano seguinte, é realizada a Proposta de Emenda à Constituição nº 17/19 (CÂMARA, 2019), que traz como objetivo principal a inclusão como direito e garantia fundamental na Constituição Federal a proteção de dados pessoais, passando também à competência privativa da União os atos de fiscalização e deliberação.

O Código Civil (BRASIL, 2002) também ampara a privacidade do indivíduo em seu Art. 21, com a redação: “A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma”.

A ampliação do conceito de privacidade se deu, em grande medida, por conta da evolução das formas de divulgação e apreensão de dados pessoais. Com o advento de novas tecnologias, notadamente o desenvolvimento da biotecnologia e da Internet, o acesso a dados sensíveis e, consequentemente, a sua divulgação, foram facilitados de forma extrema. Como resultado, existe uma expansão das formas potenciais de violação da esfera privada, na medida em que se mostra a facilidade por meio da qual é possível o acesso não autorizado de terceiros a esses dados. Com isso, a tutela da privacidade passa a ser vista não só como o direito de não ser molestado, mas também como o direito de ter controle sobre os dados pessoais e, com isso, impedir a sua circulação indesejada.

No rol de documentos que buscam proteger tais direitos, também é possível mencionar a Lei 13.718/2018, que, além de tipificar os crimes de importunação sexual e divulgação de cena de estupro, adiciona o artigo 218-C ao Código Penal brasileiro, passando a vigorar a seguinte redação:

> Art. 218-C. 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, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia:
> Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave. Aumento de pena § 1º A pena é aumentada de 1/3 (um terço) a 2/3 (dois terços) se 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 (BRASIL, 2018).

O Direito desenvolveu, portanto, mecanismos modernos de defesa da privacidade. Esses mecanismos não seriam suficientes se considerassem somente algum tipo de punição, ou seja, uma reparação do dano. Foi preciso ir além, encontrando na proteção e controle dos dados o maior indicativo de possível eficácia da lei. A coleta de dados, seja por agentes públicos ou privados, existe, e é feita diariamente. É o que se chama de direito à autodeterminação informativa.

Nas palavras de Stinghen (2018):

> Tradicionalmente, a privacidade se protege por três instrumentos básicos. Primeiramente, tem-se o direito ao sigilo, isto é, a vedação à coleta de informações sensíveis, sem a devida justificativa. Além dele, também existe o direito de acesso, que é ter ciência dos próprios dados pessoais, pelo contato com os bancos de dados em que são armazenados. Por fim, é consagrado o uso da responsabilidade civil, para reparar danos gerados pela má utilização de informações pessoais (STINGHEN, 2018, n.p.).

No que se refere ao entendimento do magistrado, em meio à tantas novidades da seara jurídica, é possível exemplificar com a decisão do Relator Alexandre Pimentel Cruz:

> ESTADO DO RIO DE JANEIRO PODER JUDICIÁRIO Conselho Recursal dos Juizados Especiais - Segunda Turma Recursal Cível Processo nº 0075614-49.2013.8.19.0002 RECORRENTE:RAFAEL ALEXANDRE LOJA VITORINO RECORRIDOS:FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA. GOOGLE BRASIL INTERNET LTDA. APPLE COMPUTER BRASIL LTDA. VOTO EMENTA Responsabilidade civil de empresas provedoras de conteúdo de internet e de manutenção de loja virtual. Aplicativo 'Lulu' que atribui notas e dispõe de designações pré-definidas para qualificação do titular masculino de perfil público na rede social da 1ª Ré. Alegação de violação à intimidade e privacidade. Pretensão do Autor de exclusão do seu perfil no aplicativo, exclusão do sítio eletrônico e compensação por danos morais. Fatos ocorridos antes da vigência da Lei nº 12.965/14 (Marco Civil da Internet). Sentença de improcedência dos pedidos. (...) Motivo que também impede a condenação de qualquer das Rés à exclusão do perfil do Autor do aplicativo em tela, valendo salientar a existência de ferramenta na própria plataforma para atingir tal objetivo. Sentença que se prestigia. Recurso improvido. Diante do exposto, VOTO no sentido de conhecer e NEGAR PROVIMENTO ao recurso e manter a improcedência dos pedidos. Condena-se o Recorrente ao pagamento de custas processuais e honorários advocatícios arbitrados em 20% (vinte por cento) sobre o valor da causa, observado o disposto no art. 12 da Lei nº 1.060/50. Rio de Janeiro, 14 de julho de 2014. ALEXANDRE PIMENTEL CRUZ Juiz Relator Processo nº 0075614-49.2013.8.19.0002Página 1 de 2
> (TJ-RJ - RI: 00756144920138190002 RJ 0075614-49.2013.8.19.0002, Relator: ALEXANDRE PIMENTEL CRUZ, Segunda Turma Recursal, Data de Publicação: 29/08/2014 00:00)

A jurisprudência acima deixa clara a dificuldade de responsabilização dos sujeitos. O recorrente elencou em ação as empresas responsáveis pela rede social, mas, neste caso, seus dados eram públicos, por opção própria, estando liberados os acessos à qualquer um que participe da rede social. Pela impossibilidade de responsabilização à estas empresas, a causa se perdeu.

Já nos casos onde é possível identificar o autor, a decisão consegue ser mais assertiva, orientando o magistrado de quais ações podem ser tomadas no sentido de garantir os direitos fundamentais da privacidade e intimidade. Como exemplificado abaixo:

> CIVIL E PROCESSUAL CIVIL. RECURSO ESPECIAL. AGRAVO DE INSTRUMENTO. ANTECIPAÇÃO DOS EFEITOS DA TUTELA. AÇÃO DE OBRIGAÇÃO DE FAZER. RETIRADA DE CONTEÚDO ILEGAL. PREQUESTIONAMENTO. AUSÊNCIA. PROVEDOR DE PESQUISA. FILTRAGEM PRÉVIA DAS BUSCAS. IMPOSSIBILIDADE. RETIRADA DE URLS DOS RESULTADOS DE BUSCA. POSSIBILIDADE. EXPOSIÇÃO PORNOGRÁFICA NÃO CONSENTIDA. PORNOGRAFIA DE VINGANÇA. DIREITOS DE PERSONALIDADE. INTIMIDADE. PRIVACIDADE. GRAVE LESÃO. 1. Ação ajuizada em 20/11/2012. Recurso especial interposto em 08/05/2015 e distribuído a este gabinete em 25/08/2016. 2. Na hipótese, o MP/SP ajuizou ação de obrigação de fazer, em defesa de adolescente, cujo cartão de memória do telefone celular foi furtado por colega de escola, o que ocasionou a divulgação de conteúdo íntimo de caráter sexual, um vídeo feito pela jovem que estava armazenado em seu telefone. 3. É cabível o recurso especial contra acórdão proferido em agravo de instrumento em hipóteses de antecipação de efeito da tutela, especificamente para a delimitação de seu alcance frente à legislação federal. 4. (...) 7. A "exposição pornográfica não consentida", da qual a "pornografia de vingança" é uma espécie, constituiu uma grave lesão aos direitos de personalidade da pessoa exposta indevidamente, além de configurar uma grave forma de violência de gênero que deve ser combatida de forma contundente pelos meios jurídicos disponíveis. 8. A única exceção à reserva de jurisdição para a retirada de conteúdo infringente da internet, prevista na Lei 12.965/2014, está relacionada a "vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado", conforme disposto em seu art. 21 (...). Nessas circunstâncias, o provedor passa a ser subsidiariamente responsável a partir da notificação extrajudicial formulada pelo particular interessado na remoção desse conteúdo, e não a partir da ordem judicial com esse comando. 9. Na hipótese em julgamento, a adolescente foi vítima de "exposição pornográfica não consentida" e, assim, é cabível para sua proteção a ordem de exclusão de conteúdos (indicados por URL) dos resultados de pesquisas feitas pelos provedores de busca, por meio de antecipação de tutela. 10. Recurso especial parcialmente conhecido e, nessa parte, provido.
> (STJ - REsp: 1679465 SP 2016/0204216-5, Relator: Ministra NANCY ANDRIGHI, Data de Julgamento: 13/03/2018, T3 - TERCEIRA TURMA, Data de Publicação: DJe 19/03/2018)

Resta claro, à luz do que já foi exposto, que a autodeterminação sobre a própria imagem abarca o controle das informações, sensíveis ou não e de maneira antecipada, sem a necessidade de se demonstrar quaisquer danos. Nessa senda, o

consentimento é instrumento de importante relevância no que se refere à privacidade. Esse consentimento assume dupla função nas lides processuais, onde é capaz de legitimar a coleta pelos agentes públicos e privados de um lado, e de outro, a garantir a autodeterminação informacional da pessoa (STINGHEN, 2018).

Rodotà (2008) apresenta em sua obra os princípios gerais elencados para a tutela da privacidade. Entre eles aponta-se o princípio da correção e da exatidão (veracidade dos fatos), o da segurança, o da publicidade e acesso individual, e o da finalidade (destinos específicos para cada informação), princípio último este de onde se extraem os subprincípios da pertinência, da utilização não abusiva e da eliminação (os dados devem ser eliminados assim que cumprirem com sua finalidade).

No geral, portanto, o Estado, figura legítima, tem o poder de legislar a respeito das situações externas à pessoa, que gravitam ou a afetam de alguma forma, mas jamais ditar regras ou impor sanções a respeito do que lhe diz respeito em sua intimidade. Nas palavras de Stinghen (2018, n.p.) “Trata-se de um campo indevassável, que permite única e exclusivamente o acesso do titular do direito.”

A intimidade, em complemento ao conceito antes exposto de privacidade, possui embasamento também no inciso X do artigo 5º da Constituição Federal: "São invioláveis a intimidade, a vida privada , a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 1988).

Assim como a privacidade, a intimidade compõe, e é núcleo, da esfera de proteção do indivíduo. É comumente conceituada pelo ‘direito de estar só’, ou seja, são informações e situações onde somente o indivíduo em questão possui o direito de acessar. Seus pensamentos, suas ações isoladas (desde que não afetem a terceiro), um campo discreto frequentado unicamente pelo interessado.

Nas palavras de Eudes Quintino de Oliveira Júnior (2018):

> É o espaço em que vai encontrar consigo mesmo, sem qualquer acesso à curiosidade privada. Neste reino pode desfilar tudo que é mais precioso para a pessoa, desde a sua crença religiosa até os segredos mais recônditos, sem qualquer risco de invasões arbitrárias e, principalmente, de se chegar ao conhecimento público porque não há qualquer registro materializado (OLIVEIRA JUNIOR, 2018, n.p.).

A intimidade, em contrapartida à privacidade, é o conceito do que há de mais pessoal ao ser humano, e por sua característica, mais difícil de ser atingida (mas não impossível).

4. MARCO CIVIL DA INTERNET E LEIS DE CRIMES VIRTUAIS

Para que a sociedade e o ordenamento iniciassem seu caminho no sentido de compreender a tecnologia e o que poderia advir dela, uma decisão importante foi tomada, especificamente com a criação do Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014).

O início de seu esboço surgiu através do projeto de lei em 2009, mas somente foi sancionado em 2014, cinco anos após, pela então Presidente da República Dilma Rousseff. O Marco Civil da Internet tem, para a legislação brasileira, o peso de uma ‘constituição’, por regulamentar os direitos e deveres dos indivíduos, assim como a Carta Magna, porém, em nível digital (virtual).

Um de seus princípios aponta para a neutralidade na rede, ou seja, a igualdade perante todos. A rede é igual para todos, sem diferença entre indivíduos ou tipo de uso, o que garante igualdade inclusive no que se refere ao pagamento pela sua utilização.

O Marco traz também o conceito de privacidade na rede, através da inviolabilidade e sigilo das comunicações e informações. Essa garantia abre exceção somente às ordens judiciais, específicas aos fins de investigação criminal. No entanto, sua criação só ocorreu após diversos crimes cometidos, inclusive contra celebridades brasileiras, como o caso já mencionado da atriz Carolina Dieckmann. Os crimes apontados envolviam o cyberbullying, a intimidação, o assédio (de diferentes formas), a extorsão, plágios sobre obras e até mesmo a pornografia (adulta e infantil).

A principal diferença é que, antes do Marco Digital, dificilmente alguém que cometesse um crime virtual seria punido, seja pela ausência de evidências reconhecidas ou pela simples ausência de legislação para tanto, conforme art. 1º do próprio Código Penal: “Art. 1º - Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal.” (BRASIL, 1940).

Além de possibilitar a definição dos princípios referentes ao uso da internet, como a proteção da privacidade, dos dados pessoais e da liberdade de expressão, o Marco Digital também estabeleceu formas mais eficazes para identificação e responsabilização daqueles que cometem crimes pela internet, em qualquer das esferas (cível ou criminal).

Passa a ser possível, então, àquele que se sentir lesado moral ou materialmente, pleitear a reparação por seus dados. Esse pleito é realizado através da determinação ao responsável pela guarda de registros de conexão ou de acesso, formando o devido conjunto probatório, que incluirá o material ilícito produzido pelo infrator. A redação da lei exige, para tanto, os indícios da ocorrência, a justificativa da utilidade (real necessidade) da disponibilização dos registros e o período de sua ocorrência.

Um dos cuidados no que se refere aos conteúdos publicados ilegalmente em redes sociais se apresentou na determinação de que a empresa proprietária da plataforma bloqueie o perfil e forneça à justiça os dados pessoais e residenciais do usuário, elementos de sua qualificação e localização, sob pena de multa pecuniária em caso de descumprimento. Trata-se, portanto, de verdadeiro marco na luta contra os crimes virtuais, sendo inclusive desse documento que se originou a LGPD (Lei Geral de Proteção de Dados Pessoais) mencionada em capítulo anterior.

4.1. A EVOLUÇÃO LEGISLATIVA DIANTE DA TECNOLOGIA

O presente texto colocou em pauta alguns dos documentos legislativos que agora embasam as decisões judiciais no que se refere aos crimes virtuais. Assim como a própria evolução tecnológica, a legislativa também foi gradual, apesar de a velocidade entre ambas ser um abismo (CARVALHO, 2015).

Existem, no entanto, mudanças no ordenamento jurídico nacional que agora possibilitam a correta criminalização e responsabilização penal do sujeito ativo. Uma das primeiras mudanças nesse sentido foi a Lei 7.716/1989. Sua redação, voltada à definição dos crimes de preconceito de raça ou de cor, passou a considerar, através do art. 20, §2º, como qualificadora do delito a prática por intermédio dos meios de comunicação social ou publicação de qualquer natureza. Esta redação incluiu, portanto, as manifestações eletrônicas. Além disso, no §3, inc. III, conferiu também poderes ao magistrado para emitir provimento judicial de forma a realizar “a interdição das respectivas mensagens ou páginas de informação na rede mundial de computadores”.

No ano de 1990, com a promulgação do Estatuto da Criança e do Adolescente, mais uma vez o meio eletrônico foi considerado, embora não houvesse à época sequer a noção de seu alcance na atualidade. A Lei n.º 8.069/90, art. 241-A, classificou como crime contra a criança e ao adolescente a conduta de:

> [...] oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente (BRASIL, 1990a).

A este crime foi atribuída a pena de reclusão de até seis anos ao infrator. O ECA ainda equiparou os meios eletrônicos aos convencionais, em seu art. 244-B:

> Art. 244-B. Corromper ou facilitar a corrupção de menor de 18 (dezoito) anos, com ele praticando infração penal ou induzindo-o a praticá-la: (Incluído pela Lei nº 12.015, de 2009)
> Pena - reclusão, de 1 (um) a 4 (quatro) anos. (Incluído pela Lei nº 12.015, de 2009)
> § 1 o Incorre nas penas previstas no caput deste artigo quem pratica as condutas ali tipificadas utilizando-se de quaisquer meios eletrônicos, inclusive salas de bate-papo da internet (BRASIL, 1990a).

Já no que se refere à ordem tributária, a Lei 8.137/1990, em seu art. 2º, inciso V, considera crime a conduta de “utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública” (BRASIL, 1990b).

Em 1996, com a Lei 9.296/96, que trata da interceptação de comunicações telefônicas para prova em investigação criminal, seu art. 10 estabelece como crime a interceptação sem a devida autorização, conforme versa:

> Art. 10. 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: (Redação dada pela Lei nº 13.869. de 2019)
> Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 13.869. de 2019)
> 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 (BRASIL, 1996).

A referida Lei abre espaço, no entanto, à possibilidade de uma das partes envolvidas na comunicação utilizar-se dela, no art. 10-A, § 1º “Não há crime se a captação é realizada por um dos interlocutores” (BRASIL, 1996).

No ano seguinte, 1997, a Lei 9.504/97, que trata a respeito das normas eleitorais, considerou como crime o acesso ao sistema eleitoral, com o objetivo de alterar a apuração ou contagem de votos. Essa tipificação se estendeu ao ato de “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”, no mesmo artigo, inciso II (BRASIL, 1997).

Ainda, no ano seguinte, a Lei n.º 9.609/98, que trata sobre a propriedade intelectual dos programas de computador, os chamados softwares, traz em seu art. 12, a consideração como crime da conduta de “violar direitos de autor de programa de computador”. A pena estabelecida pode chegar até a quatro anos de reclusão (BRASIL, 1998).

Dois anos depois, no ano 2000, a Lei n.º 9.983/00 trouxe importantes modificações para o direito material penal. Através dela foram acrescidos ao Código Penal os tipos penais fechados e a inclusão de texto em outros dispositivos,. Após as mudanças da Lei 9.983, um maior número de condutas praticadas no meio eletrônico foi considerado como conduta criminosa.

A primeira alteração foi a realizada através do Decreto-Lei n.º 2.848/40, art. 153, §1º-A, que tipificou a divulgação de segredo institucional. Sua redação trouxe como criminosa a conduta de “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” (BRASIL, 1940);

A segunda alteração veio através do Art. 313-A, pela inserção de dados falsos em sistema de informações. O referido artigo classificou como criminosa a conduta de “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”.

A terceira veio através do art. 313-B, que considera crime a conduta de “modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente”.

Ainda para complementar, cabe reforçar a lei criada e intitulada popularmente como Lei Carolina Dieckmann (Lei 12.737 de 2012). Ela tornou crime a invasão de

aparelhos eletrônicos para obtenção de dados particulares. Assim como a Lei 9.983/00, alterou o Código Penal, incluindo uma nova redação aos artigos 154-A a 154-B, classificados como crimes contra a liberdade individual, conforme versa:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com 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 [...]
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal e Municípios ou contra empresas concessionárias de serviços públicos (BRASIL, 1940).

O rol de documentos no ordenamento pátrio é, portanto, abrangente no que se refere aos crimes virtuais. No entanto, ainda é reconhecida a necessidade premente de maiores esclarecimentos e penalidades mais duras para crimes que envolvem o meio digital, mas se estendem ao risco físico do indivíduo. Diversos são os relatos de extorsão, quando o sujeito ativo obtém, por meio eletrônico, informação sigilosa ou íntima da vítima, assim como os casos onde o sujeito ativo se utiliza, por exemplo, de uma rede social para conhecer o paradeiro da vítima a quem pretende atacar.

Nesses casos, o meio eletrônico, apesar de não ser o único, é um agente facilitador, mas que foge à instância do Direito. Cabe também à sociedade aprender como utilizar as ferramentas que a modernidade lhes oferece. Vê-se, tanto adultos quanto crianças (cada vez mais novas) expondo fotos familiares, vídeos, localizações, de modo público em redes sociais, contrariando todas as recomendações de segurança que sempre foram dadas.

Um dos exemplos mais fáceis de prevenir a respeito dos crimes virtuais é o chamado *reveng porn*, onde, munido de fotos ou vídeos íntimos, o ex-companheiro os utiliza para se vingar da vítima, pela humilhação pública. No entanto, este é um assunto que deverá ser tratado posteriormente.

5. CONSIDERAÇÕES FINAIS

A evolução tecnológica, quando comparada à evolução da própria humanidade, dispara com uma velocidade impressionante, cabendo à sociedade adaptar-se a ela, e não o oposto. As últimas décadas presenciaram o surgimento de soluções antes mesmo que os problemas fossem vistos, realmente, como problemas.

A ideia inicial da tecnologia era a de facilitar as atividades do homem, especialmente ao que se refere à força de produção, agilizando processos, potencializando lucros, tornando o mundo mais rápido. Em nenhuma previsão, por mais absurda, alguém jamais ousou dizer que chegaria o tempo onde quase 70% da população mundial teria, em seu bolso, um dispositivo tecnológico com tamanho alcance.

Essa subestima a respeito do alcance da tecnologia para o usuário comum foi uma das razões pelas quais não foi prevista a possibilidade dos crimes virtuais, e, assim sendo, não houvesse até poucos anos um rol de leis que protegesse o indivíduo e sua privacidade.

O presente trabalho buscou mostrar, à luz do ordenamento pátrio, que apesar de ainda existir um grande caminho a ser seguido, as leis que hoje englobam os crimes virtuais também conseguem evoluir, se aperfeiçoar e até mesmo se antecipar, possibilitando que o real papel das leis seja cumprido: o de prevenir o crime.

Os objetivos elencados na elaboração do pré-projeto e apontados na introdução do presente trabalho, foram baseados na questão “Quais os procedimentos legais para impedir a violação de privacidade digital?”. Entende-se, portanto, que a pesquisa aqui realizada cumpriu seu papel, apontando os diversos procedimentos legais relacionados à proteção da privacidade digital.

É compreensível, no entanto, que os referidos instrumentos sirvam em grande parte para a penalização, e pouco para a prevenção, já que a internet ainda conta muito com o fenômeno do anonimato. Associado a este fenômeno, está a capacidade ainda restrita dos órgãos competentes fiscalizarem e localizarem os sujeitos ativos de condutas criminosas.

Os objetivos, tanto geral quanto específicos, foram alcançados, já que foram analisadas as mudanças na sociedade aliadas à tecnologia que possibilitaram a

problemática da violação de privacidade digital. O conceito de privacidade e intimidade, assim como os dispositivos que os protegem foram explorados, assim como os instrumentos legais que classificam tais violações como crimes virtuais.

Foi ainda possível constatar que, apesar de não caber nunca à vítima a culpa pelo dano que lhe foi causado, é possível através de atitudes simples, evitar esse tipo de problema. A exposição em redes sociais de fotos íntimas, localizações, informações pessoais e outros ainda é um prato cheio para pessoas com má-intenção.

O tema é ainda muito amplo, sendo possível abordar ramificações do mesmo, como as invasões a sistemas de dados pessoais, a utilização dos mesmos em crimes de estelionato, as divulgações de imagens íntimas do *reveng porn* e mais uma gama de condutas que são incrivelmente comuns no meio eletrônico. No entanto, esses são temas para futuras publicações.

REFERÊNCIAS

CALHEIROS, Tânia da Costa; TAKADA, Thalles Alexandre. **Reflexões sobre a privacidade na sociedade da informação**. Inf. Prof., Londrina, v. 4, n. 1, p. 120 – 134, jan./jun. 2015. Disponível em: http://www.uel.br/revistas/uel/index.php/infoprof/article/view/22564. Acesso em 02 mar. 2022.

CARVALHO, Paulo Roberto de Lima. Crimes cibernéticos: uma nova roupagem para a criminalidade. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 20, n. 4246, 15 fev. 2015. Disponível em: https://jus.com.br/artigos/31282. Acesso em: 19 mar. 2022.

DONEDA, Danilo Cesar Maganhoto. Considerações iniciais sobre bancos de dados informatizados e o direito à privacidade. In: TEPEDINO, Gustavo (org.) **Problemas de direito civil-constitucional**. Rio de Janeiro: Renovar, 2000, pp. 111-136.

LINS, Bernardo Felipe Estellita. A evolução da internet: uma perspectiva histórica. **Artigos & Ensaios.** Cadernos ASLEGIS | 48 • Janeiro/Abril • 2013. Disponível em: http://www.belins.eng.br/ac01/papers/aslegis48_art01_hist_internet.pdf. Acesso em 09 mar. 2022.

MOGNON, Mateus. **Chantagem online, exposição e invasão de webcam que aparecem em Black Mirror já são realidade**. UOL. 2016. Disponível em: https://adrenaline.uol.com.br/2016/11/13/46766/chantagem-online-exposicao-e-invasao-de-webcam-que-aparecem-em-black-mirror-ja-sao-realidade/. Acesso em: 03 mar. 2022.

OTOBONI, Gustavo Henrique dos Santos; ALMEIDA, Jeilton Frausto de. Crimes Cibernéticos: Phishing. **Revista Âmbito Jurídico**. 2019. Disponível em: https://ambitojuridico.com.br/edicoes/revista-191/crimes-ciberneticos-phishing/. Acesso em 06 mar. 2022.

PCS. Departamento de Engenharia de Computação e Sistemas Digitais. **A Computação na Poli – 20 anos antes do PCS**. S/d. Disponível em: https://pcs.usp.br/departamento/historia/. Acesso em 12 mar. 2022.

POZZEBOM, Rafaela. Oficina da net. **Quais são os crimes virtuais mais comuns?** 2015. Disponível em: http://www.oficinadanet.com.br/post/14450-quais-os-crimes-virtuais-mais-comuns. Acesso em 05 mar. 2022.

RODOTÀ, Stefano. **A Vida na Sociedade de Vigilância.** A privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar, 2008.

RODRIGUES, Talissa. **Crimes digitais**. MEDIUM. 2017. Disponível em: https://medium.com/tendências- digitais/crimes-digitais-3ffe0affc12b. Acesso em: 01 mar. 2022.

SOUZA, Karina Cristina Neves**. Invasão de privacidade através da internet**. Comunicação Científica, v. 1 n. 2 (2015): Caderno de Resumos. Disponível em: https://portaldeperiodicos.unibrasil.com.br/index.php/anaisevinci/article/view/645. Acesso em: 01 mar. 2022.

TALAMONE, Rose. **Influência da tecnologia nas relações é tema do "USP Analisa".** Out. 2017. Disponível em: https://jornal.usp.br/radio-usp/radioagencia-usp/influencia-da-tecnologia-nas-relacoes-e-tema-do-usp-analisa/#:~:text=A%20tecnologia%20influencia%20tantos%20aspectos,o%20ser%20humano%20se%20relaciona.&text=Para%20ela%2C%20a%20tecnologia%20pode,e%20tamb%C3%A9m%20de%20proporcionar%20isolamento. Acesso em 12 mar. 2022.

ZAMBARDA, Pedro. **Apple faz 37 anos;** conheça a história da empresa criada por Steve Jobs. Portal Techtudo, 2013. Disponível em: https://www.techtudo.com.br/artigos/noticia/2013/04/apple-faz-37-anos-conheca-historia-da-empresa-criada-por-steve-jobs.html. Acesso em 12 mar. 2022.