USO DA TECNOLOGIA PARA FINS ILÍCITOS: A violação da intimidade por meio de crimes informáticos

USE OF TECHNOLOGY FOR ILLEGAL PURPOSES: Violation of intimacy by means of cyber crimes

Lislene Ledier Aylon

Doutora pela FADISP (Faculdade Autônoma de Direito) em São Paulo/SP. Mestre em Direito Privado pela Universidade de Franca (2002). Pós-graduada em Direito Penal e Processual Penal pela Faculdade de Direito de Franca (1995). Graduada em Direito pela Universidade Estadual Paulista Júlio de Mesquita Filho (1989), Professora na Faculdade de Direito de Franca/SP, da disciplina Direito Civil III (Contratos) e coordenadora do Núcleo de Assistência Judiciária da Faculdade de Direito de Franca.
E-mail: llaylon@gmail.com.

Cildo Giolo Júnior

Pós-Doutor em Direitos Humanos pelo "Ius Gentium Conimbrigae" (IGC/CDH) da Faculdade de Direito da Universidade de Coimbra (Portugal). Doutor em Direito pela Universidade Metropolitana de Santos (Unimes - 2013). Doutor em Ciências Jurídicas e Sociais pela UMSA (Buenos Aires - Argentina - 2007). Mestre em Direito Público pela Universidade de Franca (2001). Especialista em Direito Processual Civil na Faculdade de Direito de Franca (1994). Graduado em Direito pela Faculdade de Direito de Franca (1991). Professor Titular das cadeiras de Direito Civil na Faculdade de Direito de Franca e de Direito Processual Civil na Universidade do Estado de Minas Gerais, tendo sido admitido em ambas por concursos públicos de provas e títulos. Docente e Advogado. Avaliador do MEC/INEP para os Cursos de Direito.
E-mail: drcildo@gmail.com.

Recebido em: 16/03/2021
Aprovado em: 25/08/2021

RESUMO: O presente artigo tem como objeto de pesquisa os crimes informáticos quando violam a intimidade das pessoas, visando compreender como a internet, ao mesmo tempo em que facilitou a vida dos seres humanos, trouxe uma total invasão à sua privacidade, com a prática de delitos antes dela inimagináveis. Inicialmente, foi analisado o direito à intimidade, garantido pela Constituição Federal e por leis ordinárias. Em seguida, adentrou-se ao estudo da Informática, com o surgimento da internet e dos crimes informáticos, em seus aspectos técnicos e a legislação pátria pertinente. Por fim, chegou-se à análise da violação da intimidade praticada por meios virtuais. Após todas essas etapas, verificou-se ser insuficientes as leis que existem no Brasil, capazes de conter os avanços da criminalidade virtual.

Palavras-chave: Crimes informáticos. Direito à intimidade. Violação.

ABSTRACT: This article aims to investigate computer crimes that violate privacy, to understand how the Internet, while making human lives easier, has brought a total invasion of their privacy, with the practice of crimes never imagined before. Initially, the right to privacy, guaranteed by the Federal Constitution and by ordinary laws, was analyzed. Next, a study of computer science was

conducted, focusing on the Internet and computer crimes, in their technical aspects and considering the relevant national legislation. Finally, an analysis was made regarding the violation of intimacy through virtual means. After all these steps, the conclusion was that there is a lack of laws in Brazil, capable of containing the advances of virtual crime.

Keywords: Computer crimes. Right to privacy. Violation.

INTRODUÇÃO

Depois da Constituição de 1988 e do Código Civil de 2002, inegável que o direito à intimidade faz parte do rol dos direitos da personalidade, que são relacionados à dignidade da pessoa humana. A intimidade é um direito fundamental que exige proteção estatal de todo e qualquer ataque, podendo gerar sanções de natureza civil e penal.

Ocorre que, de algumas décadas para cá, esse direito vem sendo violado de maneira constante e crescente, através dos chamados crimes informáticos, criando grandes prejuízos às pessoas, tanto físicas quanto jurídicas. Diante do perigo trazido pela internet e seu mau uso, essa pesquisa objetiva analisar essas violações e as soluções encontradas pela legislação e jurisprudência para enfrentar tal problema.

A problemática enfrentada pela pesquisa é responder até que ponto estamos protegidos pela legislação de potenciais violações a direitos fundamentais que essa tecnologia pode instrumentalizar, principalmente a privacidade e intimidade.

Esta pesquisa foi dividida em cinco capítulos para contextualizar o tema, principalmente diante dos princípios constitucionais penais. Assim, o primeiro capítulo analisa o direito à intimidade, como um dos direitos da personalidade, buscando sua conceituação e alcance, além de ser tratado como direito fundamental. Em seguida, expõe-se o direito à intimidade como decorrência do princípio maior que é o da dignidade da pessoa humana, o que acarreta a sua tutela penal. No terceiro capítulo busca-se trazer dados sobre o surgimento da internet e, especificamente dos crimes dela decorrentes. Trata dos crimes aspectos conceituais e técnicos dos crimes informáticos, delineando sua enorme abrangência. Em capítulo seguinte, estuda-se o problema da aplicação da lei no espaço, diante da dificuldade de se definir o lugar do crime nos crimes praticados pela internet. Aqui foram compilados alguns julgados dos Tribunais Superiores, demonstrando que existe divergência quanto à esta problemática. Finalmente, fecha-se a pesquisa com o link entre o direito à intimidade e os crimes informáticos, alertando para a violação contínua desse direito fundamental, que vem preocupando Nações e pessoas, principalmente pais de crianças, diante do imensurável conteúdo trazido pela internet e o perigo da exposição da vida privada e de informações pessoais na rede.

Para tanto, foi utilizado o método lógico-dedutivo, por meio de várias obras nacionais, artigos científicos publicados e decisões jurisprudenciais a respeito do tema.

1 O DIREITO À INTIMIDADE

De grande relevância no contexto psíquico da pessoa é o direito à intimidade, que se destina a resguardar a privacidade em seus múltiplos aspectos: pessoais, familiares e negociais.

Deve-se preservar a pessoa de qualquer atentado a aspectos particulares ou íntimos da sua vida, em sua consciência, ou em seu circuito próprio, compreendendo-se o seu lar, a sua família e a sua correspondência.

A Declaração Universal dos Direitos Humanos, adotada pela ONU em 1948, estabelece, em seu art. 12, que a privacidade do indivíduo é um dos direitos humanos fundamentais a serem respeitados e assegurados: "Art. 12 – Ninguém sofrerá intromissões na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques a sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito à proteção da lei." (ONU, 1948)

O art. 21 do Código Civil dispõe: "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar o ato contrário a esta norma" (BRASIL, 2002). Referido dispositivo, juntamente com o art. 5º, X, da CRFB/88, protege todos os aspectos da intimidade da pessoa, concedendo ao prejudicado a prerrogativa de pleitear que cesse o ato abusivo ou ilegal. Caso o dano já tenha ocorrido, assegura-se o direito a indenização.

Três são as teorias sobre o direito à intimidade. A primeira delas, chamada teoria objetiva, adota a chamada *teoria das esferas*, do direito alemão, onde se pode visualizar figurativamente, vários círculos concêntricos, sendo que no centro encontra-se o que há de mais íntimo, reservado; ao redor, a intimidade familiar; e por último, na parte externa, a área destinada à esfera pública. A segunda teoria, conhecida como subjetiva, entende que a pessoa, e ninguém mais, pode determinar o que é ou não íntimo. Modernamente, surgiu a *teoria do mosaico*, como uma necessidade de proteção da intimidade do indivíduo conforme ressalta DELGADO:

> [...] frente às ameaças que de forma genérica os novos engenhos tecnológicos e em concreto a informática supõem. Foi formulada por Madrid Conesa que entende que a teoria das esferas não é válida, haja vista que hoje os conceitos de público e privado são relativos, pois existem dados que a priori são irrelevantes desde o ponto de vista do direito à intimidade, mas que unidos uns com os outros podem servir para configurar uma ideia praticamente completa de qualquer indivíduo, tal como ocorre com as pequenas pedras que formam um mosaico, que em si não dizem nada, mas quando unidas podem formar conjuntos plenos de significado. (*apud*, GRECO, 2007, p. 104)

Neste mesmo sentido, afirma GONÇALVES:

> A proteção à vida privada visa resguardar o direito das pessoas de intromissões indevidas em seu lar, em sua família, em sua correspondência, em sua economia, etc. O direito de estar só, de se isolar, de exercer as suas idiossincrasias se vê hoje, muitas vezes, ameaçado pelo avanço tecnológico, pelas fotografias obtidas com teleobjetivas de longo alcance, pelas minicâmeras, pelos grampeamentos telefônicos, pelos abusos cometidos na Internet e por outros expedientes que se prestam a esse fim. (2016, p. 209)

Almir de Oliveira (2000, p.172) alerta para a gravidade das ofensas à vida privada, proclamando que "o devassamento da intimidade é um dos fenômenos mais perturbadores do nosso tempo, seriamente agravado pelo veloz desenvolvimento da informática.".

Sobre a importância da do direito da intimidade e da sua separação do direito à honra, chama-nos a atenção Carlos Alberto Bittar:

> O ponto nodal desse direito encontra-se na exigência de isolamento mental ínsita no psiquismo humano, que leva a pessoa a não desejar que certos aspectos de sua personalidade e de sua vida, cheguem ao conhecimento de terceiros. Veda-se qualquer interferência arbitrária na vida privada, na família, no domicílio e na

> correspondência, bem como – na fórmula adotada pela Declaração Universal – coíbem-se os ataques à sua honra ou reputação, permitindo-nos distinguir, em sua pureza, os componentes do direito à intimidade, o qual se aparta, por sua vez, do direito à honra. (2001, p. 107)

Existe muita dificuldade em se conceituar o direito à intimidade, e cada autor tem sua ótica e forma de fazê-lo. Entende-se que a definição de Edson Ferreira da Silva (1998), é a mais simples e completa, qual seja: "O direito à intimidade deve compreender o poder jurídico de subtrair ao conhecimento alheio e de impedir qualquer forma de divulgação de aspectos de nossa vida privada, que segundo um sentimento comum, detectável em cada época e lugar, interessa manter sob reserva." (p.39).

Enquanto a privacidade ocupa um âmbito com raio maior, a intimidade já é bem mais restrita, pois nesse caso a pessoa guarda apenas para si tal fato e resguarda o direito de dividi-lo com quem for de sua vontade. Para René Ariel Dotti, a vida privada abrange todos os aspectos que por qualquer razão não gostaríamos de ver cair no domínio público; é tudo aquilo que não deve ser objeto do direito à informação nem da curiosidade da sociedade moderna que, para tanto, conta com aparelhos altamente sofisticados. (1980, p. 71)

Para o atual Ministro da Justiça, Alexandre de Moraes, o conceito de intimidade engloba as relações subjetivas e íntimas da pessoa, além de suas relações familiares e de amizade; por outro lado, a vida privada tem uma dimensão maior, incluindo os relacionamentos humanos objetivos (comerciais, de trabalho, de estudo, etc.). (2016, p. 55).

Em caso de pessoas dotadas de notoriedade e no exercício de sua atividade, pode ocorrer a revelação de fatos de interesse público, independentemente do seu consentimento. Nessas situações, diz-se que existe redução espontânea dos limites da privacidade (políticos, atletas, artistas, etc). Mas o limite da confidencialidade persiste preservado. Deste modo, sobre fatos íntimos, sobre a vida familiar, sobre a reserva no domicílio e na correspondência, não é lícita a comunicação sem consulta ao interessado.

Cabe a cada pessoa, individualmente, saber o limite de preservar ou não sua privacidade e intimidade, sendo um direito constitucionalmente tutelado, onde o Estado exerce a função de zelar por este direito.

A privacidade é "o conjunto de informações acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso poder ser legalmente sujeito". A esfera de inviolabilidade, assim, é ampla, "abrange o modo de vista doméstico, nas relações familiares e afetivas em geral, fatos, hábitos, local, nome, imagem, pensamentos, segredos, e, bem assim, as origens e planos futuros do indivíduo". (SILVA, 2009, p. 206).

1.1 O DIREITO À INTIMIDADE COMO DECORRÊNCIA DO PRINCÍPIO DA DIGNIDADE DA PESSOA HUMANA E SEU FUNDAMENTO CONSTITUCIONAL

O Direito Penal, em um Estado Democrático e Social de Direito, não pode ficar imune ao filtro constitucional, retirando-se da hierarquia dos valores contida na Constituição Federal seu conteúdo material, bem como a sua legitimação, conforme salienta SBARDELOTTO:

> Sob esse prisma, afigura-se evidente a necessidade de o conteúdo das normas penais direcionarem-se estabelecidos, sendo inegável que representam eles o que de mais relevante há para a sociedade brasileira. Aliás, irretorquível que a proteção da dignidade humana, da cidadania, dos valores sociais do trabalho, o repúdio ao terrorismo, ao racismo, aos crimes hediondos, o desiderato de erradicação da pobreza e da marginalização, a redução das desigualdades sociais, o estabelecimento de uma sociedade justa, sem preconceitos de origem, raça,

> sexo, cor, idade ou qualquer outra forma de discriminação, a prestação de saúde, educação e lazer ao povo, a dignidade e o acesso ao trabalho, às condições de vida dignas, são valores que, inseridos na Constituição, conduzem impositivamente o Direito Penal à sua tutela. Esta tutela é o desiderato maior do Direito Penal, o sumo de sua legitimação, sendo esta a fonte de prospecção dos bens jurídicos penalmente tuteláveis. (2001, p. 83)

O princípio da dignidade da pessoa humana é a fonte de onde emanam os demais os direitos fundamentais; é a espinha dorsal de todo ordenamento jurídico.

Segundo PRADO, a dignidade da pessoa humana pode assumir contornos de verdadeira categoria lógico-objetiva ou lógico-concreta, inerente ao homem enquanto pessoa, sendo um atributo ontológico do homem, valendo em si e por si mesmo. (2014, p.111)

As Constituições mais modernas, como a espanhola e a brasileira, não apenas preveem expressamente o princípio da dignidade da pessoa humana, mas também direitos que lhe são decorrentes, como acontece com o direito à intimidade, como se vê no art. 18.1 da Constituição Espanhola: "[...] se garantiza el derecho al honor, a la intimidad personal y familiar a la própria imagen"; E no item 4 do mesmo artigo, que complementa: " *la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*". (ESPANHA, 1978).

O direito à intimidade, como posto por Paulo José da Costa Júnior:

> [...] é o direito que dispõe que o indivíduo de não ser arrastado para a ribalta contra a vontade. De subtrair-se à publicidade e de permanecer recolhido em sua intimidade. Direito ao recato, portanto, não é o direito de ser recatado, mas o direito de manter afastados dessa esfera de reserva olhos e ouvidos indiscretos, bem como o direito de impedir a divulgação de palavras, escritos ou atos realizados nessa esfera de intimidade. (1997, p. 33)

O próprio conceito de direito à intimidade não tem natureza absoluta, variando de pessoa a pessoa, de sociedade para sociedade, de cultura para cultura, de época para época, como ocorre com os bens jurídicos tutelados. Desta maneira, o que pode configurar uma violação a esse direito, numa determinada sociedade, já não o será em outra. Assim, essa reserva íntima tem natureza relativa.

Elevado ao nível de direito fundamental, o direito à intimidade passou a gozar de um regime jurídico especial. Passou a ter garantia de "cláusulas pétreas" (art. 60, § 4º, IV) e aplicação imediata (art. 5º, § 1º). O Constituinte brasileiro também tutelou o direito à intimidade, ainda que de forma indireta, através de vários outros dispositivos, tais como: o direito de resposta (art. 5º, V); a inviolabilidade do domicílio (art. 5º, XI); a inviolabilidade do sigilo da correspondência, das comunicações telegráficas, de dados e das comunicações telefônicas, salvo restrição judicial (art. 5º, XII); o resguardo da fonte, quando necessário ao exercício profissional, em se tratando ao acesso à informação (art. 5º, XIV); o direito de inédito no direito autoral e da propriedade industrial (art. 5º, XXVIII, alínea "a"); a restrição à publicidade dos atos processuais (art. 5°, LX) e o *habeas data* (art. 5º, LXXII). (1988, *on line*)

Como ensina Alexandre de Moraes:

> Encontra-se em clara e ostensiva contradição com o fundamento constitucional da dignidade da pessoa humana, com o direito à honra, à intimidade e à vida privada converter em instrumento de diversão ou entretenimento assuntos de natureza tão íntima quanto falecimentos, padecimentos ou quaisquer desgraças alheias, que não demonstrem nenhuma finalidade pública e de caráter jornalístico em sua divulgação. Assim, não existe qualquer dúvida de que a divulgação de fotos, imagens ou notícias apelativas, injuriosas, desnecessárias para a informação

> objetiva e de interesse público (CF, art. 5º, XIV), que acarretem injustificado dano à dignidade humana autoriza a ocorrência de indenização por danos materiais e morais, além do respectivo direito de resposta. (2016, p. 55).

2 INFORMÁTICA E CRIMINALIDADE

2.1 INTERNET

Para melhor compreender a temática, torna-se importante a análise dos principais fatos históricos que motivaram o surgimento do que atualmente denomina-se internet. De acordo com Gimenes, a informática teve início na II Guerra Mundial, quando foram desenvolvidos os primeiros computadores, notoriamente sob o protótipo Mark I. Ao longo da segunda metade do século XX, os computadores sofreram importantes modificações, chegando a sua atual 5ª geração, tendo a disseminação da internet como sua principal função. (2013, *on line*)

A internet, como destacado por Pinheiro, teve início em 1969, quando uma subdivisão do Departamento de Defesa dos Estados Unidos, ARPA, criou a ARPANET, a qual tinha como finalidade imediata atender às exigências de guerra da época, como espalhar as informações mais importantes por vários departamentos americanos, evitando que o ataque a um deles provocasse a perda dessas informações. (PINHEIRO, 2016, *on line*)

Com o fim da Guerra Fria, a ARPANET deixou de ser de uso exclusivo dos militares, sendo liberada para as universidades norte-americanas, possibilitando aos estudiosos uma rápida troca de informações. Paulatinamente, este acesso foi expandido para universidades de outros países, criando uma grande rede interligada de informações relacionadas à pesquisa científica. Em 1987, a internet foi liberada para o uso comercial, sendo esta etapa considerada como o "o grande marco para o desenvolvimento desta tecnologia", pois, dentre outras consequências, motivou o fim das operações da ARPANET em 1990, sendo a mesma substituída por outros sistemas mais rápidos. Em 1993, com o desenvolvimento do *World Wide Web* – WWW –, a internet se popularizou. (COSTA, 2011, *on line*).

Especificamente no Brasil, a internet deu seus primeiros passos apenas em 1988, quando a Rede Nacional de Pesquisa – RNP – e o Ministério da Ciência e Tecnologia começaram a investir na tecnologia. Em 1992, os primeiros pontos de pesquisas foram instalados em algumas universidades e, em 1995, a rede mundial de computadores foi liberada para uso comercial, dando início aos grandes avanços das telecomunicações no Brasil.

Segundo Rita de Cássia Lopes da Silva:

> Não há um único centro que governa, ou mesmo gerencia, a internet. As redes constituintes pertencem a alguma organização, mas ela não é de ninguém. Quando se fala em decisões sobre a internet, sendo estas penas em padrões tecnológicos, elas são de responsabilidade de órgãos como a Internet Numbers Authority, a Internet Engineering Task Force e a Isoc, que é uma organização de membros voluntários conhecida como Internet Society, tendo como membro qualquer pessoa ou organização que apresentar interesse em aderir a ela. (SILVA, 2011, p. 38).

Hoje, a internet é um conjunto de mais de 40 mil redes no mundo inteiro. O que essas redes têm em comum é o protocolo *Transmission Control Protocol/Internet Protocol* (TCP/IP) que permite a comunicação entre elas." (SILVA, 2011, p. 39)

2.2 CRIMES INFORMÁTICOS

2.2.1 Introdução

Ao lado de todos os benefícios trazidos pela internet, surgiram novas formas de violação de bens jurídicos protegidos pelo ordenamento, os quais passaram a ser realizados não mais no plano físico, mas, sim, no plano virtual. Conforme afirma COLLI, "{...] apesar de a internet facilitar e ampliar a intercomunicabilidade entre as pessoas, ela pode ter sua finalidade transformada em um meio para a prática e a organização de infrações penais. Dentre estas despontam os chamados crimes informáticos [...]". Ressalta, ainda, que a internet pode ser tanto ambiente propício para a consumação de crimes, quanto para a realização de seus atos preparatórios, como nos casos de rixas entre torcidas organizadas. (2009, *on line*)

No intuito de compreender e, consequentemente, encontrar meios de reprimir estes novos delitos, foi desenvolvido um novo ramo jurídico especializado nos crimes virtuais, qual seja, o direito informático. SYDOW (2009) explica que este ramo jurídico foi resultado da reação da sociedade ao se deparar com a ocorrência de inúmeras violações aos bens jurídicos tutelados pelo ordenamento sem que houvesse um meio legal de combatê-los.

Acerca da possibilidade de regulação da esfera virtual, deve-se enfatizar a seguinte reflexão: a internet não é um bem jurídico sobre o qual repousa posse, propriedade. Não existe relação de domínio entre a pessoa e a internet. No entanto, não por isso se deva dizer que o ciberespaço é um ambiente não regulável. A despeito de o ambiente cibernético ser um ambiente não físico, deve ele ser passível de ser regido pelo direito, até porque seus resultados são materiais.

Outro argumento que merece destaque é o de GUARDIA, quando o mesmo faz uma correlação entre a carta tradicional e o correio eletrônico, ambos condutores de informações e pensamentos escritos, bens jurídicos protegidos pela Constituição Federal, como se pode observar a seguir:

> Embora distintos o suporte empregado e o canal de circulação de comunicação, tanto a carta como o correio eletrônico são meios de difusão de ideias e pensamentos que utilizam principalmente caracteres escritos. O caráter íntimo da comunicação, destinada a um receptor determinado, exige total reserva de conhecimento de terceiros. Por razão, o regime de inviolabilidade das comunicações postais igualmente se aplica às interceptações ou acessos a mensagens de correio eletrônico. Concluída a comunicação, não cessa a tutela jurisdicional para o conhecimento de seu conteúdo, portanto, não há que diferenciar a proteção das comunicações e a proteção dos em si mesmos. (2012, p.7-8)

Portanto, por mais que os delitos informáticos ocorram numa esfera em que, em princípio, não há a possibilidade de delimitá-los fisicamente, todas as consequências geradas no campo virtual são passíveis de valoração no ordenamento jurídico, fato que gera a necessidade de ser feita a sua devida regulamentação.

2.2.2 Conceito

A conceituação do delito informático não é simples, pois envolve aspectos não apenas jurídicos, mas também de conceitos relacionados à área cibernética. De forma simples, pode-se afirmar que crimes informáticos são aqueles praticados mediante a obtenção indevida de dados – informações – que foram ou estão sendo processados por um terceiro. Segundo KERR, delito

informático seria "toda a ação típica, antijurídica e culpável, praticada contra ou através da transmissão, processamento e armazenamento automático de dados". (2011, p.3)

Como aponta FELICIANO, criminalidade informática é o recente fenômeno histórico-sociocultural caracterizado pela elevada incidência de ilícitos penais que têm por objeto material ou meio de execução o objeto tecnológico informático (hardware, software, redes, etc). Já a infração penal típica pode ser denominada crime informático ou por computador. (2001, p. 31)

2.2.3 Classificação

Os crimes de informática podem ser classificados em: delitos informáticos puros (correspondentes aos novos tipos penais, surgidos com o uso progressivamente maior dos computadores e que deles necessitam para existir) e delitos informáticos impuros (tipos penais já existentes, com vida própria, independentemente do objeto informático)

De outra maneira, em relação à classificação destes delitos, destaque-se a existência de dois grandes grupos de crimes virtuais: o primeiro tem como objeto a violação dos sistemas de informática, independente do motivo; o segundo tem como objeto a violação de outros bens jurídicos ou valores sociais, usando a informática apenas como meio de cometer o ilícito.

Analisando a temática, VIANA (2001) elenca os crimes virtuais da seguinte forma: crimes informáticos impróprios, nos quais o computador é mero instrumento de realização do crime, não havendo violação de dados, como nos casos de difamação, calúnia e injúria; crimes informáticos próprios, nos quais o bem jurídico violado são os dados computacionais; crimes informáticos mistos, nos quais há a violação de dados computacionais e de outros bens jurídicos distintos; crimes informáticos mediatos ou indiretos, os quais servem de instrumento para a consumação de outro delito não-informático, como no caso de furto de dinheiro de contas bancárias pelo computador.

Por mais distinções que possam apresentar ou nomenclaturas que possam receber (virtuais, informáticos, cibernéticos, de informática, dentre outros), deve-se subdividir os crimes informáticos em dois grandes grupos, ficando o primeiro com os crimes violadores do computador e seus componentes; e o segundo com os crimes violadores de bens jurídicos já protegidos pelo ordenamento há tempos, sendo o computador o instrumento para sua realização.

São crimes informáticos impuros ou impróprios: furto, apropriação indébita, dano, divulgação de segredo, violação de segredo profissional e violação e sonegação de correspondência.

São crimes informáticos puros ou próprios: pirataria, vírus, estelionato (pirâmides e correntes), apologia ou incitação ao crime (terrorismo e racismo), pornografia e pedofilia, crimes contra a honra, interceptação de fluxo de dados em tráfego por serviços de telecomunicações (escuta), corrupção de menores e congêneres (salas de chat), uso não autorizado de senha de acesso a serviço prestado por provedor, engano ao consumidor quanto à garantia de produtos comprados pela Internet, lavagem de dinheiro, crimes informáticos funcionais (Lei n. 9.983/2000), usurpação de nome ou pseudônimo alheio, condutas criminosas de provedores de acesso, desobediência, débito não autorizado em cartão de crédito, favorecimento real de usuário criminoso, etc.

2.2.4 Sujeitos ativo e passivo

Em princípio, como ensina CASTRO (2003, p. 11-12), qualquer pessoa pode ser sujeito ativo dos crimes de informática, um estelionato através da Internet, por exemplo, não requer nenhuma qualidade especial do agente. Como este, a maioria dos crimes de informática é comum em relação ao sujeito. Quanto ao sujeito passivo, também pode ser qualquer pessoa. Seja que for conectado à Internet, pode receber um vírus e ter destruídos seus programas e devassada toda a sua vida privada.

Faz-se necessário compreender também uma distinção importante: hacker e cracker. Os dois são grandes conhecedores da informática, mas o que os diferem é a forma de utilização deste conhecimento, pois, enquanto o hacker entra nos sistemas computacionais para provar que existem falhas pendentes de correção, não provocando danos em seus proprietários, o cracker invade os computadores com a finalidade de causar danos, de cometer ilícitos, de se aproveitar das falhas existentes no sistema para obter vantagem indevida. Enquanto esta cria um problema para os usuários, aquele tenta solucioná-lo. (BARBOSA JÚNIOR, 2014, *on line*)

2.2.5 Legislação específica

O ordenamento é formado por vários ramos jurídicos, cada qual com sua legislação específica, ocorrendo o mesmo com os crimes informáticos. No entanto, durante muitos anos, esta parte do ordenamento esteve sem cobertura legal específica, pois foi apenas em 2012 que o legislador federal editou as duas leis que atualmente norteiam o direito informático, quais sejam, a Lei n.º 12.735 e a Lei n.º 12.737, ambas do dia 30 de novembro de 2012.

A Lei n.º 12.735 de 2012 tipifica as condutas realizadas mediante uso de sistema eletrônico, digital ou semelhante, que sejam praticadas contra sistemas informatizados e similares. É um verdadeiro suporte para as demais legislações que venham a ser aprovadas no ordenamento brasileiro, pois traz em seu art. 4º a determinação de que os órgãos da polícia judiciária devem estruturar setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado, tudo de acordo como determinar o regulamento específico.

Com esta determinação legal, todos os setores da polícia judiciária brasileira deverão organizar setores especializados nos crimes cometidos na esfera virtual, criando no sistema jurídico brasileiro o suporte necessário para a edição de legislações dedicadas ao assunto.

Ademais, o seu art. 5º incluiu o inciso II no § 3º do art. 20 da Lei n.º 7.716 de 5 de janeiro de 1989, prevendo a possibilidade de o juiz, verificando a ocorrência de crimes cometidos na esfera virtual relacionados a raça, cor, etnia, religião ou procedência nacional, determinar a cessação da transmissão que contenha o referido delito.

No mesmo dia foi editada a segunda legislação direcionada para os delitos praticados no mundo virtual: a Lei n.º 12.737 de 30 de novembro de 2012, apelidada de "Lei Carolina Dieckmann", porque na época de sua tramitação na Câmara dos Deputados, a atriz teve fotos pessoais divulgadas sem autorização. Desta vez, o legislador foi mais além, editando a tipificação criminal dos principais delitos informáticos, relacionados com a invasão de dispositivos informáticos e a divulgação indevida de dados computacionais.

O seu art. 2º alterou o Código Penal Brasileiro, incluindo os arts. 154-A e 154-B ao diploma legal referido. Estes artigos dispõem sobre as condutas combatidas na esfera virtual, a respectiva sanção legal a ser aplicada aos futuros infratores e a forma de procedimento da respectiva ação penal, conforme discorrido a seguir.

O caput do art. 154-A inclui no ordenamento o crime de invasão de dispositivo informático. Além da multa, o caput prevê a detenção de 3 (três) meses a 1 (um) ano para quem invadir dispositivo informático, mediante violação dos mecanismos de segurança, visando a obtenção, alteração ou destruição de dados computacionais sem a devida autorização de seu proprietário, ou, ainda, para instalar vulnerabilidades nos dispositivos a fim de obter vantagem ilícita.

O § 1º do referido artigo esclarece que incorrerá na mesma pena quem produzir, oferecer, distribuir, vender ou difundir dispositivo informático que permita o cometimento do crime mencionado no parágrafo anterior. Incluindo todas estas ações no tipo penal, o legislador evitou que alguns membros da atitude delituosa se esquivassem da sanção penal por não cometer o ato de

invadir o dispositivo, dando mais respaldo ao cidadão para exigir a proteção de seus bens jurídicos, quando violados.

Ademais, se a vítima auferir algum prejuízo econômico, a pena, de acordo com o parágrafo segundo, será aumentada de um sexto a um terço, ampliando o número de bens jurídicos abarcados pela legislação, neste caso, o patrimônio.

Por sua vez, o § 3º prevê, além de multa, a pena de reclusão de 6 (seis) meses a 2 (dois) anos para os casos em que a invasão permita a obtenção de dados sigilosos, de segredos comerciais ou industriais ou, ainda, o acesso a correspondências eletrônicas privadas, tratando de forma mais severa, assim, os casos que repercutam não só na esfera profissional do lesado, mas, também, de sua vida privada. Se estes dados sigilosos forem repassados para terceiro, a pena será aumentada de um a dois terços, conforme a redação do § 4º do art. 154-A.

Por fim, o § 5º deste artigo determina que a pena seja aumentada de um terço a metade se a invasão for cometida contra os chefes dos poderes legislativo, executivo e judiciário, mais especificamente, contra o Presidente da República, os governadores, prefeitos, presidentes do Supremo Tribunal Federal, da Câmara dos Deputados, do Senado Federal, das Assembleias Legislativas, da Câmara Legislativa, da Câmara Municipal, ou, ainda, do dirigente máximo da administração pública, seja ela federal, estadual, distrital ou municipal.

Este aumento de pena foi necessário devido ao alto grau de responsabilidade administrado pelos cargos mencionados acima, pois os mesmos estão diretamente ligados ao futuro da nação e qualquer uso indevido de seus dados computacionais tem a capacidade de gerar graves lesões a todos os cidadãos brasileiros e a segurança nacional. Mostra-se correta, assim, a deferência conferida pelo legislador aos líderes dos poderes republicanos.

O art. 154-B, incluído no Código Penal Brasileiro, pela Lei n.º 12.737 de 2012, estabelece que as ações penais que versem sobre delitos informáticos só poderão ser processadas mediante representação, exceto se o crime for cometido contra a administração direta ou indireta federal, estadual, distrital ou municipal, ou, ainda, contra empresas concessionárias de serviços públicos. Neste segundo caso, por envolver questões de segurança nacional, como destacado anteriormente, a ação penal tem natureza totalmente pública, sendo desnecessária a apresentação de representação e, como conseguinte, a demonstração do interesse particular no processamento da demanda.

Afora toda a inovação trazida apenas pelo art. 2º, a Lei 12.737 de 2012, em seu art. 3º, acrescentou parágrafos aos arts. 266 e 298 do Código Penal Brasileiro.

O art. 266 tipifica o crime de perturbação ou interrupção de serviços ligados à comunicação, estabelecendo a pena de 1 (um) a 3 (anos), e multa, para quem cometer o crime. Ao incluir os parágrafos, o ordenamento expande o alcance da norma para os serviços telemáticos ou de utilidade pública, abarcando, assim, os ilícitos cometidos não só contra o interesse público, mas, também, contra dados informáticos, norte principal da inovação legislativa ora analisada.

Já o parágrafo incluído no art. 298, que tipifica o crime de falsificação de documento particular, estende os efeitos da norma aos cartões de crédito e de débito, os quais receberam do legislador a qualidade de documento particular devidamente reconhecido, e protegido, pelo ordenamento.

Por fim, por mais que tenha repercussão na esfera cível, deve-se mencionar o Marco Civil da Internet, Lei nº 12.965 de 2014, lei que funciona como uma Constituição para o uso da rede no Brasil. O projeto foi sancionado após tramitar por dois anos na Câmara dos Deputados e estabelece princípios e garantias, direitos e deveres para internautas e empresas. Esta lei foi regulamentada pelo Decreto nº 8.771, de 11 de maio de 2016.

Um dos pontos positivos de maior destaque é o fato de que o decreto trouxe regras sobre proteção de dados pessoais, como a introdução de uma definição de dado pessoal e de tratamento de dados – que ainda não eram expressos em lei. Agora, dado pessoal é definido como aquele "relacionado à pessoa natural identificada ou identificável, inclusive números identificativos,

dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa". (BRASIL, 2016)

Como se vê, várias são as infrações cometidas através da informática, mas aqui se abordará apenas as relacionadas à ameaça ou lesão ao direito à intimidade, como proposto.

2.2.6 O problema do lugar do crime nos crimes informáticos

A soberania dos Estados impõe a aplicação da lei penal em todo o seu território, assim considerados: superfície terrestre, espaço aéreo e águas territoriais. Ocorre que, por muitas vezes, o crime informático não respeita fronteiras, ultrapassando os limites territoriais do Estado. Como bem leciona PRADO:

> Nesse contexto – quando um delito ofende interesses de mais de um Estado que confere a si o direito de puni-lo – surge o Direito Penal Internacional, como o ramo do Direito Penal que regula o complexo de problemas penais que se apresentam no plano internacional, de modo a prevenir e resolver conflitos que surjam entre várias soberanias. (2014, p. 165)

Todavia, a intrincada questão da extraterritorialidade não encontra, lugar em tão rápida pesquisa como essa, sendo objeto de uma abordagem futura própria, diante da especificidade que o tema comporta, os princípios fundamentais que o regem, as hipóteses de aplicação da lei brasileira a crimes ocorridos fora do território nacional, assim como o Poder Judiciário pátrio tem tratado tais questões.

3 A VIOLAÇÃO DO DIREITO À INTIMIDADE E OS PERIGOS DA INFORMÁTICA

Como ensina Paulo José da Costa Júnior, são consideradas manifestações do direito à intimidade, o direito à imagem, à defesa do nome, à tutela da obra intelectual, o direito ao segredo (doméstico, epistolar, documental, profissional). São estes alguns dos aspectos dos direitos a intimidade, mas não todos. A tutela da intimidade poderá ser estendida a outros atributos da personalidade como a voz. (COSTA JÚNIOR, 1970, p. 49)

Uma das formas tradicionais de violação da intimidade é a quebra do sigilo epistolar. Direito ao sigilo da correspondência deflui do direito da intimidade e surgiu com a própria criação do serviço postal. O princípio da inviolabilidade da correspondência se manifesta como tutela indireta do direito à intimidade. Tem por objeto a revelação de sentimentos, opiniões pessoais, desejos, anseios, expectativas e demandas manifestados em qualquer tipo de comunicação.

O sigilo da correspondência é assegurado na Constituição Federal vigente no art. 5º, 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 nas formas que a lei estabelecer para fins de investigação criminal ou instrução processual penal".

Esse sigilo está atualmente estendido às comunicações telegráficas, de dados e telefônicas.

O direito à quietude, à paz interior, à solidão, passou a reclamar tutela mais sólida com o progresso tecnológico, social e econômico da sociedade contemporânea. Assim, como aponta Michele Keiko Mori, ao indivíduo é assegurado o direito de manter-se na reserva, de velar a sua intimidade, de não permitir que seja devassada sua vida privada, de fechar o seu lar à curiosidade alheia. Contudo, esse direito sofre limitações naturais. As delimitações de sua esfera privada deverão ser aceitas tanto pelas necessidades impostas pelo Estado, quanto pelas esferas pessoais das demais pessoas, que poderão conflitar ou penetrar por ela. (2001, p. 51-52)

Na sociedade atual, as novas tecnologias converteram a informação em uma riqueza fundamental da sociedade. Os dados colhidos por estes meios traduzem aspectos da personalidade, revelam comportamentos e preferências, permitindo inclusive se traçar um perfil psicológico do usuário. Com os meios de comunicação cada vez mais interativos, que se estabeleceram de forma contínua e direta entre os gestores dos novos serviços e o indivíduo, permitem não só um controle de comportamento do usuário, mas expõe seus costumes, inclinações e gostos.

Há de se destacar que quanto mais sofisticados são os serviços prestados aos usuários, maior é quota de informação pessoal deixada no provedor do serviço. A necessária proteção à intimidade neste caso é a possibilidade de tais informações serem mal utilizadas, possibilitando a criação de perfis individuais e coletivos.

Concretamente, como afirma Pereira (2008, p. 140), no que tange as garantias fundamentais e, consequentemente, ao direito à intimidade, o advento das novas tecnologias podem acarretar consequências negativas que venham a impedir o exercício de tais direitos, o que implicaria uma adaptação dos direitos já existentes ou até mesmo a criação de outros para que seja possível a salvaguarda dos direitos fundamentais do cidadão.

A cada dia são mais numerosos os processos descobertos pela ciência e pela técnica que permitem a invasão da intimidade. A tarefa do direito consiste em determinar a licitude ou ilicitude dos fins a que se destinam esses recursos tecnológicos.

O progresso da ciência sempre traz consigo uma mudança nos hábitos e comportamentos das pessoas. Nunca, porém o avanço da tecnologia se fez tão presente no cotidiano como ocorre nos dias de hoje, com a informática. Essa evolução, além de proporcionar ao indivíduo diversos benefícios, traz consigo novos perigos, entre eles, ameaças à vida privada.

Assim, na medida em que a computação avança, torna-se importante a proteção da vida privada, uma vez que as informações constantes em bancos de dados nem sempre se destinam apenas a fins científicos, técnicos ou estatísticos.

Muitos desses bancos são criados com o objetivo de armazenar dados pessoais e arquivos confidenciais. Sua finalidade é captar e arquivar a intimidade alheia. Além desse armazenamento de dados, através do computador é possível realizar o cruzamento de informações provenientes de múltiplas fontes, ocasionando a intromissão de terceiros na vida alheia.

Pode-se identificar, entre as fontes de violação, a questão do e-mail e do chat em relação ao direito à intimidade.

> A NET, como é chamada pelos usuários, permite que se faça virtualmente qualquer coisa: comunicação via e-mail, pesquisa, acesso a informações, aquisição de bens ou contratos de serviços, realização de negócios, procura de artigos de jornais, revistas ou músicas de qualquer país do mundo, tudo no conforto e privacidade do lar ou escritório. (2001, p. 6)

Além disso, existe a questão da necessidade de o Estado exercer um certo controle sobre seus administrados, os quais possuem a obrigação de facilitar àquele algumas informações, em troca de uma aparente segurança. Imagine-se a situação de uma prisão em flagrante, onde se questiona a licitude do comportamento dos policiais ao realizar busca em eventual aparelho celular apreendido, consultando imagens, registros de ligações efetuadas e recebidas, bem como o acesso a aplicativos de comunicação, tais como *WhatsApp*, *Skype*, *Snapchat*, *Facebook*, *Instagram* e outros. A questão é complexa, uma vez que as mensagens armazenadas nesses aplicativos podem ser apagadas de maneira remota. Dessa forma, a necessidade de prévia ordem judicial para legitimar o acesso a referidos aplicativos poderá conduzir a perda dos elementos informativos que os órgãos de persecução penal necessitavam para repressão dos delitos.

Trata-se de questão complexa, envolvendo a discussão quanto aos limites da atuação estatal em virtude da proteção da intimidade e do sigilo das comunicações. O debate quanto aos limites impostos pela ordem constitucional à obtenção das provas em respeito à expectativa de

privacidade, é pautado pela análise do uso da tecnologia e seu poder de penetração na intimidade do indivíduo.

Esses questionamentos estão ligados ao denominado direito probatório de terceira geração. Por essas razões, a terceira geração do direito probatório foi ventilada pelo Ministro Rogério Schietti no julgamento do HC nº 51.531-RO (BRASIL, 2016), ao tratar do acesso direto por policiais aos aplicativos instalados em aparelhos de telefonia celular apreendidos. No referido voto, o Ministro promoveu a distinção entre o caso subjacente ao Habeas Corpus e o precedente do Supremo Tribunal Federal o HC 91.867-PA (BRASIL, 2012), que reputando lícita a análise, logo após a prisão em flagrante, dos últimos registros telefônicos armazenados nos aparelhos de telefonia celular apreendidos, sem a necessidade de autorização judicial.

No HC 51.531-RO, a 6ª Turma do STJ entendeu ser ilícita a "a devassa de dados, bem como das conversas de *whatsapp*, obtidas diretamente pela polícia em celular apreendido no flagrante, sem prévia autorização judicial". O Min. Rogério Schietti apontou a distinção em relação ao HC nº 91.867-PA, afastando o precedente do STF. A decisão do STF (HC 91.867/PA) versava sobre o acesso ao registro de chamadas telefônicas efetuadas e recebidas. De tal forma, no precedente da Suprema Corte as autoridades policiais não tiveram acesso às conversas mantidas entre os investigados.

Eis o trecho do HC 91.867-PA que sintetiza o objeto do *writ*:

> Suposta ilegalidade decorrente do fato de os policiais, após a prisão em flagrante do corréu, terem realizado a análise dos últimos registros telefônicos dos dois aparelhos celulares apreendidos. Não ocorrência. 2.2 Não se confundem comunicação telefônica e registros telefônicos, que recebem, inclusive, proteção jurídica distinta. Não se pode interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional é da comunicação de dados e não dos dados. 2.3 Art. 6º do CPP: dever da autoridade policial de proceder à coleta do material comprobatório da prática da infração penal. Ao proceder à pesquisa na agenda eletrônica dos aparelhos devidamente apreendidos, meio material indireto de prova, a autoridade policial, cumprindo o seu mister, buscou, unicamente, colher elementos de informação hábeis a esclarecer a autoria e a materialidade do delito.

Fixadas estas distinções, considerou-se que os atuais *smartphones* são dotados de aplicativos de comunicação em tempo real, razão pela qual a invasão direta ao aparelho de telefonia celular de pessoa presa em flagrante possibilitaria à autoridade policial o acesso a inúmeros aplicativos de comunicação on-line, todos com as mesmas funcionalidades de envio e recebimento de mensagens, fotos, vídeos e documentos em tempo real.

O Min. Nefi Cordeiro salientou que nas "conversas mantidas pelo programa *whatsapp*, que é forma de comunicação escrita, imediata, entre interlocutores, tem-se efetiva interceptação inautorizada de comunicações. É situação similar às conversas mantidas por *e-mail*, onde para o acesso tem-se igualmente exigido a prévia ordem judicial". Por fim, o Min. Rogério Schietti salientou que a "doutrina nomeia o chamado direito probatório de terceira geração, que trata de 'provas invasivas, altamente tecnológicas, que permitem alcançar conhecimentos e resultados inatingíveis pelos sentidos e pelas técnicas tradicionais'". (BRASIL, 2016)

Para corroborar a argumentação, o Min. Schietti citou trecho da obra de autoria de Danilo Knijnik (2014, p. 160):

> A menção a elementos tangíveis tendeu, por longa data, a condicionar a teoria e prática jurídicas. Contudo, a penetração do mundo virtual como nova realidade, demonstra claramente que tais elementos vinculados à propriedade, longe está de abarcar todo o âmbito de incidência de buscas e apreensões, que, de ordinário, exigiriam mandado judicial, impondo reinterpretar o que são "coisas" ou

> "qualquer elemento de convicção", para abranger todos os elementos que hoje contém dados informacionais.

Nesse sentido, tome-se o exemplo de um smartphone: ali, estão e-mails, mensagens, informações sobre usos e costumes do usuário, enfim, um conjunto extenso de informações que extrapolam em muito o conceito de coisa ou de telefone.

Supondo-se que a polícia encontre incidentalmente a uma busca um smartphone, poderá apreendê-lo e acessá-lo sem ordem judicial para tanto? Suponha-se, de outra parte, que se pretenda utilizar um sistema de captação de calor de uma residência, para, assim, levantar indícios suficientes à obtenção de um mandado de busca e apreensão: se estará a restringir algum direito fundamento do interessado, a demandar a obtenção de um mandado expedido por magistrado imparcial de equidistante, sob pena de inutilizabilidade? O e-mail, incidentalmente alcançado por via da apreensão de um notebook, é uma "carta aberta ou não"? Enfim, o conceito de coisa, enquanto res tangível e sujeita a uma relação de pertencimento, persiste como referencial constitucionalmente ainda aplicável à tutela dos direitos fundamentais ou, caso concreto, deveria ser substituído por outro paradigma? Esse é um dos questionamentos básicos da aqui denominada de prova de terceira geração: "chega-se ao problema com o qual as Cortes interminavelmente se deparam, quando consideram os novos avanços tecnológicos: como aplicar a regra baseada em tecnologias passadas, aos presentes e aos futuros avanços tecnológicos"." Trata-se, pois, de um questionamento bem mais amplo, que convém, todavia, melhor examinar. (KNIJNIK, 2014, p. 179)

Concluindo assim que, diante do direito probatório de terceira geração, "o precedente do HC n. 91.867/PA não é mais adequado para analisar a vulnerabilidade da intimidade dos cidadãos na hipótese da apreensão de um aparelho de telefonia celular em uma prisão em flagrante".

Trata-se de um precedente de extrema relevância para a preservação da intimidade do cidadão, uma vez que não há dúvida de que os dados armazenados nos modernos *smartphones*, a exemplo de outros tantos equipamentos eletrônicos, são altamente privativos. A prática inquisitiva de devassar aparelhos que contém este grau de informações deve ser contida pelo Judiciário e autorizada apenas em casos excepcionalíssimos, de forma séria, fundamentada e mediante adequada ponderação dos interesses incidentes.

De não se esquecer que, por outro lado, determinados setores empresariais têm muito interesse na obtenção de informações relativas a potenciais consumidores, ainda que se trate de informações relativas a aspectos íntimos dos mesmos, já que tais informações são importantes para suas políticas de marketing.

Relativamente à utilização da informática e da telemática no tratamento das informações pessoais, o volume de dados que circula diariamente pela Internet é enorme. Algumas dessas informações são fornecidas por seus titulares, mas parte desses dados é recolhida na rede de forma dissimulada.

O direito à intimidade, em sua concepção clássica, é um direito de defesa contra intromissões alheias. Com o fenômeno informático, esse direito vem sofrendo graves ameaças e lesões, o que vem trazendo à baila a necessidade ou não da criação de um ramo autônomo do Direito para tratar a questão. Nesse aspecto, existem juristas que defendem essa necessidade, diante da especificidade do bem jurídico a ser protegido por esse novo direito, e a insuficiência dos mecanismos legais para a proteção da intimidade; e outros que entendem que o bem jurídico protegido continua sendo o mesmo, ou seja, a intimidade, dispensando um novo sistema.

Há de se destacar que quanto mais sofisticados são os serviços prestados aos usuários, maior é quota de informação pessoal deixada no provedor do serviço. A necessária proteção à intimidade neste caso é a possibilidade de tais informações serem mal utilizadas, possibilitando a criação de perfis individuais e coletivos. Concretamente, como afirma Marcelo Pereira (2008, p. 140), no que tange as garantias fundamentais e, consequentemente, ao direito à intimidade, o advento das novas tecnologias podem acarretar consequências negativas que venham a impedir o

exercício de tais direitos, o que implicaria uma adaptação dos direitos já existentes ou até mesmo a criação de outros para se poder salvaguardar os direitos fundamentais do cidadão.

CONCLUSÃO

O que deve ser evidenciado aqui, é que com o tratamento dos dados pessoais por meio da internet, a intimidade passou a estar muito mais vulnerável, visto que os meios informáticos e telemáticos facilitam enormemente o tratamento dessas informações. O direito à intimidade em sua concepção mais tradicional é um direito de defesa contra intromissões alheias, que faculta ao indivíduo um direito negativo que resulta na possibilidade de afastamento dos demais do seu âmbito privado, estabelecido pelo próprio detentor do direito.

Assim, como afirma Marcelo Pereira (2008, p. 144), será preciso verificar se o direito à intimidade foi capaz de evoluir e se adaptar a esse novo desafio, que consiste especificamente na coexistência pacífica do uso cada vez mais constante das novas tecnologias e o respeito às pessoas.

Dessa forma, o direito à intimidade começa com um aspecto negativo, o direito a não ser molestado, e evolui em direção a um aspecto positivo, o direito de pedir a prestação do Estado.

Daí, resultam a objetividade dos dados, o direito ao esquecimento, a necessidade de prazo para armazenamento de informações negativas e a comunicação de repasse de dados, a fim de favorecer o direito de acesso e retificação de dados. (LIMBERGER, 2007, p. 40)

De não se olvidar que o Direito tem por finalidade manter a paz social, bem como promover o bem comum, motivo pelo qual deve atuar em todas as áreas de interesse do indivíduo, entre as quais está a Internet, que revolucionou o modo de vida do homem moderno.

Por mais que a utilização das tecnologias ligadas ao mundo virtual esteja altamente interligada ao cotidiano do brasileiro, a legislação pátria ainda está bastante aquém de uma fiscalização adequada deste meio de comunicação. A cada dia, novas formas de violação de direitos pela internet são verificadas pelas autoridades sem que exista uma legislação contemporânea capaz de, ao menos, conter a reiteração destes delitos no ordenamento pátrio.

Surge a partir dessa situação uma colisão de direitos fundamentais, uma vez que o direito à liberdade de expressão e de informação afronta-se diretamente com a intimidade dos indivíduos, visto que as novas tecnologias apresentam caráter libertário, já que qualquer pessoa pode ser emissora ou receptora de informações.

A divulgação de dados pessoais e de informações que interferem diretamente na vida intima das pessoas e até mesmo a veiculação de vídeos não autorizados são situações que se tornam cada vez mais comuns no chamado espaço virtual. Cabe ao Judiciário adequar-se a essas situações, aperfeiçoando o processo de ponderação de direitos a ser aplicado nos casos concretos a ele apresentados, a fim de se evitarem prejuízos excessivos às partes litigantes.

É fundamental se destacar que o advento das novas tecnologias requer uma mudança de comportamentos, inclusive dos próprios usuários da Internet, pois esses deverão ter precaução ao disponibilizar informações ou dados pessoais junto a serviços oferecidos na web, uma vez que o fim a que se destinam muitas vezes é incerto e pode trazer consequências gravosas à sua intimidade e vida privada. No entanto, algo se mostra extremamente importante em todo o contexto apresentado é a necessidade de uma inovação legislativa com o fim de garantir ao cidadão o respeito a direitos fundamentais que são constantemente violados em face das novas tecnologias.

O Direito deve acompanhar a evolução social, tutelando situações que, se outrora pareciam pacificadas, hoje ganharam novos contornos e carecem, pois de uma proteção específica, como é caso da intimidade frente às novas tecnologias da informação. Mesmo cercado de todos os cuidados possíveis, o cidadão ainda continua vulnerável a lesões, já que o processo informático se encontra, hoje, amplamente utilizado nas relações sociais e profissionais. Muitos países já implementaram reformas em seu ordenamento jurídico no sentido de dar maior proteção aos dados e informações que circulam na Internet.

O Direito à intimidade e à vida privada ganhou novos contornos e o Brasil não pode ficar alijado desse processo de modernização legislativa. Os institutos jurídicos existentes não são mais suficientes para dirimir os conflitos surgidos com as inúmeras inovações tecnológicas

Enquanto a criminalidade virtual avança em paços largos, a legislação caminha calmamente, pois, como foi demonstrado nesta pesquisa, há apenas duas leis completamente dedicadas aos crimes informáticos atualmente em vigor no Brasil. No entanto, o cometimento destes crimes só aumenta, violando direitos fundamentais e deixando a sociedade à margem de uma proteção efetiva. Este crescimento de delitos provoca uma avalanche processual no judiciário, o qual, sem uma legislação forte e contemporânea, precisa recorrer a outros institutos jurídicos para tentar solucionar os casos da melhor forma possível, o que causa uma maior lentidão neste poder.

Por isso, mostra-se extremamente necessário que o legislador trabalhe no sentido de editar legislações mais completas, que atinjam todas as vertentes dos crimes informáticos, punindo desde os delitos mais simples até aqueles que violam a sociedade como um todo, como o racismo, o preconceito, dentre outros. Ademais, devem ser criados instrumentos legais adaptáveis às contínuas mudanças tecnológicas, evitando, assim, a criação de normas ultrapassadas, engessadas à realidade vigente em sua concepção e que, consequentemente, não tem os mecanismos necessários ao combate dos delitos informáticos desenvolvidos após a sua edição.

Sem esta ação legislativa, o Brasil continuará nas mãos de criminosos ardilosos, conhecedores dos mais secretos detalhes do mundo virtual, exigindo cada vez mais esforço interpretativo dos tribunais para tentar punir os delitos que, até então, permanecem no ordenamento pátrio sem os tão desejados óbices legais.

REFERÊNCIAS BIBLIOGRÁFICAS

AMARAL, Francisco. *Direito civil: introdução*. 4. Ed. Rio de Janeiro: Renovar, 2002.

BARBOSA JÚNIOR, Sérgio José. *Crimes informáticos: breves considerações sobre os delitos virtuais no ordenamento jurídico brasileiro*. https://jus.com.br/artigos/29634. Acesso em: 09/10/2019.

BITTAR, Carlos Alberto. *Os direitos da personalidade*. 5. ed. Rio de Janeiro: Forense Universitária, 2001.

BRASIL. *Código Civil, Lei 10.406*, de 10 de janeiro de 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406.htm. Acesso em: 09/10/2019.

BRASIL. *Constituição da República Federativa do Brasil*, de 05 de outubro 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 09/10/2019.

BRASIL. Decreto nº 8.771, De 11 de maio de 2016. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2016/Decreto/D8771.htm. Acesso em: 09/10/2019.

BRASIL. Superior Tribunal de Justiça. HC nº 51.531-RO. 6 Turma. Rel. Min. Nefi Cordeiro. DJe: 09/05/2016. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/340165638/recurso-ordinario-em-habeas-corpus-rhc-51531-ro-2014-0232367-7. Acesso em:11/10/2019.

BRASIL. Supremo Tribunal Federal Justiça. HC nº 91.867-PA. 6 Turma. Rel. Min. Gilmar Mendes. DJe: 20/09/2012. Disponível em:

https://stf.jusbrasil.com.br/jurisprudencia/22869954/habeas-corpus-hc-91867-pa-stf/inteiro-teor-111144852?ref=juris-tabs. Acesso em:11/10/2019.

CAPUTO, Vitor. *Pornografia infantil é o crime virtual mais comum no Brasil*. Exame.com. São Paulo: Abril, 2014. Disponível em: http://exame.abril.com.br/tecnologia/noticias/pornografia-infantil-e-o-crime-virtual-mais-comum-no-brasil. Acesso em: 09/10/2019.

CASTRO, Carla Rodrigues Araújo de. *Crimes de informática e seus aspectos processuais*, 2. Ed. Rio de Janeiro: Editora Lúmen Juris, 2003.

COLLI, Maciel. *Cibercrimes: limites e perspectivas para a investigação preliminar policial brasileira de crimes cibernéticos*. Porto Alegre: PUCRS, 2009. Disponível em: http://tede.pucrs.br/tde_busca/arquivo.php?codArquivo=2477 Acesso em: 09/10/2019.

COSTA, Fernando José da. *Locus delicti nos crimes informáticos*. São Paulo: USP, 2011. Disponível em: http://www.teses.usp.br/teses/disponiveis/2/2136/tde-24042012-112445/pt-br.php.Acesso em: 09/10/2019.

COSTA JÚNIOR, Paulo José da. *Agressões à intimidade*. São Paulo, Malheiros, 1997.

_____. *O direito de estar só: tutela penal da intimidade.* São Paulo: Editora Revista dos Tribunais, 1970.

DELGADO, Lucrecio Rebollo. *Derechos fundamentales y proteción de datos, apud*, GRECO, Rogério. *Princípios penais constitucionais*. Salvador: Editora JusPODIVM, 2007.

DOTTI. René Ariel. *Proteção da vida privada e liberdade de informação*. São Paulo: Editora Revista dos Tribunais, 1980.

ESPANHA, *Constitucion Española, de 27 de diciembre de 1978*. Disponível em: https://www.iberley.es/legislacion/constitucion-espanola-27-dic-1978-715707 Acesso em: 09/10/2019.

FELICIANO, Guilherme Guimarães. *Informática e criminalidade: primeiras linhas*. Ribeirão Preto: Nacional de Direito Livraria Editora, 2001.

GIMENES, Emanuel Alberto Sperandio Garcia. *Crimes virtuais*. Revista de Doutrina n.º 55. Porto Alegre: TRF4, 2013. Disponível em: http://www.revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html. Acesso em: 09/10/2019.

GONÇALVES, Carlos Roberto. *Direito civil brasileiro*. 14. ed. São Paulo: Saraiva, 2016. v.1.

GUARDIA, Gregório Edoardo Raphael Selingardi. *Comunicações eletrônicas e dados digitais no processo penal.* São Paulo: USP, 2012. Disponível em: http://www.teses.usp.br/teses/disponiveis/2/2137/tde-02042013-02504/publico/DissertaParcial_Gregorio_Edoardo_Raphael_Selingardi_Guardia.pdf. Acesso em: 21/09/2019.

KNIJNIK, Danilo. *Temas de direito penal, criminologia e processo penal. A trilogia Olmstead-Katz-Kyllo: o art. 5º da Constituição Federal do Século XXI*. Porto Alegre: Livraria do Advogado, 2014.

KERR, Vera Kaiser Sanches. *A disciplina, pela legislação processual penal brasileira, da prova pericial relacionada ao crime informático praticado por meio da internet.* São Paulo: USP, 2011. Disponível em: http://www.teses.usp.br/teses/ disponiveis/3/3142/tde-07112011 Acesso em: 09/10/2019.

LIMBERGER, Têmis. *Direito à intimidade na era da informática: a necessidade proteção dos dados pessoais.* Porto Alegre: Livraria do Advogado, 2007.

MORAES, Alexandre de. *Direito constitucional*. 32 ed. São Paulo: Atlas, 2016.

MORI, Michele Keiko. *Direito à intimidade versus informática*. Curitiba: Juruá, 2001.

NUCCI, Guilherme de Souza. *Manual de direito penal*. 10 ed. Rio de Janeiro: Forense, 2014.

OLIVEIRA, Almir de. *Curso de Direitos Humanos*, Rio de Janeiro: Editora Forense, 2000.

ONU. Declaração Universal dos Direitos Humanos. Gabinete do Alto Comissionado. Direitos Humanos. 10 de dezembro de 1948. Disponível em: https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/por.pdf. Acesso em: 21/09/2019.

PEREIRA, Marcelo Cardoso. *Direito à intimidade na internet*. Curitiba: Juruá, 2008.

PINHEIRO, Emeline Piva. *Crimes virtuais: uma análise da criminalidade informática e da resposta estatal.* Porto Alegre: PUCRS, 2016. Disponível em: http://www3.pucrs.br/pucrs/files/uni/poa/direito/graduacao/tcc/tcc2/trabalhos2006_1/emeline.pdf. Acesso em: 21/09/2019.

PRADO. Luiz Regis. *Curso de direito penal brasileiro*. 13 ed. São Paulo: Editora Revista dos Tribunais, 2014.

SBARDELOTTO, Fábio Roque. *Direito penal no estado democrático de direito: perspectivas (re)legitimadoras*. Porto Alegre: Livraria do Advogado, 2001.

SCHIMITT, Ricardo Augusto (organizador). *Princípios penais constitucionais: direito e processo penal à luz da constituição federal*. Salvador: Editora Juspodivm, 2007.

SILVA, Edson Ferreira da. *Direito à intimidade*. São Paulo: Oliveira Mendes, 1998.

SILVA, José Afonso da, *Curso de direito constitucional positivo*, 33. ed. São Paulo: Malheiros, 2009

SILVA, Rita de Cássia Lopes da. *Direito penal e sistema informático*. São Paulo: Editora Revista dos Tribunais, 2003.

SYDOW, Spencer Toth. *Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática.* São Paulo: USP, 2009. http://www.teses. usp.br/teses/disponiveis/2/2136/tde-15062011-161113 Acesso em: 21/09/2019.

VIANA, Túlio Lima. *Do acesso não autorizado a sistemas computacionais: fundamentos do direito penal informático*. Belo Horizonte: UFMG, 2001. Disponível em: http://www.bibliotecadigital.ufmg.br/dspace/handle/1843/BUOS-96MPWG Acesso em: 21/09/2019.