Revista Juris UniToledo

PROTEÇÃO ESTATAL CONFERIDA ÀS RELAÇÕES VIRTUAIS

STATE PROTECTION CONFERRED TO VIRTUAL RELATIONS

Marcela Pache Lopes Rodrigues[1]
Renata Ortega Rodrigues Mungo[2]
Renato Alexandre da Silva Freitas[3]

RESUMO: Devido aos inúmeros avanços vivenciados pela humanidade nas últimas décadas, vivemos atualmente em uma sociedade globalizada. Entretanto, em que pese as consideráveis facilidades e utilidades que os meios tecnológicos propiciaram ao ser humano, valores como privacidade, intimidade e a honra, enquanto elementos constitutivos

[1] Pós-graduada em Direito Civil e Direito Processual civil pelo Centro Universitário Toledo – Unitoledo. Pós-graduada em Direito Penal pelo Damásio Educacional. Bacharel em direito pelo Centro Universitário Toledo – Unitoledo (2016). Mediadora judicial. Membro da Comissão Estadual de Diversidade Sexual e de Gênero (2019-2021). Membro da Comissão Estadual da Mulher Advogada (2019-2021). Presidente da Comissão da Mulher Advogada da 68ª Subseção Birigui/SP (2019-2021). Presidente da Comissão de Cultura e Eventos da 68ª Subseção Birigui/SP (2019-2021). Vice-Presidente da Comissão da Jovem Advocacia da 68ª Subseção Birigui/SP (2019-2021). Coordenadora do Projeto OAB VAI À ESCOLA da 68ª Subseção Birigui/SP (2019-2021). Membro da Comissão Especial de Ação Social e Cidadania da 68ª Subseção Birigui/SP (2019-2021). Advogada.

[2] Pós-graduanda em Direito Civil e Direito Processual Civil pelo Centro Universitário Toledo – Unitoledo. Advogada.

[3] Doutorando em Ciências Jurídicas pela Universidade Estadual do Norte do Paraná (UENP) – Jacarezinho/PR. Mestre em Direito na área de concentração de Tutela Jurisdicional no Estado Democrático de Direito, pelo Centro Universitário Toledo (UNITOLEDO) – Araçatuba/SP. Especialista em Direito Processual, Direito Tributário e Docência no Ensino Superior pelo UNITOLEDO. Graduado em Direito pelo UNITOLEDO. Coordenador da Graduação e da Pós-Graduação em Direito do UNITOLEDO. Professor de Direito Tributário e Direito Empresarial no Curso de Graduação em Direito e de Legislação Tributária no Curso de Administração da Instituição. Mediador com certificação expedida pela Escola Paulista da Magistratura. Membro do Conselho Nacional de Pesquisa e Pós-Graduação em Direito (CONPEDI) e da Comissão Científica do Encontro de Ensino, Pesquisa e Extensão (ENPEX). Coordenador do Fórum Jurídico do UNITOLEDO. Autor e coautor de obras jurídicas. Advogado.

Artigo submetido em 20/06/2019 e aprovado em 05/03/2020

de sua personalidade estão sendo relativizados, pois, constata-se, cada vez mais, a confusão entre a vida privada das pessoas e o ambiente digital. Por essa razão, o presente artigo apresenta como principal finalidade o estudo desse fenômeno social e de que forma ele tem afetado esses valores constitucionalmente consagrados. Para tanto, serão expostas neste estudo algumas considerações a respeito dos principais problemas enfrentados pelos usuários da rede mundial de computadores na atualidade. Consequentemente, também será analisado o tratamento conferido pelo ordenamento jurídico pátrio em razão da violação de direitos e garantias fundamentais também em ambiente digital.

Palavras-Chave: Internet. Direitos e Garantias Fundamentais. Direito Digital.

ABSTRACT: Due to the many advances that humanity has experienced over the last decades, we are currently living in a globalized society. However, in spite of the considerable facilities and utilities that the technological means provided to the human being, values such as privacy, intimacy and honor, as constitutive elements of their personality are being relativized, since, it is increasingly evident the confusion between people's private lives and the digital environment. For this reason, the main purpose of this article is to study this social phenomenon and how it has affected these constitutionally consecrated values. To this end, we will present in this study some considerations regarding the main problems faced by the users of the world wide computer network today. Consequently, it will also analyze the treatment conferred by the national legal order for violation of fundamental rights and guarantees also in the digital environment.

Keywords: Internet. Fundamental Rights and Guarantees. Digital Right.

INTRODUÇÃO

É evidente que os avanços tecnológicos vivenciados pela humanidade nas últimas décadas, em especial o desenvolvimento de mecanismos informáticos e de comunicação, influenciaram a forma de organização da sociedade contemporânea.

Entretanto, em que pese os grandes avanços propiciados pelas inovações desenvolvidas no ambiente digital, a intensificação da utilização dessas plataformas tecnológicas vem ocasionado, em contrapartida, diversas desvantagens aos seus usuários.

Dentre esses malefícios, destacam-se a violação de valores e garantias fundamentais elencadas pela Carta Magna brasileira, a exemplo do Direito à privacidade e intimidade dos seus usuários. Por outro lado, a maximização desses mecanismos informáticos também tem colaborado para o aumento dos chamados "crimes cibernéticos", facilitando a prática das mais variadas condutas delituosas na internet.

Embora ainda não seja um ramo autônomo do Direito, a tendência é que futuramente, com a edição de outras normas atinentes à matéria, a legislação seja unificada, a fim de garantir melhor aplicabilidade, e consequentemente, maior resguardo jurídico aos usuários da internet, os quais só tendem a aumentar nos próximos anos.

Em razão disso, o objetivo principal da presente pesquisa acadêmica é o de analisar o atual panorama do Direito Digital em âmbito nacional, assim, serão analisadas as atuais ferramentas jurídicas existentes voltadas à proteção dos internautas brasileiros, a fim de resguardar direitos e garantias constitucionalmente estabelecidas coladas em risco pela utilização das vias digitais, em especial o direito à privacidade e o da intimidade.

1- Lei "Carolina Dieckmann": 12.737/2012

A Lei nº 12.737/2012, também intitulada de "Lei Carolina Dieckmann", representa um precedente para legislação brasileira no que concerne à tipificação de crimes informáticos. Antes de adentrarmos nas disposições normativas propriamente ditas, convém abordar as circunstâncias que à época acarretaram a edição do referido diploma legal.

No ano de 2012, o computador pessoal da atriz Carolina Dieckmann foi atacado por hackers, os quais divulgaram inúmeras fotos da atriz em momentos íntimos nas redes sociais e plataformas digitais.

Segundo laudo pericial realizado pela Polícia Civil, a atriz teria clicado em um link malicioso enviado para o seu e-mail pessoal, e por consequência, involuntariamente, teria feito o download de um vírus conhecido como "cavalo de troia", espécie de malware que

se aloja em programas e acessórios do computador e obtém acesso aos dados e arquivos pessoais do usuário.

Devido à grande repercussão do caso, aliada à necessidade de subsunção dessa conduta a algum tipo penal, foi sancionada no mesmo ano, pela então Presidente da República, Dilma Rousseff, o referido diploma legal em comento, o qual acrescentou e alterou artigos do Código Penal, a fim de garantir uma resposta estatal aos delitos cibernéticos.

Pela análise das disposições trazidas por essa inovação legislativa, verifica-se que o legislador, ao elaborar o artigo 2º, da Lei nº 12.737/2012, criou um novo comando normativo, o qual foi acrescido por meio do artigo 154-A ao Código Penal, nestes termos:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. (BRASIL, 2012)

Pela análise da norma incriminadora, vislumbra-se que para configuração do crime em questão, é necessária a existência concomitante de três elementos: Primeiramente, deverá haver a invasão ou tentativa de invasão de dispositivo de informática. Da mesma forma, com o emprego da expressão “alheio”, percebe-se que a propriedade do dispositivo deverá ser de uma terceira pessoa, que não a do invasor. Por fim, é prescindível que o dispositivo invadido esteja conectado ou não à internet, eis que restará configurado o tipo penal em comento mesmo se ele estiver desconectado.

Neste momento uma ressalva. Para a fácil compreensão das próximas colocações, necessária a distinção entre os conceitos informáticos de hardware e software. Logo, por hardware, entendem-se todos os mecanismos físicos do dispositivo informático, como por exemplo, o monitor, a impressora, e o dispositivo de armazenamento propriamente dito (Central Processing Unit). Por sua vez, software refere-se aos aplicativos, programas e sistemas operacionais que viabilizam o funcionamento do dispositivo, e consequentemente, o desempenho de outras funções, como é o caso do acesso à internet.

Justamente com base nessa definição, a lei em questão recebeu duras críticas por parte dos estudiosos do Direito quando de sua aprovação, principalmente pelo elemento do tipo constante no artigo 154-A, eis que segundo eles, a utilização da expressão “dispositivo

informático" seria muito abstrato, e que por consequência, pela falta de delimitação da referida locução, algumas possíveis interpretações poderiam acabar por excluir os delitos cibernéticos nos quais a invasão ocorre em plataformas digitais, independentes da invasão do hardware propriamente dito, como é o caso da invasão e roubo de contas pessoais em redes sociais.

Ademais, outra crítica reside no elemento subjetivo do tipo, qual seja, a invasão desautorizada do dispositivo com o intuito de "obter, adulterar ou destruir dados ou informações" do usuário, pois segundo alguns estudiosos, ao prever essa finalidade específica, a lei deixou de englobar ingressos desautorizadas com outras finalidades. Nesse sentido, cabe reproduzir os ensinamentos trazidos por Sydow (2013, p. 292):

> Acreditamos ser imprescindível que o dolo seja o de afetar dados ou informações específicas, bem como que as mudanças em arquivos ocorridas com a mera finalidade de ingresso no sistema (por exemplo leitura dos arquivos de log para descobrimento da senha de acesso a uma determinada pasta), por si sós, não bastam para a caracterização do delito por serem meramente meio e não finalidade do agente. Isso porque não restou como conduta tipificada o mero ingresso desautorizado sem finalidade específica. Vinculou o legislador a conduta de ingresso forçado à finalidade do agente acerca de dados ou acerca de vantagem.

Em que pese as mencionadas críticas, deve-se ressaltar os inúmeros progressos propiciados pela referida lei. Dentre esses benéficos, a incriminação de uma conduta muito frequente na atualidade: a elaboração, distribuição e venda de programas voltados para a invasão de dispositivos informáticos.

A negociação dos referidos softwares, na maioria das vezes, acontece na chamada "Deep Web", um lado obscuro e paralelo da rede mundial de computadores, muito utilizada por criminosos, devido à difícil localização e registro das atividades realizadas por seus usuários.

Sendo assim, para inibir a prática dessas condutas, a Lei nº 12.737/2012, estabeleceu que as consequências jurídicas para esta modalidade de crime cibernético seriam as mesmas previstas para o delito de invasão de dispositivo de informática. Nesse sentido, as disposições trazidas pelo art.154-A, §1º, do Código Penal:

> § 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. (BRASIL, 2012)

Ademais, segundo o mesmo diploma legal, se a invasão digital ocasionar prejuízos econômicos à vítima, a pena estabelecida pelo caput do art. 154-A, será aumentada na proporção de um sexto até um terço.

Por outro lado, outra importante inovação trazida pela Lei nº 12.737/2012, refere-se à punição mais gravosa dessa modalidade de crime digital, quando a invasão do dispositivo de informática objetivar a captação de conversas privadas em meios eletrônicos, segredos ligados às atividades comerciais ou industriais, dados sigilosos (assim considerados por lei), ou ainda, apresentem como finalidade o controle remoto do aparelho eletrônico, conforme enunciado trazido pelo art. 154-A, §3º, do Código Penal:

> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. (BRASIL, 2012)

Além disso, haverá um aumento de pena, na proporção de um a dois terços, caso as informações obtidas sejam divulgadas, transmitidas ou repassadas a um terceiro, seja a título gratuito ou oneroso, conforme previsão do art. 154-A, §4º, do Código Penal:

> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

De igual forma, haverá também um aumento de pena do crime em questão, na proporção de um terço à metade, nas hipóteses em que a invasão digital apresentar como alvo dispositivos informáticos pertencentes a membros do Poder Judiciário, Legislativo ou Executivo, assim como, de dirigentes de entidades integrantes da administração indireta, a exemplo das empresas estatais. Nesta orientação, as disposições trazidas pelo art. 154-A, §5º, incisos I, II, III e IV, do Código Penal:

> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (BRASIL, 2012)

Por fim, registra-se que segundo as atuais configurações do sistema processual penal brasileiro, a propositura da ação penal nos casos de crime cibernético está condicionada, em regra, à representação da vítima. Entretanto, quando o delito é cometido contra administração pública, direta ou indireta, bem como, por equiparação, contra empresas concessionárias de serviços públicos, a ação penal nesses casos será pública incondicionada, viabilizando o oferecimento imediato da respectiva denúncia por parte do Ministério Público. Sobre referida regra, o comando normativo consubstanciado no art. 154-B, do Código Penal, trazido pela Lei nº 12.737/2012, nestes termos:

> 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 ou Municípios ou contra empresas concessionárias de serviços públicos.

Como se percebe, a Lei nº 12.737/2012, intitulada de "Lei Carolina Dieckmann", representou um grande avanço para a responsabilização de infratores em âmbito cibernético, os quais, antes do advento da referida disposição normativa, eram agraciados pela impunidade.

Por consequência, oportuno analisarmos neste momento outra importante legislação no que diz respeito à utilização dos meios digitais no Brasil, assim, a Lei nº 12.965/2014, conhecida como "Marco Civil de Internet".

2- Lei nº 12.965/2014: Marco Civil da Internet

Sancionada pela então Presidenta da República, Dilma Rousseff, a Lei nº 12.965/2014, também conhecida como Marco Civil da Internet, representou avanço significativo para a proteção dos usuários em ambiente digital em plano nacional, pois através da edição desse diploma legal foram estabelecidos inúmeros fundamentos, regras e princípios para a utilização da internet no Brasil, assim como, obrigações e direitos até então nunca previstos para os usuários das plataformas digitais.

Ademais, registra-se a importância da promulgação de referida lei, eis que se demonstrou necessária para o preenchimento de diversas lacunas jurídicas em relação ao tema em questão, assim, as garantias dos usuários da internet.

Dentre os fundamentos estabelecidos para utilização da internet em âmbito nacional, consubstanciados pelo comando normativo supracitado, destacam-se o respeito pela liberdade de expressão no ambiente digital, o resguardo e proteção aos direitos humanos, e a finalidade social intrínseca ao uso da rede mundial de computadores. Neste sentido, os preceitos emanados pelo art. 2º, incisos I, II, III, IV, V e VI da Lei nº 12.965/2014, nestes termos:

> Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
> I - o reconhecimento da escala mundial da rede;
> II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
> III - a pluralidade e a diversidade;
> IV - a abertura e a colaboração;
> V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VI - a finalidade social da rede. (BRASIL, 2014)

Ademais, outras importantes diretrizes no que tange à utilização da internet em plano nacional foram consagradas pelo diploma legal em comento, a exemplo da garantia de neutralidade da rede, liberdade para o empreendedorismo em âmbito digital e o respeito à segurança e preservação de dados dos usuários das plataformas digitais. Nesse sentido, as disposições elencadas pelo artigo 3º, incisos III, IV e VIII, da Lei nº 12.965/2014, nestes termos:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: [...]
> III - proteção dos dados pessoais, na forma da lei;
> IV - preservação e garantia da neutralidade de rede; [...]
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei. (BRASIL, 2014)

Por consequência, verifica-se que o advento da norma em questão só veio efetivar direitos e garantias fundamentais já previstos pela carta constitucional também em âmbito digital. Prova disso é o resguardo normativo com relação à inviolabilidade do sigilo dos dados e informações trocadas pelo usuário em ambiente digital. Nesta linha de raciocínio, o enunciado do artigo 7º, inciso II, da Lei nº 12.965/2014:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; (BRASIL, 2014)

Nesta mesma orientação, a previsibilidade quanto ao resguardo e proteção da privacidade e da intimidade do usuário das plataformas digitais, garantindo, consequentemente, o direito à indenização pelos danos morais e materiais sofridos em decorrência da violação, conforme assegurado pelo art. 7º, inciso I, da Lei nº 12.965/2014:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; (BRASIL, 2014)

Por outro lado, estabelece também como garantia do usuário do ambiente digital o direito de não fornecimento e disseminação de seus dados e informações pessoais a terceiros. Apesar de vedada, essa prática ainda é muito utilizada por diversas empresas brasileiras, em especial, por aquelas ligadas à prestação de serviços e do setor varejista. Contra referida prática, as disposições normativas do artigo 7º, inciso VII, da Lei nº 12.965/2014:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; (BRASIL, 2014)

Reforçando esse dever de respeito à intimidade do usuário, a Lei nº 12.965/2014 elenca a garantia à privacidade como condição para o pleno exercício do direito de acesso à internet, conforme disposição consubstanciada pelo artigo 8º, caput, da referida lei:

> Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet. (BRASIL, 2014)

Consequentemente, serão consideradas nulas eventuais cláusulas contratuais que violem os deveres de sigilo das comunicações dos usuários em ambiente digital ou privacidade (artigo 8º, parágrafo único, inciso I, da Lei nº 12.965/2014). Como exemplo dessas disposições abusivas, poderíamos citar eventual disposição contratual condicionando a prestação dos serviços digitais mediante autorização do usuário para captura e repasse de suas informações pessoais.

Ademais, da mesma forma em que zela pela preservação de dados e informações pessoais dos usuários, a Lei nº 12.965/2014 confere proteção normativa também ao sigilo

das mensagens trocadas entre os internautas, de carácter privado, prevendo também a inviolabilidade de segredo dessas informações. Nesta linha de raciocínio, as disposições consagradas pelo artigo 10º, caput, do referido diploma legal:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. (BRASIL, 2014)

Além disso, convém destacar que o fornecimento desses dados sigilosos somente será procedido pelo servidor responsável pela guarda dessas informações mediante ordem judicial, devidamente fundamentada, conforme ensinamentos contidos no artigo 10º, §1º e §2º, da Lei nº 12.965/2014, nestes termos:

> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no **caput,** de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.
> § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º. (BRASIL, 2014)

Ainda sobre as principais regras consubstanciadas pelo Marco Civil da Internet, cumpre analisar a responsabilidade do provedor de internet com relação ao conteúdo disponibilizado nas plataformas digitais por terceiros. De acordo com o artigo 18 da Lei nº 12.965/2014, em regra, o provedor não será civilmente responsabilizado pelos danos morais ou materiais decorrentes de publicações ou conteúdo disponibilizado em suas plataformas por outros usuários.

Entretanto, haverá a responsabilização do provedor de internet, caso devidamente cientificado por ordem judicial, não realize no prazo assinalado a retira de conteúdo disponibilizado em suas plataformas digitais por terceiros, julgados impróprios ou que apresentem conteúdo ofensivo. Nesse sentido, as disposições trazidas pelo artigo 19, *caput*, da Lei nº 12.965/2014:

> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível

> o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário. (BRASIL, 2014)

Por fim, segundo as orientações emanadas pelo Marco Civil da Internet, é de responsabilidade do ente público formular e financiar estudos relacionados à utilização da internet em âmbito nacional, a fim de que sejam desenvolvidos mecanismos digitais no Brasil, bem como, com a finalidade de se aprimorar aqueles já existentes (artigo 28 da Lei nº 12.965/2014).

3- A interceptação de dados para fins investigativos: Lei nº 9.296/96

Antes de adentrarmos nas considerações trazidas pela Lei nº 9.296/96 propriamente ditas, necessário reproduzir um debate doutrinário e jurisprudencial que por muito estende na ordem jurídica brasileira: a possibilidade ou não da interceptação de dados telemáticos para fins investigativos.

Como visto, o artigo 5º, inciso XII, da Constituição Federal de 1988, garante a inviolabilidade de sigilo das comunicações telegráficas, de dados e das comunicações telefônicas. Por outro lado, estabelece também que referido sigilo poderá ser relativizado, quando o acesso aos mencionados dados for imprescindível para instrução criminal.

O grande problema reside na distribuição das expressões do referido comando normativo, eis que a previsão estabelecida pelo constituinte no artigo 5º, inciso XII, leva a entender que essa "quebra de sigilo" se estenderia apenas às comunicações telefônicas, pois utilizada a seguinte frase "[...] 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).

Por consequência, dois posicionamentos distintos foram criados entre os estudiosos do Direito, dessa forma, para os defensores da primeira corrente a inviolabilidade de sigilo das comunicações seria de natureza absoluta em relação às correspondências telegráficas e de dados telemáticos, pois a carta constitucional expressamente prevê a relativização apenas às comunicações telefônicas.

Por outro lado, os adeptos da segunda linha de pensamento defendem que a relativização do sigilo se estenderia também aos outros meios de comunicação, pois inexiste na ordem constitucional vigente direito ou garantia individual de natureza

absoluta. Como defensores desta corrente, destacam-se os ensinamentos trazidos por Mendes, Coelho e Branco (2009, p. 435)

> A leitura do preceito pode levar à conclusão de que apenas nos casos de comunicações telefônicas seria possível que o Poder Público quebrasse o sigilo e que seria impossível abrir ao seu conhecimento os dados constantes de correspondência postal, telegráfica ou de comunicações telemáticas. Sabe-se, porém, que a restrição de direitos fundamentais pode ocorrer mesmo sem autorização expressa do constituinte, sempre que se fizer necessária a concretização do princípio da concordância prática entre ditames constitucionais. Não havendo direitos absolutos, também o sigilo de correspondência e o de comunicações telegráficas são passíveis de ser restringidos em casos recomendados pelo princípio da proporcionalidade.

Corroborando este entendimento, os pronunciamentos proferidos pelo Supremo Tribunal Federal em relação ao assunto, destacando-se o julgamento das seguintes ações: Recurso Ordinário em Habeas Corpus (RHC) 132115 e HC 70814. Como fundamento, os ministros da Suprema Corte destacaram que nenhuma garantia constitucional é absoluta e, consequentemente, os sigilos dos dados telemáticos poderão ser alcançados para fins investigativos mediante decisão judicial fundamentada.

Ora, concordamos com o posicionamento supracitado. Limitar o alcance da Lei nº 9.296/96 às comunicações telefônicas tornaria a norma extremamente obsoleta, frente às inúmeras tecnologias desenvolvidas atualmente, as quais vêm tornando o uso das ligações telefônicas menos frequentes.

Feitas tais considerações, analisaremos agora as disposições normativas trazidas pelo referido diploma legal. Como mencionado, apesar de amplamente conhecida como "Lei da Interceptação Telefônica", os preceitos e regras nela estabelecidos também são aplicáveis às comunicações telemáticas. Nesse sentido, o enunciado contido no art. 1º, parágrafo único, da Lei nº 9.296/96:

> Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.
> Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática. (BRASIL, 1996)

Como se vê, referida medida investigativa poderá ser solicitada pelo *parquet* ou pela autoridade policial já na fase de investigação criminal (Inquérito Policial), assim como, para embasar eventual instrução probatória na fase processual.

Ademais, o deferimento da medida está condicionado ao preenchimento de três requisitos cumulativos, dessa forma, existirem indícios suficientes sobre autoria da infração penal investigada, ser a interceptação a única saída possível para produção de provas no concreto (ser inviável a produção de provas por outro meio), e por fim, ser a infração investigada punida, no mínimo, com reclusão, conforme ensinamentos trazidos pelo artigo 2º, incisos I, II e III da Lei n° 9.296/96:

> Art. 2° Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses:
> I - não houver indícios razoáveis da autoria ou participação em infração penal;
> II - a prova puder ser feita por outros meios disponíveis;
> III - o fato investigado constituir infração penal punida, no máximo, com pena de detenção. (BRASIL, 1996)

Sobre essa peculiaridade ligada à pena do delito, Reis e Gonçalves (2012, p. 258) destacam:

> É importante ressaltar que a interceptação de comunicações telefônicas ou de dados só é admitida para fins de produção de prova em investigação criminal ou em instrução processual penal referente a crimes apenados com reclusão e seus conexos.

A decisão para deferimento da medida deverá ser devidamente fundamentada pela autoridade judiciária. Em regra, a interceptação apresentará como prazo máximo o período de 15 dias, podendo, entretanto, ser renovada por igual período quando a prolongação da medida for imprescindível para colheita de provas necessárias à elucidação dos delitos investigados. Além disso, a jurisprudência dominante do Supremo Tribunal Federal e do Superior Tribunal de Justiça tem se manifestado favoravelmente em relação à possibilidade de sucessivas prorrogações do prazo da medida investigativa.

A respeito dessa circunstância, as considerações apresentadas por Reis e Gonçalves (2012, p. 258)

> Embora seja de 15 dias, renovável por igual período, o prazo previsto para a duração da diligência, o Supremo Tribunal Federal proclamou a possibilidade de prorrogações sucessivas do monitoramento em casos complexos que exijam investigação diferenciada e contínua.

Sobre a possibilidade de sucessivas prorrogações, concordamos com os entendimentos proferidos pelos tribunais superiores. Ora, figura-se altamente inviável a fixação do prazo de 15 dias (renovável por apenas uma vez) para a investigação de casos

complexos, a exemplo da averiguação de delitos praticados por associações e organizações criminosas, seja pela pluralidade de crimes que poderão ser constatados na prática, assim como, pela imensa quantidade de envolvidos nas infrações investigadas.

Além disso, conforme as disposições consubstanciadas pela Lei de Interceptações, constitui crime a realização de interceptação telefônica, informática ou telemática sem prévia autorização judicial, ou aquelas efetuadas em razão de situações não englobadas pelo ordenamento processual penal. Nesse sentido, o comando normativo previsto pelo artigo 10º da Lei nº 9.296/96:

> Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.
> Pena: reclusão, de dois a quatro anos, e multa. (BRASIL, 1996)

Por fim, registra-se que a interceptação de dados telemáticos figura-se como elemento fundamental para os procedimentos investigativos pátrios na atualidade, pois devido à organização e sofisticação das organizações criminosas, as plataformas digitais vêm sendo cada vez mais utilizadas como ferramenta de comunicação para esses indivíduos, assim como, meio para a prática das mais variadas condutas delituosas.

Como exemplos de condutas delituosas praticadas por meio das plataformas digitais, destacam-se as infrações ligadas à prática de estelionato e tráfico de drogas.

CONCLUSÃO

As inovações tecnológicas são uma realidade indissociável da sociedade contemporânea. Por consequência, diariamente são criadas inúmeras formas de comunicação digital, o que sem sombra de dúvidas, altera o modo de interação social.

São notórias as modificações trazidas pelo ambiente tecnológico aos relacionamentos pessoais e interpessoais, assim, a tecnologia está sendo empregada para resolução de diversas tarefas inerentes ao cotidiano da população mundial, desde a mais simples até a mais complexas.

Entretanto, o desenvolvimento desses mecanismos e a consecutiva "reestruturação social" em torno da utilização dessas tecnologias, tem ocasionado sérios problemas na atualidade, principalmente no que concerne à proteção e conservação de garantias e

direitos fundamentais estabelecidas pelo texto constitucional pátrio, em especial o Direito à privacidade e intimidade, inerentes à personalidade humana.

Como abordado, a maximização das estruturas de relacionamento e informação no ambiente digital tem abalado a conservação e proteção dessas garantias fundamentais. Apesar de apresentar-se como uma importante ferramenta para a exposição das mais variadas ideias e pensamentos individuais ou coletivos, muitos das opiniões proferidas no ambiente digital acabam que por extrapolar os limites da liberdade de expressão constitucionalmente assegurada.

Ademais, outra desvantagem constatada, refere-se à utilização da internet como ferramenta de manipulação das massas, principalmente no que se refere aos assuntos ligados à esfera política nacional. Além disso, destaca-se o emprego das inovações tecnológicas para o aprimoramento e sofisticação das mais variadas práticas delituosas.

Neste contexto, cabe ao Direito, enquanto ciência jurídica que é, acompanhar a evolução dessa sociedade digitalizada e globalizada, a fim de consagrar elementos legais e estruturas normativas capazes de escoltar as evoluções digitais constatadas. Não no sentido de eliminá-las ou limitá-las, mas de apresentar uma solução conciliadora entre as vantagens ocasionadas por essas inovações, e a preservação dos preceitos fundantes do Estado Democrático de Direito, colocados em risco pelo aprimoramento digital.

Pelo exposto na presente pesquisa, constata-se que as normas pertinentes ao resguardo dos usuários do ambiente digital brasileiro ainda estão em fase evolutiva. Consequentemente, devido às incessantes evoluções das plataformas tecnológicas, os diplomas legais já existentes não conseguem englobar de uma só vez as inúmeras situações visualizadas no cotidiano dos internautas em âmbito nacional.

Consequentemente, acreditamos que a unificação e a atualização legislativa dessas normas protetivas relativas aos usuários da internet apresentam-se como medidas extremamente necessárias para o futuro do Direito Digital em plano nacional.

REFERÊNCIAS

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 13/06/2019.

_____. Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Código Penal. Diário Oficial da União, 31 de dezembro de 1940, Brasília, 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 13/06/2019.

_____. Lei nº 9.296 de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Diário Oficial da União, 25 de julho de 1996, Brasília, 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9296.htm >. Acesso em: 17/06/2019.

_____. Lei nº 12.737 de 30 de novembro de 2012. Diário Oficial da União, 3 de dezembro de 2012, Brasília, 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 07/06/2019.

_____. Lei nº 12.965, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, 15 de agosto de 2018, Brasília, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 19/06/2019.

_____. Lei nº 13.709, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Diário Oficial da União, 24 de abril de 2014, Brasília, 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 17/06/2019.

CASTRO, Carla Rodrigues Araújo de. *Crimes de Informática e seus Aspectos Processuais*. 2. Ed. Rio de Janeiro: Lumen Juris, 2003.

LENZA, Pedro. *Direito Constitucional Esquematizado*. 16ª ed. São Paulo: Saraiva, 2012.

LEONARDI, Marcel. *Tutela e privacidade na internet***.** São Paulo: Saraiva, 2012.

MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. *Curso de Direito Constitucional.* 4ª ed. São Paulo: Saraiva, 2009.

MORAES, Alexandre de. *Direito Constitucional*. 15. ed. São Paulo: Atlas, 2004.

REIS, Alexandre Cebrian Araújo; GONÇALVES, Victor Eduardo Rios. *Direito Processual Penal Esquematizado.* São Paulo: Saraiva, 2012.

SYDOW, Spencer Toth. *Crimes Informáticos e suas Vítimas.* São Paulo: Saraiva, 2013.