 

RAQUEL PEREIRA SANTOS

# A LGPD NO ÂMBITO DIGITAL E SEUS POSSÍVEIS REFLEXOS NA RESPONSABILIDADE CIVIL

**SÃO LOURENÇO**

**2023**

 

RAQUEL PEREIRA SANTOS

# A LGPD NO ÂMBITO DIGITAL E SEUS POSSÍVEIS REFLEXOS NA RESPONSABILIDADE CIVIL

Trabalho de Conclusão de Curso apresentado pela aluna Raquel Pereira Santos como requisito parcial para obtenção do título de Bacharel, do Curso de Direito, da Faculdade de São Lourenço.

Orientador: Professor Me. Marcos Teixeira.

**SÃO LOURENÇO**

**2023**

**A LGPD NO ÂMBITO DIGITAL E SEUS POSSÍVEIS REFLEXOS NA RESPONSABILIDADE CIVIL**

RAQUEL PEREIRA SANTOS [[1]](#footnote-1)

PROF. ME. MARCOS TEIXEIRA [[2]](#footnote-2)

RESUMO: O presente trabalho tem como tema uma discussão em torno da LGPD no âmbito digital e seus possíveis reflexos na responsabilidade civil. Para tanto, objetiva compreender como funciona o instituto jurídico referente à Responsabilidade Civil na Lei Geral de Proteção de Dados contra crimes virtuais, analisando a Lei 13.709/2018, Lei Geral de Proteção de Dados, no contexto da Responsabilidade Civil; conhecendo a trajetória das normativas que disciplinam os crimes virtuais e sua aplicabilidade no decorrer dos anos e, ainda, entendendo a natureza jurídica da ação penal nos crimes virtuais. Foi adotada como metodologia a pesquisa bibliográfica, na qual foi realizada a leitura crítica, a redação de resumos e paráfrases das obras pertinentes ao enfrentamento do tema e à comprovação das hipóteses. Esta pesquisa constatou que, o cidadão exposto em situação de crime virtual gozando do amplo conhecimento da Lei de nº 13.709/2018, Lei Geral de Proteção de Dados e as medidas de proteção que lhe são oferecidas, tornar-se-ia mais incentivado a cuidar de seus aparelhos eletrônicos, não passando senhas e sempre tomando o devido cuidado ao usar alguns sites não confiáveis.

Palavras-chave: Responsabilidade Civil. Proteção de Dados. Crimes Virtuais.

ABSTRACT: The present work has as its theme a discussion around Civil Responsibility in the General Data Protection Law and its aspects in the digital scope. Therefore, it aims to understand how the legal institute regarding Civil Liability in the General Data Protection Law against virtual crimes works, analyzing Law 13.709/2018, General Data Protection Law, in the context of Civil Liability; knowing the trajectory of the regulations that govern virtual crimes and their applicability over the years, and also understanding the legal nature of criminal action in virtual crimes. Bibliographical research was adopted as a methodology, in which critical reading was carried out, summaries and paraphrases of relevant works were written to tackle the theme and to prove hypotheses. This research found that, the citizen exposed in a virtual crime situation enjoying the broad knowledge of the Law nº 13.709/2018, General Data Protection Law and the protection measures that are offered to him, would become more encouraged to take care of of their electronic devices, not passing passwords and always taking due care when using some unreliable sites.

Keywords: Civil Liability. Data Protection. Virtual Crimes.

**1 – INTRODUÇÃO**

Os crimes virtuais contra a honra ocorrem basicamente devido às invasões de dispositivos eletrônicos alheios conectados ou não a redes de computadores, mediante violação indevida de mecanismo de segurança e com a finalidade de obter, adulterar ou destruir dados ou informações sem autorização do titular.

Perante o panorama destacado, este estudo defende-se pela necessidade contínua de informações que possam demonstrar não só o conteúdo dos mecanismos de proteção da lei, como também a execução e a efetividade destes dispositivos.

Neste sentido o presente trabalho tem como tema a LGPD no âmbito digital e seus possíveis reflexos na responsabilidade civil.

Para tanto, parte-se do seguinte problema de pesquisa: Quais os desafios relacionados a informática e o ambiente virtual?

Aventa-se a hipótese de que, o cidadão exposto em situação de crime virtual gozando do amplo conhecimento da Lei de nº 13.709/2018, Lei Geral de Proteção de Dados e as medidas de proteção que lhe são oferecidas, tornar-se-ia mais incentivado a cuidar de seus aparelhos eletrônicos, não passando senhas e sempre tomando o devido cuidado ao usar alguns sites não confiáveis.

Defende-se, também, a hipótese de que, não é somente a invasão de dispositivos eletrônicos que são alvos dos criminosos, pois a prática de crimes como a pornografia infantil, o racismo, o abuso sexual entre vários outros que se encaixam no contexto dos crimes virtuais, já eram bem praticados em nosso país e já existiam bem antes do surgimento do computador. Com o grande avanço da tecnologia, a consumação desses tipos de crimes se tornou muito mais fácil e nesse sentido, a Lei de nº 13.709/2018, Lei Geral de Proteção de Dados foi umas das leis criadas para tentar inibir as ações de criminosos.

O objetivo geral da pesquisa é compreender como funciona o instituto jurídico referente à Responsabilidade Civil na Lei Geral de Proteção de Dados contra crimes virtuais. Pretende-se para tanto, através dos objetivos específicos, analisar a Lei 13.709/2018, Lei Geral de Proteção de Dados, no contexto da Responsabilidade Civil; conhecer a trajetória das normativas que disciplinam os crimes virtuais e sua aplicabilidade no decorrer dos anos e, ainda, entender a natureza jurídica da ação penal nos crimes virtuais.

A relevância da pesquisa possui tripla dimensão: científica, social e pessoal. No que diz respeito à contribuição ao conhecimento científico, qualquer estudo que se preocupe em colocar em relevo as novas abordagens sobre as discussões em torno da relação entre a Responsabilidade Civil na Lei Geral de Proteção de Dados como forma de combate aos crimes virtuais no âmbito digital, é pertinente, pois trata-se de um importante campo de conhecimento para o processo de transformação das práticas jurídicas.

Em razão das lacunas ainda existentes em um amplo processo de aprendizagem sobre a relevância dos aspectos gerais que norteiam a legislação sobre a Lei Geral de Proteção de Dados, a presente pesquisa objetiva contribuir com os estudos sobre novos enfoques que desejem contribuir para formar profissionais do futuro.

Como a pesquisadora é concluinte do curso de Direito, a pesquisa torna-se relevante, pois desperta-lhe um interesse especial não só em razão disso, mas também por entender que pode lhe agregar benefícios para seu futuro profissional.

Como metodologia, foi adotada a pesquisa bibliográfica. Foi realizada a leitura crítica, a redação de resumos e paráfrases e a elaboração de fichamentos das obras pertinentes ao enfrentamento do tema e à comprovação das hipóteses. Além da leitura de livros pertinentes ao objeto da pesquisa, foram consultados documentos disponíveis online, devidamente consignados nas referências.

Em seu desenvolvimento, o trabalho está estruturado em quatro capítulos, sendo que, no primeiro capítulo trata-se da definição de crimes virtuais e os seus tipos. Já o segundo capítulo aborda a evolução jurídica e criação da Lei 12.737/12. O terceiro capítulo expõe acerca do Marco Civil da Internet e a Lei Geral de Proteção de Dados – LGPD – Lei nº 13.709/2018. Por fim, o quarto e último capítulo discute sobre os direitos do usuário de internet.

Seguem por fim considerações sobre a metodologia, conclusão e referências.

**2 – DESENVOLVIMENTO**

**2.1 - DEFINIÇÃO DE CRIMES VIRTUAIS E OS SEUS TIPOS**

Historicamente, a atenção à legalidade da criminalização a partir de uma perspectiva comportamental só surgiu como um estudo detalhado do bem do direito: da atenção dos estudiosos aos objetos protegidos pelas normas penais, surgiu um conceito material de crime, que se opôs ao bem jurídico. Embora o foco principal do conceito formal seja puramente legalista (se a lei diz que é um crime, isso é suficiente), o conceito substantivo preocupa-se principalmente com crimes contra o bem jurídico que a norma procura proteger.

Segundo Rosa (2005, p. 44), a Internet é a maior rede global capaz de fornecer um número cada vez maior de serviços e informações, permitindo que um número sem precedentes de pessoas se comunique e interaja entre si através de diversos recursos e múltiplas tecnologias.

Tendo estes fatores em conta, é compreensível que o controle preventivo e repressivo do crime se torne logicamente um enorme desafio: onde há riqueza, há crime, e onde há pouco ou nenhum controlo estatal, é mais provável que a riqueza se torne alvo de criminosos.

Nesta linha, Rosa (2005, p. 48) afirma que existem vários tipos específicos de crimes virtuais: crimes virtuais, crimes informáticos, crimes cometidos através da Internet, e ainda crimes cibernéticos e crimes, bem como vários outros tipos, nomeadamente no que diz respeito ao conceito de crime virtual, com múltiplas disposições.

Nesse sentido, é importante compreender que, em geral, crime virtual refere-se a qualquer ato que utiliza um computador ou mesmo um dispositivo móvel (seja um tablet, um celular ou uma rede de computadores) como ferramenta para a prática de crimes.

É preciso enfatizar que os tribunais brasileiros geralmente consideram qualquer ato ilícito e criminoso cometido por meio da Internet como um conceito de crime virtual. Portanto, percebe-se que, de fato, os tribunais brasileiros estão dispostos a compreender que nem todos, mas vários dos crimes que podem ser cometidos no mundo real também podem ser cometidos no mundo virtual (ROSA, 2005, p. 52).

Portanto, a tipificação desses crimes costuma ser regulamentada pelo Código Penal, mas existem outras leis que tratam disso, como a Lei Carolina Dickman e o Código do Marco Civil, que serão discutidas mais adiante.

Segundo Nogueira (2008, p. 316), os códigos penais costumam regular uma série de crimes que podem ser cometidos no mundo real, como ameaças, difamação, calúnia e insulto, mas que utilizam a Internet como meio para cometer crimes.

Dito isto, temos estes diferentes conceitos que juntos nos dão uma visão mais variada e pluralista do crime virtual, porque dado o próprio ano em que a Lei Carolina Dickman se referia, o crime virtual foi relativamente considerado novo para a sociedade em 2012.

Portanto, é necessário entender que o objetivo do crime virtual é, na verdade, causar algum tipo de prejuízo às empresas e indivíduos, seja perda financeira ou dano à imagem. Assim, os crimes virtuais podem ser cometidos contra cidadãos comuns, ou mesmo contra indivíduos, políticos, empresas, sociedades, que de fato representam grupos.

Para John Draper, o inventor do phreaking (cracker de telefonia), acontece que o propósito do crime virtual é exatamente esse, que é causar algum tipo de transtorno a alguém, causar algum tipo de prejuízo, talvez até prejuízo financeiro. Mesmo quando os criminosos obtêm algum tipo de vantagem ilegal, inclusive vantagem financeira, mas não só isso, mas qualquer outro tipo de vantagem, como vantagem sexual, como algum tipo de favor sexual, favoritismo, e algumas outras coisas (NOGUEIRA, 2008, p. 320).

Percebe-se que a tecnologia está se desenvolvendo em um ritmo extremamente rápido, mas as novas relações jurídicas precisam ser monitoradas, e essas novas relações jurídicas requerem regulamentação e apoio adequado do sistema jurídico.

Como se pode perceber, a lei é um reflexo da sociedade como um todo e do comportamento das pessoas e, portanto, está em constante evolução. Diante dessa situação, é necessário acelerar a dinâmica que envolve as normas jurídicas e os comportamentos recentes ocorridos no ambiente digital para alcançar a segurança jurídica e social.

Nesse sentido, a seguir serão discutidas questões sobre análise e princípios jurídicos, atendimento à cooperação legislativa e algumas alternativas de como lidar com alguns atos e a efetiva aplicação do direito.

Existem duas razões básicas para o enorme aumento da criminalidade cibernética no nosso país: a primeira está diretamente relacionada com o fato de a Internet permitir aos criminosos acenderem livremente a um grande número de vítimas em um país que pouco se preocupa com o uso da Internet e um país com educação básica em segurança; além disso, as técnicas usadas para ocultar as atividades dos criminosos e os hackers que eles recrutam são extremamente sofisticadas e encontram pouca resistência nas frágeis estruturas investigativas e judiciais do Brasil.

Segundo Bomfati (2020, p. 88), ser vítima de crimes virtuais é uma situação comum nos dias de hoje. Talvez seja porque as nossas vidas estão atualmente expostas à Internet. Tudo o que precisamos hoje está online: registro em sites de compras, pedidos de comida online, cheques bancários, aplicações de chat, etc. Grande parte envolve sistemas virtuais online.

Percebe-se que os crimes virtuais incluem tipos de crimes puros, bem como crimes mistos e conjuntos. No entanto, é importante compreender que estes crimes geralmente utilizam a Internet ou redes de computadores com o objetivo principal de invadir o dispositivo de alguém, o sistema de alguém, ou causar algum tipo de inconveniente para atingir um propósito específico, principalmente benefícios financeiros.

Exemplos comuns desse comportamento incluem hackear sites, sistemas, software, dispositivos móveis, computadores e vários outros tipos de invasões. Tomamos também como exemplo a comercialização, produção, venda e até mesmo compra e compartilhamento de sistemas e programas utilizados para fins criminosos. Esses aplicativos enviam mensagens para o celular e solicitam que o usuário confirme ou clique, por exemplo, em um link afirmando que o cartão de crédito será bloqueado e os criminosos terão acesso a todos os dados dessa pessoa (BOMFATI, 2020, p. 89).

Nesse sentido, as fraudes bancárias também são diversas e um bom exemplo são os roubos cometidos por múltiplos criminosos com o objetivo de roubar valores das contas correntes de correntistas no Brasil.

Como lembra Bomfati (2020, p. 92), um caso muito famoso aqui no Brasil foi o “caso Pablo”, em que um golpista usou um programa para roubar pequenas quantias das contas das pessoas, como noventa centavos, setenta centavos, oitenta centavos. Mas isso foi feito nas contas de milhares de pessoas, então ele acabou ficando muito rico.

Pablo é acusado de roubar cerca de 400 milhões de reais de diversas contas correntes, roubo que passou despercebido porque o dinheiro estava em centavos. Por outras palavras, este crime foi de fato muito inteligente e foi impressionante que os criminosos estivessem completamente comprometidos com o crime. Também pode-se mencionar fraudes com cartões, utilização de sites falsos ou utilização de perfis falsos e lojas online falsas.

Mais recentemente, nos últimos três anos, os tribunais brasileiros tornaram-se cada vez mais conscientes da possibilidade de estupro virtual. Como a legislação que envolve o estudo foi alterada para delinear vários tipos de comportamento sexual no estupro, ou seja, em teoria, a relação sexual em si não precisava ocorrer para que o estupro ocorresse; portanto, também foi possível que o estupro virtual ocorresse, ou seja, estupro, onde uma pessoa obtém alguns dados íntimos sobre outra pessoa e exige certos favores sexuais em troca de não divulgar esses dados, ou seja, acabam forçando a pessoa a fazer qualquer coisa que vise a obtenção de prazer sexual (COLARES, 2002, pág. 103).

Sob essa mesma ótica, tem-se ainda a divulgação de material pornográfico envolvendo pedofilia, principalmente pornografia infantil; tem-se vários tipos de fraude, envolvendo também boletos bancários e de loteria; tem-se também violação de propriedade intelectual e por fim, as fake news.

Segundo Colares (2002, p. 107), o caso mais icônico de hackeamento de equipamentos de informática que desencadeou esse incidente envolveu a atriz global Carolina Dieckmann. Em maio de 2012, mais de 30 fotos íntimas da atriz foram postadas online, causando grande repercussão. Antes da postagem, os criminosos exigiram R$ 10 mil da atriz para impedir que as fotos fossem publicadas. Após uma investigação, a polícia concluiu que os e-mails da artista foram hackeados, gerando uma grande discussão e estímulo a lei.

Portanto, nesta fase pode-se observar a necessidade e a complexidade da classificação dos atos cibercriminosos no direito brasileiro, estudando os tipos de crimes criados pela primeira vez em nossa legislação com características de crimes puramente informáticos.

**3 - EVOLUÇÃO JURÍDICA E CRIAÇÃO DA LEI 12.737/12**

Há uma necessidade urgente de legislação que esteja mais alinhada com a realidade atual. Apesar do crescimento exponencial da Internet, a justiça no Brasil tem progredido, ainda que em ritmo tímido. Na verdade, enfrentamos um problema global, um problema entre a liberdade e a segurança na Internet, mas, infelizmente, podemos dizer que este novo mundo, ou cibernética, ainda é uma terra sem lei.

Segundo Viana e Machado (2013, p. 31), em nosso país, até 2012, esses atos, que são chamados de crimes cibernéticos, não possuíam leis específicas que estabelecessem penalidades para a prática de atos ilícitos neste âmbito. É importante notar que antes da promulgação das leis sobre crimes cibernéticos, não havia diferença entre crimes virtuais e crimes presenciais.

Nesse sentido, o Brasil aprovou a Lei Carolina Dickman, que trata da tipificação criminal dos crimes informáticos. Outra lei, a Lei nº 12.683/2012, acrescentou o artigo 17-B à lei de lavagem de dinheiro, permitindo a solicitação de dados cadastrais sem necessidade de autorização judicial ao provedor de Internet. A Lei 12.830/2013 prevê expressamente o direito de solicitação de documentos ao Delegado de Polícia. Há também um projeto de lei que permite a aquisição de dados cadastrais na investigação de organizações criminosas (VIANA; MACHADO, 2013, p. 32).

Portanto, cabe destacar que a legislação que enfrentamos ainda é tímida, assim como a falta de regulamentação da Internet no que diz respeito ao armazenamento de logs. Isso facilita muito a atividade criminosa, acabando por causar danos e até inviabilizar as investigações.

Continuando com a discussão sobre a abordagem legislativa do Brasil ao crime virtual, e o Código Penal, que geralmente regula crimes que podem ser cometidos no mundo real e, até certo ponto, no mundo virtual, ou seja, usando a internet como meio, tem-se alguns crimes e leis muito específicos que detalham alguns desses crimes, como a Lei Carolina Dickman (Lei 12.737) de 2012.

A Lei Carolina Dickman trata principalmente da intrusão de dispositivos móveis, mas também da interferência ou interrupção de equipamentos informáticos, telégrafos, telefônicos, e a lei sempre trata esse assunto de forma básica.

A lei também fala sobre falsificação de cartões e outros dispositivos, mas entre outros fatores, não é tão relevante para aumentar penas. Mas é importante notar que a lei recebeu algumas críticas de que é muito simplista porque não cobre todos os tipos de crimes aos quais somos vulneráveis ​​no mundo virtual. Vários aspectos da lei permanecem sem solução na parte processual. Portanto, esta é uma crítica recorrente (VIANA; MACHADO, 2013, p. 37).

Nesse sentido, a lei realmente não é tão eficaz na prática, embora seja um marco, o primeiro passo no desenvolvimento relacionado ao crime virtual no Brasil, há problemas aí porque a lei não é muito eficiente, porque atualmente vemos vários incidentes de crimes cibernéticos acontecendo todos os dias.

Obviamente, estas críticas referem-se muitas vezes às penas impostas pela lei. Por exemplo, a lei prevê penas que variam de três meses a um ano, podendo até aumentar. Muitas vezes, muitas pessoas escapam impunes e o país carece de fiscalização (PINHEIRO, 2013, p. 255).

Portanto, pode-se dizer que as agências investigativas e judiciais ainda estão mal preparadas para lidar com este crime, uma vez que a Internet e todas as tecnologias relacionadas surgiram apenas recentemente e estão a desenvolver-se rapidamente.

Por mais inacreditável que pareça, na visão de Pinheiro (2013, p. 256), ainda existem agentes despreparados na maioria dos órgãos federais, estaduais, municipais, etc., que nada sabe sobre essas novas tecnologias.

A falta de compreensão da terminologia e das necessidades das investigações de crimes cibernéticos também é vista como uma falha, tornando a sociedade mais vulnerável. São emergenciais as questões que envolvem o preparo adequado desses agentes para que possam manejar ou pelo menos dominar os conceitos básicos dessas novas tecnologias e terminologias.

**4 - O MARCO CIVIL DA INTERNET E A LEI GERAL DE PROTEÇÃO DE DADOS – LGPD – LEI Nº 13.709/2018**

O Marco Civil da Internet é regulamentado pela Lei Federal nº 12.965/2004 e é a referência legislativa brasileira sobre o assunto. Alguns juristas referem-se ao Marco Civil como a Constituição da Internet. Isso porque a legislação não só nos traz os princípios para o uso da Internet no Brasil, mas também fornece parâmetros gerais. Desta forma podemos compreender os princípios, direitos e obrigações, bem como as diretrizes que as autoridades públicas devem adotar.

Nesse sentido, O’brien (2004, p. 11) questiona:

Ressalte-se que o Marco Civil da Internet pode ser utilizado para consolidar a liberdade de expressão, pois auxilia os cidadãos não apenas a se comunicarem, mas também a expressarem suas opiniões sobre qualquer assunto. Dessa forma, os medos decorrentes de possíveis inseguranças sobre o assunto devem ser eliminados.

Vale ressaltar que antes da introdução das leis acima mencionadas, as autoridades públicas, especialmente o judiciário, encontravam-se sem legislação dedicada para tratar e debater este tema. Vale ressaltar que não há base legal suficiente na decisão judicial para resolver o litígio.

Busca-se, portanto, maior transparência no processo legislativo, contando com a participação dos cidadãos como usuários, bibliotecários, funcionários de empresas de tecnologia, enfim, cidadãos com alguma relação com a Internet. Além disso, uma das dificuldades encontradas, mas ainda enfrentadas neste debate, é a questão da terminologia técnica. Por um lado, os operadores jurídicos aplicam os seus termos à investigação cibernética; por outro lado, a terminologia técnica utilizada pelos indivíduos que lidam com tecnologia também pode causar confusão aos juristas.

Contudo, vejamos os objetivos desta legislação com base no verbo de seu artigo primeiro *in verbis*: “Artigo 1º: Esta lei estabelece os princípios, garantias, direitos e obrigações relativos ao uso da Internet no Brasil e determina as diretrizes para ação da União, do Estado, do Distrito Federal e das decisões dos Governos Municipais sobre a matéria” (Brasil, 1998, p. 12).

Esses ideais orientam as decisões judiciais. A legislação estabelece que o Estado deve proteger os direitos dos cidadãos, incluindo quando a tecnologia da informação está envolvida. Portanto, no nosso mundo globalizado, é necessário prestar atenção a esta questão.

Neste contexto, é importante lembrar sempre que a Internet é altamente maleável, ou seja, desenvolve e adapta os seus meios e comportamento em alta velocidade. A compreensão de que as redes se destinam a promover o desenvolvimento humano e social é um guia para o pensamento jurídico nesta Lei.

Nesse sentido, a LGPD – Lei Geral e de Proteção de Dados (Lei nº 13.709/2018) foi criada especificamente para controlar e proteger os dados pessoais e, portanto, além de conceder o máximo de autonomia possível, busca garantir a todos os possíveis titulares de direitos sem excluir casos específicos.

Enquanto o Marco Civil da Internet tem a privacidade como um dos seus pontos-chave, a Proteção Geral de Dados Pessoais (LGPD) estabelece as regras para uso, proteção e transferência de dados pessoais. A LGPD pode ter diversas aplicações relacionadas às plataformas digitais.

**5 - DIREITOS DO USUÁRIO DE INTERNET**

O artigo 7º da Lei Federal nº 12.965/2014 traz direitos fundamentais para respeitar os direitos humanos de cada cidadão e salvaguardar todo o sistema jurídico e, de forma mais ampla, não apenas digital. Vejamos o literal legal *in verbis*:

O acesso à Internet é essencial para o exercício da cidadania e os usuários têm os seguintes direitos: I - à inviolabilidade das relações íntimas e da vida privada, proteção dos mesmos e indenização pelos danos materiais ou morais causados ​​pela violação; II - nos termos do disposto da lei, a inviolabilidade e confidencialidade do seu fluxo de comunicações pela Internet, salvo ordem judicial; III - a inviolabilidade e confidencialidade das suas comunicações privadas armazenadas, salvo ordem judicial; IV - não suspender a sua ligação à Internet, salvo por ordem judicial Exceto dívidas diretamente contraídas; V - a qualidade do contrato de manutenção da conexão à Internet; VI - informações claras e completas contidas no contrato de prestação do serviço, detalhando o sistema de proteção dos registros de conexão e Internet registros de acesso a aplicações, bem como gerenciamento de redes que possam afetar sua qualidade Prática; VII - Não fornecer seus dados pessoais, inclusive registros de conexão e acesso a aplicações de Internet, a terceiros, exceto com consentimento livre, claro e informado ou conforme exigido por lei; VIII - No que diz respeito à coleta, utilização de seus dados pessoais, armazenar, processar e proteger informações claras e completas que somente poderão ser utilizadas para os seguintes fins: a) justificar sua coleta; b) não proibido por lei; c) em o contrato de prestação de serviço ou os termos de uso do aplicativo de Internet expressamente previstos; IX - consentimento explícito para a coleta, utilização, armazenamento e tratamento de dados pessoais, que deverá ser feito separadamente de outras disposições contratuais; Exceções à presunção de obrigatoriedade manutenção de registros; XI - Divulgação e clareza de qualquer política de utilização do provedor de conexão à Internet e do aplicativo de Internet; ; XIII - Aplicação de normas de proteção e defesa do consumidor às relações de consumo realizadas pela Internet.

A primeira parte, ao mesmo tempo em que propõe a inviolabilidade da vida privada, estabelece que será prevista indenização em caso de dano material ou moral. Portanto, caso a legislação sobre tecnologia digital seja violada, especialmente os direitos fundamentais elencados no artigo 5º da Constituição Federal, a vítima tem o dever de indenizar.

Alguns estudiosos acreditam que a intimidade pode ser conceituada como um espaço na vida de um indivíduo que ele tem o direito legal de reservar para si. Esse conjunto de informações deve estar sob seu controle, mesmo que presente em alguns sistemas (SILVA, 2018, p. 128).

Dessa forma, não se pode confundir: mesmo que o usuário forneça alguns dados na rede, ele poderá fazê-lo apenas para conscientizar determinado provedor, mas não os divulgar e os disponibilizar para outras fontes.

A Seção 2 busca a inviolabilidade e confidencialidade do processo de comunicação. Como acontece nas comunicações telefônicas, as redes também devem manter a confidencialidade das comunicações entre as pessoas. A Parte III também traz a mesma segurança às comunicações armazenadas em mídias sociais e programas de comunicação (SILVA, 2018, p. 129).

Desta forma, apenas quem responde à situação em tribunal pode revelar as suas informações confidenciais online. Ocasionalmente, os autores de crimes psiquiátricos ou relacionados com substâncias químicas podem ser confrontados com processos judiciais, pelo que, para recolher provas e compreender melhor os detalhes do incidente, as autoridades judiciais podem solicitar informações aos programas e prestadores.

Segundo Teixeira (2015, p. 307), o artigo 4º estabelece que o único motivo para a suspensão da ligação à Internet é o não pagamento das taxas de utilização. O acesso às grandes redes é um dos objetivos da legislação; portanto, o Brasil pretende estender esse direito a todos.

Além disso, o item 5 dispõe sobre a manutenção da qualidade da conexão à Internet de acordo com o contrato de serviço. A agência nacional de telecomunicações Anatel já monitora o acesso à internet via banda larga fixa ou móvel no país. No passado, havia muitos fatores de instabilidade na prestação desse serviço, o que também causava transtornos e obrigava os usuários a buscarem proteção nos órgãos de defesa do consumidor.

A Seção 6 está bastante alinhada com a filosofia da Lei de Proteção ao Consumidor. Pode-se, portanto, traçar um paralelo com o artigo 31 do CDC (Brasil, década de 1990/p.), que ratifica o dever de diligência dos legisladores para com os internautas, reconhecendo que as mesmas deficiências podem existir nas relações contratuais com os internautas, *in verbis*:

Artigo 31.º A disponibilização e exposição de produtos ou serviços deve garantir a prestação de informação correta, clara, precisa e visível em língua portuguesa, incluindo dados sobre as suas características, qualidade, quantidade, ingredientes, preço, garantia, prazo de validade e origem, e os riscos que representam para a saúde e segurança dos consumidores (Brasil, 1990).

O artigo 7º, por sua vez, enfatiza a necessidade de atribuir grande importância aos dados pessoais dos internautas. Um possível exemplo é uma situação famosa: quando dados foram vazados e utilizados por inúmeras empresas que promoviam marketing online e pautavam suas campanhas publicitárias com base nessas informações.

A Seção 8 é outro aprimoramento que visa manter a transparência no uso da Internet e nos dados fornecidos. Portanto, reconhecendo que existem diversas regras que regem a custódia e proteção dessas informações, a legislação prevê uma série de finalidades que autorizam a coleta dessas informações.

Na verdade, com a criação de esquadras de polícia dedicadas à investigação de crimes digitais, tornou-se imperativo identificar novos crimes e esclarecer a conduta. Então, como vimos antes, o fato de os sistemas de dados da atriz Carolina Dickmann terem sido supostamente hackeados e suas fotos íntimas terem sido postadas na internet atraiu a atenção nacional e estamos ouvindo autoridades públicas acelerarem o processo legislativo.

Portanto, em resposta aos riscos enfrentados pela sociedade contemporânea, os legisladores brasileiros optaram por elaborar legislação sobre crimes cibernéticos, mas sem muita profundidade. Em outras palavras, as normas penais são ratificadas em resposta a determinados comportamentos que podem causar desordem e insegurança, mesmo sem amplo debate sobre o assunto, para proteger os direitos transindividuais.

**6 - A RESPONSABILIDADE CIVIL NA LGPD**

A LGPD possui uma seção dedicada à responsabilidade por danos e indenizações, que contém regras para o tratamento de casos de responsabilidade civil. Porém, nem todas essas interações se darão por meio do Código Civil, mas também por meio do Código de Defesa do Consumidor, conforme previsto no art. Artigo 45 da LGPD.

Dessa forma, podem ser identificadas duas situações de responsabilidade civil na LGPD: a) violação de normas legais de microssistemas de proteção de dados; b) violação de normas técnicas voltadas à segurança e proteção de dados pessoais.

Além disso, fica claro que a responsabilidade civil somente será caracterizada quando a violação de normas legais ou técnicas causar dano material ou moral ao titular ou à coletividade.

Art. 42 limita a responsabilidade civil do controlador ou operador. A presença da conjunção alternativa “ou” estabelece uma alternância entre um (controlador) ou outro (operador). Obviamente, se a relação jurídica entre o titular e o controlador ou operador for de natureza consumerista, aplicar-se-ão as regras de responsabilidade solidária do Código de Processo Civil. Artigos 12 e 18 do CDC.

O artigo 1.º abre uma exceção à regra da alternância no limite, permitindo a solidariedade em duas circunstâncias específicas para “garantir uma compensação efetiva ao titular dos dados”.

Na Seção 1, o operador responderá solidariamente em duas situações: se a legislação de proteção de dados não for cumprida, ou se “não forem seguidas as instruções lícitas do controlador, caso em que o operador atua como controlador”. Nos termos do art. 679, CC16.

Na Secção 2, haverá solidariedade entre “responsáveis ​​pelo tratamento diretamente envolvidos no tratamento”, ou seja, responsáveis ​​pelo tratamento que tomem conjuntamente decisões que violem o microssistema de proteção de dados ou as normas técnicas aplicáveis.

Esta presunção de solidariedade será excluída se uma presunção excludente de responsabilidade estiver prevista no art. 43.

A LGPD não menciona a responsabilidade civil do responsável, mas a responsabilidade civil pode surgir, por exemplo, quando as funções são exercidas por pessoa física ou jurídica distinta do controlador e operador na relação de consumo. Por se tratar de alguém da cadeia produtiva, você poderá ser responsabilizado solidariamente pelos danos causados.

O § 2º permite que o juiz tenha o poder discricionário de inverter o ônus da prova em favor do titular dos dados quando a alegação for credível, a finalidade para a qual a prova é oferecida ou as deficiências nas provas fornecidas pelo titular dos dados forem indevidamente onerosas. Existem regras relativas à redistribuição/inversão do ônus da prova também encontradas em outras leis: as regras do art são muito semelhantes. 373, CPC17 § 1º e outro no art. Os artigos 6º e VIII do CDC18 são aplicáveis ​​aos comportamentos consumistas e possuem menos exigências.

Além da inversão do ônus da prova, o reconhecimento da insuficiência do titular se reflete no fato de a responsabilidade civil da polícia local ter forma objetiva e não discutir a culpa do agente.

**CONCLUSÃO OU CONSIDERAÇÕES FINAIS**

Diante da relevância que o atual cenário jurídico brasileiro vem tomando nos últimos tempos, uma abordagem e discussão a respeito do regulamento e proteção das vítimas de crimes virtuais e cibercrime no Brasil, se faz importante e necessária uma conduta civilizada que busque romper os laços da má conduta que tem adoecido o quadro social do país.

Essa complexidade traz para as pessoas os desafios contínuos de aprimoramento de suas opiniões, visando oferecer argumentos de qualidade e bem fundamentados, na busca de assumir uma posição de liderança e combate ao não cumprimento da lei em vigor.

Retomando ao problema proposto, o presente trabalho pretendeu investigar quais os desafios relacionados a informática e o ambiente virtual.

A pesquisa confirmou, portanto, que, o cidadão exposto em situação de crime virtual gozando do amplo conhecimento da Lei de nº 13.709/2018, Lei Geral de Proteção de Dados e as medidas de proteção que lhe são oferecidas, tornar-se-ia mais incentivado a cuidar de seus aparelhos eletrônicos, não passando senhas e sempre tomando o devido cuidado ao usar alguns sites não confiáveis.

Além disso, não é somente a invasão de dispositivos eletrônicos que são alvos dos criminosos, pois a prática de crimes como a pornografia infantil, o racismo, o abuso sexual entre vários outros que se encaixam no contexto dos crimes virtuais, já eram bem praticados em nosso país e já existiam bem antes do surgimento do computador. Com o grande avanço da tecnologia, a consumação desses tipos de crimes se tornou muito mais fácil e nesse sentido, a Lei de nº 13.709/2018, Lei Geral de Proteção de Dados foi umas das leis criadas para tentar inibir as ações de criminosos.

Ainda nesse contexto, esta pesquisa pretendeu compreender como funciona o instituto jurídico referente à Responsabilidade Civil na Lei Geral de Proteção de Dados contra crimes virtuais. Buscou ainda analisar a Lei 13.709/2018, Lei Geral de Proteção de Dados, no contexto da Responsabilidade Civil; conhecer a trajetória das normativas que disciplinam os crimes virtuais e sua aplicabilidade no decorrer dos anos e, ainda, entender a natureza jurídica da ação penal nos crimes virtuais.

De fácil localização, podendo ser encontradas em sites e livros, assuntos relacionados aos crimes virtuais no Brasil, transformam-se em poderosas ferramentas ao alcance da população que se interesse em trabalhar e discutir com maior veemência o assunto.

No entanto, enfatizamos a necessidade de se conhecer a fundo o método com que irá trabalhar, a fim de não o subaproveitar com práticas estereotipadas, mecanicistas e limitadoras. Por fim, todo trabalho que envolva discussões no campo dos cibercrimes, deve levar em consideração o contexto social em que este ou aquele assunto é produzido.

A partir do recorte temático adotado, outras pesquisas podem ser realizadas, apenas substituindo-se a variável dos crimes virtuais, por outras configurações penais que podem ser praticadas no campo judiciário brasileiro.

Em reforço a essas considerações, vale frisar que nossa pesquisa não esgota o assunto, pois ela pode desdobrar-se em pesquisas de maior fôlego, que exijam maior tempo de consulta teórica sobre o assunto aqui trabalhado, além da pesquisa meramente bibliográfica, tais como pesquisas de campo e pesquisa-ação, a fim de se confrontarem os pressupostos teóricos com os dados empíricos coletados na vivência em diversas instituições públicas.

Todavia, em que pesem as limitações deste trabalho, ele tem a virtude de apontar caminhos para futuros pesquisadores, além servir de referencial teórico inicial para quem já trabalha na área, sem, no entanto, ter tido ainda a oportunidade de conhecer as ricas e amplas possibilidades pertinentes a este encantador legado.

**6 – REFERÊNCIAS**

BOMFATI, Cláudio Adriano. **Crimes cibernéticos**. Curitiba: Intersaberes, 2020.

BRASIL. **Lei nº 13.709, 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).

\_\_\_\_\_\_\_\_. **Lei nº 12.737, de 30 de novembro de 2012**. Lei Carolina Dieckmann Disponível em: <http://www.planalto.gov.br/ccivil\_03/\_ato20112014/2012/lei/l12737.htm>. Acesso em 28 mar. 2023.

\_\_\_\_\_\_\_\_. **Lei nº. 8.078, de 11 de setembro de 1990**. Código de Defesa do Consumidor. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil\_03/Leis/L8078.htm>. Acesso em 03 mar. 2023.

COLARES, Rodrigo Guimarães. **Cybercrimes**: os crimes na era da informática, 2002. In: Jus Navigandi, Teresina, ano 6, n. 59, out. 2002. Disponível em: http://jus2.uol.com.br/doutrina. Acesso em: 10 abr. 2023.

NOGUEIRA, Sandro D’Amato. **Crimes de informática**. São Paulo: BH, 2008.

O´BRIEN, J. A. **Sistemas de informações e as decisões gerencias na era da Internet**. 9 ed. São Paulo: Saraiva, 2004.

PINHEIRO, Patrícia Peck. **Direito Digital**. São Paulo: Saraiva, 2013.

ROSA, Fabrizio. **Crimes de informática**. 2 ed. Campinas: Bookseller, 2005.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

SILVA, A. R. I. **Crimes cibernéticos**: racismo, Cyber bullying, deep web, pornografia, pornografia infanto-juvenil, infiltração de agentes por meio virtual, obtenção de provas digitais, nova lei antiterrorismo, e outros temas. 2 ed. Porto Alegre: Livraria do Advogado, 2018.

TEIXEIRA, T. **Direito das novas tecnologias**: legislação eletrônica comentada, mobile Law e segurança digital. São Paulo: Revista dos Tribunais, 2015.

VIANNA, T.; MACHADO, F. **Crimes informáticos**: Conforme a Lei nº 12737/2012. Belo Horizonte: Fórum, 2013.

1. Bacharelando em Direito pela Faculdade de São Lourenço – UNISEPE. Email: raquelpsbr@gmail.com [↑](#footnote-ref-1)
2. Professor Mestre: Marcos Teixeira. Email: [↑](#footnote-ref-2)