CRIMES CIBERNÉTICOS, INVASÃO DE PRIVACIDADE E A EFETIVIDADE DA RESPOSTA ESTATAL: OS IMPACTOS DA LEI 12.737/2012 – LEI CAROLINA DIECKMANN E DA LEI GERAL DE PROTEÇÃO DE DADOS NO COMBATE AOS CRIMES CIBERNÉTICOS DE INVASÃO DE PRIVACIDADE

CYBER CRIMES, PRIVACY INVASION AND THE EFFECTIVENESS OF THE STATE RESPONSE: THE IMPACTS OF LAW 12,737/2012 – CAROLINA DIECKMANN LAW AND THE GENERAL DATA PROTECTION LAW IN FIGHTING CYBER PRIVACY INVASIONS

Rafael Lopes Kassem Machado
Neuziane Lima Duarte

RESUMO

O espaço cibernético sofre constantes mudanças e, à medida em que a tecnologia avança, é proporcionado aos seus usuários um ambiente de acesso facilitado para as mais diversificadas tarefas, seja para o entretenimento, negócios, trabalho, estudo e outras infinidades de opções nesse universo digital. O grande problema é que o avanço tecnológico oportuniza às pessoas o cometimento de crimes no ambiente virtual, que por ser um novo modo de cometer crimes, não há tantas formas de rastrear e punir esses cibercriminosos. Sob essa ótica, o objetivo deste trabalho foi analisar a efetividade da resposta do Estado Brasileiro aos crimes cibernéticos de invasão de privacidade à luz da Lei 12.737/12 – denominada Lei Carolina Dieckmann – e Lei 13.709/18 – Lei Geral de Proteção de Dados (LGPD) – a qual ainda está em período de *vacatio legis*. O presente estudo foi desenvolvido utilizando pesquisas bibliográficas, em especial artigos científicos que tratam sobre o tema. A relevância e justificativa deste estudo baseia-se no fato de que os crimes de invasão de privacidade cometidos no ambiente virtual estão crescendo cada vez mais, prova disso é que os legisladores têm criado leis visando proteger a privacidade do indivíduo também no ambiente virtual. A partir deste estudo foi possível concluir que, em que pese o avanço da legislação brasileira na tentativa de proteger a privacidade dos usuários no ambiente virtual, a Lei 12.737/12 vigente infelizmente ainda apresenta falhas, não cumprindo amplamente seu caráter protecionista. Do mesmo modo, a Lei 13.709/18 não apresenta avanços concretos no que se refere à tutela penal do direito à inviolabilidade da privacidade.

Palavras-chave: Cibercrime; Privacidade; Internet; Proteção; Penal.

ABSTRACT

The cyber environment undergoes constant changes and, as technology advances, its users are provided with an environment of easy access for the most diverse tasks, be it for entertainment, business, work, study and other endless options in this digital universe. The big problem is that technological advancement gives people the opportunity to commit crimes in the virtual environment, which, being a new way of committing crimes, there are not so many ways to track and punish these

cybercriminals. From this perspective, the objective of this work was to analyze the effectiveness of the Brazilian State's response to cyber crimes of invasion of privacy in the light of Law 12.737 / 12 - called Carolina Dieckmann Law - and Law 13.709 / 18 - General Data Protection Law (LGPD) - which is still in a period of vacatio legis. This study was developed using bibliographic research, in particular scientific articles dealing with the topic. The relevance and justification of this study is based on the fact that crimes of invasion of privacy committed in the virtual environment are growing more and more, proof of this is that legislators have created laws aimed at protecting the privacy of the individual also in the virtual environment. From this study it was possible to conclude that, despite the advancement of Brazilian legislation in an attempt to protect the privacy of users in the virtual environment, the Law 12.737 / 12 in force still has flaws, not fully fulfilling its protectionist character. In the same way, Law 13.709 / 18 does not present concrete advances regarding the penal protection of the right to privacy inviolability.

Keywords: *Cybercrime; Privacy; Internet; Protection; Criminal law.*

Introdução

O ambiente virtual é um espaço que a todo mundo sofre constantes mudanças, sendo que o acesso à internet e divulgação de dados crescente evolução. As pessoas usam a internet para diversas atividades, dentre as quais obter variadas informações sobre notícias do mundo todo, notícias sobre famosos, visitar sites de relacionamentos, redes sociais, estudar, trabalhar e, alguns até mesmo, chegam ao extremo de usarem a tecnologia para cometer crimes.

Em regra, as pessoas que cometem crimes no ambiente virtual são dotadas de um grande conhecimento na área que sobrepujam o conhecimento que a maioria das pessoas têm sobre tecnologia. É importante salientar que a internet surgiu durante a Guerra Fria em resposta ao Projeto Sputnik como uma forma de estabelecer comunicação segura entre os militares.

O cibercrime pode ser classificado como a prática de crimes contra ou por meio de utilização de sistemas de computador e dispositivos de informática. Nessa modalidade podem ser cometidos diversas condutas ilícitas, em especial de violação de privacidade, cenas íntimas são divulgadas a todo o tempo no ambiente virtual, sabotagem e até espionagem, dentre outras tipificações.

A Constituição Federal da República Federativa do Brasil assegura aos cidadãos o direito à inviolabilidade da vida privada, isso significa dizer que o indivíduo deve ter segurança e controle sobre as informações acerca de si e que serão de domínio comum, bem como a forma que essas informações serão publicizadas.

Assim como a intimidade possui proteção constitucional, a internet também é protegida, inclusive tendo o Marco Civil da Internet, a qual estabelece a essencialidade do direito ao uso da internet como forma de garantir o exercício regular da cidadania do indivíduo.

Em que pese a legislação garantir a inviolabilidade do direito à intimidade e à vida privada, há indivíduos que usam do direito ao uso da internet para cometer crimes de violação de privacidade, sendo que à medida que surgem novas tecnologias o ambiente virtual fica mais propício ao cometimento de crimes cibernéticos.

No ordenamento jurídico brasileiro não há lei específica para a criminalização e punição dos criminosos virtuais, apesar dos constantes casos. Apesar disso, há

várias leis na legislação brasileira que tratam de casos específicos de crimes que são ser cometidos no ambiente virtual.

Algumas das leis criadas para punir certas práticas criminosas no ambiente virtual alteraram o Código Penal Brasileiro, como é o caso da Lei 9.983/2000, a qual inseriu no artigo 153 o parágrafo 1º-A, inseriu também os artigos 313-A e 313-B e acrescentou, ainda, o parágrafo 1º no artigo 325 do Código Penal.

Ademais, ainda tem a Lei 12.737 sancionada em 2012, que é o foco deste trabalho, a qual inseriu o artigo 154-A e 154-B no Código Penal. A Lei 12.737/12, também conhecida como Lei Carolina Dieckmann trata sobre crimes de invasão de dispositivos eletrônicos

Além da Lei 12.737/12, esse trabalho faz uma análise da Lei 13.709/2018 – denominada Lei Geral de Proteção de Dados – sob a perspectiva penal, embora ainda não esteja em vigor, a sociedade já se prepara para o período em que deverão observar esta lei em suas relações comerciais e pessoais.

Este trabalho tem como propósito analisar a efetividade da resposta estatal nos crimes cibernéticos de invasão de privacidade e determinar quais são os impactos da Lei Carolina Dieckmann e da Lei Geral de Proteção de Dados no combate aos crimes cibernéticos de invasão de privacidade.

A problemática deste trabalho revela-se no fato de que considerando as transformações propiciadas pelos avanços tecnológicos que oportunizam o surgimento de novas práticas criminosas e permitem uma maior exposição da vida privada da pessoas, questiona-se se as normas penais materiais e processuais existentes, em especial a Lei 12.737/12 – Lei Carolina Dieckmann e a Lei Geral de Proteção de Dados, estão aptas a dar efetividade a resposta estatal aos chamados delitos cibernéticos de invasão de privacidade?

Desse modo, este trabalho se justifica pela necessidade de análise das leis existentes, em especial a lei 12.737/12 e Lei 13.709/18, sob a ótica de proteção penal à privacidade no ambiente virtual, uma vez que a vida privada é assegurada constitucionalmente, não importando o ambiente, este direito deve ser respeitado.

O objetivo geral desse trabalho são analisar as leis mencionados determinando seus impactos nos crimes cibernéticos de invasão de privacidade, e os objetivos específicos que darão base para o alcance do objetivo geral são: determinar o início da internet, conceituar cibercrime, discorrer sobre o direto à privacidade e a tutela penal a esse direito, bem como discorrer sobre os impactos das leis 12.737/12 e 13.709/18 na proteção penal à privacidade no ambiente cibernético.

Para a produção deste trabalho foi utilizada pesquisa bibliográfica, utilizando livros e artigos científicos. As hipóteses a serem respondidas são de que as leis protegem à integridade do direito à privacidade no ambiente virtual; ou ambas as leis auxiliam de algum modo na proteção a esse direito, mas não o protege integralmente, temos, ainda, a hipótese que uma lei garante alguma proteção, mas a outra não e, nenhuma das leis protegem o direito à privacidade.

2. Cibercrime

2.1 Histórico da internet

A internet foi criada durante a Guerra Fria pelo Departamento de Defesa dos Estados Unidos da América, com o objetivo unicamente militar, a finalidade da internet, à época designada ARPA (Advanced Research Projec Agency) era de

estabelecer uma rede de comunicação e investigação entre os militares nos locais mais críticos (GOETHALS, AGUIAR e ALMEIDA, 2000).

Abreu (2009) acrescenta que a criação do Projeto ARPA foi em resposta ao Projeto Sputnik desenvolvido pela União Soviética.Em meados de 1970 a internet passou a ser utilizada nas universidades, sendo o meio pelo qual docentes e discentes trocavam informações sobre pesquisas acadêmicas. Sendo a Universidade da Califórnia a primeira instituição a receber um microprocessador, afirma Lacerda (2019).

No ano de 1973 foi-se utilizado pela primeira vez o termo internet, isto posto porque desde 1972 aplicava-se o termo “internetwork”, que se tratava de interligações de redes que permitiam o desenvolvimento de investigações por meio da ARPA (GOETHALS, AGUIAR e ALMEIDA, 2000).

A utilização da internet se desenvolveu de maneira veloz pelos mais variados meios, em 1980 e 1981 tanto os militares, quanto universidades e cientistas já faziam uso da internet (GOETHALS, AGUIAR e ALMEIDA, 2000). É importante salientar que algumas universidades e pesquisadores científicos utilizavam redes distintas da ARPANET, posto que, por razões políticas e/ou financeiras, não possuíam autorização para utilizar-se das redes ligadas ao governo, desse modo, utilizavam redes como *BitNET, CSNET, FREENET*, entre outras redes, assim afirmam Carvalho e CUKIERMAN (2006).

Rocha (1997) assegura que o protocolo TCP-IP, que trata dos endereços de localização utilizados até os dias de hoje, foram introduzidos e seu acesso se tornou público em 1982. A autora acrescenta ainda que a comercialização da internet se tornou possível apenas no ano de 1991, sendo que em 1992 a internet alcançou a velocidade máxima de 45 Mbps e em 1995 foi possível o tráfego de áudio e vídeos pela internet.

O primeiro *Internet Service Provider* comercial surgiu no ano de 1990, momento em que a ARPANET foi extinta (GOETHALS, AGUIAR e ALMEIDA, 2000). O sistema World Wide Web foi desenvolvido em 1991 na Suíça pelo cientista da computação, físico e professor Tim Berners-Lee, até este momento o acesso à internet permitia a troca de e-mails, transferência de dados e conferências eletrônicas, a criação do sistema *World Wide Web* possibilitou a criação de servidores de informação multimídia formando uma cadeia de informação (GOETHALS, AGUIAR e ALMEIDA, 2000).

A internet no Brasil se desenvolveu a partir de 1980, sendo que em 1988 fora criado a Rede Nacional de Pesquisa – RPN – através de uma cooperação entre os Ministérios de Ciência e Tecnologia e das Comunicações. O objetivo destes era formar uma infraestrutura capaz de possibilitar o acesso à internet por todo território brasileiro, assegura Santos *apud* Teixeira e Silva (2019).

A partir de 1995 a internet passou a ser utilizada nos setores privados, gerando um crescimento desenfreado da tecnologia, nesse período foram desenvolvidos sites, provedores de pesquisa, redes sociais entre outros sistemas que o usuário decidia desenvolver (JOANA SIERRA *apud* PONTICELLI, 2018).

A disseminação e o rápido desenvolvimento da internet afetou para além das relações tecnologia – homem, uma vez que fora inserida no cotidiano das pessoas, sendo utilizada nas relações trabalhista, educacionais ou apenas para que a pessoa se informasse sobre os acontecimentos no mundo, impactando, assim, as relações sociais, ponderam Teixeira e Silva (2019).

Destarte, Ponticelli (2018) certifica que a Rede Mundial de Computadores é uma grande cadeia de informações, as quais são inseridas em uma estrutura que contém ilimitados espaços sem preenchimento, aguardando um usuário preenche-los e, assim que nele são inseridas informações é possível que outros usuários acessem, armazenem e até mesmo modifiquem o conteúdo lá inserido.

2.2 Conceito de cibercrime

A Lei 12.965, promulgada em 23 de abril de 2014 - denominada Marco Civil da Internet - prescreve em seu artigo 7º que a internet é essencial ao exercício da cidadania, sendo aos seus usuários assegurado o direito à inviolabilidade da intimidade e vida privada, bem como a inviolabilidade e o sigilo do fluxo de comunicações realizadas e armazenadas privativamente na internet, entre outras garantias asseguradas na Lei (BRASIL, 2014).

Considerando a prescrição no dispositivo mencionado alhures, a violação do direito ao acesso à internet e suas garantias é passível de indenização por dano material ou, ainda, de ordem moral, isto posto porque o artigo 5º, inciso X, da Constituição Federal garante a inviolabilidade da intimidade e vida privada (BRASIL, 1988), assim como o art. 7º, inciso I, da Lei 12.965/2014.

Castro *apud* Lacerda (2019) afirma que o cibercrime é a conduta praticada por meio de dispositivos de informática, contra ou através destes. A autora afirma, ainda, que os crimes cometidos no ambiente virtual são, em sua grande maioria, cometidos com uso da internet e o meio pelo qual são praticados é o computador.

O doutrinador Greco *apud* Cardoso (2019) reconhece que o avanço tecnológico é assunto cada vez mais discutido, posto que muito tem-se discorrido acerca dos crimes de internet, os quais também são conhecidos como crimes de informática, delitos cibernéticos, crimes digitais, delitos via computador, entre outras nomenclaturas atribuídas aos crimes cometidos com uso de tecnologia.

Ferreira *apud* CARDOSO (2019) afirma que os criadores da tecnologia não anteviram as vulnerabilidades da rede e, desse modo, à medida que a tecnologia avançava os crimes cibernéticos também aumentavam, crimes estes que envolviam caixas eletrônicos, telecomunicações e pornografia.

Segundo o autor o marco do surgimento de crimes no ambiente virtual foi a prática de crimes envolvendo manipulação, sabotagem, espionagem e uso impróprio das redes de computadores, tudo isso era divulgado na imprensa por meio de jornais e literaturas científicas.

PASOVEZ e PRADO (2019) esclarecem que os crimes cibernéticos são comuns, ou seja, não exigem qualquer característica privativa de quem comete ou contra quem é cometido o *cibercrime*, no entanto, a característica desses crimes está no fato de que são cometidos contra ou com uso de tecnologia.

O *cibercrime* pode ser classificado como conduta típica, ilícita, praticada por qualquer pessoa seja ela física ou jurídica, com intenção ou não por meio da tecnologia e que afete diretamente ou indiretamente a rede de informática e sua segurança ofendendo sua intangibilidade, fidedignidade e disponibilidade, assim Rossine *apud* Pasovez e Prado (2019) conceituam os delitos informáticos.

Nessa esteira Greco *apud* Pasovez e Prado (2019) estabelece divisão para estes crimes, sendo que os crimes próprios são cometidos contra o sistema de computação ou informática propriamente dita e os crimes impróprios são cometidos

quando o indivíduo faz uso do sistema informático com o objetivo de ferir outro bem jurídico tutelado, que não seja a internet, para cometer o crime.

A rede de computadores é utilizada para diversos assuntos e por diversos métodos de acesso. Nunes e Madrid, (2019) afirma que há pessoas que buscam utilizar-se desse meio para praticar atos ilícitos e assim obter vantagem sobre a pessoa lesada. Corroborando com esse entendimento Paesani *apud* Nunes e Madrid (2019) classifica as pessoas que se utilizam da internet para invadir sistemas informáticos para benefício ou malefício como hackers éticos e não éticos.

De acordo com o Paesani *apud* Nunes e Madrid (2019) o hacker ético é aquele que invade sistemas de informática com o fito de corrigir falhas e garantir a segurança e acesso exclusivo nas redes, enquanto o hacker não ético, também chamado cracker, diz respeito ao indivíduo que utiliza seus conhecimentos avançados para fins destrutivos e criminosos, esse indivíduo invade a rede de internet com o objetivo de sequestrar dados e obter vantagem pecuniária sobre a vítima ou simplesmente para expor os dados na internet. Destarte os dois usam o *cibermundo* para demonstrar seus conhecimentos, em pese na maioria das vezes prefiram o anonimato, afirma o autor.

3. Da tutela constitucional ao direito à privacidade

3.1 Direito à vida privada

A Constituição Federal, também conhecida como Carta Magna ou Lei Maior, recebe esse nome em razão de ser a lei regente de todo o ordenamento jurídico brasileiro, posto isto, todas as demais leis criadas ou recepcionadas no ordenamento jurídico brasileiro devem estar em consonância com a Constituição Federal. O direito à vida privada faz parte dos direitos fundamentais e tem sua garantia positivada no artigo 5º, inciso X da Constituição da República, sendo este inviolável, conforme previsão do dispositivo retro mencionado (BRASIL, 1988).

O direito à vida privada é um direito fundamental de primeira geração, porquanto, segundo Bonavides apud Lenza (2013), os direitos dessa geração são inerentes ao indivíduo e possuem a subjetividade como característica mais marcante. Destarte, Moraes (2002), ensina que a constituição da dignidade da pessoa fundamentada na Carta Magna foi fator propulsor para a positivação do direito à vida privada.

Além da Constituição Federal, o Código Civil também disciplina e traz em seu bojo disposições acerca do tema. A vida privada é, segundo o artigo 21 do Código Civil Brasileiro (BRASIL, 2002), inviolável podendo, inclusive, o magistrado adotar medidas para impedir ou aplacar atos que lesionem ou ameacem de lesão esse direito garantido também na Carta Magna.

Ferraz apud Mendes e Branco leciona que o direito à privacidade é subjetivo e fundamental, cuja titularidade pode pertencer tanto à pessoa física quanto à pessoa jurídica, seja ela brasileira ou estrangeira, sendo que diz respeito às situações em que o titular do direito pretende, por meio de decisão discricionária, guardar para si, com a finalidade de proteger sua integridade moral. Nesse sentido também instruem Gagliano e Filho (2010), afirmando que a manifestação da vontade do indivíduo em não publicitar fatos de sua vida constitui elemento essencial do direito à privacidade, dessa forma, o direito à privacidade nada mais é do que o "*direito de estar só (Right to be alone)"* .

Nesse sentido, pode se dizer que o direito à privacidade em *stricto sensu* se concretiza no indivíduo quando este, segundo entendimento de Mendes e Branco (2012), almeja não ter seus assuntos pessoais, e por que não dizer íntimos, tais como dados e características pessoais sendo de domínio de terceiros e público em geral. Destarte, o anseio direito fundamental à privacidade é o indivíduo ter sob seu domínio suas próprias informações tidas como de cunho pessoal (MENDES e BRANCO, 2012).

Corroborando com o discorrido até o presente momento Miranda *apud* Doneda (2006) afirma que a concretização do direito à privacidade é quando o indivíduo tem seus dados, características e particularidades salvaguardados, ou seja, fora dos sentidos alheios, fora do domínio de pessoas externas.

Silva (2009) vai além e afirma que o direito à privacidade é todo o arcabouço de informações que o indivíduo tem de si mesmo, possuindo, para além disso, a faculdade de expor como, onde e a quem entender necessário, e, ainda assim, não se tornar sujeito a isso. Posto isto, pode se inferir que em *latu sensu* o direito à privacidade é o domínio que o indivíduo tem das informações acerca de si. O autor leciona, ainda, que inviolabilidade do direito à vida privada não está somente no que concerne às informações da intimidade do indivíduo, mas também às informações relativas à suas relações interpessoais, profissionais e comerciais.

Nesse mesmo contexto, e considerando que todos os indivíduos continuamente e diariamente consomem e são expostos a um grande volume de informações, necessário é fazer a adequação do conceito de direito à privacidade no atual contexto social, em que as mídias socias e a internet fazem parte da vida da maioria das pessoas. Desta feita, Doneda (2006) afirma que diante da constante evolução da sociedade e crescente aumento no consumo de dados por intermédio de meios de comunicação em massa, o conceito de privacidade anteriormente aceito pela sociedade vem tomando forma e se adequando à sociedade em evolução.

Paesani (2014), faz a adequação do conceito do direito à privacidade no contexto de divulgação de informações e massa, em especial nos ambientes virtuais como o direito de o indivíduo, sujeito de direitos, ter sob seu domínio a utilização ou não de seus dados pessoais inseridos em um dispositivo eletrônico. Nesse sentido, leciona Diniz (2008) ao afirmar que os dispostos no art. 5º, inciso X, da CF e no art. 21, do CC ultrapassam o interesse do particular e atinge o interesse jurídico do Estado em manter os dados de cada indivíduo sob o domínio do próprio titular, por conseguinte esse direito também se estende ao ambiente virtual.

Posto isto, Carvalho e Pedrini (2019) afirmam que pode se inferir que o direito à vida privada tem como principal objetivo proteger à pessoa natural em sua individualidade, sendo que dados, informações e características pessoais poderão ser publicitadas ou não, mediante decisão, de caráter discricionário, do titular dos direitos, porém toda divulgação, que permite o acesso de dados pessoais a terceiros deverá observar a legislação vigente.

3.2 Proteção penal à privacidade

Costa *apud* Damasceno (2019) pondera que alguns doutrinadores se posicionam no sentido de que em que pese o legislador compreenda a necessidade de positivar na Constituição Federal a proteção à inviolabilidade da vida privada, concretizado isso no artigo 5º, X, da CF, a legislação penal brasileira não protege amplamente a intimidade e privacidade no âmbito cibernético.

Sob outra perspectiva Costa Júnior *apud* Damasceno (2019) afirma que alguns doutrinadores adotam o entendimento de que o direito penal tutela a intimidade de forma mediata e diminuta, o que é realizado a partir da formalização de leis, as quais têm a finalidade de garantir proteção à honra e a privacidade.

Não obstante a insuficiência da legislação penal em assegurar proteção à intimidade e privacidade, Damasceno (2019) cita sete leis que visam positivar e garantir a tutela jurisdicional à privacidade no que concerne ao cometimento de crimes de violação da vida privada no ambiente virtual, passo a citá-las:

A Lei 9.296/96 visa criminalizar as interceptações telefônicas, telemática e quebras de sigilo; em 1998 foi promulgada a lei 9.609, a qual define como crime a violação de direitos autorais de programas de computador, posteriormente, em 14 de julho de 2000 foi criada a Lei 9.983 que alterou o Código Penal Brasileiro, acrescentando ao artigo 153 o parágrafo 1º-A, constituindo crime a propagação de informações confidenciais ou reservadas contidas ou não nos sistemas de informação da Administração Pública, (DAMASCENO, 2019).

Ademais, essa mesma lei incluiu os artigos 313-A e 313-B no Código Penal, tornando crime, respectivamente, a inserção de dados falsos em sistemas de informações e a modificação ou alteração não autorizada de sistemas de informações. Por último, em relação aos delitos de informática, a lei 9.983/2000 inseriu o primeiro parágrafo no artigo 325, do CP criminalizando a conduta de permitir ou facilitar, por senha ou qualquer outro meio, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública. Ademais o inciso II tipifica a conduta de utilizar indevidamente o acesso restrito (DAMASCENO, 2019).

Em 2008 foi sancionada a Lei 11.829, a qual acrescentou o artigo 241-A no Estatuto da Criança e do Adolescente, essa alteração criminalizou o oferecimento, troca, disponibilização, transmissão, distribuição, publicação ou divulgação por qualquer meio, inclusive sistemas de informática, arquivos com cenas de sexo explícito ou pornografia envolvendo crianças e adolescentes (DAMASCENO, 2019).

A seguir, o autor cita que em 30 de novembro de 2012 foram sancionadas duas leis aplicadas a crimes no contexto cibernético, sendo que a Lei nº. 12.735 visa punir o indivíduo que, por meio eletrônico, digital ou similar, pratiquem atos atentatórios aos sistemas de informática ou similar, a lei ainda prevê a instalação de setores especializados no combate a esses crimes. Nunes e Madrid (2019) explicam que esses setores especializados se tratam, na forma da lei, de delegacias com profissionais específicos especializados para combater toda forma de ilicitude praticada na rede de informática.

A Lei 12.735/12 alterou, ainda, o artigo 20, §3º, II da lei sobre crimes raciais - Lei 7.716/89 – autorizando o magistrado poderá determinar a cessação de transmissões de mensagens de cunho racista por qualquer meio, inclusive em sistema de informática. Já a Lei 12.737/12 alterou alguns artigos do Código Penal criminalizando a conduta de invasão de dispositivos informáticos sem autorização. Francesco *apud* EGEWARTH (2020) acrescenta que a Lei 12.737/12 – denominada “Lei Carolina Dieckmann” – visa tornar típica as práticas dos chamados “delitos ou crimes informáticos”.

Damasceno (2019) cita a Lei 12.965/2014, também conhecida como Marco Civil da Internet, que, em que pese não tipificar nenhuma conduta, o autor afirma que a lei futuramente poderá exercer influência na apuração de cibercrimes.

Em 2018 foi sancionada a Lei 13.718/2018, a qual acrescentou no Código Penal o artigo 329-C que, segundo Padovez e Prado (2019), estabelece um tipo penal

misto alternativo que visa controlar os crimes praticados, em especial nas das redes sociais. O artigo tipifica a conduta de oferecer, trocar, disponibilizar, transmitir, vender, entre outras práticas, por meios de comunicação em massa, sistema de informática ou qualquer outro meio. Segundo Padovez e prado (2019) esse tipo penal traz diversas formas de coibir e punir o indivíduo que pratica crimes no ambiente virtual.

Diante de tantas alterações no Código Penal e outras leis que visam tipificar as condutas praticadas no ambiente cibernético, Pinheiro (2006) assegura que, ainda que não haja lei específica para tratar sobre o assunto, não há de se falar em aplicação analógica da legislação brasileira aos crimes virtuais, vez que não há novidade no que concerne ao crime, mas sim ao "*modus operandi"*, obrigando, assim, o legislador a penas em novas formas de assegurar a punição desses criminosos virtuais.

4. Lei 12.737/12 e a lei geral de proteção de dados como instrumentos de resposta aos crimes cibernéticos

4.1 Invasão de privacidade e a lei 12.737/12

De acordo com Soares e Barbosa (2016) a sociedade viveu momentos de incerteza de punibilidade aos agentes invasores de dispositivos antes da sanção da Lei 12.737/12, posto que, a legislação brasileira, bem como os princípios penais impedem a cominação de pena punitiva que não esteja estabelecida em lei.

A lei 12.737/12 foi sancionada em 2012 e teve como fato precursor para sua criação a invasão do dispositivo informático da atriz Carolina Dieckmann e divulgação de fotos e vídeos íntimos na rede mundial de computadores, afirma Cardoso (2019) após surgiram inúmeros casos semelhantes de violação de privacidade, diante disso, Greco *apud* Cardoso (2019) assegura que foi necessária a criação da lei com o intuito de proteger o cidadão que tem seu dispositivo invadido.

Soares e Barbosa (2016) afirmam que lei 12.737/12 tem por finalidade fundamentar e tornar a típica a conduta a fim de favorecer a punibilidade dos indivíduos que invadem dispositivos eletrônicos e comentem os chamados "crimes cibernéticos". Contudo, afirma, ainda, o autor, que a lei 12.737/12 não tutela todas as possibilidades de crimes de invasão de privacidade no âmbito cibernético.

Corroborando com esse entendimento, Greco *apud* Cardoso (2019) afirma que se o dispositivo utilizado para o cometimento do crime for da própria vítima, então não se aplica o artigo 154-A do Código Penal - adicionado por força da Lei 12.737/12 – vez que o caput do artigo é específico ao estabelecer que o dispositivo invadido deve ser alheio, isto é, para a caracterização do crime é necessário que a invasão ocorra a partir de um dispositivo desconectado da rede do dispositivo invadido.

Greco *apud* Cardoso (2019) acrescenta, ademais, que a invasão sem finalidade específica não caracteriza infração ao dispositivo em comento, porquanto, o dispositivo assegura que a invasão deve ter finalidade específica, qual seja, obter, adulterar ou destruir dados ou informações em autorização expressa ou tácita do titular do dispositivo.

Para além disso, Greco *apud* Cardoso (2019) acrescenta, ainda, que caso o dispositivo invadido não possua senha a conduta torna-se atípica, considerando que o texto do caput do artigo 154-A descreve que a conduta deve ser a invasão, mediante violação de mecanismo de defesa, desse modo, a ausência de mecanismo de defesa no dispositivo invadido retira a tipicidade da conduta.

Sendo assim, Soares e Barbosa (2016) aduzem que a Lei 12.737/12 tem o objetivo de proteger os titulares de dispositivos invadidos, tipificando os cibercrimes. Contudo, essa proteção se restringe às possibilidades e peculiaridades estabelecidas no artigo 154-A do Código Penal.

4.2 Lei geral de proteção de dados e crimes cibernéticos

A Lei 13.709, sancionada em 15 de agosto de 2018, denominada Lei Geral de proteção de dados ou, simplesmente, LGPD, dispõe sobre o tratamento de dados pessoais de toda pessoa natural. A LGPD tem como escopo a proteção de dados de pessoas físicas e jurídicas quanto à privacidade, liberdade de expressão, informação, comunicação, inviolabilidade da intimidade, imagem, honra, livre iniciativa, direito do consumidor, entre outros fundamentos (BRASIL, 2018).

É importante mencionar que, em que pese, a sanção da lei tenha ocorrido em agosto de 2018, o projeto que deu origem à lei foi apresentado na Câmara dos Deputados em 2012 sob o número PL 4060/2012, este projeto teve como fundamento a necessidade de estabelecer critérios e limites na manipulação de dados pessoais com o intuito de proteger direito garantido pela Constituição Federal, qual seja, o direito à intimidade e a privacidade, porém, sem violar o direito da livre iniciativa comercial e de comunicação (BRASIL, Projeto de Lei 4060, 2012).

A LGDP tem como base a proteção e a garantia da inviolabilidade do direito à intimidade e vida privada. Essa preocupação em legislar sobre proteção de dados demonstra que a LGPD entende que proteger os dados pessoais é efetivamente proteger o indivíduo titular daqueles dados, sobre a Lei 13.709/2018, afirmou Cots & Oliveira (2018) que, proteger o indivíduo, garantindo a proteção a um de seus direitos constitucionais é, de fato, proteger uma unidade, ou seja, os dados pessoais formam o próprio indivíduo titular daqueles dados.

Pinheiro *apud* Cardoso (2019) afirma que a Lei Geral de Proteção de Dados trouxe consigo inovações no que diz respeito ao tratamento de dados, sem as quais as violações nesse tratamento permaneceriam impunes. O autor afirma, ainda, que apesar das inovações a LGPD possui lacunas e esse fator é capaz de gerar insegurança jurídica, posto que deixou espaço para interpretação extensiva onde o legislador deveria ser mais assertivo.

Em que pese, a restrição a ser aplicada no tratamento dos dados, a Lei Geral de Proteção de Dados nos artigos 7º ao 16 da Lei 13.709/18 disciplinam desde os atos permissivos que autorizam para a manipulação de dados, que em regra são confidenciais (BRASIL, 2018).

É importante ressaltar que a LGPD não se aplica às investigações penais, conforme descreve o artigo 4, III, d, da lei (BRASIL, 2018) e, para além disso, Pinheiro *apud* Cardoso (2019) aduz que a Lei Geral de Proteção de Dados estabelece sanções aplicáveis ao indivíduo ou empresa que violar as suas determinações da Lei 13.709/12.

Segundo o autor tais medidas estão descritas no artigo 52 da lei, são elas: advertência, multa simples no percentual de 2% do faturamento da pessoa jurídica (limitado ao valor de R$50.000.000,00, cinquenta milhões), multa diária, publicização da infração apurada e confirmada, bloqueio dos dados até a regularização, eliminação dos dados concernentes à infração, bem como suspensão total ou parcial do banco de dados ou atividade de tratamento de dados e proibição do exercício de atividades

concernentes ao tratamento de dados. Nesse contexto, Carvalho e Pedrini (2019) afirmam que as penalidades aos infratores se mostram extremamente frágeis.

Para além disso, Pinheiro *apud* Cardoso (2019) aduz que a própria legislação de proteção de dados traz circunstâncias minorantes para as sanções determinadas, tais circunstâncias dizem respeito à gravidade da infração, boa-fé do infrator, vantagem obtida, reincidência, dano causado, entre outras.

4.3 A efetividade da resposta estatal aos crimes cibernéticos

O Código Penal é a parte do ordenamento jurídico brasileiro no qual está a maior parte das tipificações penais. Contudo, no que concerne aos crimes cibernéticos há a carência de uma legislação penal específica que contenha punições e penas específicas a serem cominadas, no caso de cometimento desse crime, assim entende Padovez e Prado (2019).

Segundo os autores, a previsão legal e as punições cominadas aos crimes virtuais são insuficientes para proteger o cidadão e punir o criminoso ao ponto de impeli-lo de reiterar a prática ou até mesmo constranger o indivíduo a não praticar o crime, uma vez que a parte mais sensível e que mais afligida é a vítima, chegando até mesmo a suportar danos psicológicos em razão de ter sua privacidade invadida.

Padovez e Prado (2019) afirmam, ainda, que o problema relativos à punibilidade dos crimes virtuais ocorrem também em leis específicas, como é o caso da Lei 12.737/12, vez que a pena prevista no artigo 154-A é de três meses a um ano, sendo possível até a substituição da pena por pecúnia, equivalendo, assim, a um crime de médio potencial ofensivo. Desse modo, entende os autores que a lei não cumpre seu papel repressivo.

Soares e Barbosa (2016) acrescentam que a lei em comento vem recebendo inúmeras críticas, uma delas é pelo fato de a lei ser criada em decorrência da pressão da mídia e da população, esse fato gerou consequências, tais como a ausência de discussão por profissionais especializados na área. Os autores asseguram, ainda, que Ferreira (2014) corrobora com esse entendimento ao afirmar que a influência da mídia e a pressão sofrida por todos os lados colaborou para que o legislativo editasse e aprovasse a lei, e que a consequência da edição de lei sem a devida discussão acerca do assunto foi uma legislação ineficiente e que não atende à sua finalidade.

Para além disso, Ferreira *apud* Soares e Barbosa, afirma que por outra vertente merece crítica também o fato de não haver profissionais técnicos especializados para o processo investigativos dos crimes virtuais, segundo o doutrinador, esse tipo de investigação exige investigadores altamente capacitados, equipamentos de última geração, bem como conexão de alta qualidade e colaboração de outros países.

Ademais, Padovez e Prado (2019) ressaltam que as leis brasileiras não estão aptas para reprimir os crimes cibernéticos, vez que até mesmo as legislações específicas não preveem em seus textos a criminalização do uso e instalação de vírus, *malware* e *ransomware,* os quais são usados no ambiente virtual para roubar dados.

Para além disso, os autores afirmam que até mesmo as leis específicas deixam a desejar em seus textos, a exemplo a lei 12.737/12 não abrange os televisores, que também são dispositivos que podem ser usados no cometimento de crimes virtuais. Corroborando com esse entendimento, Macedo *apud* Soares e Barbosa (2016) afirma que, em que pese a Lei 12.737/12 ser um tipo penal misto, deixa a desejar em sua redação, sendo que a ausência de termos técnicos praticamente inviabiliza a aplicação da lei.

5. Considerações finais

A internet é um ambiente que pode favorecer, desfavorecer e até mesmo destruir uma pessoa. No decorrer deste trabalho pode-se perceber que há pessoas que usam do conhecimento avançado em informática para ajudar outras pessoas, sendo que algumas destas pessoas com conhecimento acima da média trabalham para empresas a fim de criar e aprimorar sistemas, bem como corrigir erros nos sistemas já existentes.

Contudo, da mesma forma que há pessoas que utilizam das redes para benefício de outrem, há também o indivíduo que se utiliza do conhecimento em redes e sistemas de informática para malefício de outras pessoas, cometendo diversificadas tipificações, inclusive violando a privacidade de pessoas, invadindo dispositivos informáticos e divulgando dados e arquivos pessoais de suas vítimas para receber dinheiro ou apenas para prejudica-la por pura diversão.

Desse modo, o presente estudo teve como escopo analisar a tutela jurisdicional penal à vítimas de crimes de violação de privacidade no âmbito virtual, posto que, conforme estudado, o cometimento de crimes nessa modalidade representa algo novo e ainda não há no ordenamento jurídico brasileiro uma legislação específica que trate deste assunto.

Há um adágio que diz que “a internet não é terra de ninguém”, por certo aquele que costuma usar esta frase imagina que a internet é um ambiente em que a legislação não alcança, sendo que nesse ambiente é possível fazer todas as coisas.

Em que pese não haver legislação específica para tratar do assunto, algumas leis foram criadas para proteger a sociedade dentro do ambiente virtual, logo, o adágio é refutado, posto que a internet não é um ambiente inalcançável para a legislação, seja ela penal ou não.

A Lei 12.737/12, a qual alterou o Código penal, foi criada com o fito de proteger o indivíduo no ambiente virtual e, da mesma forma, fora criada a Lei Geral de Proteção de Dados, que ainda não está em vigor. Essas duas leis, em especial, foram objetos de análise neste estudo. Sendo que, o objetivo deste trabalho foi analisar os impactos e a eficiência dessas leis.

Para alcançar o objetivo do trabalho e responder à problemática proposta, incialmente foi apresentado o histórico da internet, estabelecendo período, local, como surgiu e como se desenvolveu a internet até que chegasse ao domínio público e, em seguida, discorreu-se sobre o cibercrime, seu conceito e as considerações de doutrinadores e pesquisadores sobre o tema.

Após foi necessário discorrer sobre a tutela constitucional e penal ao direito à privacidade, considerando que este é um direito fundamental estabelecido pela Constituição Federal. Ademais, sendo a inviolabilidade à privacidade um direito constitucionalmente garantido, como se comporta as normas infraconstitucionais, em especial o Direito penal, diante disso? Este assunto foi abordado em tópico específico sobre a proteção penal à privacidade.

Assim, foi necessário, ainda, discorrer sobre as legislações especificas deste estudo, quais sejam, a Lei Carolina Dieckmann e a Lei Geral de Proteção de Dados, frente aos crimes cibernéticos, bem como a efetividade da resposta estatal aos crimes de violação de privacidade.

A partir deste estudo foi possível aferir que a internet representa grande avanço no mundo e, quando bem utilizada, tende apenas a beneficiar à sociedade. Contudo, os criadores da internet e até mesmo os hackers éticos não previram que o avanço

tecnológico se desenvolveria de forma tão rápida ao ponto de pessoas se utilizarem dessa ferramenta para cometer crimes e prejudicar pessoas.

Posto isto, os legisladores foram apresentando diversos projetos a fim de punir os criminosos virtuais e, também, dar uma resposta à sociedade, mas principalmente às vítimas desses crimes. Apesar da boa-fé dos legisladores, as leis criadas até o presente momento não são suficientes para coibir a prática de crimes cibernéticos.

A Lei 12.737/12 – Lei Carolina Dieckmann – apresenta falhas, no estudo pode-se perceber que o texto do art. 154-A criminaliza as práticas apenas em ou por meio de dispositivos informáticos, desse modo, está excluído os dispositivos eletrônicos, a exemplo os televisores. Ademais, a lei não abarca o caso em que dispositivo utilizado para o crime é da própria vítima, bem como para punir o criminoso cibernético há de se considerar a finalidade para a qual cometeu o crime, a depender deste, o indivíduo também não responderá penalmente pela ação.

Para além disso, a Lei 13.709/18 – Lei Geral de Proteção de Dados não apresenta avanço algum no que diz respeito à tutela penal ao direito a inviolabilidade do direito à privacidade. É sabido que esta lei visa proteger o indivíduo desde o planejamento de coleta de dados até mesmo o tratamento dispensado no momento de eliminação dos dados do indivíduo.

Contudo, a LGPD não traz em seu texto nenhuma previsão de sanção penal, todas as penalidades são de natureza cível, tais como, advertência, suspensão, multa e ainda há possibilidade de minorar a sanção aplicada. Isso significa que o indivíduo ao violar a Lei 13.709/18 não responderá penalmente, a menos que o órgão acusador consiga enquadrar a conduta em uma tipificação da legislação penal comum, ou seja, caso consiga adequar a conduta à alguma tipificação do Código Penal.

Destarte, conclui-se que a resposta estatal aos crimes cibernéticos de invasão de privacidade, apesar de prever algumas condutas e objetivar puni-las, ainda é insuficiente para coibir a reiteração da conduta ou que novos indivíduos se insiram nesse meio. Para tanto, é necessária a criação de delegacias específica para tratamento desses crimes, bem como recursos humanos especializados e recursos tecnológicos avançados para possibilitar uma investigação precisa e eficiente.

Há de se falar, ainda, na criação de uma lei específica que verse sobre crimes cibernéticos. Neste contexto, é importante destacar que tramita no Senado Federal Projeto de Lei 236/12, que visa alterar o Código Penal, nesse projeto há um capítulo com quatro artigos sobre crimes cibernéticos.

Referências

ABREU, Karen Cristina Kraemer. **História e usos da Internet**. Biblioteca on-line de Ciências da Comunicação. Universidade da Beira Interior. Covilhã, 2009. Disponível em: http://www.bocc.ubi.pt/~boccmirror/pag/abreu-karen-historia-e-usos-da-internet.pdf. Acesso em 26 abr. de 2020.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 4060, de 2012**. **Lei Geral de proteção de Dados.** Dispõe sobre tratamento de dados pessoas e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=0D8091FA647B23D22E218F64D064A344.proposicoesWebExterno1?codteor=1001750&filename=PL+4060/2012. Acesso em 15 abr. 2020. Texto original.

BRASIL, Código Civil (2002). **Institui Código Civil Brasileiro**. Brasília, DF: Senado Federal, 2002.

BRASIL, Constituição (1998). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988.

BRASIL. Lei 13.709, de 14 de agosto de 2018, **Lei Geral de Proteção de Dados**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 10 mar. 2020.

CARDOSO, Júlia Furtado. **A Apuração dos Crimes Cibernéticos e o Direito à Intimidade**. 2019. Disponível em http://localhost:80/jspui/handle/123456789/250. Acesso em 10 mar 2020.

CARVALHO, Gisele Primo; PEDRINI, Tainá Fernanda. **Direito à Privacidade na Lei Geral de Proteção de Dados Pessoais.** REVISTA DA ESMESC, v.26, n.32, p. 363-382, 2019. Disponível em https://doi.org/10.14295/revistadaesmesc.v26i32.p363. Acesso em 22 mai de 2020.

CARVALHO, Marcelo Sávio Revoredo Menezes de; CUKIERMAN, Luiz Henrique. Os primórdios da Internet no Brasil. ***Historia de la informática en América y Latina: Investigaciones y testimonios***. Disponível em http://www.nethistory.info/Resources/Os%20primordios%20da%20Internet%20no%20Brasil.pdf. Acesso em 22 mai de 2020.

COTS, M. & OLIVEIRA, R. **Lei geral de proteção de dados pessoais comentada.** São Paulo: Thompson Reuters Brasil, 2018.

DAMASCENO, Paulo Victor Medeiros. **A invasão de dispositivo informático e a tutela penal da privacidade**. 2014. Dispnível em http://repositorio.ufc.br/bitstream/riufc/27736/1/2014_tcc_pvmdamasceno.pdf. Acesso em 30 mai 2020.

DINIZ, Maria Helena. **Curso de direito civil brasileiro:** responsabilidade civil. 22. ed. rev. amp. atual. São Paulo: Saraiva, 2008.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006

EGEWARTH, Arthur Bernardo. **Os crimes cibernéticos e a ineficácia da lei "Carolina Dieckmann"**. 2020. Disponível em http://bibliodigital.unijui.edu.br:8080/xmlui/handle/123456789/6497. Acesso em 08 mai 2020.

GOETHALS, Karen; AGUIAR, Antónia; ALMEIDA, Eugénia. História da Internet. **Faculdade de Engenharia da Universidade do Porto, Mestrado em Gestão da Informação**, 2000.

LACERDA, Júlia Thereza Saraiva de. **O Direito a Privacidade e as Omissões da Legislação Frente aos Avanços Tecnológicos da Atual Era Digital:** Uma Análise à Luz dos Crimes Cibernéticos. Portal de Trabalhos Acadêmicos, v. 2, n. 2, 2019. Disponível em https://faculdadedamas.edu.br/revistafd/index.php/academico/article/view/932/753. Acesso em 08 mai 2020.

LENZA, Pedro. **Direito constitucional esquematizado**. 17ª ed. ver., atual, e ampl. – São Paulo: Saraiva, 2013.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional.** 7. ed. rev. e atual. São Paulo: Saraiva, 2012.

MORAES, Alexandre de. **Direitos humanos fundamentais.** 4. ed. São Paulo: Jurídico, 2002.

NUNES AZEVEDO, Mário Vinicius de; MADRID, Fernanda de Matos Lima. **Crimes Virtuais:** O Desafio do Código Penal na Atualidade e a Impunidade dos Agentes. ETIC-ENCONTRO DE INICIAÇÃO CIENTÍFICA-ISSN 21-76-8498, v. 15, n. 15, 2019. Disponível em http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/7895/67648632. Acesso em 10 mar 2020.

PADOVEZ, Rafael Silva; DO PRADO, Florestan Rodrigo. **O Direito Penal Brasileiro no Contexto dos Crimes Cibernéticos**. ETIC-ENCONTRO DE INICIAÇÃO CIENTÍFICA-ISSN 21-76-8498, v. 15, n. 15, 2019. Disponível em http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/7962/67648763. Acesso em 10 mar 2020.

PAESANI, Liliana Minardi. **Direito e internet:** liberdade de informação, privacidade e responsabilidade civil. 7. ed. São Paulo: Atlas. 2014.

PINHEIRO, Emeline Piva. **Crimes virtuais**: uma análise da criminalidade informática e da resposta estatal. Graduaçao, Pontificia Universidade Católica do Rio Grande do Sul (PUCRS), Porto alegre, RS, 2006.

PONTICELLI, Murilo Meneghel. **O direito fundamental à privacidade no âmbito da rede mundial de computadores com o advento da Lei Geral de Proteção de Dados**. **Direito-Tubarão**, 2018. Disponível em https://www.riuni.unisul.br/bitstream/handle/12345/6288/TCC%20Murilo%20Assinado.pdf?sequence=1&isAllowed=y. Acesso em 25 abr de 2020.

ROCHA, Maristela Dourado. **A conexão da Metodista à internet: a maior rede do planeta**. Informação & Informação, v. 2, n. 2, p. 13-22, 1997. Disponível em http://www.uel.br/seer/index.php/informacao/article/view/1623/1377. Acesso em 22 mai 2020.

SILVA, José Afonso da. **Curso de direito constitucional positivo.** 32. ed. São Paulo: Malheiros, 2009.

SOARES, Jéssica Marques; BARBOSA, Jesuíno. 13. **A Lei nº 12.737/2012 (Denominada Lei Carolina Dieckmann) Frente aos Crimes Virtuais de Invasão de Privacidade.** Disponível em https://sfo2.digitaloceanspaces.com/indexiscdn/cesut/2018/08/ab-origine-2017-1-13-A-LEI-N%C2%B0-12.7372012-DENOMINADA-LEI-CAROLINA-DIECKMANN-FRENTE-AOS-CRIMES-VIRTUAIS-DE-INVASA%CC%83O-DE-PRIVACIDADE.pdf. Acesso em 30 mai 2020.

TEIXEIRA, Apollo Lima; SILVA, Rubens Alves da. **Proteção de Dados Pessoais e as Novas Tecnologias**:(IN) SEGURANÇA QUANTO AOS DIREITOS FUNDAMENTAIS. Revista Artigos. Com, v. 7, p. e1875-e1875, 2019. Disponível em https://acervomais.com.br/index.php/artigos/article/view/1875/850. Acesso em 25 abr de 2020.