CONEXÃO UNIFAMETRO 2020
XVI SEMANA ACADÊMICA
ISSN: 2357-8645

A PROTEÇÃO DA PRIVACIDADE EM DECORRÊNCIA DA CRESCENTE PRÁTICA ENVOLVENDO OS CRIMES CIBERNÉTICOS

Ingrid Vanessa Mendes de Lima
Discente-Centro Universitário Fametro – Unifametro
ingrid.lima@aluno.unifametro.edu.br
Isaac de Araújo Lima
Discente-Centro Universitário Fametro – Unifametro
isaac.lima@unifametro.edu.br

Área Temática: Constituição, Cidadania e Efetivação de Direitos
Encontro Científico: VIII Encontro de Iniciação à Pesquisa

RESUMO

Introdução: Diante do uso de tecnologias que hoje se tornou comum e de fácil acesso à maioria das pessoas, cresce também o uso destas por parte de pessoas com más intenções, que usam de diversos modos, artifícios e má fé para ludibriar suas vítimas, passando a ferir sua privacidade. Portanto, a legislação brasileira precisou se adaptar para proteger a privacidade através de leis que normatizassem o direito à privacidade e sanções para quem violassem as normas. **Objetivo:** Demonstrar as leis que protegem a privacidade e como o cidadão pode proteger-se no meio virtual contra ataques indesejados. **Métodos:** A metodologia utilizada foi a pesquisa bibliográfica identificando as principais leis que relatavam sobre o direito à privacidade e métodos qualitativos para garantir a segurança no sistema virtual. **Resultados:** O direito à privacidade é garantido em dispositivos como a Constituição Federal, o Código Civil, a Lei 12.965/2014, a Lei Geral de Proteção de Dados e a Lei dos Crimes Cibernéticos (Lei 12.737/2012) que dispõe sobre a tipificação criminal de delitos informáticos, e métodos para dificultar a ação de criminosos. **Conclusão/Considerações Finais:** A proteção do direito à privacidade está acobertada pela Constituição Federal, Código Civil, Lei Geral de Proteção de Dados e o Marco Civil da internet (Lei 12.965/2014). A Lei dos Crimes Cibernéticos determina a sanção cabível para os crimes cibernéticos. Apesar disso, é necessário que o usuário tenha precaução ao utilizar a internet, buscando sempre sites confiáveis, produzindo senhas fortes contendo letras, números e caracteres para evitar a ação de criminosos.

Palavras-chave: Direito à privacidade; Internet; Proteção aos dados pessoais; Crimes cibernéticos.

INTRODUÇÃO

A crescente prática de crimes cibernéticos está sendo possibilitada devido à disponibilidade da internet ocasionando a exposição de informações pessoais e da

ISSN: 2357-8645

vida particular através de fotos e vídeos, além de descuidos com senhas que podem ser facilmente descobertas, “e-mails” fraudulentos que são abertos sem a devida precaução e a entrada em sites inseguros.

Constata-se que nos acessos a mídias sociais digitais em dispositivos eletrônicos tais como celulares, notebooks, desktops e tablets, ou meramente fazendo uso da internet para trabalho, são alvos de criminosos, pois quanto maior o uso, mais correm riscos de terem sua privacidade invadida, dentre outros crimes.

De acordo com Sarlet et al. (2019, p.448) o direito à privacidade é considerado direito da personalidade associado à dignidade da pessoa humana assumindo especial relevância para o desenvolvimento e a proteção da personalidade. Situa-se no campo do direito privado, sendo que o próprio indivíduo tem o poder de decidir qualquer questão atinente a esse valor da sua personalidade, sendo ilegítima qualquer tentativa do Estado ou de particulares de se apropriar de aspectos da privacidade.

A privacidade também possui valores extrapatrimoniais que não são avaliáveis em dinheiro, não possuem valoração econômica, mas caso haja violação do direito à privacidade poderá haver repercussão de ordem econômica, seja por previsão contratual ou como compensação pecuniária (CAPELO DE SOUZA, 2011, p. 397).

Para garantir o direito à privacidade a legislação brasileira precisou se adaptar para protegê-la no ambiente virtual. A Constituição Federal e o Código Civil iniciaram sobre esse tema. Em 2014 foi regulamentada a Lei 12.965 que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil sendo a proteção à privacidade citada em vários incisos. Em 2018 a Lei Geral de Proteção de Dados – LGPD (13.709) que tem por objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Apesar da proteção dessas normas é necessário que o usuário defina prioridades no tocante à segurança, há depender das suas atividades e objetivos através de meios eletrônicos, ajustar a frequência com que mantém o acesso a aplicativos bancários, e-mails e sites onde contém informações pessoais.

Aparelho de uso individual já por sua própria terminologia define-se que o uso deve ser restrito ao proprietário ou responsável pelo mesmo, quando este tem por obrigação de mantê-lo seguro ao fazer uso dele. Desta feita, basta um simples descuido para o criminoso utilizando-se de meios ardilosos, conseguir instalar

aplicativos, vírus ou malware e assim passar a acessar os dados e a privacidade.

Seguir alguns cuidados por menores que sejam podem fazer a diferença, pois as garantias atuais voltadas ao combate de crimes cibernéticos não conseguem suprir a velocidade que aflora novos e velhos crimes. Diante de tal realidade é impreterível a constante observação e cuidados necessários para a manutenção da mínima segurança possível.

Desse modo, o presente trabalho tem como objetivos realizar uma revisão bibliográfica sobre as leis que asseguram o direito à privacidade e métodos que o próprio cidadão pode realizar para não ser vítima de golpes pela internet.

METODOLOGIA

Esta pesquisa consistiu na forma descritiva exploratória uma vez que de forma explicativa expôs os detalhes sobre o tema através da coleta de informações possíveis, contribuindo para que o conhecimento sobre privacidade.

Assim, foi utilizada a pesquisa bibliográfica cuja desenvoltura tem como base materiais já existentes, constituído principalmente por livros, dissertações, teses, artigos científicos e sites jurídicos.

Em face do tipo de abordagem, o método utilizado foi o qualitativo, pois foram adotados métodos abertos à complexidade do tema em busca de uma maneira de manter a privacidade assegurada.

Contudo, a abordagem indutiva adotada é baseada em princípios, descrevendo de maneira concreta e real suas causas e efeitos diante das leis.

RESULTADOS E DISCUSSÃO

O direito deve estar sempre atento à evolução humana no aspecto cultural e regulador das condutas humanas vide que para Hans Kelsen, o comportamento é normatizado pelo Direito, que lhe confere um tributo de valor e uma sanção, sem a qual não há como garantir a eficácia da norma, coexistindo com o sistema coercitivo ao qual exerce o poder de Estado sobre o indivíduo, determinando normas e efetivando a sua aplicabilidade (PINHEIRO, 2010, p. 51).

De acordo com Pinheiro (2010, p. 85): “[...] é evidente que o direito à privacidade constitui um limite natural ao direito à informação.” As discussões tornam-

se cada vez mais constantes, visto que alguns julgam estes que de alguma forma expõe por vontade própria algo sobre si mesmo, não poderá fazer mais uso da privacidade, enquanto outros divergem veementemente por defender que é dado ao indivíduo o limite a terceiros a fazerem parte da sua privacidade.

Diante das diversas classificações e inúmeros crimes que acontecem por meios digitais através da internet é necessário levantar que de acordo com Pinheiro (2010, p. 297): “Os crimes eletrônicos ou cibernéticos têm modalidades distintas, dependendo do bem jurídico tutelado.” Isso nos leva a analisar especificamente qual direito está sendo atingido.

Os criminosos se utilizam das brechas do sistema operacional para buscar informações pessoais ou ter acesso a contas bancárias podendo ainda ocasionar danos ao equipamento do usuário hardware[1] e software[2], por fazer mau uso dos dados coletados atacando assim a privacidade, honra, imagem e intimidade de suas vítimas.

Como menciona Pinheiro (2010, p. 297): “O crime de interceptação telefônica e de dados, que tem como bem jurídico tutelado os dados, ou seja, o que se quer é proteger a transmissão de dados e coibir o uso dessas informações para fins delituosos, como, por exemplo, captura de informações para envio de “e-mail bombing[3]”, o “e-mail com vírus[4]”, o “spam[5]”.”

Diante da vulnerabilidade humana frente a sítios da internet a Constituição Federal consagra a proteção à privacidade em seu inciso X artigo 5º assegurando a indenização por dano material ou moral caso seja violada. No artigo 21 do Código Civil revela que caso a vida privada seja violada o juiz a requerimento do interessado adotará providências necessárias para impedir ou fazer cessar ato.

A Lei 12.965/2014 tem, também, como princípio a proteção da privacidade e dos dados pessoais como descrito nos incisos II e III do artigo 3°. No capítulo II que

[1] Palavra usada para definir a parte física de um equipamento. Além do computador formado por placas, discos e microprocessadores, incluem-se nesta definição as impressoras, os monitores de vídeo, os scanners, o mouse, entre outros. É a parte de um sistema de computador que pode ser vista ou tocada. (SILVA JÚNIOR, 2009, p.23).

[2] Programas que dão função aos computadores. Os programas são escritos em linguagem de programação e comandam todo o funcionamento do computador. Software é a parte lógica do computador, que nos permite administrar, operar, manter e usar o equipamento. (SILVA JÚNIOR, 2009, p.23).

[3] Envio de *e-mails* imensos ou vários *e-mails.* Causa atraso na recepção e gasto adicional com contas telefônicas. Aplicável o artigo 163 do Código Penal Brasileiro (crime de dano).

[4] Envio de vírus anexado ao *e-mail*. São aplicáveis os arts. 151 § 1º, II e III, e 163 de Código Penal Brasileiro, com aplicação do art. 65 da LCP, com pena de prisão simples de 15 dias a 2 meses, ou multa por perturbação da tranquilidade.

[5] É o termo usado para referir-se aos e-mails não solicitados, que geralmente são enviados para muitas pessoas.

trata dos direitos e das garantias dos usuários em seu artigo 7º inciso I determina a proteção e a indenização pelo dano material ou moral caso haja a inviolabilidade de intimidade e da vida privada. No artigo 8º descreve que 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.

A Lei Geral de Proteção de Dados – LGPD (13.709/2018) dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Em seu artigo 2º inciso I declara que tem como fundamento o respeito à privacidade. Na seção II nas boas práticas e governança no inciso I do artigo 50 determina que para a proteção da privacidade se estabeleçam políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade. Ao longo de toda a lei aborda os direitos à privacidade.

Nesse sentido, a Lei dos Crimes Cibernéticos (Lei 12.737/2012) ou Lei Carolina Dieckmann dispõe sobre a tipificação criminal de delitos informáticos. No artigo 154-A parágrafo 3º do artigo determina que se da invasão a dispositivo informático alheio, conectado ou não à rede de computadores resultar a obtenção de conteúdo de comunicações eletrônicas privadas a Pena será de reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

Apesar da proteção através das normas jurídicas é necessário que os usuários busquem ferramentas que auxiliem na sua proteção virtual como a criação de senhas fortes contendo letras, números e caracteres tanto para bloquear celulares, notebooks, tablets, como para acessar redes sociais, e-mails, contas bancárias e fazer compras pela internet. Outro recurso indispensável à segurança do usuário é a cautela ao abrir e-mails com emissores desconhecidos ou sites que apresentem ofertas mirabolantes.

Portanto, o mundo virtual impacta diretamente na vida das pessoas, assim como os crimes que nele são praticados, devendo o usuário ter sempre atenção e procurar se cercar de cuidados básicos, mas indispensáveis, visto que, após a identificação de um crime ou mesmo de uma tentativa que sejam denunciados às autoridades competentes, pois, somente com o registro da ocorrência mediante uma

investigação serão elaboradas estratégias para identificar e coibir estes crimes.

CONSIDERAÇÕES FINAIS/CONCLUSÃO

A constante evolução das tecnologias, bem como o aumento proporcional ao número de pessoas que passam a ter acesso e fazem uso de redes sociais digitais e dispositivos eletrônicos conectados à internet, contudo, são as maiores vítimas dos crimes virtuais.

Para a proteção do direito à privacidade há um tratamento jurídico para tal. A Constituição Federal e o Código Civil consagram a proteção à privacidade e a Carta Magna assegura a indenização por dano material ou moral caso seja violada. A Lei 12.965/2014 tem, também, como princípio a proteção da privacidade e dos dados pessoais. A Lei Geral de Proteção de Dados protege os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. A Lei dos Crimes Cibernéticos dispõe sobre a tipificação criminal de delitos informáticos.

Assim, conclui-se que existem normas que protegem o direito à privacidade, porém o cidadão precisa prevenir-se para não incorrer em atividades criminosas virtualmente existentes e as quais em suma não há mera tipificação penal, devendo o magistrado recorrer a interpretação de outras normas, quais a conduta do agente seja compatível com os atos praticados. Se busca tipificar, mas até mesmo o crime evolui, devendo os legisladores a incessante perquisição sobre as práticas transgressoras utilizadas em meios eletrônicos.

REFERÊNCIAS

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Senado Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 05 out. 2020.

BRASIL. Lei nº 12.965 de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 05 out. 2020.

BRASIL. Lei nº 13.709 de 15 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais**. Disponível em: <http://www.normaslegais.com.br/legislacao/lei-13709-2018.htm>. Acesso em: 05 out. 2020.

BRASIL. Lei nº 12.737 de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011- 2014/2012/lei/l12737.htm>. Acesso em: 06 de out. 2020.

_____. Lei N º 10.406, de 10 de janeiro de 2002. **Código Civil.** Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em: 06 out. 2020.

_____. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal.** Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 06 out. 2020.

_____. Decreto-Lei nº 3.688, de 3 de outubro de 1941. **Lei das Contravenções Penais.** Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3688.htm>. Acesso em: 06 out. 2020.

PINHEIRO, Patricia Peck. **Direito Digital**, p. 85-257. São Paulo, Ed. Saraiva, 4ª edição, 2010.

SARLET, Ingo Wolfgang.; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de Direito Constitucional**, p. 448. 8.ed. São Paulo: Saraiva, 2019.

SILVA JÚNIOR, Edson Nascimento. **Introdução à computação**, p. 23. Manaus: Universidade Federal do Amazonas, CETAM, 2009.