

LEGAL TECH

DIREITO

RECRUDESCIMENTO DE PENAS PARA OS CRIMES CIBERNÉTICOS EM 2021

Lara Maria Willember Würzius¹; Alexandre Marques Silveira²

1 Graduada em Direito pela Faculdade Meridional (IMED). Atualmente, atua como estagiária forense no Ministério Público do Estado do Rio Grande do Sul. E-mail: laramariaww@hotmail.com.

2 Mestre em Direito pela Faculdade Meridional de Passo Fundo (IMED) e Especialista em Direito Penal pela Faculdade de Direito Prof. Damásio de Jesus. Atualmente, atua como professor do curso de Direito da Faculdade Meridional (IMED). E-mail: alexandre.silveira@imed.edu.br

1 INTRODUÇÃO

A presente pesquisa tem por objetivo primário analisar a recente Lei nº 14.155 de 27 de maio de 2021, a qual tornou mais grave os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet. O objetivo do estudo apresentado é elucidar o problema que guiará essa pesquisa, o qual é: O recrudescimento de penas para crimes cibernéticos, trazido pela Lei nº 14.155/21, era realmente necessário?

2 METODOLOGIA

Esta pesquisa possui o método de abordagem que servirá de referência para análise das ideias, informações e resultados desta pesquisa é o método dedutivo e a técnica de pesquisa consistirá na investigação de documentação indireta através de pesquisa bibliográfica com exame de fontes normativas e doutrinárias de maneira que examina informações já demonstradas em outros documentos.

3 RESULTADOS E DISCUSSÃO

Com a conexão à Internet em dispositivos móveis, os conceitos de temporalidade e espacialidade foram reformulados, alterando as relações interpessoais ao permitir a interação no ciberespaço (LOVE, 2005, p. 222). Porém, tal fator abriu um novo campo para a criminalidade se espalhar.



Antes da pandemia, em 2019, o Brasil já era o terceiro país no ranking dos que sofrem mais ataques cibernéticos, ficando atrás apenas da China e dos Estados Unidos, de acordo com um relatório global divulgado pela *Symantec* (2019). Sob essa perspectiva, a *Fortinet Threat Intelligence Insider Latin America* (2021), empresa que analisa incidentes de segurança cibernética, divulgou que o Brasil sofreu mais de 3,4 bilhões de tentativas de ataques na internet, de janeiro a setembro de 2020.

Frente ao exposto, cumpre esclarecer o que são crimes cibernéticos: os doutrinadores não têm uma nomenclatura estabelecida para o conceito de crime cibernético. Em qualquer caso, os nomes desses crimes sofrem alteração, posto que devem ser observados o uso de dispositivos informáticos, a rede de transmissão de dados para delinquir, o bem jurídico lesado, e ainda deve a conduta ser típica, antijurídica e culpável. (SILVA, 2015, p.39).

Perante o aumento significativo de delitos por meio eletrônico durante a pandemia, foi sancionada a Lei nº 14.155 de 27 de maio de 2021, que tornou mais grave os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet. Sobre os tipos penais, deve-se esclarecer que:

A mencionada Lei incluiu o artigo 154-A ao Código Penal, o qual trata de penalizar em reclusão, de 1 (um) a 4 (quatro) anos, e multa o agente que violar dispositivos informáticos, de forma indevida burlando o mecanismo de segurança, a fim de obter, adulterar ou destruir dados ou informações sem a autorização explícita ou tácita do proprietário do dispositivo, ou instalar brechas para obter vantagens ilegais, deixando desprotegida a privacidade da vítima (BESERRA et al, 2020).

A lei em questão ainda incluiu aos tipos penais furto e estelionato a sua forma eletrônica. Para o furto, basta que seja cometido mediante fraude eletrônica; já para o estelionato, a qualificação tange sobre a respectiva forma como as informações fornecidas pela vítima foram obtidas pelo autor, dando-se ênfase aos meios eletrônicos como forma de execução do crime. Ambos os tipos penais indicam a pena de reclusão, de 4 (quatro) a 8 (oito) anos e duas causas majorantes, as quais são: praticado mediante a utilização de servidor mantido fora do território nacional e praticado contra idoso ou vulnerável.

Sobre estes novos patamares, as causas de aumento de pena para furto e fraude eletrônica têm sido objeto de críticas da doutrina quanto à sua desproporcionalidade.



Sob outra vista, denota-se que os tipos penais apresentados pela lei já vem sendo penalizados por analogia a outros dispositivos legais vigentes.

Dessarte, outro ponto que merece destaque é a recente alteração na Lei de Organizações Criminosas – Lei nº 12.850/13, promovida pelo Pacote Anticrime – Lei nº 13.964/19, a qual incluiu o artigo 10-A, que regulamenta a permissão da ação de agentes de polícia infiltrados virtuais na internet, com o fim de investigar os crimes que tutelam a lei ou a eles conexos, desde que demonstrada sua necessidade (BRASIL, 2019).

Além disso, elenca-se que a principal dificuldade de se conter os delitos virtuais é a falta de equipes de investigação regularmente treinadas para tal trabalho, ou seja, “capacitação dos profissionais, como uma condição imprescindível à formação da justa causa para a ação penal”. (CERQUEIRA; ROCHA 2013, p. 131).

Diante dos argumentos anteriores, conclui-se que os métodos de investigação e punição de criminosos enfrentam muitos desafios, envolvendo a necessidade de mecanismos de operação legalmente regulamentados e de recursos especializados. Logo, antes de sancionar uma nova lei para recrudescer penas para crimes cibernéticos seria mais efetivo aprimorar as equipes e meios de investigação de tais delitos e a capacitação de intérpretes da lei para melhor aplicabilidade de normas anteriores que vigoram sobre o assunto.

Frente ao exposto, denota-se que o recrudesimento penal não satisfaz nenhum ímpeto humano. Conforme pensamento freudiano (1915), a pulsão humana terá sua satisfação garantida custe o que custar; sem percepção de penalização ou de um endurecimento de penas.

Nessa perspectiva, ressalta-se o encarceramento em massa e a pena com caráter de mera incapacidade, os quais são consequências da mídia e de lideranças políticas que exigem o recrudesimento irracional de leis, a supressão de garantia e a expansão do Estado penal, sob a visão leiga acerca da realidade (GARLANG, 2008, p. 426).

Assim, a questão da criminalidade necessita ser revista por políticas públicas que reafirmem uma reconstrução do tecido social em sua integralidade. Dessa maneira, o aumento da punição não impedirá a ocorrência de comportamentos desviantes, nem controlará os impulsos das pessoas.



4 CONSIDERAÇÕES

O recrudescimento de penas para crimes cibernéticos, ocorrido pela Lei nº 14.155/21, não se mostra urgente perante a atual situação do país. Embora existisse uma lacuna legislativa sobre a penalização de violação de dispositivos informáticos, bem como acerca do furto e fraude eletrônica, os mesmos já vinham sendo penalizados por analogia.

Ademais, o endurecimento de penas mostra-se em desproporcionalidade com as necessidades do país, haja vista o exacerbado encarceramento em massa, a penalização em contraponto com o objetivo de promover a ressocialização do agente, bem como a necessidade imperiosa da capacitação de profissionais para a investigação de delitos cibernéticos.

REFERÊNCIAS BIBLIOGRÁFICAS

BESERRA, Beatriz Cavalcante. SANTOS, Érika Rocsany Rodrigues dos. AMARAL, Mariana Moreno. **Invasão de dispositivos informáticos no Ordenamento Jurídico Brasileiro**. v. 12 (2020): II Mostra Científica Interdisciplinar do Vale do Araguaia (Edição Especial)

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**: Aperfeiçoa a legislação penal e processual penal. Brasília/DF. Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/ato20192022/2019/lei/L13964.htm. Acesso em: 14 jun. 2021.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**: Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato, 27 mai. 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/ato2019-2022/2021/Lei/L14155.htm. Acesso em: 14 jun. 2021.

CERQUEIRA, Sílvio Castro e ROCHA, Claudionor. **Crimes cibernéticos: desafios da investigação: Cadernos Aslegis**, 2013. Disponível em: <http://bd.camara.gov.br/bd/handle/bdcamara/27420#>. Acesso em: 14 jun. 2021

FORTINET. **Threat intelligence insider**. 2021. Disponível em: <https://www.fortiguardthreatinsider.com/pt/bulletin/Q1-2021>. Acesso em 14 jun. 2021

FREUD, Sigmund. **O inconsciente**. In Edição standart brasileira das obras completas de Sigmund Freud, vol. XIV. s.t. Rio de Janeiro: Imago, 1915/1996, pp. 163-222.

GARLAND, David. **As condições da “sociedade punitiva”: o caso britânico**, s.t. In Revista de sociologia e política, Curitiba, n. 13, 1999, p. 59-80.



LOVE, S. Introduction. In R. Ling & P. E. Pedersen (Eds.), 2005. **Mobile communications: re-negotiation of the social sphere** (p. 221-224). Haslemere (UK): Springer. ISBN 1-85233-931-4.

SILVA, Patrícia Santos da. **Direito e crime cibernético: análise da competência em razão do lugar no julgamento de ações penais**. Brasília: Vestnik, 2015.

SYMANTEC. **ISTR: Internet Security Threat Report, volume 24**. Fev. 2019. Disponível em: <https://docs.broadcom.com/doc/istr-24-2019-en>. Acesso em: 14 jun. 2021.

