Revista Jurídica Direito, Sociedade e Justiça/RJDSJ

Curso de Direito, UEMS – Dourados/MS

NUANCES DA APLICABILIDADE DA LEGÍTIMA DEFESA AO CENÁRIO INFORMÁTICO DA ERA DIGITAL

SILVA, Bruno Dutra Maciel[1]

NOLASCO, Loreci Gottschalk[2]

Resumo: O presente trabalho busca apontar possíveis respostas ativas à criminalidade virtual que, no cenário proveniente da revolução digital, ameaça significativamente bens empresariais juridicamente tutelados. Encontrado o mais promissor dos meios já aplicados na prevenção e enfrentamento dos delitos informáticos, a saber, o *ethical hacking,* visa analisá-lo sob a lente do art. 25 do Código Penal, que postula acerca da legítima defesa, a fim de constatar sua categorização como resposta eficaz, lícita e segura frente aos ilícitos cibernéticos que colocam em risco a integridade de sistemas e bens imateriais, como o segredo industrial e a propriedade intelectual, no contexto das instituições.

Palavras-chaves: Legítima Defesa; Delitos Informáticos; Direito Penal Informático; Cibersegurança; Ethical Hacking.

Introdução

O alvorecer da tecnologia trouxe consigo uma nova formatação de sociedade na qual os indivíduos encontram-se globalmente interligados pela cibercultura e pelo ciberespaço, sem limitações físicas, fatores responsáveis pela estruturação de circunstâncias até então não experimentadas pela humanidade e, consequentemente, pelo Direito. Entre essas, estão aquelas socialmente desagradáveis como os delitos, que, em razão da virtualização de riquezas até então físicas e do surgimento de novos bens imateriais próprios do meio digital, passam a suceder no mundo informático.

Frente à tamanha problemática, algumas questões acerca da segurança dos bens ameaçados pela complexa criminalidade cibernética são levantadas no cenário empresarial/institucional onde as informações possuem um papel de grande relevância: Se a proteção estatal falha na assistência aos bens juridicamente tutelados já consagrados, o que assegurará a integridade das riquezas imateriais que requerem

[1] Acadêmica do Curso de Direito da Universidade Estadual de Mato Grosso do Sul (UEMS)
2 Doutora em Biotecnologia e Biodiversidade pela Universidade Federal de Goiás (UFG). Mestre em Direito pela Universidade de Brasília (UnB). Docente e Pesquisadora do quadro efetivo do Curso de Direito da Universidade Estadual de Mato Grosso do Sul (UEMS). E-mail. lorecign@gmail.com

monitoramento permanente e respostas fugazes mediante o mínimo indício de risco? Além disso, dada a óbvia inviabilidade de tal defesa por parte do Estado, poderiam agentes particulares atuar, licitamente, nesta alçada quando medidas preventivas, como antivírus, já foram superadas pelo agressor?

Estas são as interrogações que o presente trabalho pretende responder mediante o estudo da prática organizacional denominada ethical hacking na modalidade de hacking back, isto é, nas medidas de teor ativo onde grupos de especialistas na área da cibersegurança respondem aos ataques virtuais invadindo os aparelhos utilizados pelos agressores a fim de zelar pelos bens imateriais alvejados.

Nesta toada, o artigo 25 do Código Penal será utilizado como alicerce para determinar a licitude ou não do exercício mencionado ao passo em que se transporta o instituto da legítima defesa, da dimensão física, ao cenário cibernético.

Metodologia

A pesquisa utiliza de referências bibliográficas de caráter dedutivo e da análise da legislação penal e constitucional, sobretudo, aquela relativa à alçada dos crimes virtuais.

Resultados e Discussão

Diante da crescente quantidade de incidentes informáticos, as instituições preocupam-se mais e mais com a proteção de seus bens imateriais. Com efeito, prestam-se a contratar profissionais especializados no ramo da informática objetivando inibir as mazelas do mundo virtual, sejam elas a obtenção de dados sem autorização, “pichações”, disseminação de vírus, etc.

Essas figuras especializadas, intituladas hackers éticos, correspondem à parcela de hackers que se submete à lei e tem a proteção de computadores, software, redes e infraestruturas de TI como norte de suas ações. Em assim sendo, “em um mundo dicotômico, eles seriam os mocinhos” (JAQUET-CHEFFELE; LOI, 2020, p. 182).

Costumeiramente, essas figuras surgem no cenário institucional como componentes de Times de Respostas a Incidentes de Segurança, o que, para o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, correspondem à organizações encarregadas de tratar de "qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores" (2017) ao qual a entidade sob tutela, seja empresarial, governamental ou acadêmica, encontra-se submetida.

Neste contexto, com o fito de promover a tutela que lhe cabe, o ethical hacking emprega a defesa cibernética que, comumente, é concebida em duas perspectivas: a ativa, caracterizada pela ação direta contra as ameaças virtuais com o propósito de aniquilá-las ou reduzir seus efeitos, e a passiva que encerra quaisquer formatos de proteção desde que indiretos, visando a minimização dos resultados dos ataques cibernéticos (DENNING; STRAWSER, 2017).

Ocorre que durante o exercício da defesa ativa, onde o objetivo é repelir a violação e/ou recuperar os bens maculados pelo cracker, faz-se necessário o emprego dos mesmos meios que o infrator o que pode levantar a hipótese de que o agente ético, ainda que agindo com boa-fé, incorre no crime estipulado pelo art. 154-A do Código Penal, além de outros tipos do dispositivo normativo, como o crime de falsa identidade, ensejando a responsabilização cível e criminal dos profissionais, assim como da entidade contratante.

Noutro norte, uma alegação mais assertiva é de que o *hacker* ético, na prática do *ethical hacking*, atuando na tutela necessária de bens jurídicos, encontra-se resguardado por formato já assentado de excludente de ilicitude, a legítima defesa, disciplinada no Código Penal em seu art. 25, o qual dispõe, *ipsis litteris*, que: "Entende-se em legítima defesa quem, usando moderadamente dos meios necessários, repele injusta agressão, atual ou iminente, a direito seu ou de outrem" (BRASIL, 1940).

Para Nucci, a legítima defesa corresponde ao "mais tradicional exemplo de justificação para a prática de fatos típicos", podendo ser vista sob dois ângulos distintos, como bem elucida em menção a Jescheck (2020, p. 343):

> a) no prisma jurídico-individual, é o direito que todo homem possui de defender seus bens juridicamente tutelados [...]; b) no prisma jurídico-social,é justamente o preceito de que o ordenamento jurídico não deve ceder ao injusto, daí porque a legítima defesa manifesta-se somente quando for essencialmente necessária, devendo cessar no momento em que desaparecer o interesse de afirmação do direito ou, ainda, em caso de manifesta desproporção entre os bens em conflito.

Nesta esteira, aludindo aos ensinamentos de Capez (2019), cumpre recordar que a legítima defesa no ordenamento jurídico brasileiro se fundamenta na ausência de condições do Estado em oferecer proteção aos cidadãos a todo instante e em todos os lugares, sendo essencial a permissão para autodefesa nos casos em que não haja outro meio de resguardar o bem jurídico ameaçado.

Aliás, vale pontuar que a doutrina assevera que não só a vida e integridade física estão sujeitas à essa tutela, mas também o patrimônio (CUNHA, 2019), como no caso em análise, onde o objeto em risco são os recém consagrados bens imateriais que, como quaisquer outros — ou até mesmo mais do que outros, dada a complexidade da criminalidade virtual, encontram-se vulneráveis longe da permanente guarda estatal, merecendo, nesse contexto, a defesa privada que lhe é devida.

Quanto aos requisitos para a configuração da legítima defesa, pode-se elencar: I) a existência de uma agressão injusta; II) a atualidade ou iminência da agressão; III) contra direito próprio ou alheio; IV) conhecimento da situação justificante; V) o uso moderado dos meios necessários para repeli-la (CUNHA, 2019).

No tocante à agressão injusta, refere-se às condutas humanas que lesam ou colocam em perigo bens jurídicos tutelados (ESTEFAM; GONÇALVES, 2020), tais quais os incidentes enfrentados pelos agentes de cibersegurança, que, como conceituados anteriormente, abrangem quaisquer ocasiões hostis contra a segurança dos sistemas ou das redes de computadores que possam lesionar, em algum grau, o patrimônio informacional da instituição e, concorrentemente, à privacidade e inviolabilidade de suas informações, fator que também preenche o ponto “III” da listagem acima.

Com relação ao tempo da agressão exigido para que o ato seja enquadrado no art. 25/CP, deve ser presente ou estar prestes a ocorrer, não se admitindo a legítima defesa contra agressão passada ou futura, uma vez que caracterizaria, sucessivamente, vingança ou mera suposição. Decerto, o desenvolvimento do ethical hacking pelos grupos de resposta a incidente, que costumeiramente possuem atividade contínua com o intuito de identificar de imediato quaisquer possibilidades de violação, compartilha da mesma necessidade de celeridade na reação aos incidentes, afinal, como já comentado, no mínimo tardar da resposta, o bem jurídico pode ser maculado sem chances de emenda, a exemplo das informações que sob posse do agressor por poucos instantes está sujeita à divulgação na rede mundial de computadores, não restando muitas medidas para sanar integralmente os prejuízos que a exposição pode causar.

Ademais, nas ocasiões em que a reação não é ágil o suficiente para conter a invasão, que acaba por perpetuar-se com a obtenção dos bens informacionais, não são ilegítimas as ações com o intuito de recuperá-los mediante a obstrução dos sistemas e dispositivos do delinquente, ainda que já consumado o ato típico. Em analogia ao estabelecido por Rogério Sanches Cunha, tratar-se-ia de óbvia falta que equidade a responsabilização do agente de boa-fé em ações para proteger bem jurídico de sua titularidade por acometer prejuízo ao transgressor. Para o autor, em ocasiões como essa, a solução mais justa é “estender a percepção do que constitui a agressão atual”, assim, “se a agressão cometida pelo agente enseja a reação imediata da vítima, ainda que, na esfera do tempo do crime, tenha havido consumação, é justo que se viabilize a incidência de excludente de ilicitude” (2019, p. 311-312).

No que pertine ao elemento subjetivo do ato para que seja abrangido pela excludente de ilicitude, há a necessidade de que o agente tenha plena compreensão acerca da situação justificante, isto é, o animus defendendi, o que não se esperaria menos dos profissionais do ramo da informática responsáveis pela detecção e rastreamento do incidente de segurança que, para devido tratamento, requer plena ciência de suas condições e, certamente, vontade de defender-se.

Por fim, com respeito à exigência de emprego moderado dos meios necessários para repelir a agressão injusta, pode-se dizer que corresponde à limitação do *ethical hacking* enquanto exercício de legítima defesa, e, nesse sentido, a condição que garante a sua atuação como mantenedor da estabilidade e segurança do meio digital, e não o inverso.

Segundo a doutrina, entende-se por meios necessários aqueles que sendo os menos lesivos, contenham com suficiência e eficácia a transgressão. Há de se salientar que, encontrado, deve ser utilizado com moderação, em outras palavras, sem excessos, mas com razoável proporção entre a defesa desempenhada e a agressão sofrida, o que, de acordo com a jurisprudência, demanda análise das circunstâncias caso a caso (NUCCI, 2020, p. 355).

Damásio de Jesus, lecionando sobre a legítima defesa informática, acentua a afirmativa supra, enunciando que a resposta ativa “deve se valer de proporcionalidade e não pode servir de subterfúgio para ataques digitais ou exercício arbitrário das próprias razões” (2019). Dessas palavras, pode-se abstrair a vedação às ações de caráter meramente ofensivo, ou seja, com o intuito de unicamente gerar prejuízo a outrem mediante ataque social ou politicamente motivados, o que, de acordo com Dorothy Denning, configura “hacktivism” (2008, p. 442).

Longe disso, para que sejam beneficiados pela excludente de ilicitude em pauta, o *hacker* ético deve usufruir dos instrumentos que infrinjam o menor dano possível ao agressor o que oscila de acordo com a modalidade de incidente de segurança. Por vezes, o simples acesso à conta do *cracker* em plataformas de armazenamento em nuvem será bastante para a resolução da problemática, enquanto em outras ocasiões, envolvendo maior quantidade de dados violados, a medida necessária pode a ser a exclusão integral dos arquivos mediante o cancelamento da conta (CRESPO, 2011).

Indubitavelmente, não se verificando a devida proporcionalidade da resposta, os profissionais, assim como a entidade, serão responsabilizados pela ausência de tato, incorrendo nos termos do parágrafo único do art. 23/CP, qual, em suma, dispõe que o

agente, ainda que em uma inicial situação de legalidade, responderá pelo excesso doloso, com consciência e vontade, ou culposo, nos casos de negligência (CUNHA, 2019, p. 324).

Conclusões

Enfim, superado o enquadramento da atividade em tela ao instituto de legítima defesa, enquanto uma modalidade cibernética desse, resta assentar que, apesar de incidir nas circunstâncias previstas no art. 154-A do Código Penal, nos termos da Lei nº. 12.737/2012, o *ethical hacking* no exercício do *hacking back* não possui caráter antijurídico, posto que beneficiado por uma excludente de ilicitude elencada no art. 23/CP.

Nessa alçada, conclui-se que, acolhendo os efeitos do instituto, qual serve justamente afastar um dos elementos do crime, que é a contrariedade da conduta ao direito (NUCCI, 2020, p. 330), o agente ético no desempenho do ofício supra analisado encontra-se isento de quaisquer penalizações ou responsabilidades oriundas da defesa ativa contra-ataque cibernético, desde que comprovada a proporcionalidade da resposta (JESUS, 2016).

Referências

BRITO, A. Direito Penal Informático. São Paulo: Saraiva, 2013.

CAPEZ, F. Curso de direito penal 1 - parte geral. 23. ed. São Paulo: Saraiva, 2019.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. FAQ: Perguntas Freqüentes ao CERT.br. Brasil, 2017. Disponível em: <https://www.cert.br/docs/certbr-faq.html#6>. Acesso em: 18 jul. 2020.

CRESPO, M. CRIMES DIGITAIS. São Paulo: Saraiva, 2011.

CUNHA, R. S. Manual de Direito Penal: parte geral (arts. 1º ao 120). 7. ed. Salvador: JusPODIVM, 2019.

Constituição da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso: 10 abr. 2020.

DENNING, Dorothy E. The Ethics of Cyber Conflict. In: HIMMA, Kenneth Einar; TAVANI, Herman T. The Handbook of Information and Computer Ethics. Hoboken, New Jersey: Wiley, 2008. Disponível em: < http://www.cems.uwe.ac.uk/~pchatter/2011/pepi/The_Handbook_of_Information_and_Computer_Ethics.pdf>. Acesso em: 03 jul. 2020.

DENNING, Dorothy E.; STRAWSER, BRADLEY J. Active cyber defence: applying air defence to the cyber domain. Carnegie Endowment for International Peace, 2017. Disponível em: <https://carnegieendowment.org/2017/10/16/active-cyber-defence-applying-air-defence-to-cyber-domain-pub-73416>. Acesso em: 20 jul. 2020.

Decreto-Lei 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: 10 abr. 2020.

ESTEFAM, A.; LENZA, P.; GONÇALVES, V. E. R. Direito penal esquematizado® - parte geral. 8. ed. São Paulo: Saraiva, 2019.

FRONTINI, Peter. Hapvida diz que sofreu ataque cibernético, com possível vazamento de dados cadastrais de clientes. Reuters, São Paulo, 06 jul. 2020. Disponível em: <https://br.reuters.com/article/idBRKBN2471KZ-OBRIN>. Acesso em: 14 jul. 2020.

GREICE PATRICIA FULLER, G. P.; SOARES, R. S. M. A tutela penal dos dados empresariais na sociedade da informação no ordenamento jurídico brasileiro. Revista Jurídica da Presidência Brasília, v. 20, n. 121, p. 408-438, 2018. Disponível em: <http://dx.doi.org/10.20499/2236-3645.RJP2018v20e121-1487>. Acesso em: 20 jul. 2020.

JAQUET-CHEFFELE, David-Olivier; LOI, Michele. Ethical and Unethical Hacking. In: The Ethical of Cybersecurity, Springer International Publishing, 2020. Disponível em: <https://link.springer.com/book/10.1007%2F978-3-030-29053-5>. Acesso em: 03 jul. 2013.

JESUS, D. D. Manual de Crimes Informáticos. São Paulo: Saraiva, 2016.

KESAN, Jay P.; HAYES, Carol M. Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace. In: Harvard Journal of Law & Technology, Cambridge, Massachusetts, vol. 25, nº 2, 2012. Disponível em:

<http://jolt.law.harvard.edu/articles/pdf/v25/25HarvJLTech415.pdf>. Acesso em: 03 jul. 2020.

PINHEIRO, P. P. DIREITO DIGITAL. 6. ed. São Paulo:Saraiva, 2015.

SHIRLEY, Robert Weaver. Antropologia Jurídica. São Paulo: Saraiva, 1987.

SOFTWARE ENGINEERING INSTITUTE. Create a CSIRT. Carnegie Mellon University, 2017. Disponível em: <https://resources.sei.cmu.edu/asset_files/WhitePaper/2017_019_001_485695.pdf>. Acesso em: 17 jul 2020.

SYDOW, S. T. COL. SABERES MONOGRÁFICOS: CRIMES INFORMÁTICOS E SUAS VÍTIMAS. 2. ed. São Paulo, Saraiva, 2015.

TEIXEIRA, T. Curso de direito e processo eletrônico. 4. ed. São Paulo, Saraiva, 2018.