DESAFIOS NA TIPIFICAÇÃO PENAL DO SEQUESTRO DIGITAL (*RANSOMWARE*)

CHALLENGES IN THE CRIMINAL TYPIFICATION OF DIGITAL KIDNAPPING (RANSOMWARE)

Claudia da Costa Bonard de Carvalho[1]
Criminal Compliance Business School, Rio de Janeiro/RJ
bonarddecarvalho.adv@gmail.com

DOI: https://doi.org/10.5281/zenodo.13630626

Resumo: O artigo visa examinar as dificuldades da tipificação do *ransomware* no Direito Penal brasileiro, para cumprimento dos compromissos da Convenção de Budapeste contra o cibercrime, pela gravidade dos ataques cibernéticos contra empresas e a inadequação de vários projetos de lei sobre o tema, que não tutelam os vários bens jurídicos lesados nesse delito, quais sejam privacidade, patrimônio e segredos comerciais, e não definem o seu sujeito passivo, que deve ser a pessoa jurídica, bem como não o tipifica como sequestro digital, conforme revisão bibliográfica e análise dos textos dos projetos de lei.

Palavras-chave: *ransomware*; sequestro digital; lei penal.

Abstract: The article aims to examine the challenges of categorizing ransomware under Brazilian Criminal Law, to fulfill the commitments of the Budapest Convention on cybercrime, due to the severity of cyberattacks against companies and the inadequacy of various proposed bills on the subject, which do not protect the multiple legal interests harmed by this crime, such as privacy, property, and trade secrets. Furthermore, these bills fail to define the victim, which should be the legal entity, and do not classify ransomware as digital kidnapping, as highlighted by a literature review and analysis of the proposed legislation.

Keywords: ransomware, digital kidnapping, criminal law.

1. Introdução

Os ataques cibernéticos não são recentes, mas a necessidade de expansão digital acelerada de atividades, derivada da pandemia de COVID-19, expôs as fragilidades dos sistemas corporativos, que foram alvo de intensa atividade criminosa, no mundo todo.

Com isso, inúmeras empresas tiveram que adaptar seus sistemas para prevenção da atividade de cibercriminosos, que justamente aproveitaram esse momento de transição e intensificaram um tipo de ataque extremamente perigoso, denominado *ransomware*.

O *ransomware* não é novidade no mundo cibernético, tendo sido criado em 1989, como um *malware* que causa danos em sistemas, após acessar a rede das vítimas, pelo bloqueio do acesso a bancos de dados, por meio de criptografia, que transforma textos em códigos constituídos de números e letras, anonimizando seu conteúdo, e visa proteger arquivos contra acessos indevidos (***Ransomware*** [...], 2023).

Assim, no antigo *ransomware* era exigido o pagamento de dinheiro para liberar esses arquivos criptografados, sendo que, posteriormente, o *ransomware* evoluiu a partir do *malware* Wannacry, detectado em 2017, passando-se a exigir o pagamento de criptomoedas para desbloqueio dos bancos de dados.

Desde então, diversas atividades e instituições passaram a ser afetadas por *ransomwares*, como serviços hospitalares e de transporte, ou seja, as denominadas infraestruturas críticas, prejudicando diversos cidadãos.

Nesse cenário, foi assinada, em 23 de maio de 2001, a Convenção de Budapeste contra o cibercrime, onde consta a criminalização de condutas como o *ransomware*, sendo que o Brasil somente a

[1] Especialista em Direito Penal e Processo Penal pela UNESA. Graduada em Direito pela UERJ. Advogada. Link Lattes: https://lattes.cnpq.br/7806591550241197. ORCID: https://orcid.org/0000-0001-8497-810-X. LinkedIn: https://www.linkedin.com/in/claudiabonarddecarvalho/. *Site* institucional: criminalcompliancebs.com.

internalizou em seu ordenamento jurídico em abril de 2023 pelo Decreto-Lei 11.491 (**Brasil**, 2023).

Ocorre que, devido ao crescimento dos ataques de infraestrutura crítica, as polícias de diversos países agora realizam operações complexas para combate ao *ransomware*, como a de fevereiro de 2024, contra a gangue Lockbit, que envolveu 10 países para derrubar 34 servidores usados pelos criminosos em diversos locais (***Law enforcement*** [...], 2024).

O Brasil também foi alvo das gangues de *ransomware*, como o caso do ataque ao sistema do Ministério da Saúde em 2021, que pôs em risco diversos pacientes, de modo a levantar-se a discussão sobre sua criminalização em nossa lei penal, para que o *law enforcement* brasileiro seja efetivado (**Andrade**, 2021).

No entanto o combate ao *ransomware* no Brasil ainda necessita de sua tutela penal, de forma a ser tipificado como sequestro digital, apesar dos vários projetos de lei no Congresso Nacional, que enfrentam desafios de ordem dogmática, que serão examinados a seguir.

2. Metodologia

A questão da tipificação do *ransomware* foi examinada mediante a combinação de revisão bibliográfica do tema com análise comparativa de projetos de lei em tramitação no Congresso Nacional, para que haja melhor adequação do referido ataque cibernético a um tipo penal específico, qual seja, sequestro digital, conforme suas características e a lei penal brasileira.

3. Crimes informáticos no Código Penal

O texto da Convenção de Budapeste (**Council of Europe**, 2021, tradução nossa) evidencia a necessidade de criminalização mundial do acesso indevido a bancos de dados:

> Artigo 2 – Acesso ilegal
> Cada Parte deverá adotar as medidas legislativas e outras que forem necessárias para estabelecer como delitos penais, de acordo com sua legislação nacional, o acesso intencional a todo ou a qualquer parte de um sistema de computador sem direito. Uma Parte poderá exigir que o delito seja cometido por meio da violação de medidas de segurança, com a intenção de obter dados de computador ou outra intenção desonesta, ou em relação a um sistema de computador que esteja conectado a outro sistema de computador.

Nesse sentido, há que se destacar também a definição do fenômeno do *ransomware* na teoria da cibersegurança, que seria o

> [...] acesso ilícito aos computadores de uma empresa, seguindo-se a posterior encriptação dos dados aí armazenados. De seguida, os atacantes iniciam a fase da extorsão à empresa, exigindo avultadas quantias em dinheiro para que os dados fiquem novamente acessíveis (**Antunes; Baltazar**, 2018, p. 127).

Com isso, percebe-se que o ataque *ransomware* envolve diversos aspectos que precisariam ser abordados pela lei em sua criminalização, o que ainda não encontramos em tipo penal equivalente no nosso ordenamento jurídico nacional, senão vejamos:

No Brasil há apenas poucas normas esparsas sobre crimes informáticos no nosso Código Penal (CP), inseridas a partir de 2012, tendo destaque a do artigo 154-A (invasão de dispositivo informático), sendo que ainda não havia sido inserido um dispositivo específico sobre acesso indevido a bancos de dados de empresas, uma vez que, o tipo penal daquele delito está voltado para proteção de pessoas físicas, pela sua posição no CP:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita (**Brasil**, 1940).

No entanto, ainda que o delito do artigo 154-A pareça semelhante à prática do *ransomware* (pela invasão de sistemas desautorizados), ele seria, a princípio, um crime-meio para a sua prática, integrando somente uma etapa do aspecto objetivo dessa conduta.

Não bastasse isso, a extorsão (artigo 158 do CP) seria outra etapa do ataque, praticada com extrema complexidade tecnológica (muitas vezes com inteligência artificial) e não dirigida a ninguém especificamente, de forma que sua definição tradicional seria insuficiente:

> Art. 158. Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa:
> Pena - reclusão, de quatro a dez anos, e multa (**Brasil**, 1940).

Por fim, o *ransomware* ainda atinge de forma reflexa a privacidade dos titulares dos dados armazenados pela empresa, tão importante em tempos de Lei Geral de Proteção de Dados Pessoais, de modo que a adequação típica do *ransomware* gera diversas dúvidas relacionadas ao seu sujeito passivo, bem jurídico tutelado e *nomen juris* adequado, conforme a seguir será demonstrado.

4. Sujeito passivo do crime de *ransomware*

Toda essa inadequação típica do *ransomware* aos dispositivos penais brasileiros decorre da dificuldade de definição, entre outros aspectos, de quem seria o seu sujeito passivo, ou seja, sua vítima, que, em geral, no nosso ordenamento penal, tem como destinatário a pessoa humana.

Ora, se podemos entender que o sujeito passivo de "é o titular do bem jurídico atingido pela conduta criminosa" (**Bitencourt**, 2006, p. 231), e que tal conclusão permitiria incluir a pessoa jurídica como vítima em crimes contra a honra e o patrimônio, não haveria óbice para que o *ransomware* também pudesse ser tipificado como delito praticado contra pessoa jurídica.

Assim sendo, em seu aspecto objetivo, a ação típica de *ransomware* atingiria o sistema da empresa, para se obter o acesso a seu banco de dados, que pode conter informações de diversas naturezas (contratos, pagamentos etc.), para depois criptografá-los em troca de resgate de criptomoedas.

Nessa situação, é fundamental esclarecer que o atacante cibernético não visa atingir nenhuma pessoa específica, sendo os ataques direcionados a sistemas, que são de propriedade de pessoas jurídicas:

> De acordo com o artigo 153 bis do Código Penal, são protegidos a confidencialidade, o sigilo e o direito à privacidade do proprietário do sistema e dos dados informáticos. Tal proprietário pode ser uma pessoa física ou jurídica. Isso pode ser difícil de entender no caso dessa última, como será na maioria dos casos, ou de uma sociedade comercial. Mas é importante lembrar que essas pessoas também têm direito à reserva e ao sigilo de seus documentos particulares (252) e à proteção de seus dados pessoais [...] (**Pallazi**, 2016, p. 65, tradução nossa).

Logo, não se pode confundir a prática do *ransomware* com o delito de invasão de dispositivo informático, que tem por sujeito passivo pessoas físicas e jurídicas, sem necessidade de criptografia de dados, de forma que há que se reconhecer a pessoa jurídica como o sujeito passivo do delito de *ransomware*.

5. Bem jurídico digital e *ransomware*

Outra questão relevante é a adaptação do Direito Penal ao mundo digital em que vivemos, pois "o direito penal vem ao mundo (ou seja, é legislado) para cumprir funções concretas dentro de e para uma sociedade que concretamente se organizou de determinada maneira" (**Batista**, 2005, p. 19), de forma que seus impactos também devem ser estudados pelo Direito Penal.

Com isso, surgiram novos bens jurídicos digitais a serem tutelados pelo Direito Penal, para que sejam assegurados os direitos constitucionais do cidadão, como a proteção dos dados pessoais, já consagrada na Emenda Constitucional 115/2022.

Logo, ainda que se considere o caráter fragmentário do Direito Penal, não se pode ignorar as graves consequências dos ataques cibernéticos contra empresas, que facilitam fraudes financeiras ou expõem a público situações delicadas de pessoas, que, por exemplo, perdem suas economias em uma conta bancária indevidamente acessada ou descobrem que seus dados de saúde foram vazados (exames de HIV, câncer) em laboratórios, o que já não pode ser relegado apenas ao campo civil.

Não bastasse isso, ainda que se considerasse que todo crime cibernético está ligado a um bem jurídico difuso, que seria a segurança informática (**Sydow**, 2015, p. 84), não se pode esquecer que os ataques *ransomware* atingem em sua ação criminosa uma variedade de bens jurídicos tutelados pela lei penal e não somente a navegação na rede.

Logo, há que se definir qual bem jurídico seria tutelado pelo tipo penal a ser criado sobre o *ransomware*, o que afetaria até mesmo o aspecto do nome mais adequado para o delito, diante das questões levantadas anteriormente.

Com isso, temos que considerar que o *ransomware* envolve vários elementos, como a invasão de sistemas corporativos, violação da privacidade das pessoas titulares dos dados bloqueados, bem como prejuízos financeiros corporativos decorrentes do delito, o que dificulta seu enquadramento em algum capítulo específico do Código Penal.

Partindo-se do pressuposto de que "não é necessário que os bens jurídicos possuam realidade material" (**Roxin**, 2009, p. 18), podemos considerar que bancos de dados, apesar de serem ativos virtuais, podem ser protegidos pela lei penal, pelo seu valor de mercado, de forma que o *ransomware* poderia ser considerado, a princípio, um delito patrimonial, ou seja, uma espécie de extorsão digital.

Interessante destacar que a doutrina nacional, representada por Crespo, Damásio de Jesus, Massena, Milagre, Sydow, Wendt *apud* **Barbosa** (2022, p. 114), reconhece o *ransomware* como extorsão, o que ainda dependeria da demonstração de algum prejuízo financeiro, como pagamento de resgate etc. (**Barbosa**, 2022, p. 170), conforme o dolo do atacante, o que não condiz com seus objetivos, uma vez que, a maioria das gangues (Revil, LockBit), salvo aquelas ligadas ao hackativismo, que ataca empresas somente com finalidade financeira (**As maiores quadrilhas** [...], 2024).

Além disso, há necessidade de tutela dos segredos comerciais, que podem ser descobertos no acesso aos bancos de dados de pessoas jurídicas atingidas por *ransomware*, sendo que, em 2021, foi criada uma espécie qualificada de invasão de dispositivo informático, pelo acesso indevido a segredos corporativos, incluindo-se um parágrafo 3º no tipo penal do artigo 154-A:

> Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave (**Brasil**, 1940).

No entanto essa hipótese qualificada não deveria ter sido incluída porque esse delito tutela a intimidade de pessoas físicas, bem como seu tipo objetivo difere do *ransomware*, porque não inclui a criptografia dos dados.

Ainda se afirma que o *ransomware* não poderia ser tipificado como extorsão mediante sequestro (artigo 159 do CP), porque este envolve pessoa física como vítima, o que realmente não se adequa ao caso, porque o sujeito passivo será necessariamente pessoa jurídica (**Crespo**, 2015).

Assim sendo, o *ransomware* seria o sequestro digital de dados, sendo um tipo híbrido penal, que tutelaria ao mesmo tempo o patrimônio, a inviolabilidade de segredos comerciais e a privacidade de terceiros.

6. Projetos de lei sobre *ransomware*

No meio das discussões sobre a adequação típica do *ransomware* na nossa lei penal, há que se comentar os projetos de lei que propõem sua criminalização, em andamento no Congresso Nacional, como o PL 2.232/21, apresentado em 2021 e apensado ao PL 5.441/20, que aguarda pauta de votação no plenário, propõe que o *ransomware* seja apenas uma qualificadora para o delito de extorsão:

> Extorsão cibernética.
> 4º Se o crime é cometido por meio de extorsão cibernética.
> 5º Considera-se extorsão cibernética a exigência de vantagem indevida por parte do agente criminoso com a finalidade de impedir ou suspender um ataque cibernético provocado em sistemas corporativos públicos ou privados (**Brasil**, 2021).

O projeto trata o *ransomware* como qualificadora do crime de extorsão e considera a pessoa jurídica como sujeito passivo, mas ignora a questão da forma de invasão de sistemas, pois extorsão cibernética pode ser feita sem o bloqueio de bancos de dados por criptografia, causando apenas o congelamento de sistemas (ataque DDOS), o que possui consequências menos graves, como derrubada temporária de *sites* de atendimento de empresas e não acarreta perda de dados.

Já o PL 879/22, que também aguarda inclusão em pauta da Comissão de Comunicação e Direito Digital, desde 6 de maio de 2024, aposta no sequestro de dados, considerando-o um delito ligado à privacidade e liberdade individual, ao propor a criação de um tipo penal especial de invasão de dispositivo informático.

> Sequestro de dados informáticos.
> Art. 154-C. Tornar inutilizáveis ou inacessíveis, por qualquer meio, e com o fim de causar constrangimento, transtorno ou dano, sistemas ou dados informáticos alheios:
> Pena – reclusão, de três a seis anos, e multa (**Brasil**, 2022a).

Essa proposta legislativa não enfrenta a questão da definição do sujeito passivo do *ransomware*, o que ignoraria os prejuízos causados aos cidadãos.

Por fim, o PL 1.049/22, que aguarda ainda a designação de relator desde dezembro de 2023, propõe a criação do delito de extorsão digital:

> Extorsão Digital.
> Art. 158-A. Constranger alguém, mediante o uso de softwares ou outro meio apto para o sequestro de dados, tornando-os indisponíveis para o titular, com o intuito de obter para si ou para outrem vantagem econômica indevida, a fazer, tolerar que se faça ou deixar de fazer alguma coisa.
> Pena – reclusão, de seis a dez anos, e multa (**Brasil**, 2022b).

Esse projeto considera a complexidade tecnológica do delito e o insere na categoria patrimonial, abstraindo eventuais reflexos sobre questões de privacidade, como um tipo penal especial.

Mesmo assim, comete-se o erro de considerar o sujeito passivo do delito como a pessoa física, o que não se adequa ao *modus operandi* do *ransomware*, conforme já explanado.

7. Conclusão

Percebe-se, então, a necessidade de criminalização do *ransomware* como sequestro digital, tendo como vítima a pessoa jurídica, tutelando-se o patrimônio, a privacidade e os segredos industriais, o que não se enquadra em qualquer das propostas legislativas analisadas, para proteção adequada de suas vítimas.

Informações adicionais e declarações da autora (integridade científica)

Declaração de conflito de interesses: a autora confirma que não há conflitos de interesses na condução desta pesquisa e na redação deste artigo. **Declaração de autoria:** somente a pesquisadora que cumpre o requisito de autoria deste artigo é listada como autora. **Declaração de originalidade:** a autora garante que o texto aqui publicado não foi publicado anteriormente em nenhum outro recurso e que futuras republicações somente ocorrerão com a indicação expressa da referência desta publicação original; ela também atesta que não há plágio de terceiros ou autoplágio.

Como citar (ABNT Brasil)

CARVALHO, Claudia da Costa Bonard. Desafios na tipificação penal do sequestro digital (*ransomware*). **Boletim IBCCRIM**, São Paulo, v. 32, n. 383, p. 7-10, 2024. DOI: https://doi.org/10.5281/zenodo.13630626. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1221. Acesso em: 1 out. 2024.

Referências

ANDRADE, Henrique. Site do Ministério da Saúde sofre ataque hacker durante madrugada e sai do ar. *CNN Brasil*, 10 dez. 2021. Disponível em: https://www.cnnbrasil.com.br/nacional/site-do-ministerio-da-saude-sofre-ataque-hacker-durante-madrugada-e-sai-do-ar/. Acesso em: 18 ago. 2024.

ANTUNES, Mário; RODRIGUES, Baltazar. *Introdução à cibersegurança*. Lisboa: FCA, 2018.

AS MAIORES QUADRILHAS de *ransomware* e como elas operam. *ExpressVPN*, 28 maio 2024. Disponível em: https://www.expressvpn.com/pt/blog/biggest-ransomware-syndicates-and-how-they-work/. Acesso em: 17 jul. 2024.

BARBOSA, Guilherme Gueiros de Freitas. *A tipicidade dos ataques de* ransomware *no Brasil*: uma interseção entre criptovirologia e Direito Penal. São Paulo: D'Plácido, 2022.

BATISTA, Nilo. *Introdução crítica ao Direito Penal brasileiro*. 10. ed. Rio de Janeiro: Revan, 2005.

BITENCOURT, Cezar Roberto. *Tratado de Direito Penal*: Parte Geral. v. 1. 11. ed. São Paulo: Saraiva, 2006.

BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil*. Brasília: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 16 ago. 2024.

BRASIL. Câmara dos Deputados. *PL 2232/2021*. Altera o art. 158 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever a qualificadora da extorsão cibernética. Brasília: Câmara dos Deputados, 2021. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2287526. Acesso em: 18 ago. 2024.

BRASIL. *Decreto nº 11.491, de 12 de abril de 2023*. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Brasília: Presidência da República, 2023.

BRASIL. *Decreto-lei nº 2.848, de 7 de dezembro de 1940*. Código Penal. Rio de Janeiro: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 16 maio 2024.

BRASIL. Senado Federal. *PL 1049/2022*. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, que institui o Código Penal, para acrescentar ao rol de crimes o Crime de Extorsão Digital. Brasília: Senado Federal, 2022b. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/152857. Acesso em: 18 ago. 2024.

BRASIL. Senado Federal. *PL 879/2022*. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, para qualificar o crime de invasão de dispositivo informático quando houver a obtenção de dados pessoais e criar o crime de sequestro de dados informáticos. Brasília: Senado Federal, 2022a. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/152669. Acesso em: 18 ago. 2024.

COUNCIL OF EUROPE. *Convention on cybercrime*: Special edition dedicated to the drafters of the convention (1997-2001). Estrasburgo: Council of Europe, 2021. Disponível em: https://rm.coe.int/special-edition-budapest-convention-en-2022/1680a6992e. Acesso em: 15 ago. 2024.

CRESPO, Marcelo. *Ransonware* e sua tipificação no Brasil. *Canal Ciências Criminais*, 28 out. 2015. Disponível em: https://canalcienciascriminais.com.br/ransonware-e-sua-tipificacao-no-brasil/. Acesso em: 1 ago. 2024.

LAW ENFORCEMENT disrupt world's biggest ransomware operation: LockBit was the most deployed ransomware variant across the world. *Europol*, 20 fev. 2024. Disponível em: https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation. Acesso em: 17 ago. 2024.

PALAZZI, Pablo A. *Los delitos informáticos en el Código Penal*. 3. ed. Buenos Aires: Abedello Perrot, 2016.

RANSOMWARE: O que é? Como funciona? E outras perguntas frequentes. *International IT*, 29 set. 2023. Disponível em: https://www.internationalit.com/post/ransomware-o-que-%C3%A9-como-funciona-e-outras-perguntas-frequentes. Acesso em: 15 mar. 2024.

ROXIN, Claus. *A proteção dos bens jurídicos como função do Direito Penal*. Porto Alegre: Livraria do Advogado, 2009.

SYDOW, Spencer Toth. *Crimes informáticos e suas vítimas*. 2. ed. São Paulo: Saraiva, 2015.

Recebido em: 07.06.2024. Aprovado em: 15.08.2024. Última atualização da autora: 23.08.2024.