ISSN 2447-1097

Direito & TI–Porto Alegre / RS www.direitoeti.com.br

LEI CAROLINA DIECKMAN E A INVASÃO DE DISPOSITIVO INFORMÁTICO: NECESSIDADE DE ALTERAÇÃO LEGISLATIVA

Alesandro Gonçalves Barreto[1]

RESUMO

O acesso de maneira criminosa a conteúdos de mensagens em aplicativos de mensageria, notadamente o Telegram, traz à baila a discussão sob o crime de dispositivo informático, previsto no art. 154-A do Código Penal. Com penas brandas cominadas, a prática criminosa permanece convidativa para o cometimento de novas ações, caso não seja readequada pelo legislador.

Palavras-chave: *Internet; Invasão; Projeto de Lei.*

INTRODUÇÃO

O crime de invasão de dispositivo informático tem previsão legal no art. 154-A do Código Penal Brasileiro. Nos últimos dias, essa modalidade criminosa assumiu evidência pública, notadamente pela divulgação de 'supostas' conversas em aplicativos de mensageria atribuídos a autoridades brasileiras.

A criminalização dessa conduta decorre do Projeto de Lei nº 2.793, de 29 de novembro de 2011. De acordo com a justificativa apresentada[i]:

> São inegáveis os avanços para a sociedade decorrentes do uso da Internet e das novas tecnologias. Estes avanços trazem a necessidade da regulamentação de aspectos relativos à sociedade da informação, com o intuito de assegurar os direitos dos cidadãos e garantir que a utilização destas tecnologias possa ser potencializada em seus efeitos positivos e minimizada em seus impactos negativos. Nesta discussão, ganha relevo constante, sendo objeto de amplos debates sociais, a temática da repressão criminal a condutas indesejadas praticadas por estes meios.

[1] Delegado de Polícia Civil do Estado do Piauí e coautor dos livros *Inteligência Digital*, *Manual de Investigação Cibernética e Investigação Digital em Fontes Abertas*, Editora Brasport; *Vingança Digital*, Mallet Editora e do e-book Cybercards. Contato: delbarreto@gmail.com

Transformado na Lei Ordinária nº 12.737/12, o diploma previu ainda a equiparação de cartão de crédito ou débito à documento particular, bem como a alteração do crime previsto no art. 266 do Código Penal.

As penas cominadas para essa prática criminosa são, em princípio, convidativas. De todas as condutas previstas, ocorrerá o maior sancionamento quando a invasão resultar na obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou ainda o controle remoto não autorizado do dispositivo invadido. Nesse caso, a pena cominada será de seis meses a dois anos de reclusão com aumento de um a dois terços, se houver divulgação, comercialização ou transmissão do dado ou informação obtida.

Por conseguinte, quase todas as modalidades de invasão de dispositivo informático são consideradas infrações penais de menor potencial ofensivo, devendo ser processadas e julgadas no âmbito dos juizados especiais criminais. Além do mais, a ação penal é, por regra, de natureza pública condicionada, salvo quando o crime for cometido contra a administração pública direta ou indireta de qualquer dos poderes da União, Estados, Distrito Federal ou Municípios, ou contra empresas concessionárias de serviços públicos.

Da forma como consta na legislação nacional, invadir um smartphone visando a obter, adulterar ou destruir dados ou informações de terceiro, e sem a expressa autorização, configura um delito que, caso a autoria e a materialidade sejam individualizadas, a pena cominada é irrisória.

Outrora utilizados apenas para fazer ligações telefônicas, os smartphones apresentam hoje uma infinidade de funcionalidades e de aplicações hospedadas, o que acaba por se tornar providencial para criminosos e usuários mal-intencionados. A instalação de *spywares* em um telefone de terceiros permite, por exemplo, acesso remoto de informações relevantes dos usuários, entre as quais vale destacar: conteúdo de aplicativos de mensageria (mensagens de texto, áudio, vídeo, imagens, chamadas originadas e recebidas); posicionamento *gps*; SMS; registro de chamadas; *webcam*; gravar áudio ambiente; fazer backup de conteúdo armazenado no drive; *e-mails* enviados, recebidos e armazenados; contas em redes sociais; sites acessados; fotos; vídeos, áudios e outras atividades.

Nesse sentido, Goodman ressalta sobre os perigos da exposição no ambiente virtual e sobre quão vulneráveis somos[ii]:

> Os crimes da velha guarda estão sendo viabilizados cada vez mais pelas novas tecnologias, e o big data permite que os criminosos tradicionais nos rastreiem com uma precisão cada vez maior. Devido ao nosso estilo de vida online 24 horas, sete dias por semana, estamos acessíveis o tempo todo, mesmo por aquele que não gostaríamos. O que é estranho sobre esse fenômeno é que muitas vezes nós, a partir do fornecimento voluntário de informações ou via vazamento de dados, estamos tornando mais fácil para os perseguidores, assediadores e criminosos nos encontrarem. (GOODMAN, 2015, p. 101).

Sem dúvida, a virtualização de nossas vidas vem criando cenários atrativos para os criminosos. Urge, pois, a necessidade de adequação legislativa a fim de agravar as pífias sanções atualmente atribuídas ao crime de invasão de dispositivo informático. A punição deve ser exemplar, pois, caso contrário, estaremos cada vez mais suscetíveis a ações de criminosos na busca hábil e inescrupulosa de nossos dados e informações.

REFERÊNCIAS

BARRETO, Alesandro Gonçalves. BRASIL, Beatriz Silveira. *Manual de Investigação Cibernética à Luz do Marco Civil da Internet*. Rio de Janeiro: Ed. Brasport, 2016.

_____. *Aplicativo Simphony: criptografia responsável e boas práticas em tempos de going dark*. Disponível em: <https://www.migalhas.com.br/dePeso/16,MI281303,41046-Aplicativo+Simphony+criptografia+responsavel+e+boas+praticas+em/>. Acesso em: 22 jun. 2019.

BRASIL. 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: 22 jun. 2019.

_____. Lei nº 9.099, de 26 de setembro de1995. Dispõe sobre os Juizados Especiais Cíveis e Criminais e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l9099.htm>. Acesso em: 22 jun. 2019.

_____. 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#art2>. Acesso em: 22 jun. 2019.

_____. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. In: Diário Oficial da República Federativa do Brasil, Brasília, DF, 24 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 22 jun. 2019.

ISSN 2447-1097

CÂMARA DOS DEPUTADOS. Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=944218&filename=PL+2793/2011>. Acesso em: 22 jun. 2019.

GOODMAN, Marc. Future Crimes: Tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso. São Paulo: HSM Editora, 2015.

[i] Câmara dos Deputados. Projeto de Lei nº 2.793, de 29 de novembro de 2011.
[ii] GOODMAN, Marc. *Future Crimes: Tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso*. Estado: Editora, 2015.