Lei nº 14.155/2021 dos crimes cibernéticos

Sauvei Lai*
Pedro Borges Mourão**

Sumário

1. Introdução

Em abril de 1965, o então presidente da Intel, Gordon Moore, previu que a capacidade de processamento de informação iria dobrar a cada 18 meses sem aumento de custo. A profecia, com alguns ajustes, vem se revelando verdadeira. Neste cenário de transformação digital exponencial, o legislativo é chamado para atualizar o conjunto normativo, editando leis que sejam capazes de tutelar de forma eficiente condutas penalmente relevantes que migraram massivamente para o meio virtual, especialmente durante a pandemia da COVID-19, quando as pessoas passaram a trabalhar de casa e a utilizar serviços de internet com maior intensidade e frequência.

Nesta esteira, é boa a notícia da sanção e da publicação da Lei 14.155/2021, que altera o Código Penal (CP) para tornar mais graves as penas dos crimes de violação

* Promotor de Justiça do Ministério Público do Estado do Rio de Janeiro desde 1999. Professor (licenciado) de Direito Processual Penal da EMERJ e da AMPERJ. Membro do grupo de trabalho da sub-relatoria da revisão do CPP na Câmara dos Deputados em 2019. Representante da CONAMP junto à Câmara dos Deputados na discussão do novo CPP em 2021. Coautor do anteprojeto da Lei n. 4.939/2020 sobre Diretrizes do Direito da Tecnologia da Informação e outros assuntos. Examinador do concurso para Delegado de Polícia da PCERJ. Ex-Defensor Público/RJ em 1998.

** Promotor de Justiça do Ministério Público do Estado do Rio de Janeiro desde 2003. Coautor do anteprojeto da Lei n. 4.939/2020 sobre Diretrizes do Direito da Tecnologia da Informação e outros assuntos. Menção Honrosa Prêmio Innovare 2010 Categoria Ministério Público – Programa de Identificação de Vítimas (PIV – MPRJ). Subcoordenador do Centro Integrado de Apuração Criminal 2011-2013. Prêmio Innovare 2011 Categoria Ministério Público – Programa de Resolução Operacional de Homicídios. Prêmios Gestão de Excelência Ministério Público do Estado do Rio de Janeiro 2010 e 2011 – Programa de Identificação de Vítimas (PIV) e Programa de Localização e Identificação de Desaparecidos (PLID) respectivamente. Menção Honrosa Prêmio Conselho Nacional do Ministério Público 2012 - Programa de Localização e Identificação de Desaparecidos. Secretário de Tecnologia da Informação do Ministério Público do Estado do Rio de Janeiro 2013-2014. Usuário Tableau avançado – Treinamento Path Data Governance Innovation 2013. Coordenador de Análises, Diagnósticos e Georreferenciamento do Ministério Público do Estado do Rio de Janeiro (MP em Mapas) 2018-2019. Gerador de conteúdo para a 1ª Edição do Curso de Ciência de Dados para membros e servidores do Ministério Público do Estado do Rio de Janeiro – Realização da Pontifícia Universidade Católica - RJ – 2019. Professor IERBB/MPRJ e Academia de Forense Digital.

de dispositivo informático, de furto e de estelionato (arts. 154-A, 155 e 171), previstos originalmente no texto de 1941, se cometidos de forma eletrônica ou pela internet, além de modificar a competência de certas modalidades de estelionato no art. 70, § 4º do Código de Processo Penal (CPP).

Deveras, o emprego dos meios eletrônicos e das técnicas de engenharia social aumentaram, de modo também exponencial, a lesividade destes delitos. Em vez de causarem prejuízo a alguns, as condutas agora podem atingir milhões de pessoas. Entretanto, soluções que visam a adequar tipicidades concebidas na primeira metade do século XX correm graves riscos de nato-obsolescência diante do contexto do atual estado da tecnologia (e sua constante evolução), como analisaremos a seguir.

2. Invasão de dispositivo informático do art. 154-A do CP

O primeiro destaque que se percebe é a mudança das elementares "Invadir dispositivo informático alheio" para "Invadir dispositivo informático *de uso* alheio" (grifo nosso), além da exclusão da necessidade de "violação indevida de mecanismo de segurança" para a devida tipificação. Portanto, ainda que o dispositivo seja de propriedade do autor do fato, mas emprestado para o colega de trabalho (ou namorada), aquele comete crime ao acessá-lo sem autorização do usuário, mesmo que não haja o emprego de técnicas para ultrapassar barreiras de proteção, como senhas, antivírus, *firewall* e estratégias de verificação em dois fatores.

Assim, a mera "dedução" das credenciais de acesso (senhas óbvias ou muito comuns), sem emprego de estratégias de força bruta, tipificará a conduta. Entretanto, remanesceu-se o especial fim de agir da redação original, isto é, "de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita".

Em complemento, não se pode perder de vista a natureza sistêmica e distributiva da rede pela qual se usa o dispositivo informático invadido, a fim de prevenir equívocos, de modo que, numa invasão remota do servidor de backup de mensagens eletrônicas (recebidas e originadas do dispositivo eletrônico da vítima), não haverá acesso direto ao aparelho dela, mas aos servidores de backup, que são contratualmente disponibilizados ao usuário do serviço pelo provedor de aplicação, para que ele utilize e armazene seus dados digitais. Se o autor do fato consegue as credenciais necessárias para acessar os dados hospedados no servidor de backup do usuário, praticará a conduta típica em questão, eis que, sem autorização, poderá coletar ilicitamente os dados que estão em dispositivo informático do provedor, mesmo sem invadir o dispositivo pessoal da vítima.

Nota-se, outrossim, a clara exasperação da pena do *caput*, que era de 3 meses a 1 ano de detenção, passando a ser de 1 a 4 anos de reclusão e, consequentemente, deixando de ser mera infração de menor potencial ofensivo da competência do Juizado Especial Criminal com a possibilidade das medidas despenalizadoras da composição de danos civis e da transação penal (art. 74 e 76 da Lei 9.099/95), apesar de admitir

ainda outros benefícios, a exemplo da suspensão condicional do processo (art. 89) e do acordo de não persecução penal (art. 28-A do CPP). No entanto, a mudança da natureza da pena de detenção para reclusão permite doravante o cumprimento da sanção em regime prisional inicialmente fechado do art. 33, § 2º do CP (se reincidente ou se houver causa de aumento de pena ou qualificadora), além do uso de interceptação telefônica, objetivando investigar tal crime (art. 2º, III da Lei 9.296/96), sem embargo de ser, na prática, inútil, sendo mais eficientes as modernas técnicas de interceptação telemática por infecção de dispositivo.

Ademais, a lei manteve o texto primitivo da causa de aumento de pena do § 2º e da qualificadora do § 2º, limitando-se a agravar os parâmetros sancionais: de 1/6 a 1/3 para 1/3 a 2/3, no primeiro caso; de 6 meses a 2 anos para 2 anos a 5 anos, no segundo, porém deixa de adotar expressamente o princípio da subsidiariedade, ao eliminar a parte final do preceito secundário da norma "se a conduta não constitui crime mais grave", que constava na redação original, mas que não muda tanto na prática, quando o juiz aplicará ou não o princípio da consunção, dependendo das circunstâncias do caso concreto. De qualquer forma, extrapolando o patamar de 4 anos da pena máxima, viabiliza-se eventualmente a decretação da prisão preventiva, de acordo com a condição do art. 313, I do CPP.

3. Furto do art. 155

Concebeu-se uma nova qualificadora no § 4º-B, quando o "furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer *outro meio fraudulento análogo*" (grifo nosso), diminuindo-se a vigilância da vítima para facilitar a subtração de bens ou valores sem a percepção dela, através do emprego de programa malicioso, como ocorre com a infecção da máquina-alvo por Vírus, *Worms, Bots* e *Trojans*, códigos cuja nocividade se dirige a explorar as capacidades e as informações que o dispositivo ostenta, na maioria das vezes sem que o usuário perceba.

Outro meio fraudulento análogo ao programa malicioso acontece na hipótese de instalação física e ilegítima de *hardwares*[1] *sniffers*, que são instrumentos eletrônicos que "farejam" pacotes de dados, coletando-os e os enviando para o autor do fato para posterior utilização ilícita, embora os criminosos prefiram o *sniffer software*.

[1] Os *sniffers* podem ser *hardware* ou *software*, sendo estes últimos mais próximos de códigos maliciosos quando empregados de modo ilegítimo.

4. Estelionato do art. 171

Por sua vez, o novel § 2º-A estabelece sanção mais grave "se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo".

É válido rememorar que no estelionato existe uma participação ativa e consentida da vítima ou de terceiro, ainda que enganado pela fraude, que entrega suas informações para propiciar um desfalque patrimonial, a exemplo do fornecimento do código de verificação do *Whatsapp* ao criminoso, permitindo que ele "clone" a conta da vítima e peça dinheiro aos seus contatos. Ironicamente, essa regra jurídica, ao contrário do art. 155, o § 4º-B não reivindica o uso de dispositivo eletrônico ou informático, mas sim de "redes sociais, contatos *telefônicos* ou envio de correio eletrônico fraudulento" (grifo nosso), que pressupõe aqueles, por óbvio.

As fraudes eletrônicas mais conhecidas consistem na conjugação de técnicas de engenharia social e de infecção por códigos maliciosos (*malware*), tais como o *Phishing* (mensagens com conteúdo enganoso que estimulam o acesso a páginas maliciosas simuladas que coletam dados pessoais), o *Vishing* (criminoso que explora a confiança da vítima, fazendo-a crer que a ligação telefônica é autêntica e segura, a fim de induzi-la a praticar ações por ele demandadas), o *Man-in-the-midle* (criminoso que se coloca artificialmente entre duas partes que estão em comunicação e, interceptando seu conteúdo, finge ser uma delas para obter dados úteis ao seu intento) e o *Sim Swap* (criminoso que compra um *chip "*em branco", explora os protocolos de autenticação da operadora e, assim, ao clonar o número, obtém acesso às mensagens, senhas e até contas de aplicativos da vítima).

Deste modo, considerando o emprego massivo de inventivas técnicas de engenharia social e de outras estratégias de fraudes, como o desvio de URL (*typosquatting),* para invasão de dispositivos informáticos e/ou coleta de dados pessoais, poderá ocorrer dificuldade de se enquadrar suas variedades nas clássicas distinções entre furto mediante fraude e estelionato, ocasionando certa confusão típica (com margem para amplos debates), ao se ter previsões de causa de aumento no § 2º do art. 154-A em razão de prejuízo econômico, quando já é também cominada outra causa de aumento no § 4º-B do art. 155, quando o furto mediante fraude é cometido por meio eletrônico, sem prejuízo da hipótese de fraude eletrônica do § 2º A do art. 171, ao expressar "qualquer outro meio fraudulento".

5. Causa especial de aumento de pena: idoso e vulnerável

É de se observar que o § 4º-C, II do art. 155 e o § 4º do art. 171 introduzem causa especial de aumento de pena de 1/3 ao dobro quando esses crimes são praticados contra idoso ou qualquer outro vulnerável, podendo resultar, teoricamente, em até 16 anos no caso de furto qualificado e majorado, sanção superior a do tipo derivado do roubo do art. 157, § 2º.

Quanto à condição de idoso, trata-se de norma penal em branco, cujo preceito é incompleto, genérico ou indeterminado, dependendo da complementação de outras normas. No caso, o conceito de idoso (igual ou superior a 60 anos) se acha no art. 1º da Lei 10.741/03 (Estatuto do Idoso). Salvo melhor juízo, essa única qualidade de idoso não justifica o agravamento da sanção, fazendo presumir que todos sejam desinformados no campo da tecnologia. Imaginemos que Bill Gates (65 anos) fosse brasileiro e, numa noite mal dormida, ficasse desatento e acessasse uma URL adulterada (*Typosquatting*), simulando o sítio eletrônico da sua instituição financeira. Em seguida, digitasse seus dados bancários, entregando o acesso à sua conta ao *hacker*.

De outra sorte, a vulnerabilidade genérica descrita no dispositivo peca, a nosso ver, pela violação ao princípio da legalidade estrita do Direito Penal (art. 5º, XXXIX da CR), que reclama uma melhor especificação, a exemplo do art. 217-A, *caput* e § 1º do CP e do art. 313, III do CPP, que poderiam ter sido apontados expressamente pelo legislador, não obstante o raciocínio apadrinhado pelo relator do Projeto de Lei 4.554/2020 que resultou na Lei 14.155/2021, o Senador Rodrigo Cunha, *ipsis litteris*:

> O conceito será preenchido, no caso concreto, pelo juiz criminal, tendo por referência o art. 217-A do próprio Código Penal, *caput* e parágrafo primeiro (menores de 14 anos e aqueles que enfermidade ou deficiência mental, não tem o necessário discernimento para a prática do ato, ou que, por qualquer outra causa, não pode oferecer resistência).[2]

No plano ideal, o recomendável seria proteger o vulnerável tecnológico, situação a ser provada pela acusação no caso concreto (art. 156 do CPP), isto é, aquele que, independentemente da idade, gênero ou condição física, simplesmente não detém conhecimento tecnológico, sendo facilmente ludibriado, como a vítima semianalfabeta.

6. Causa especial de aumento de pena: servidor em território estrangeiro

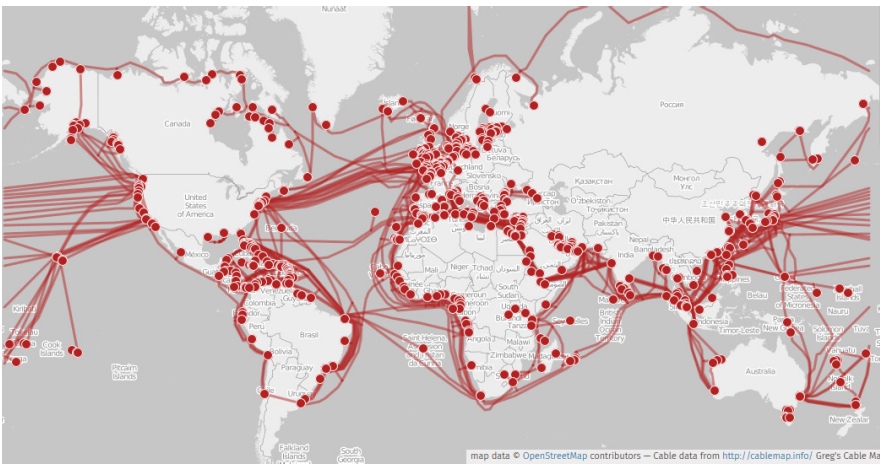
O § 4º-C, I do art. 155 e o § 4º-B do art. 171 majoram a pena de 1/3 a 2/3 no cenário de utilização de servidor[3] mantido fora do território nacional, como na hipótese de um *hacker* que roteia sua conexão a partir do Brasil para que ela aparente advir de um servidor localizado nas Ilhas Seychelles, visando a dificultar a identificação do seu terminal e de si próprio e, no final, armazena os dados obtidos em um servidor instalado em um país com baixo nível de rastreamento de conexões.

Haverá dificuldade de interpretação dessas normas. Diante do caráter naturalmente transnacional do roteamento das comunicações eletrônicas e do crescente armazenamento e processamento de dados distribuídos em nuvem, bem

[2] https://legis.senado.leg.br/sdleg-getter/documento?dm=8908668&ts=1622176912862&disposition=inline

[3] A expressão parece ter sido usada em sentido amplo, isto é, qualquer sistema computacional, físico ou virtual, composto por *hardware* e *software*, dedicado a atender solicitações e prestar serviços para outros dispositivos.

como de modernas técnicas de ocultação e roteamento de conexões, a regra parece ser bem complexa de ser empregada, porquanto parece ser necessária a prova do uso intencional (dolo) e da finalidade de se dificultar ou ocultar a identificação do usuário, visto que a utilização de um servidor situado no estrangeiro é cada vez mais "natural" diante da arquitetura da rede disponível a todos os usuários. É possível, por exemplo, que um criminoso, localizado no Brasil, utilize seu terminal para estabelecer uma conexão com um servidor de dados instalado em solo nacional buscando encriptar dados para obter resgate (*ransonware)*, mas, por uma circunstância técnica sequer conhecida pelo autor[4], a conexão é roteada por servidores localizados no estrangeiro, inexistindo qualquer ato de ocultação que impeça a sua identificação. Essa hipótese não aparenta ser caso de aplicação da majorante. O Mapa dos Cabos de Internet no Mundo abaixo mostra que uma conexão feita a partir do Brasil, mesmo que seu destino seja um terminal dentro do nosso país, pode, potencialmente, passar por outros países antes de chegar ao destino, importando na "utilização" de servidores estrangeiros.



https://pt.wikipedia.org/wiki/Cabo_submarino

De outra sorte, não é impossível que um usuário na Argentina, por exemplo, explore uma vulnerabilidade em um servidor de empresa brasileira, pretendendo infectar servidores brasileiros, criptografar seus dados e, em seguida, cobrar resgate. Se não houver a preocupação de se usar alguma técnica de ocultação, qual seria a razão da majorante? O mero fato de o *hacker* se encontrar no exterior, dificultando a investigação? O mesmo não se aplicaria ao homicida que foge para o estrangeiro?

[4] Muito embora o roteador de borda conheça o "*next-hop*", isto é o próximo salto para que os pacotes de dados cheguem ao destino e, portanto, não vá escolher roteamentos menos eficientes, em um último caso poderá ocorrer a opção por roteamento maior do que a melhor métrica possível (triangulando por servidores estrangeiros) diante de impedimentos técnicos, como manutenção em cabos e congestionamento.

Sabe-se das dificuldades oriundas da inevitável cooperação jurídica internacional para se desvendar o crime nesses casos, porém, aumentá-la até 2/3 seria proporcional, ao invés de simplesmente considerar como circunstância judicial do art. 59 do CP, a fim de exasperá-la na primeira fase da fixação da pena?

Outra circunstância que se deve conjecturar é quando uma organização criminosa brasileira desenvolve ações a partir da utilização ilegítima de um servidor instalado no estrangeiro para disparar ataques de *Phishing,* por exemplo, mirando dispositivos localizados em solo brasileiro. Como o Brasil é signatário da Convenção de Palermo de 2000 (Dec. 5.015/04), atrai-se a competência da Justiça Federal (art. 109, V da CR/88).

7. Relevância do resultado gravoso

As majorantes do § 4º-C do art. 155 e §§ 2º-B e § 4º do art. 171 fazem referência à expressão "considerada a relevância do resultado gravoso", que servirá de critério para a dosagem da fração do aumento de pena (1/3 a 2/3) a ser infligida pelo Juízo. Em outras palavras, à medida que se causa maior prejuízo econômico à vítima, mais se deve se aproximar do patamar máximo fracional na 3ª fase do cálculo da sanção, como se depreende do próprio parecer do relator do PL 4.554/2020 que resultou na Lei 14.155/2021, o Senador Rodrigo Cunha, *in verbis*: "(...) a elevação de pena se justificará diante da relevância do resultado gravoso, como exemplo, quando gera graves prejuízos para a sobrevivência da vítima. Ademais, a elevação não deve se dar de forma estanque, mas em um patamar flexível".[5]

8. Competência territorial do estelionato plurilocal

Inseriu-se o § 4º no art. 70 do CPP, mudando a competência de algumas situações de estelionato plurilocal (conduta e resultado em comarcas distintas), "quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo *local do domicílio da vítima*, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção" (grifo nosso).

No primeiro cenário (fraude via emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado), pode haver, de certo modo, incompatibilidade com a jurisprudência da súmula n. 521 do STF: "O foro competente para o processo e julgamento dos crimes de estelionato, sob a modalidade da emissão dolosa de cheque sem provisão de fundos, é o do local onde se deu a recusa do pagamento pelo sacado", pois normalmente a agência bancária da vítima (banco sacado) se situa na mesma cidade onde mora, mas, às vezes, se localiza em comarca diversa, onde ela morou anteriormente ou onde trabalha, prevalecendo

[5] https://legis.senado.leg.br/sdleg-getter/documento?dm=8908668&ts=1622176912862&disposition=inline

daqui em diante a nova regra processual, ou seja, do local do domicílio daquela, independente do endereço da sua agência.

No segundo contexto (mediante transferência de valores), superou-se o posicionamento esposado pelo STJ no cenário de depósito e de transferência de valores (CC 169.053/DF, Rel. Ministro Sebastião Reis Júnior, 3ª Seção, julgado em 11/12/2019), *in textus*: "Se o crime de estelionato só se consuma com a efetiva obtenção da vantagem indevida pelo agente ativo, é certo que só há falar em consumação, nas hipóteses de transferência e depósito, quando o valor efetivamente ingressa na conta bancária *do beneficiário do crime*". (grifo nosso)

9. Outras condutas não tipificadas

A legislação em comento, ao meramente ampliar as consequências de tipicidades previstas no ano de 1941, data da edição do atual CP, deixou de trazer para a sociedade as garantias necessárias diante de condutas que são, a nosso ver, essencialmente distintas e praticadas em um meio específico. Tais fatores exigem a consideração de novas técnicas e meios insidiosos inimagináveis no passado, bem como a visão de que novos bens jurídicos devem ser observados nos delitos cibernéticos.

De fato, a nova lei fraqueja ao não prever, como se faz no PL 4.939/2020 de autoria do Dep. Hugo Leal e sob a coordenação dos autores deste artigo jurídico, crimes cibernéticos praticados em detrimento de serviços de infraestrutura, como os que visam à sabotagem, à destruição ou à causação de danos a dados, a dispositivos eletrônicos ou a sistemas informáticos sem que haja necessariamente a intenção de obter vantagem patrimonial.

No Brasil, por ocasião da Copa do Mundo de 2014, houve um ataque deliberado aos sítios de internet de instituições nacionais, onde estavam hospedados diversos serviços públicos essenciais para a população. A ação se utilizou de uma técnica de "afogamento" de servidores (conhecida como ataques DDoS), enviando-se a partir de computadores infectados pedidos de acessos superiores às capacidades dos servidores, que mantinham as páginas de internet funcionando. O resultado foi que os serviços providos por diversas instituições públicas, como Ministérios Públicos, Tribunais de Justiça e páginas governamentais ficaram indisponíveis.

Atente-se que a finalidade da conduta não era adulterar ou destruir dados, elementares do art. 154-A, mas sabotar serviços públicos visando fins políticos e/ou ideológicos.

No Brasil estamos em uma situação particularmente sensível. Segundo relatório de inteligência da *Check Point Software*, no início de abril deste ano os números de organizações brasileiras atacadas por códigos maliciosos que sequestram dados essenciais (encriptação de dados por *ransonware*) superaram a média global. De fato, reiteradas têm sido as notícias de ataques a instituições essenciais à democracia brasileira, como Tribunais de Justiça, Suprema Corte e Superior Tribunal de Justiça. Já

o *ransonware Darkside* causou estragos na Copel, Eletrobrás e Grupo Moura, segundo informações amplamente divulgadas na mídia.

10. Conclusão

Por derradeiro, infere-se que a evolução legislativa necessária para proteção social em um cenário delitivo 4.0 reclamará a introdução de visões inovadoras, além dos correspectivos meios de investigação adequados, não se revelando o melhor caminho a adaptação de regras legais da primeira metade do século passado já superadas pela transformação digital.

Rio de Janeiro, 31 de maio de 2021.