JCC JORNAL DE CIÊNCIAS CRIMINAIS

O DELITO DE INVASÃO DE DISPOSITIVO INFORMÁTICO E OS TESTES DE SEGURANÇA (PENTESTS)

INFORMATION TECHNOLOGY ASSET INTRUSION OFFENSE AND THE PENETRATION TESTS (PENTESTS)

Claudio Brandão

Professor titular de Direito Penal. Professor dos Programas de Pós-graduação em Direito da Faculdade Damas e da PUC Minas. Professor Visitante das Universidades de Lisboa e Roma – Tor Vergata. Professor da UFPE.
ORCID: https://orcid.org/0000-0003-3139-4148
E-mail: brandaoclaudio@hotmail.com

Sidney Cassio Alves Rocha

Mestrando em Direito pela PUC Minas.
ORCID: https://orcid.org/0000-0002-6755-7343
E-mail: contato@sidneyrocha.com.br

Resumo: A informática mudou radicalmente as relações sociais; e bens jurídicos são expostos cotidianamente como consequência dessa transformação digital. Simulando o delito de Invasão de Dispositivo Informático, testes de segurança (*PenTests*) são empregados com o objetivo de identificar vulnerabilidades e reforçar a proteção das organizações. Referido delito possui um elemento normativo constitutivo do tipo penal, que é a autorização expressa ou tácita do titular do dispositivo informático, que produz a atipicidade do delito naqueles casos.

Palavras-chave: Invasão de Dispositivo Informático. Segurança da informação. Testes de segurança. Testes de intrusão. *PenTests*.

Abstract: Information Technology radically transformed social relations and juridical goods are exposed as a consequence of this digital transformation. Simulating the information technology asset intrusion offense, penetration tests (PenTests) are performed with the aim of vulnerabilities detection and to enforce business protection. Referred offense has a normative element constitutive of its legal type, the express or tacit authorization from the asset owner, that result the non-incrimination of the PenTests.

Keywords: Information technology asset intrusion. Information security. Penetration tests. PenTests.

1. Introdução

Um dos fortes aspectos da crise do Direito Penal decorre da rápida e profunda mudança das características sociais, que se verificaram a partir dos anos noventa do século XX – portanto, do seu final – até o período hodierno. Essas mudanças reconfiguram as fronteiras do espaço tempo, eliminando antigos limites às interações sociais e trazendo novos frutos, de um lado, e novos perigos, de outro lado.

Como dizem D'Ávila e Santos, não se pode negar que a informática mudou, de forma radical, as relações de espaço e de tempo. Com efeito, "a informática permitiu o tempo instantâneo e, simultaneamente, a compressão do espaço. (…) Nada parece escapar à informática e à rede mundial de computadores. A essa nova e tão intensa dimensão relacional corresponde, por decorrência lógica, novos conflitos, a que é chamado também o direito penal. Parte deles, é verdade, já conhecidos e regulados pela legislação penal. Delitos que encontram na informática apenas um novo espaço e novas formas de realização. Outros, porém, dotados de novas características, colocam dificuldades não só na delimitação da matéria de incriminação, como, até mesmo, na identificação dos valores tutelados pela norma. Dificuldades essas das quais advêm importantes problemas de dogmática penal". (D'ÁVILA; SANTOS, 2016, p. 92)

A tomada do mundo real pelo virtual é "realidade". As inovações tecnológicas são desenvolvidas em períodos de tempo cada vez menores para uma sociedade que se moldou a uma adoção tecnológica tão veloz quanto a sua própria produção. Os ***millennials***[1] (ou Geração Y, os nascidos aproximadamente entre 1977 e 1995) tornaram-se a maior geração viva nos EUA[2]; e a tecnologia está embutida em tudo o que esta geração faz[3].

A internet foi criada no âmbito do Departamento de Defesa dos Estados Unidos da América em 1969, como resultado de um projeto chamado de ARPANET, com a função de integrar os diversos laboratórios de pesquisa e garantir que a comunicação entre militares e cientistas permaneceria, mesmo em caso de ataques militares.[4] Mas o impacto que a internet provocou nas interações sociais foi resultado da criação, no começo da década de noventa do século XX, por Tim Berners-Lee, de uma rede de alcance mundial (1992), o WWW (World Wide Web), que possibilitava a conexão de computadores em todo o mundo, seguida da criação dos primeiros navegadores (Mosaic – Netscape/1993). Nesse contexto, a Internet, concebida nessa geração ***millennials***, tornou-se a plataforma sobre a qual a sociedade moderna tem erigido seu legado.

Por conseguinte, as relações humanas nunca foram tão exploradas quanto são no mundo virtual, ao mesmo tempo que irrompem novos conceitos dignos de estudo, que moldam a maneira com que o homem moderno interage com as pessoas e com o mundo a sua volta.[5]

---

1 THE CENTER FOR GENERATIONAL KINETICS. *Generational breakdown:* info about all of the generations. Disponível em: <http://genhq.com/faq-info-about-generations>. Acesso em: 28 jun. 2019.

2 PEW RESEARCH CENTER. *Millennials overtake baby boomers as America's largest generation*. Disponível em: < http://www.pewresearch.org/fact-tank/2016/04/25/millennials-overtake-baby-boomers>. Acesso em: 28 jun. 2019.

3 SPEND MATTERS. *How millennials are driving technology adoption*. Disponível em: <http://spendmatters.com/2016/06/27/how-millennials-are-driving-technology-adoption>. Acesso em: 28 jun. 2019.

4 Sobre o tema: "Além de ter sido uma resposta às disputas tecnológicas entre o Estado norte-americano e a extinta União Soviética, a ARPANET foi projetada para ser uma rede militar de comunicação independente, com um único servidor, isto é, sem um comando central, objetivando preservar a operabilidade do sistema mediante ataques nucleares. Posteriormente, sua utilização foi disponibilizada às universidades, sendo difundida paulatinamente nos meios acadêmicos" (CAZELATTO; SEGATTO, 2014, p. 390).

5 Ressalte-se que, sobre a internet, "ao mesmo tempo em que este grande repositório de informações e conhecimentos se expande, olhares temerosos veem o desenvolvimento de uma 'outra' internet, onde os delitos virtuais são comuns, profissionalizados, difíceis de se alcançar, além de estarem conectados, por vezes, a interesses políticos, econômicos e ideológicos das transnacionais" (SILVA, 2018, p. 261).

Tal feição da sociedade moderna tem sofrido ataques cada vez maiores e mais profundos através dos crimes cibernéticos. Nações do mundo inteiro encontram-se em meio a uma discussão inevitável sobre a regulamentação do "virtual" frente a desafios importados do mundo "real", contrapesando direitos fundamentais como liberdade e privacidade e os limites e controles impostos pela atividade estatal.

Quanto mais o mundo virtual torna-se parte do cotidiano social, mais bens jurídicos são expostos ao *cybercriminoso*. A produção legislativa tem se ocupado – de maneira não muito eficiente – com a criação de tipos penais para conter o avanço exponencial do cometimento de ilícitos nos ambientes virtuais.

Para avaliar as medidas de segurança que estão implementadas nos ambientes corporativos, profissionais de segurança da informação realizam testes de invasão (***Penetration Tests*** ou ***PenTests***) quando contratados. Seus relatórios servem como guia para adequação dos seus ambientes de Tecnologia da Informação com novos investimentos, criação de procedimentos, correções de software e tudo aquilo que representar uma vulnerabilidade que possa ser explorada por uma ameaça; no caso, o *cybercriminoso*.

2. TIPICIDADE E INVASÃO DE DISPOSITIVO INFORMÁTICO

O Código Penal brasileiro tipifica o crime de invasão de dispositivo informático em seu art. 154-A:

> 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:
>
> Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.

O legislador pátrio tipificou uma conduta que a ciência penal construiu e a denominou de *cybercrime*. Esse termo designa o conjunto de condutas relativas ao acesso, apropriação, intercâmbio e disposição de informação e dados em redes telemáticas, que as constituem, cometidas sem o consentimento e autorização do titular do dispositivo (HERNANDEZ DÍEZ, 2009, p. 236). A segurança informática, que é o bem jurídico tutelado nesse tipo, é um valor que se refere ao sistema informático enquanto dado ontológico, cuja proteção evita a lesão de uma série de bens jurídicos individuais (patrimônio, dignidade sexual, honra, dentre outros), que são postos em perigo com as condutas atentatórias à segurança das redes e sistemas informáticos (CARRASCO ANDRINO, 2009, p. 344).[6] A moldura típica apresenta duas condutas nucleares, cujos núcleos tratam da *invasão* e da *instalação*. A invasão é realizada com a penetração no sistema informático, através da superação dos obstáculos oferecidos pelos mecanismos de segurança

[6] No Brasil, já se defendeu que o bem jurídico protegido é a liberdade individual, sobretudo em face da topografia do art. 154-A no Código, vez que está situado na parte da lei penal que faz referência aos crimes contra a liberdade individual. Veja-se, por exemplo: "O bem jurídico tutelado é a liberdade individual, tendo em vista estar o dispositivo inserido no Código Penal Brasileiro, no capítulo que trata dos 'crimes contra a liberdade individual' (artigos 146 a 154, CP), mais precisamente, na Seção IV, intitulada 'dos crimes contra a inviolabilidade dos segredos' (artigos 153 a 154-B, CP)". (ELIEZER; GARCIA, 2015, p. 71). Entretanto, tenha-se em conta que o tipo, acrescentado ao Código Penal pela Lei 12.737, de 2012, é dos crimes que atingem o sistema informático enquanto valor, não se tratando da utilização daquele sistema para a prática de delitos contra bens jurídicos individuais, conforme construção da Ciência Penal, sobretudo após a Convenção de Budapeste, de 2002, que traçou as linhas mestras desse delito no âmbito da dogmática penal.

daquele sistema. A quebra dos mecanismos de segurança é o evento decorrente da ação do sujeito ativo do crime; tal quebra é o meio para a conquista do acesso aos dados do sistema informático. A invasão, que conferirá o acesso não autorizado, poderá se dar através da quebra de um ou de múltiplos obstáculos, tais como senhas, programas de segurança operacional, programas de bloqueios de IP, antivírus, dentre outros. O crime é material, porquanto apresenta um resultado, produto do sucesso da conduta do sujeito ativo e distinto, no plano lógico, da sua ação. No plano subjetivo, essa modalidade típica para além do ***dolo de invadir***, exige um elemento subjetivo especial, que é a finalidade de obtenção, adulteração ou destruição de dados ou informações em decorrência da invasão do dispositivo informático. Isso, posto, a pura vontade de invadir o dispositivo informático dissociado do especial fim estabelecido na moldura típica, à luz do Princípio da Legalidade, será um fato atípico, por ausência de tipicidade subjetiva. A estrutura do art. 154-A, em comento, traz, por fim, um elemento normativo, que é a ausência de consentimento para a invasão, traduzido na expressão: ***sem autorização expressa ou tácita do titular do dispositivo***. O consentimento para a violação será, portanto, causa de atipicidade e o erro do sujeito ativo sobre o referido consentimento será consubstanciado em ***erro de tipo*** (art. 20 do Código Penal), excluindo o dolo.

A segunda modalidade típica é a instalação de vulnerabilidades para a obtenção de vantagens ilícitas. Instalar significa inserir algo no equipamento eletrônico, acarretando no sistema um acréscimo que fragiliza a segurança do dispositivo. Nesse contexto: "Instalar vulnerabilidade tem o sentido de estabelecer brecha que permita a invasão indevida ao dispositivo informático, necessitando-se, no entanto, que o agente vise a obter vantagem ilícita, o que não implica, necessariamente, vantagem econômica" (Scarmanhã; FURLAN NETO; SANTOS, 2014, p. 242). O tipo subjetivo é doloso, consistente na vontade livre e consciente de inserir a vulnerabilidade no sistema informático, acompanhada do especial fim de obtenção de vantagem não autorizada pelo direito.

No art. 154-A, como o objeto material é único e há a proibição do ***bis in*** idem, há um tipo misto alternativo, porquanto a concorrência dos dois núcleos no mesmo curso causal será tratada como crime único.

3 O TESTE DE INVASÃO DE SISTEMAS INFORMÁTICOS

Diante da crescente ameaça dos ataques cibernéticos[7], cuja incidência tem sido ampliada diante da sua "comoditização"[8], empresas e indivíduos de todo o mundo têm discutido estratégias para impedir que haja novas vítimas de ilícitos cibernéticos dos mais diversos gêneros.

O tradicional relatório anual de investigações de vazamento de dados,[9] realizado pela conceituada sociedade empresária norte-americana ***Verizon***, apresenta, em sua edição de 2018, índices alarmantes

[7] Upside TDWI. *Growth of cyberattacks explored in new report*. Disponível em: <https://upside.tdwi.org/articles/2017/01/13/growth-of-cyberattacks-report.aspx>. Acesso em: 28 jun. 19.

[8] IBM SECURITY INTELLIGENCE. *Cybercrime has become a commodity*. Disponível em: <https://securityintelligence.com/cybercrime-has-become-a-commodity>. Acesso em: 28 jun. 19.

[9] Verizon. 2018. *Data breach investigations report*. Disponível em: <https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf>. Acesso em: 04 ago. 18.

relativos a incidentes de vazamentos de dados em todo o mundo. Com índice de mais de 53.000 incidentes e 2.216 vazamentos de dados confirmados (2018, p. 4), algumas das estatísticas encontradas revelam que em 28% dos incidentes houve envolvimento de "atores internos" das corporações, 50% dos vazamentos foram organizados e realizados por organizações criminosas, 12% dos vazamentos envolveram agentes identificados como afiliados à atuação estatal (estrangeira ou não) e 68% dos vazamentos levaram meses para serem descobertos (2018, p. 5).

Tal crescimento exponencial de ameaças fez com que a União Europeia discutisse um marco legal para prevenção a vazamento de dados pessoais, a chamada GDPR (***General Data Protection Regulation***), aprovada em 14 de abril de 2016 após 4 anos de preparação e debate.[10] A vigência da GDPR europeia a partir de 25 de maio de 2018 fez com que o projeto de lei geral de proteção de dados pessoais brasileiro fosse sancionado[11] através da publicação da Lei 13.709/2018, alterada pela Lei 13.853/2019, de maneira que os legisladores brasileiros também se mostram preocupados com o problema que já existe em escala global.

Um vazamento de dados, que é um dos vários incidentes possíveis relacionados à segurança da informação, se dá através de várias possibilidades técnicas. ***Hacking***, ***malware***, ataques sociais ou engenharia social, má utilização de privilégios e até mesmo erros e eventos casuais são algumas das táticas utilizadas para se obter informações privilegiadas (VERIZON, 2018, p. 5). Nítida é a necessidade de investimento em prevenção através de ferramentas (software, ***appliances***, etc), analistas de segurança da informação, consultoria especializada, treinamento e educação para os usuários dos recursos informáticos.

Porém, tais investimentos não são a garantia de uma operação livre de riscos, vulnerabilidades e, em última instância, incidentes de segurança da informação. Faz-se necessário realizar testes programados e não programados, com o objetivo de validar se a operação corporativa se encontra realmente protegida pelos mecanismos, software e procedimentos adotados com essa intenção.

Invariavelmente os procedimentos de testes envolvem a simulação do problema que se quer evitar. No mercado automotivo, como exemplo, para se testar a segurança de um automóvel quanto à proteção de seus ocupantes em caso de colisão, submete-se um automóvel padrão da montadora a rigorosos testes que simulam tais colisões, às quais estão sujeitos esses veículos quando estão em operação. De tal maneira, a indústria da tecnologia da informação possui testes para encontrar vulnerabilidades em dispositivos, procedimentos e software. Tais testes são comumente conhecidos como testes de vulnerabilidade ou testes de invasão (***Penetration Tests*** ou ***PenTests***).

Matt Walker define o termo ***hacking*** como:

[10] EUGDPR Portal. **GDPR Portal: Site Overview**. Disponível em: <https://www.eugdpr.org/>. Acesso em: 28 jun. 19. [VER COMENTÁRIO SOBRE ESTA REFERÊNCIA NA LISTA DE REFERÊNCIAS]

[11] Senado Notícias. *Sancionada com vetos lei geral de proteção de dados pessoais*. Disponível em: <https://www12.senado.leg.br/noticias/materias/2018/08/15/sancionada-com-vetos-lei-geral-de-protecao-de-dados-pessoais>. Acesso em: 17 abr. 2019.

> "Seja para nobres ou maus propósitos, a arte de hacking permanece a mesma. Usar um conjunto especializado de ferramentas, técnicas, conhecimento e habilidades para ultrapassar medidas de segurança computacional permite que alguém "hackeie" um computador ou rede. O propósito por trás do uso dessas ferramentas e técnicas é realmente a única coisa em questão. Enquanto alguns usam essas ferramentas e técnicas para ganho pessoal ou lucro, os caras bons as praticam para melhor defenderem seus sistemas e, no processo, fornecerem uma visão de como capturar os caras maus." (WALKER, 2014, p.18, tradução livre).[12]

É importante notar, portanto, que tais testes utilizam as mesmas ferramentas, técnicas e habilidades que são utilizadas pelos *cybercriminosos* para a obtenção de vantagens de maneira ilícita. Seus fins, porém, são de obter informações sobre a segurança de seu ambiente computacional e, se possível, identificar os agentes criminosos que iniciam ou facilitam os ataques cibernéticos.

Uma sociedade empresária que possui seus segredos industriais expostos provavelmente amargará enormes prejuízos, uma vez que seus investimentos em pesquisa e desenvolvimento foram obtidos sem custos significativos pelo *cybercriminoso*. Uma prefeitura que tiver os registros de pagamentos de IPTU adulterados em seu sistema encontrará sérios problemas perante seus contribuintes. Um escritório de advocacia que tiver as informações de seus clientes (elementos de prova, documentos, etc) destruídas se encontrará em situação extremamente delicada perante a defesa dos "bens da vida" dessas pessoas.

CONCLUSÃO

O tipo penal contido no art. 154-A, como dito, possui um elemento normativo: ***sem autorização expressa ou tácita do titular do dispositivo***. Se é verdade que o Direito Penal brasileiro admite o consentimento do ofendido, para os casos nos quais se possa dispor de uma causa supralegal de exclusão de ilicitude (BRANDÃO, 2015, p. 97), aqui teremos, como o consentimento para os testes de invasão, uma causa de atipicidade da conduta. O legislador quis incluir no próprio texto normativo um elemento que só torna típico o comportamento se presente o dissenso. Os testes de invasão, apesar de serem condutas que se amoldam ao tipo objetivo descrito no art. 154-A, não completarão a moldura em função da ausência daquele elemento normativo.

Ademais, note-se que os testes de invasão, portanto, justificam-se em uma política de segurança da informação bem construída e que siga uma padronização internacional de boas práticas, como a família de padrões ISO 27000. Seu objetivo é avaliar as medidas de segurança existentes, sua efetividade e adequação, além de indicar a ausência de outras medidas que deveriam ser colocadas em prática, mas que, por alguma razão (custo de aquisição, falta de pessoal adequado para operação, falta de treinamento ou seu puro e simples desconhecimento), não se encontram implementadas.

[12] Whether for noble or bad purposes, the art of hacking remains the same. Using a specialized set of tools, techniques, knowledge, and skills to bypass computer security measures allows for someone do "hack" into a computer or network. The purpose behind their use of these tools and techniques is really the only thing in question. Whereas some use these tools and techniques for personal gain or profit, the good guys practice them in order to better defend their systems and, in the process, provide insight on how to catch the bad guys.

Referências

BRANDÃO, Cláudio. *Teoria jurídica do crime*. 4. ed. São Paulo: Atlas, 2015.

CARRASCO ANDRINO, Marial del Mar. El acceso ilícito a un sistema informático. *In*: ÁLVAREZ GARCIA, Francisco et al (coord.). *La adecuación del derecho penal español al ordenamiento de la Unión Europea*: la política criminal europea. Valencia: Tirant lo blanch, 2009.

CAZELATTO, Caio Eduardo Costa; SEGATTO, Antonio Carlos. Dos crimes informáticos sob a ótica do ambiente digital constitucionalizado e da segurança da informação. *Revista Jurídica Cesumar*, v. 14, n. 2, 2014.

CHAWKI, Mohamed et al. *Cybercrime, digital forensics and jurisdiction*. EUA: Springer, 2015.

D'ÁVILA, Fabio Roberto; SANTOS, Daniel Leonhardt. Direito penal e criminalidade informática: breves aproximações dogmáticas. *Duc in Altum – Cadernos de Direito*, *Faculdade Damas*, Recife, v. 8, n.15, 2016.

ELIEZER, Cristina; GARCIA, Tonyel. O novo crime de invasão de dispositivo informático. *Revista do Curso de Direito do UNIFOR*, v. 5, n. 1, 2014.

EUGDPR Portal. GDPR Portal: Site Overview. Disponível em: <https://www.eugdpr.org/>. Acesso em: 28 jun. 19.

HERNÁNDEZ DÍAZ, Leyre. El delito informático. *E-Eguzkilore*, San Sebastián: Universidade del País Vasco, n. 23, 2009.

IBM SECURITY INTELLIGENCE. *Cybercrime has become a commodity*. Disponível em: <https://securityintelligence.com/cybercrime-has-become-a-commodity>. Acesso em: 28 jun. 19.

PEW RESEARCH CENTER. *Millennials overtake baby boomers as America's largest generation*. Disponível em: < http://www.pewresearch.org/fact-tank/2016/04/25/millennials-overtake-baby-boomers>. Acesso em: 28 jun. 2019.

Scarmanhã , Bruna de Oliveira da Silva Guesso; FURLAN NETO, Mário; SANTOS, José Eduardo Lourenço dos. Invasão de dispositivo informático: aporte com a legislação espanhola. *Em Tempo*, Marília: UNIMAR, v. 13, 2014.

SILVA, Ricardo. Delito virtual: um diálogo sobre as transgressões online do mundo real. DELICTAE: Revista de Estudos Interdisciplinares sobre o Delito, v. 3, n. 4, 2018. Disponível em: <http://www.delictae.com.br/index.php/revista/article/view/68>. Acesso em: 1 jul. 2019. <doi: https://doi.org/10.24861/2526-5180.v3i4.68>.

SPEND MATTERS. *How millennials are driving technology adoption*. Disponível em: <http://spendmatters.com/2016/06/27/how-millennials-are-driving-technology-adoption>. Acesso em: 28 jun. 2019.

THE CENTER FOR GENERATIONAL KINETICS. *Generational breakdown*: Info about all of the generations. Disponível em: <http://genhq.com/faq-info-about-generations>. Acesso em: 28 jun. 2019.

Upside TDWI. *Growth of cyberattacks explored in new report*. Disponível em: <https://upside.tdwi.org/articles/2017/01/13/growth-of-cyberattacks-report.aspx>. Acesso em: 28 jun. 19

VERIZON, 2018. *Data breach investigations report*. 11. ed. Estados Unidos: Verizon, 2018.

WALKER, Matt. *All-in-one CEH – Certified Ethical Hacker*. 2. ed. EUA: McGraw Hill Education, 2014.