INTRODUÇÃO

Trata-se de análise preliminar sobre a Lei nº 12.737/12, conhecida extraoficialmente como Lei Carolina Dieckmann, que veio acrescentar ao Código Penal, dispositivos legais que tipificam delitos cibernéticos. Longe de exaurir a matéria em tela, abordarei aqui as primeiras impressões que tive diante dessa novidade legal. Digo novidade, pois havia uma lacuna na legislação que permitia a impunidade das condutas indesejadas praticadas tanto no ambiente virtual quanto no físico em relação à proteção de dados e informações pessoais ou corporativas. A referida lei representa um avanço considerável na garantia da segurança de dados.

Acrescentou-se ao Código Penal os artigos 154-A a 154B, situados dentro dos crimes contra a liberdade individual, seção referente aos crimes contra a inviolabilidade dos segredos profissionais, entretanto as novas tipificações são colocadas como delito e não como crime. A diferença básica é que delito (adeliquendo) se refere às transgressões legais de natureza leve, essa definição vem desde a Idade Média, as escolas clássicas francesas admitiam a divisão tripartite em que crime é transgressão legal de natureza grave, delito é a transgressão legal de natureza leve e contravenção tem natureza levíssima (PESSINA, 2006).

Toda legislação penal precisa atender ao princípio da legalidade (CF Art. 5º, XXXIX), para tanto, a lei precisa ser clara, taxativa, escrita e certa (TOLEDO, 2001). Esta lei vem tutelar o bem jurídico da liberdade individual, do direito ao sigilo pessoal e profissional, dado a sua importância para o convívio social. Carolina Dieckmann foi apenas uma das inúmeras vítimas de invasão de dispositivos de informática, o fato de ser uma pessoa pública, deu maior visibilidade a este antigo problema, mas os relatos de abusos no ambiente cibernético são inúmeros e variados.

A invasão de computadores e dispositivos similares, com finalidades ilícitas, tem causados sérios prejuízos aos direitos individuais e profissionais. A invasão em si, independente do que se siga após ela, já representa um perigo concreto à privacidade e ao segredo juridicamente protegido. Dessa forma, a prova da invasão já serva para promover a ação contra o agente.

1. Invasão de dispositivo informático

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.

A fim de proteger o direito ao sigilo de dado e informação pessoal ou profissional, o art. 154-A veio tipificar duas condutas: a principal é invadir dispositivo

informático e a acessória é instalar vulnerabilidade. Podem ocorrer na forma simples (com a aplicação da pena básica) ou qualificada (com o agravamento da pena).

O agente ativo dessa conduta pode ser uma pessoa física ou jurídica. Apesar de a lei não tratar essa matéria de forma especial, pois em nosso entender, deve haver uma legislação especial sobre o assunto, acreditamos ser esta uma espécie de crime próprio, pois para o cometimento de crimes eletrônicos, cibernéticos, exige-se do agente ativo que tenha certa habilidade no campo da informática, por mínima que seja, por isso esse não é um crime comum. Não é qualquer pessoa que o pratica, o chamado “analfabeto digital”, aquele que não tem contato algum com aparelhos eletrônicos. Sem conhecimento técnico, mesmo que seja o simples fato de saber ligar e desligar um dispositivo informático, a conduta se torna impossível.

O agente passivo é o proprietário do aparelho. Também poderá ser pessoa física ou jurídica. A administração pública também pode figurar como agente passivo. Não esquecendo que a sociedade será sempre a vítima permanente dessas condutas, portanto o Estado estará sempre presente como agente passivo, já que ele é o titular do direito de punir (jus puniendi).

O objeto material do crime é o dado ou informação obtidos de forma ilícita, já o objeto jurídico, o bem tutelado, pode ser vários a depender da finalidade da conduta: no caso de o agente invadir para obter dados bancários e com eles furtar conta bancária, a proteção legal está sobre o sigilo e posteriormente sobre a propriedade. Este é o caso de delito pluriofensivo pois a invasão pode ofender mais de um bem jurídico: a lei protege o direito ao sigilo e a propriedade (material ou imaterial).

É preciso compreender que “dispositivo informático” é termo genérico para designar equipamentos eletrônicos que integram Hardware (equipamento físico) e Software (equipamento lógico). Nesse sentido, uma gama de dispositivos pode ser abarcados por esta lei, não se limitando ao PC ou notebook.

O verbo desse artigo é “invadir” dispositivo informático alheio, trata-se da conduta do agente. É uma conduta tipicamente dolosa, pois a ação de invadir depende da vontade, da determinação consciente e livre do agente. A invasão é só o meio pelo qual o agente se serve para tirar proveito. Fica evidente que quando alguém possui a capacidade técnica para invadir um sistema de informática, ele quer o resultado (Art. 18, I, CP). Quem invade um sistema ou instala uma vulnerabilidade, sabe exatamente do resultado que quer obter.

Invadir pressupõe a utilização de força, artimanha, violação indevido de mecanismo de segurança, desrespeito à vontade do proprietário do equipamento, ultrapassar o limite de autorização fornecida pelo titular do equipamento. É o tipo comissivo, em que o agente realiza a conduta proibida. Imagine uma situação em que você encosta a porta de sua casa, quem chega, não deve ir entrando só porque você não passou a fechadura, a violação do lar se configura do mesmo jeito. Se a lei não for interpretada dessa forma, ela perde

o sentido de existir. O fato de se colocar uma placa “APENAS PESSOA AUTORIZADA” ou “CONFIDENCIAL” já deve ser considerado como mecanismo de segurança. Não precisa colocar cadeado ou esconder num cofre para tipificar a invasão ou violação do sigilo.

Se não houver nenhuma forma de resistência, a invasão não pode ser caracterizada. Perceba que o delito em tela é a invasão ou instalação de vulnerabilidade, o que se faz após ela não interessa, pois a invasão já consuma o delito.

O resultado normativo da invasão poderá ser o de obter, adulterar ou destruir dados ou informações. Podem surgir resultados naturalísticos, aqueles que permeiam o mundo físico, como foi o caso da divulgação de fotos íntimas da atriz Carolina Dieckmann, pois feriu a honra, a dignidade, a liberdade pessoal da vítima, mas sua existência não é exigível na consumação do fato, mas o caráter formal do tipo independe do resultado, a consumação do delito se dá com a mera invasão, o resultado da invasão pode determinar a qualificação do tipo e o mero exaurimento da conduta delitiva.

Admite-se a tentativa do crime de invasão? Pensamos que sim. A invasão pode ser interrompida por inúmeros motivos alheios à vontade do agente. Entretanto, a tentativa não é uma conduta punível, mas pode ocorrer por que a invasão de um “dispositivo informático” se faz mediante preparação. Há um iter criminis, isto é, um caminho para se chegar ao resultado. É preciso obter a máquina ou conseguir os meios para acessá-la de forma remota, se valer de programas ou equipamentos, ferramentas que possibilitem o acesso. Há várias formas de acessar os arquivos de um Disco Rígido (HD): pode ser pela própria maquina, pode-se extrair o HD e instalá-lo em outra máquina, pode se acessar o HD a distância e até controla-lo, pode-se instalar um software espião que copia os dados e os envia para uma máquina remota ou um dispositivo móvel, é possível, inclusive, utilizando tecnologias e equipamentos específicos e avançados, extrair dados de um disco que foi parcialmente destruído, quebrado, queimado, molhado ou sofreu outras formas de danos físicos ou virtuais.

Quanto a conduta de instalar vulnerabilidade, o resultado previsto é a própria vulnerabilidade do equipamento, que pode ensejar a ocorrência dos resultados anteriores (obter, adulterar ou destruir dados ou informações). A conduta de instalar é acessória à invasão, já que aquela depende desta para ocorrer, os resultados são compartilhados, portanto.

Importante salientar aqui que o nexo causal, aquilo que liga a conduta ao resultado, neste sentido opera de forma dependente. Atendendo à teoria conditio sine quae non, sem a invasão do sistema é impossível obter, adulterar, destruir dado ou informação contida no “dispositivo informático” ou instalar vulnerabilidade.

O ato de se apoderar de dados ou informações de um “dispositivo informático” público, de uso compartilhado em ambiente de trabalho ou escolar, de livre acesso, desprovido de mecanismo de segurança não parece ser abarcado no

tipo penal, já que não ocorre o verbo “invadir”, o mesmo não pode se dizer da utilização indevida dos dados ou informações obtidos.

A violação por si só não dá substância para a ocorrência do tipo “invasão”. A violação deve ser indevida. Sugere aqui o legislador que haja casos de violação devida ou necessária. A ordem judicial é uma das exceções que torna a violação um mal necessário. A violação com a finalidade de manutenção e reparo do equipamento não pode ser alvo de penalização; a violação com finalidade de teste efetuada por empresa ou pessoa especializada em Tecnologia da Informação não deve caracterizar delito.

A invasão pode se dar por meio eletrônico, com uso da rede mundial de computadores e programas ou dispositivos que permitam o acesso remoto ao dispositivo informático ou por meio físico, isto é, quando o agente tem acesso direto ao equipamento.

O termo “mecanismo de segurança” deve ser entendido de forma ampla, pois de outra forma tornaria a lei sem eficácia já que nem sempre o titular de um dispositivo vai colocar senha, antivírus, firewall (software que protege o computador de determinados ataques virtuais) ou outra tecnologia de segurança. Além disso, se o artigo for tomado ao pé da letra, se torna antagônico: por que o legislador exigiria a violação indevida de mecanismo de segurança e, ao mesmo tempo, a ausência de autorização expressa ou tácita do titular do dispositivo? Se houve violação indevida obviamente não houve autorização, em contrapartida se houver autorização, não há que se falar em violação indevida do mecanismo de segurança.

O próprio artigo já cria um mecanismo de segurança indispensável: a autorização expressa ou tácita do titular do dispositivo, sem ela o dispositivo se quer pode ser tocado quiçá ter seus dados ou informações extraídos para qualquer que seja a finalidade. Se alguém leva seu eletrônico para uma empresa de manutenção e reparo, não tem outra intensão a não ser a de ver o bem em perfeito estado de uso, a violação dessa vontade (mecanismo pessoal de segurança) deve ser equiparada à violação de mecanismo de segurança. É preciso que se entenda que a máquina não vai para manutenção ou reparo sem que haja a necessidade. Muitas vezes o próprio defeito apresentado impede a criação/instalação de qualquer mecanismo de segurança no aparelho, como é o caso da “tela azul”, da ausência de vídeo e outros.

A ausência de um “mecanismo de segurança” não deve isentar o agente de responder dentro dessa qualificação penal, entretanto, a depender do caso, a conduta do agente pode se adequar a outros tipos penais já em voga: constrangimento ilegal, ameaça, violação de correspondência, divulgação de segredo, furto, roubo, extorsão, dano, apropriação indébita, estelionato e etc.

Ainda com relação a violação indevida de mecanismo de segurança, é preciso levar em consideração que o ambiente cibernético contem diversas armadilhas e sofisticadas formas de “invasão” remota dos dispositivos informáticos. Por este motivo, este aspecto legal não pode ser absoluto. O ato inconsciente de clicar

em um link malicioso, por imperícia ou boa fé, e ter seus dados furtados, não pode ser excluído do novo tipo penal.

Observa-se que o dispositivo pode estar ou não conectado à internet. A invasão seja ela por meio da rede, com a utilização de software, seja por meio da quebra de senhas, ou ainda se o dispositivo estiver nas mãos do agente para a finalidade específica de manutenção ou reparo, ou se for objeto de furto ou roubo, pode caracterizar o delito em tela.

Atenta-se também para a finalidade de tal invasão. A invasão deve ter o objetivo de obter, adulterar ou destruir dados ou informações sem a autorização do titular do dispositivo. Nesse caso, o legislado abre exceção para a invasão consentida com a finalidade de recuperar dados, restaurar o sistema, resgatar informações, proceder a manutenção ou reparo do dispositivo.

O consentimento para uma invasão positiva, com finalidade lícita, pode se dar de forma expressa (o que seria preferível) ou tácita. As empresas que prestam serviço na área de manutenção e reparo de “dispositivos informáticos” devem estar atentas para esse aspecto: a prestação do serviço deve se dar por meio de contrato em que as partes autorizam o serviço a ser feito. Em último caso, havendo algum laço de confiança e boa fé entre as partes, o consentimento pode se dar de forma tácita – verbal.

Outro verbo presente nessa tipificação penal e o ato de “instalar” vulnerabilidade. Como já foi dito, a invasão pode até ser consentida com a finalidade lícita, mas se dessa conduta se executar a “instalação” de vulnerabilidade, supondo-se aqui o uso da má fé, o completo desconhecimento do titular do dispositivo, há a caracterização do crime de invasão.

O legislador quis garantir a tutela do dispositivo informático contra a instalação de software malicioso, do tipo capaz de corromper, apagar, copiar, transmitir ou receber dados ou informações. Ataca diretamente a ação de hackers e experts em informática que utilizam seus conhecimentos para fins ilícitos.

2. A penalidade imposta

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

A pena é o castigo imposto ao agente transgressor da lei, aplicada pelo Estado.

A pena de detenção é aplicada mediante o trânsito em julgado da sentença condenatória pela prática do delito. Delito, compreendido nesse artigo como a conduta de médio potencial ofensivo, devido a pena básica.

Observe que a lei fala de “detenção” que é o tipo de penalidade que admite seu cumprimento no regime semiaberto (em caso de reincidência) ou diretamente no regime aberto (em caso de primeira condenação).

O art. 44, § 2º do Código Penal indica que se a pena privativa de liberdade for igual ou inferior a 1 (um) ano, o juiz pode substituir pela pena pecuniária, isto é, pelo pagamento de uma multa.

Há ainda a grande possibilidade da pena privativa de liberdade ser substituída por uma pena alternativa, ou seja, restritiva de direitos. Isso vai ocorrer se o agente for enquadrado nos quesitos do art. 44, I, II, III, do Código Penal, cumulativamente.

3. A pena aplicada aos facilitadores das invasões

O primeiro parágrafo do artigo 154-A, prescreve:

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

Nesse parágrafo, o legislador busca inibir a produção, oferecimento, distribuição, venda ou difusão de equipamentos ou software que tenham o objetivo de permitir a “invasão de dispositivo informático". Não se deve confundir com a atuação das empresas de Tecnologia da Informação que tem finalidade diversa da tipificada no caput do art. 154-A.

A tecnologia não pode ter sua produção obstruída por um artigo de lei mal interpretado. Não se pode culpar o fabricante de armas pelo mau uso delas. Dispositivos e programas de computador são desenvolvidos todos os dias, necessariamente não tem finalidade transgressiva.

Aqui se enquadra a ação de programadores, hackers, que se dedicam a criar e disseminar programas com a finalidade prescrita no caput do artigo em análise.

Divulgar e-mail com link malicioso que direciona a vítima para a instalação de uma vulnerabilidade, é um exemplo dessa tipificação.

4. Casos de aumento de pena

Casos de aumento de pena promovem a qualificação da conduta, isto é, o agravamento da reprimenda em decorrência da maior reprovabilidade do ato delitivo. Foram elencados quatro elementos qualificadores:

4.1 – Se da conduta resultar prejuízo econômico a pena será elevada de um sexto a um terço (§ 2º do Art. 145-A)

O direito brasileiro é praticamente todo voltado para a defesa da propriedade, eis mais uma vez a tutela do interesse econômico. Aqui, a conduta ganha uma importância maior dentro do ordenamento jurídico, visando desencorajar a prática de crimes cibernéticos que tenha como motivação o benefício financeiro ilícito do agente.

O agravamento da pena pelo prejuízo econômico não livra o autor do dever de reparar o dano.

4.2 – Se da conduta resultar 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 a pena será elevada para o nível de reclusão de seis meses a dois anos, multa, ou adequação em crime mais grave (§ 3º do Art. 145-A).

4.3 – Se da conduta houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos aumenta-se a pena de um a dois terços (§ 4º do Art. 145-A).

4.4 – Será aumentada de um terço à metade se for praticada contra (§ 5º do Art. 145-A):

a) Presidente da República, governadores e prefeitos;

b) Presidente do Supremo Tribunal Federal;

c) Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

d) dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

CONCLUSÃO

Ao abordarmos considerações preliminares sobre esse novo tipo penal, consideremos o delito de “invadir dispositivo informático” como tipo penal que visa proteger o sigilo de dado e informação pessoal ou profissional. Analisamos os elementos típicos do crime doloso: conduta, resultado, nexo causal, tipicidade, consumação e tentativa.

Não há pacificação doutrinária dessa legislação, tendo em visa que entrou em vigor esse mês (abril de 2013), portanto levará algum tempo para que haja de fato um debate aprofundado do tema. Entendemos que essa explanação pode ainda ser muito melhorada, mas como trabalho acadêmico, dá-se ao objetivo apenas de instigar o debate.

O novo tipo penal é benéfico na medida em que notamos uma preocupação da sociedade com a segurança e proteção do direito ao sigilo dos dados e informações no âmbito digital. A lei precisa ser aprimorada, principalmente no sentido da clareza e da aplicabilidade.

Por se tratar de crime condicionado à representação da vítima, muitos casos serão omitidos por falta de exercício do direito subjetivo (se o agente passivo for a União, Estados, DF ou Municípios ou contra empresas concessionárias de serviços públicos, a ação é incondicionada) Art. 154-B do CP

Fonte:https://abimaelborges.jusbrasil.com.br/artigos/111823710/lei-carolina-dieckmann-lei-n-12737-12-art-154-a-do-codigo-penal