Livro Marco Civil da Internet é o mais vendido da Saraiva

Nosso livro recém lançado, escrito em coautoria com o Professor Damásio de Jesus, já é referência sobre o tema e o mais vendido na livraria Saraiva. A obra está disponível na versão impressa e também digital. Você pode encontrar o livro em: http://www.saraiva.com.br/marco-civil-da-internet-comentarios-a-lei-n-1296514-7984114.html

Um abraço e até o próximo.

Implicações jurídicas em fraudes no uso do NFC e mobile payments.

O novo Iphone 6 aparentemente tem a funcionalidade NFC (Near Field Communication), que permite que seu IPhone se torne uma carteira "e-wallet", onde dados precisam estar associados a este dispositivo, sendo eles bancários. Basta aproximar o aparelho de um dispositivo e pagar através de uma aplicação que usa a tecnologia. Um operação mobile payment sem intermediários comumente fornecida por bandeiras de cartão de crédito.

O cliente logicamente esta sujeito à perda do equipamento, o que seria sua responsabilidade, mas também está sujeito à

falha nos protocolos, aplicações e códigos maliciosos e erros na aplicação, o que poderá ocasionar o vazamento de seus dados pessoais, roubo de identidade e desfalques financeiros.

Devemos lembrar que pelo Marco Civil da Internet, em seu art. 10, a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

Ainda em relação a proteção dos dados pessoais temos no art. 11 que em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

Por sua vez, as penalidades para os provedores de aplicações que falharem com as regras dos arts. 10 e 11 são graves, senão vejamos:

Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
I – advertência, com indicação de prazo para adoção de medidas corretivas;
II – multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
III – suspensão temporária das atividades que envolvam os atos

previstos no art. 11; ou
IV – proibição de exercício das atividades que envolvam os atos previstos no art. 11.
Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País.

Ademais, bem dispõe o Código de Defesa do Consumidor que:

Art. 6º São direitos básicos do consumidor:
I – a proteção da vida, saúde e segurança contra os riscos provocados por práticas no fornecimento de produtos e serviços considerados perigosos ou nocivos;

Art. 8° Os produtos e serviços colocados no mercado de consumo não acarretarão riscos à saúde ou segurança dos consumidores, exceto os considerados normais e previsíveis em decorrência de sua natureza e fruição, obrigando-se os fornecedores, em qualquer hipótese, a dar as informações necessárias e adequadas a seu respeito.

Lembrando ainda que um produto é considerado defeituoso quando não oferece a segurança que dele legitimamente se espera, levando-se em consideração as circunstâncias relevantes, entre as quais o uso e os riscos que razoavelmente dele se esperam.

Deste modo, o STJ já entendeu (AREsp 121.496) que as ferramentas de controle oferecidas pelo proprietário de site de relacionamento contra a prática de abusos devem ser realmente eficazes. Ao não desenvolvê-las, o provedor assume integralmente o ônus pela má-utilização dos serviços e responde pelos dados causados. Quem provará se tais ferramentas existes ou não e se são ou não eficazes é um perito em informática.

Assim, caberá às empresas que prestam estes serviços a contratação de grupos paralelos para garantir camadas de segurança, bem como prever em seus contratos as questões

envolvendo responsabilidade pelo NFC. Criptografia, custodia segura de chaves, mecanismos fortes de autenticação e outros recursos são bem-vindos e já considerados “estado da técnica”.

Em caso de fraude ou golpe um especialista deverá ser acionado para apurar a responsabilidade do fornecedor do equipamento e da fornecedora da aplicação (ou de ambas). Em alguns casos, a provedora de conexão poderá ser intimada a apresentar dados de invasões ou de terceiros que acessaram indevidamente a aplicação ou o sistema operacional do equipamento de um usuário.

Cada caso é um caso e um perito será chamado para esclarecer se a fraude se deu por falha no serviço ou produto da empresa fornecedora ou por culpa exclusiva do consumidor. Cabe ao fornecedor, sempre, esclarecer o consumidor sobre as questões de segurança envolvendo o uso do NFC. Cabe a consumidores e fornecedores fazerem seu papel, de modo a estarem garantidos em face de futuras e inevitáveis fraudes que surgirão, como a “negação de serviços de pagamento”, “sequestro de smartphones” ou a possibilidade de “ownar um equipamento usando NFC” ou mesmo fazer rodar a “carteira” em um dispositivo diferente, em todos os casos, com significativas perdas financeiras.

Seja como for, vale observação à Lei 12.737, que pune em seu art. 154-A a invasão de dispositivo informático, sendo que a pena pode chegar a dois anos de reclusão e multa se ocorrer 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.

Lei Carolina Dieckmann está valendo: O que muda na Segurança da Informação e quais os impactos na Sociedade?

Entra em vigor no dia 02 de abril de 2013, no Brasil, a Lei Carolina Dieckmann, número 12.737/2012, que tipifica os crimes cibernéticos (crimes informáticos). A Lei, fruto de um casuísmo, em que o inquérito policial relativo a suposta invasão do computador da atriz sequer foi concluído, e nenhuma ação penal intentada (porém os acusados mais que pré-julgados), passa a punir determinados delitos, como a "invasão de dispositivos informáticos", assim dispondo especificamente:

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.

Invadir significa devassar, entrar a força. Esta "invasão" deve se dar em um dispositivo informático, que embora esteja associado a um "hardware" que armazena, trata ou processa informações ou dados, possa ter sua interpretação estendida por autoridades nos casos de invasão de ativos lógicos como um disco virtual, rede social, webmail de um serviço web ou ativos lógicos protegidos que armazenem informações (Embora tais interpretações devam ser freadas pelo principio da legalidade, é o que esperamos.)

Deve-se esclarecer que a invasão, para ser criminosa, deve se

dar sem a autorização expressa ou tácita do titular dos dados ou do dispositivo. Logo, o agente que realiza teste de intrusão “pentest”, não pode ser punido, por não estarem reunidos os elementos do crime. Caberá, no entanto, às empresas de segurança e auditoria, adaptarem seus contratos de serviços e pesquisa neste sentido, prevendo expressamente a exclusão de eventual incidência criminosa nas atividades desenvolvidas.

Já as intrusões em sistemas cujo titular não autorizou, poderão ser consideradas condutas criminosas, desde que comprovado que o agente o fez com o objetivo de obter, adulterar ou destruir dados ou informações ou instalar vulnerabilidade para obtenção de vantagem ilícita.

A questão da finalidade de “obter dados” é também polêmica. Para um grupo de juristas, a “espiada” não seria crime, só se falando em obtenção nos casos de cópia dos dados do dispositivo, ou quando o agente entra na “posse dos dados”. Para outra corrente, o simples acesso a dados (um select na tabela da vítima, por exemplo) já agride o bem jurídico protegido pelo Direito Penal, e demonstra a “intenção em obter dados” eis que já permite ao cracker, em certos casos, se beneficiar das informações, de modo que tal “contato” com os dados estaria inserido no contexto do “obter dados”, previsto no tipo penal.

É o Judiciário quem vai interpretar esta questão, porém ao contrário do que alegam alguns advogados, não é necessário a cópia dos dados para a prática do crime, pois trata-se de crime formal e de perigo abstrato, diga-se, basta a invasão com a “intenção da obtenção dos dados”. Tal fato poderá ser provado por perícia técnica.

O agente que realiza o footprinting (levantamento de informações do alvo) com programas como nmap ou outro scanner, apenas para identificar se o alvo está ativo, as vulnerabilidades do sistema, portas abertas, serviços

desnecessários rodando, sistema operacional, dentre outros, em tese não comete crime, pois atos preparatórios não são puníveis e o agente não chegou a dar início a invasão (ato executório)

Deste modo, quem encontra vulnerabilidade em sistema alheio, mesmo sem autorização para pesquisa, e comunica o administrador, está realizado a "revelação responsável", não podendo incidir nas penas o art. 154-A, agora previsto no Código Penal. Já a prova de conceito, desenvolvida por quem descobre falha em ativo, sem autorização do titular, dependerá da apreciação pericial para se verificar como afetava o dispositivo atingido e qual foi a extensão decorrente da PoC.

É possível também se pensar na invasão tentada, onde o agente chega a executar a invasão, mas é impedido pelo time de resposta a incidentes, equipe de forense, ou IDS (Intrusion Detection System) que detecta o evento em tempo de execução. Caberá ao perito digital avaliar se os códigos executados tinham aptidão técnica para que o agente pudesse ter acesso às informações, manipulá-las ou para "instalar vulnerabilidades"(sic).

O agente que invade sistema, sem autorização, para tão somente demonstrar a insegurança e cooperar para o aprimoramento dos controles, em tese não responde pelo crime. Tal intenção poderá ser demostrada pelas fases da sua conduta (sempre menos ofensiva à empresa ou titular do dispositivo) ou mesmo pela atuação pericial ou depoimentos, no decorrer de eventual inquérito policial ou ação penal.

Outras formas de acesso indevido, onde não ocorre a "invasão", que é conduta comissiva/ativa, podem não se enquadrar no tipo penal. Assim, na engenharia social que faz com que a vitima forneça credenciais de acesso ou mesmo acesse voluntariamente determinado programa que libera o acesso a seu dispositivo, fica eliminada, em tese, a incidência do delito em comento, podendo o agente, diante do caso concreto, responder por

outros delitos do Código Penal, de acordo com a extensão do dano.

Do mesmo modo, o acesso indevido feito por um agente através de protocolo RDP (Remote Desktop Protocol) ou tecnologias como Terminal Service, VNC, PCAnywhere, Logmein, dentre outras, não caracterizam invasão se o serviço de "assistência remota" foi habilitado pelo titular do dispositivo sem qualquer mecanismo de autenticação, o que equivaleria a uma "autorização tácita" do titular do dispositivo para acessos.

No que diz respeito a empresas de pesquisa e segurança da informação, a Lei tenta "imitar" os princípios da convenção de Budapeste, também punindo aquele que produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da invasão. Temos que entender ou "ler", no intuito de permitir a prática da invasão com fins ilícitos, tal como previsto no artigo 154-A (A Convenção do Cibercrime de Budapeste recomenda até mesmo a punição de quem disponibiliza senhas para acesso a ativos de terceiros).

Assim, distribuições Linux como Backtrack, programas para invasão como sqlmap, havij, e frameworks como Metasploit, são amplamente utilizados por profissionais de segurança e empresas na consecução dos seu trabalhos, e não poderão ser confundidos, por autoridades, com por exemplo, códigos para coleta de dados de cartão de crédito, Keyloggers bancários desenvolvidos especificamente para lesar correntistas, dentre outros códigos que por sua natureza e diante do contexto do caso concreto, avaliada por perito digital, restar claro não se tratar de ferramentas usadas para "boas finalidades".

Porém repise-se. Não é a ferramenta que define a finalidade do agente, mas o próprio agente define como usar a ferramenta, para boas ou más finalidades. Infelizmente, o legislador não pensou nesta hipótese. Caberá dose extraordinária de bom-senso às autoridades e observância às conclusões da perícia em geral

para constatar que não é porque alguém é encontrado distribuindo ferramentas que permitem invasão que este alguém é um criminoso.

Para pesquisadores e profissionais que desenvolvem exploits, provas de conceito, códigos, frameworks, ferramentas de pentest, caberá a revisão das políticas de uso e distribuição dos referidos programas, fazendo menção expressa à ausência de responsabilidade do desenvolvedor diante do mau uso, consignando expressamente a finalidade lícita da criação da ferramenta.

Por fim, repise-se que a invasão, para caracterizar conduta criminosa, deve ocorrer em ativo protegido por mecanismo de segurança. Resistimos a simplicidade daqueles que entendem que basta uma senha no dispositivo para que ele esteja "protegido", logo preenchendo os requisitos da lei. Poderemos ter a hipótese de um sistema operacional, por exemplo, Windows, com senha, mas que tem uma vulnerabilidade no navegador nativo (MS11_003 por exemplo). Nestes casos a perícia deverá constatar que a despeito da senha, a máquina estava "desprotegida", com patches desatualizados e que o titular, por sua conta e risco assim mantinha o serviço na rede em um sistema defasado.

Logo, é preciso esclarecer que nem todo o dispositivo "com senha" está com efetivo "mecanismo de segurança" e, consequentemente, nem todo a invasão a dispositivo "com senha", poderá ser considerada conduta criminosa, como muitos pensam. Cada caso é um caso. Por outro lado, a lei também veio para proteger usuários comuns, pessoas físicas, logo, não se pode engessar a aplicabilidade porque tal usuário não empreendeu o "melhor" mecanismo de segurança existente para proteger seu ativo. É preciso repetir, cada caso deverá ter suas características e circunstâncias avaliadas pelo Judiciário, não existindo solução pronta.

Seja como for, a segurança da informação, agora, passa a ser

não apenas útil para impedir que o ato potencialmente criminoso ocorra, garantindo a disponibilidade, integridade e confidencialidade da informação, mas, em caso de invasão consumada, para que o criminoso possa responder criminalmente.

Como visto, a não conformidade em segurança da informação, agora, pode representar claramente a impunidade em casos de invasão, pois não se pode invadir o que está "aberto", por nítida falha, negligência, imprudência ou imperícia dos contratados e que tinham o dever de garantir segurança do ativo de informação de alguém.

***

Para saber mais sobre a Lei 12.737/2012 e impactos na segurança da informação:

***

I Congresso de Direito Digital e Segurança Informática – Primeiro Congresso após a vigência da Lei será realizado em 13/04/2013 – Inscrições gratuitas – Acesse

***

Lei na íntegra: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

***

José Antônio Milagre é Perito e Advogado especializado em Tecnologia da Informação Twitter: http://www.twitter.com/periciadigital E-mail jose.milagre@legaltech.com.br Site: www.legaltech.com.br Face: http://www.facebook.com/josemilagre