HÃ©lio JÃºnior: InvasÃ£o de dispositivo informÃ¡tico nÃ£o Ã© crime impossÃvel

A ausência de definição legal de muitos termos e expressões utilizadas na norma penal certamente será o primeiro grande desafio a ser enfrentado na aplicação da Lei 12.737/12 — conhecida como Lei Carolina Dieckmann —, por haver a necessidade de esclarecer o que se entende por dispositivo informático, mecanismo de segurança, autorização tácita, invasão, vulnerabilidades etc.

Esses obstáculos serão superados com a jurisprudência. Enquanto isso não ocorre, para solucionar essas questões, pondera-se, em relação ao conceito de dispositivo informático para fins penais, que seja possível a sua abrangência aos dispositivos que funcionam por computação em nuvem; no que tange ao mecanismo de segurança, considera-se que o seu conceito não pode ser restrito a apenas algumas formas de proteção, devendo englobar todo mecanismo computacional, desde uma senha ou um antivírus até a tecnologia mais moderna de detecção de intrusões, invasões e ataques cibernéticos.

Também é importante afastar a ideia de que haveria autorização tácita no caso de o titular do dispositivo informático, induzido a erro por engenharia social, acessar dispositivo ou programa de computador que permita o acesso e controle remoto do seu computador, pois a manifestação de vontade nesse caso estará totalmente viciada e comprometida, uma vez que o usuário não pode autorizar algo do qual nem sequer tem conhecimento.

A autorização tácita ocorre na hipótese em que o silêncio importa em anuência, quando as circunstâncias ou os usos o autorizarem, e não for necessária a declaração de vontade expressa, nos termos do artigo 111 do Código Civil. Pode ocorrer, por exemplo, quando há contratação de profissional da segurança da informação para realizar "testes de segurança" na rede de computadores da empresa do titular do dispositivo e, embora não conste no contrato autorização expressa para "invadir" tais computadores, tal anuência seja presumida pela natureza do próprio contrato.

Outro aspecto importante diz respeito ao conceito de invasão, o qual não pode ficar adstrito às hipóteses em que ocorram um "ataque" ao dispositivo informático alheio. Assim, para efeitos penais, deve-se entender que há invasão sempre que alguém tenta violar indevidamente e burlar o mecanismo de segurança do dispositivo informático.

Caso se entenda o contrário, que só há invasão se houver um ataque ao mecanismo de segurança e desde que o hacker invasor consiga obter dados e informações do dispositivo informático, não haverá possibilidade de punição do delito na sua forma tentada. Este não é o intuito da norma penal, uma vez que se trata de crime formal que se consuma independentemente do resultado de o agente obter os dados armazenados.

Desta forma, para fins de consumação do delito, a invasão pode ocorrer mesmo nos casos em que não há "ataque" ao computador, como, por exemplo, quando o invasor induz o titular do dispositivo em erro fazendo acessar algum código malicioso para ter acesso ao computador alheio, porque, nesse caso, o invasor se valeu da engenharia social como artifício fraudulento para burlar o mecanismo de segurança

com o intuito de poder ter acesso aos dados e informações do dispositivo informático invadido.

Assim, o perito forense, ao ser nomeado para verificar a ocorrência da invasão ao dispositivo informático, deverá verificar não só se houve um "ataque" ao computador, mas também se houve violação indevida ou burla a algum mecanismo de segurança, pois o fato de conseguir ultrapassar o mecanismo de segurança mediante o uso de algum artifício fraudulento implica inegavelmente a sua violação, ainda que para isso tenha colaborado a ocorrência de erros humanos ou de falhas de segurança.

Nesse aspecto, enfatiza-se que o tipo penal, embora exija violação indevida ao mecanismo de segurança, não condiciona a tutela penal ao fato de se considerar o titular do dispositivo informático “protegido” ou “desprotegido”, basta apenas que tenha proteção (mecanismo de segurança) e que esta seja violada no caso concreto.

Isso porque ninguém está totalmente protegido na internet, e a lei não estabeleceu nenhum grau de proteção que o mecanismo de segurança deve ter como condição para consumação do delito, mas, cumpre reforçar, exige, a lei, apenas que o dispositivo informático tenha algum mecanismo de segurança e que este seja violado.

Desta forma, entende-se que, se o mecanismo de proteção for um antivírus, embora seja recomendável que este se mantenha atualizado, não faz sentido algum afastar a tipicidade do delito apenas porque a vítima não estava com o seu antivírus atualizado, pois em direito penal não existe compensação de culpas, assim, a culpa concorrente vítima não afasta a tipicidade do crime do artigo 154-A, caput, do Código Penal.

Enfatiza-se que o crime ocorre justamente porque o invasor explora as fragilidades do sistema, mesmo porque, conforme já mencionado, se o mecanismo de segurança do dispositivo informático fosse inviolável, o crime seria impossível.

Nem sempre o conceito jurídico coincidirá com o conceito computacional, porém, em se tratando de aplicação do direito ao caso concreto, deve prevalecer o conceito jurídico, como é o caso do programa de computador que é definido pela própria lei, não sendo necessário que tal conceito seja o mesmo dado pela ciência da computação.

É o que ocorre, por exemplo, em relação ao conceito de “vulnerabilidades”. Uma vez que a norma penal prevê como crime a conduta de instalar vulnerabilidades em dispositivo informático alheio com o fim de obter vantagem ilícita, não seria correto afirmar, exclusivamente sob o ponto de vista computacional, que o delito em questão seria crime impossível, porque as vulnerabilidades seriam bugs (erros ou falhas no sistema) que não foram instaladas pelo invasor e que seriam preexistentes à invasão.

Para efeitos de aplicação da norma penal, as vulnerabilidades devem ser entendidas como qualquer código malicioso capaz de expor a risco a segurança dos dados e das informações armazenadas ou o próprio funcionamento do dispositivo informático, pois a lei penal deve ser interpretada teleologicamente, conforme os princípios jurídicos que lhe são próprios, buscando extrair o seu exato alcance e real significado através da busca da vontade da lei, atendendo à sua finalidade que estáexpressa no artigo 1º da Lei 12.737/12, isto é, a tipificação criminal de delitos informáticos.

Assim, infere-se que poderão ser consideradas como "vulnerabilidades" para fins de aplicação da lei penal, os vírus de computador, trojans, keyloggers dentre outros, pois, por questão de lógica, depreende-se ser esta a finalidade do legislador penal. Em regra, não haverá crime nos casos de instalação de cookies no computador do usuário, pois estes geralmente são "instalados" automaticamente pelo computador quando se acessa a página na internet e embora possam conter dados da navegação e outros fornecidos pelo usuário, os browsers (programas de navegação na internet) costumam fornecer ao internauta a opção de exclusão desses arquivos do computador.

Superando a questão da ausência de falta de definição de conceitos para os novos termos e expressões trazidos pela Lei 12.737/12, observa-se que, em se tratando de delitos informáticos, costuma-se haver o problema da identificação do autor do crime.

A navegação da internet costuma deixar um rastro por meio do qual é possível fazer uma investigação a fim de identificar o criminoso. Assim, é possível descobrir qual é o endereço de IP (Internet Protocol) utilizado pelo agente, para identificar a hora e o local de onde o hacker invasor acessou a internet para praticar o delito.

No Brasil, com a pretensão de se regulamentar o uso da internet, há uma tendência em se exigir dos estabelecimentos comerciais que forneçam serviços de acesso à internet, como as lan houses, que realizam o cadastro dos dados de seus usuários, registrando a data e o horário da navegação, como alternativa para tornar viável a responsabilização penal de quem praticar o delito nesses estabelecimentos.

Em Santa Catarina, a Lei Estadual 14.890/09 disciplina o controle de usuários em estabelecimentos voltados à comercialização do acesso a internet no âmbito estadual, inclusive determinando que os referidos estabelecimentos deverão adotar sistema de monitoramento por câmeras de vigilância, em especial nos acessos aos computadores. O mesmo também já vem ocorrendo em diversos outros estados da federação. Essa lei estadual prevê, em seu artigo 2º, que os estabelecimentos deverão manter o cadastro de usuários pelo prazo de dois anos, contendo informações como o tipo e o número do documento de identidade com foto apresentado, o endereço e o telefone, o equipamento usado, bem como os horários do início e do término de sua utilização e o IP do equipamento usado.

Finalmente, com, a obtenção desses dados, torna-se possível a identificação da autoria do crime, que, associada à constatação da materialidade do delito, com o apoio da perícia forense, faz com que estejam presentes as condições para a instauração de inquérito policial destinado a apurar a responsabilidade criminal do autor do delito de invasão de dispositivo informático, previsto no artigo 154-A do CP.