Lei 12.737/2012 – Carolina Dieckmann para quem não é advogado

A Lei 12.737/2012 também conhecida como Lei Carolina Dieckmann começa a vigorar hoje, 02/04/2013 e dispõe sobre a tipificação penal de delitos informáticos.

Mas o que isso quer dizer?

Não há crime sem tipificação penal, ou seja, sem que esteja previsto como tal em norma penal brasileira, no entanto muitos incidentes que envolvem o ambiente virtual e os recursos tecnológicos de uma forma geral conectados ou não à redes de computadores, se enquadram nas tipificações já existentes, afinal a lei regulamenta nossa conduta, independente do meio e a tecnologia é um deles.

Ocorre que em alguns casos não havia previsão legal, por exemplo, o Estatuto da Criança e do Adolescente teve que ser atualizado, por conta, entre outros motivos, mas também das tecnologias, incluindo no art. 241 situações que foram potencializadas pela tecnologia.

Para nós que lidamos com o assunto no dia a dia, principalmente no ambiente empresarial e corporativo, é comum lidar com tentativas de invasão de sistemas informatizados em busca de informações sigilosas, independente de sua destinação, portanto, seja para concorrência desleal, ou por pura curiosidade, tal fato não era regulamentado pela legislação na esfera penal, tendo as empresas que buscar amparo apenas no âmbito civil.

Portanto, antes da Lei Dieckmann o cracker que fosse identificado durante ou após uma invasão à sistema informático, poderia apenas sofrer consequências civis, que proporcionaria um resultado ou condenação provavelmente na proporção do dano causado. Se não fosse identificado o uso indevido e consequências desse acesso, poderia o cracker sair ileso aos olhos da lei.

Com a vigência da alteração apontada, temos um novo cenário, porquanto a lei inclui a tipificação conforme a seguir:

> *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.*
>
> *§ 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.*
>
> *§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.*
>
> *§ 3º Se da invasão resultar 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:*
>
> *Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.*

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

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

IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."

Acredito que a parte que menciona invadir dispositivo informático alheio, conectado ou não à rede de computadores, fica fácil de entender. Devemos entender por dispositivo informático por qualquer recurso tecnológico seja ele um computador pessoal, seja a rede de uma empresa, seja um *pendrive*, *samrtphone*, *Ipad*, entre outros, mas pode também ser algo imaterial como um banco de dados, ainda que tais dispositivos não estejam conectados à internet. Todos objetivam o mesmo fim, a informação ali contida.

A discussão começa no ponto "*mediante violação indevida de mecanismo de segurança*" alguns colegas entendem que tal mecanismo de segurança deva ser sistema e recursos rígidos de proteção avançada, um conjunto de controles. Eu discordo, a lei estaria deixando de lado, grande parte dos problemas, se assim fosse o pensamento do legislador, pois nem todos e lembro que lidamos com pessoa jurídica e física, tem preparo e condições, técnicas ou ainda que seja financeira, para implementar recursos de ponta.

Ainda que simplório este pensamento, entendo que a proteção por senha, também deva se enquadrar neste tipo penal e cito um exemplo prático, como um usuário doméstico protege sua rede sem fio? Obviamente por senha. Não estou falando do uso indevido da rede sem fio, mas sim da quebra de barreiras, transportando a autenticação necessária de seu assinante, apenas como um exemplo cotidiano.

Não importa se a barreira quebrada era rígida ou não, deve-se considerar o conjunto probatório, incluindo toda a cena do crime, desde a tentativa de acesso, identificação de vulnerabilidades, entre outros.

Ainda que seja considerado negligencia da vítima no caso de uso simplório de senha, esta não deve excluir a culpa do infrator, assim como, quando o dono de uma casa utiliza apenas da fechadura padrão para trancar sua porta. Não é porque ele não faz uso de outros recursos, como cadeados, trancas mais seguras ou mesmo de biometria que sua propriedade e seus bens ali encontrados não gozarão de proteção jurídica.

O mesmo com um automóvel, o carro blindado seria mais seguro, mas uma pequena parte da população pode pagar por este recurso.

"*com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo*" – com este complemento, podemos dizer que não se completa os elementos do tipo caso não seja comprovado o intuito de obter, adulterar ou destruir as informações devendo ainda integrar o elemento a falta de autorização expressa ou tácita.

O problema aqui é provar o seu fim, caso este não tenha se concretizado, ou seja, imaginemos que um cracker invadiu o sistema de uma empresa, mas foi identificado e interrompido quando apenas de seu acesso. Como provar que seu fim era ”de obter, adulterar ou destruir” ?

Ainda assim, imagine que ocorreu uma invasão e não houve nenhum registro de manipulação, seja cópia ou destruição, mas dependendo do tipo de informação, podem ser simplesmente copiadas manualmente ou ainda fotografadas, ambas quando acessadas remotamente sem que seja comprovado o fim a que se destinou a respectiva invasão.

Em alguns casos, poderá a perícia auxiliar na comprovação da intenção do agente, com base por exemplo, nos recursos utilizados.

Embora seja um avanço algumas lacunas terão que ser supridas ao longo do tempo.

O respectivo artigo menciona também “*ou instalar vulnerabilidades para obter vantagem ilícita”* , o que incluiria instalar vulnerabilidades?

O email de engenharia social que engana os usuários para obter vantagem, entendido por muitos como estelionato passaria a ser tratado por este artigo? Ou seja, ao enganar o usuário e instalar um programa malicioso por intermédio de suas ações, ainda que induzido à erro e que permita a sua entrada no computador ou na rede?

O artigo171 CP é mais severo:

> ***Art. 171*** *- Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:*
>
> ***Pena*** *- reclusão, de 1 (um) a 5 (cinco) anos, e multa.*

Por fim, para o que nos interessa neste comentário à lei, resta a questão de quem “ *produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.”*

Portanto, empresas que vendem na internet serviços e recursos para invasão de dispositivos tecnológicos, com o título de que obtenha informações de seu ex chefe, seu ex ou atual cônjuge /namorado(a), amigos, entre outros, estarão em desconformidade com a nova legislação. Já vi muitos anúncios, monitore sua esposa(o), rodando a internet.

Muito cuidado deve ser tomado também com desenvolvedores ou mesmo adolescentes que disponibilizam tais programas em fóruns e debates, pois na internet é difícil dimensionar a extensão de sua intenção, ou seja, como prova valerá o que está escrito.

Mas temos mais uma lacuna nesta lei, pois se o infrator camuflar sua publicação poderá esconder o real intuito de permitir e contribuir com a prática da conduta tipificada, por exemplo, se for criado um fórum com título de discussão para fins didáticos. Este ponto deve ser tratado com muito cuidado e deverá ser levado em conta o conjunto probatório as ações dos envolvidos não apenas nesse fórum, mas de todo rastro encontrado.

Por fim, será preciso muita cautela e preparo por parte das empresas, para que estas possam coletar as provas de forma lícita permitindo seu uso e não repúdio quando necessário apresenta-las em juízo. Segurança da Informação se torna ainda mais um grande aliado das empresas, sejam elas de pequeno, médio ou grande porte.

Para as empresas de Segurança Digital que praticam em seu dia a dia testes de intrusão, levantamento de vulnerabilidades, simulam incidentes, entre outros, também deverão ter seus contratos atualizados com esta nova realidade, para que não sofram consequências desastrosas no futuro. Assim, o trabalho informal deve ser abolido e substituído por contratos bem redigidos e bem estruturados.

O simples teste, desde que não haja contato com as informações ali contidas não caracterizará crime, ainda sim, recomendo previsão expressa em contrato.

Para os usuários e também jovens com sede de mostrar seu conhecimento, orientamos muita atenção, pois responder um processo penal, ainda que não seja condenado, pode ser uma grande dor de cabeça.

Como em nosso ordenamento jurídico podemos ter divergências de opiniões até mesmo entre os magistrados, achei interessante mencionar artigos de outros colegas e recomendo sua leitura:

Carlos Eduardo Miguel Sobral: http://www.emersonwendt.com.br/2013/02/artigo-analise-da-lei-carolina.html

Dr. José Milagre - http://josemilagre.com.br/blog/2013/03/30/lei-carolina-dieckmann-esta-valendo-o-que-muda-na-seguranca-da-informacao-e-quais-os-impactos-na-sociedade/

Walter Capanema - http://waltercapanema.com.br/wordpress/?p=1205

Cristina Sleiman é advogada e pedagoga, mestre em Sistemas Eletrônicos pela Escola Politécnica da USP e com extensão em Direito da Tecnologia pela FGV/RJ, extensão Educador Virtual pelo Senac São Paulo em parceria com Simon Fraser University. Sócia do escritório Cristina Sleiman Sociedade de Advogados, professora de Pós Graduação na Faculdade Impacta de Tecnologia, responsável pela coordenadoria de Prevenção do Risco Eletrônico no Ambiente Corporativo na Comissão de Direito Eletrônico e Crimes de Alta Tecnologia da OAB/SP. Co-autora do audiolivro e livro Direito Digital no Dia a Dia publicado pela Saraiva. www.cristinasleiman.com.br / cristina@sleiman.com.br.