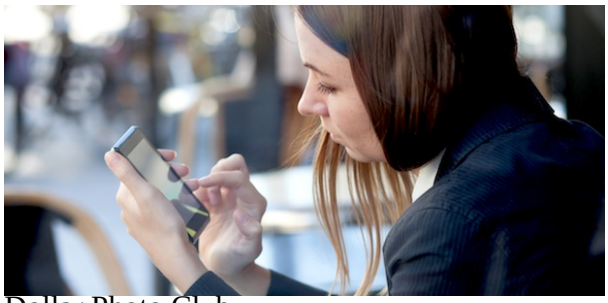
Lei Carolina Dieckmann completa 10 anos com elogio e cautela

A Lei de Combate a Crimes Cibernéticos (nº 12.737/2012), conhecida como Lei Carolina Dieckmann, completa 10 anos de existência neste mês de dezembro. Considerada um marco inicial para a proteção dos dados pessoais dos cidadãos contra os criminosos virtuais, a legislação é vista no meio jurídico como bem-sucedida.

Dollar Photo Club



Dollar Photo ClubDivulgação de dados pessoais e imagens é crime que ainda desafia o meio jurídico

Por outro lado, de acordo com especialistas ouvidos pela revista eletrônica **Consultor Jurídico**, a norma ainda carece de amadurecimento e complementações para que possam ser eliminadas as incertezas decorrentes de várias interpretações de seu texto.

O consenso existente sobre sua importância é grande, tendo como objetivo a necessidade de zelar pela segurança da privacidade *online*. Mas o debate se dá quando a análise se firma sobre o texto da lei, considerado vago e carente de aspectos técnicos.

Apesar dos dispositivos legais sobre crimes cibernéticos elencados na Lei Carolina Dieckmann, o combate à impunidade dentro do meio digital ainda é difícil hoje, devido às diferentes alternativas existentes para garantir o anonimato dos criminosos na internet.

"Entendo que são crimes difíceis de serem combatidos até porque os criminosos se utilizam de meios como a *dark web*, *deep web* e *logo;* o meio virtual é muito difícil de ser controlado. Com o esforço do legislador, pelo menos, já se tem agora tipos penais que podem ser utilizados para coibir os chamados crimes informáticos", afirma **Aldemar Monteiro**, Defensor Público do Estado do Ceará e professor de Direito Penal e Processo Penal.

Mesmo com uma década de vigência, a Lei Carolina Dieckmann ainda apresenta outras brechas que favorecem os criminosos, como por exemplo a incerteza do tipo de dispositivo em que o crime pode ser cometido. Isso deixa margem para diferentes interpretações por parte do Poder Judiciário e do Ministério Público. Até a tipificação da divulgação de conteúdo só ocorreu seis anos depois, com a Lei nº 13.718/18.

De todo modo, analisam os especialistas ouvidos pela **Conjur**, a legislação serve como conduta contra a prática de outros delitos cibernéticos e tem capacidade para resolver uma parte dos problemas, que é a invasão de dispositivos.

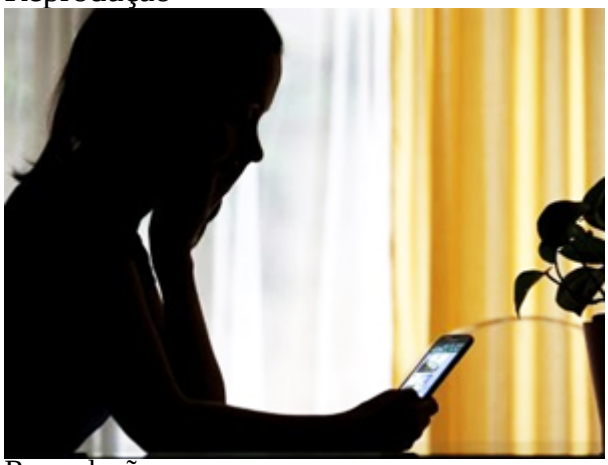
Antes de 2012, a invasão de sistema não era crime. "A lei conhecida como Carolina Dieckmann acrescentou no código penal o artigo 154 A e 154 B e um parágrafo no artigo 266, aquele que interrompe o serviço de utilidade pública. Mas as penas eram muito baixas. Nós tivemos recentemente uma atualização legislativa, com aumento de pena. A nova lei, a 1.455, atualizou os artigos 154 A e a 154 B. Agora temos uma lei efetiva. Antes, ou as penas eram muito pequenas ou o crime prescrevia ou, quando se provava (o crime), o sujeito fazia um acordo e prestava serviços para a comunidade", explica o advogado e professor **Renato Opice Blum**, especialista em Direito Digital e proteção de dados.

"A sua promulgação, assim como outras leis criadas no mesmo período, foi de vital importância para que o Brasil inaugurasse um arcabouço jurídico que possibilitasse a segurança necessária para a expansão da transformação digital da nossa sociedade ocorrida nos últimos dez anos. Assim, a Lei Carolina Dieckmann protege os direitos fundamentais da privacidade e da proteção aos dados pessoais no âmbito penal", entende a advogada especializada em Direito Digital **Elaine Keller.**

***Nudes* divulgados**

Seja motivado por paixões ou pelo desejo de obter vantagem para si ou sobre alguém, o vazamento de imagens íntimas, comumente conhecidas como *nudes*, não deve ser encarado com naturalidade. Pelo contrário, tal ação se caracteriza como uma violência, na qual a intimidade do outro é ferida e suas dores fogem às telas e alcançam a realidade.

Reprodução



Reprodução Até 2012, bisbilhotar dispositivo alheio com finalidade criminosa era 'ato preparatório'

Anteriormente à Lei nº 12.737/2012, o acesso ao dispositivo informático com a finalidade de obter ou destruir dados e informações era considerado apenas atos preparatórios, portanto, impuníveis. Se o agente não exigisse vantagem econômica ou causasse algum prejuízo, não era responsabilizado criminalmente. "Importante ainda ressaltar que, com a referida lei, a falsificação de cartões de créditos ou débitos passou a ser crime de falsificação de documento particular — Art. 298, parágrafo único, do Código Penal", observa Aldemar Monteiro.

Em 2021, a legislação passou por alterações importantes, permitindo a punição ainda que o dispositivo não seja protegido por senha e que o prejudicado não seja o proprietário. Assim, se o usuário do dispositivo tiver dados capturados sem autorização, ocorrerá o crime mesmo que ele não seja o proprietário do mecanismo informático. Outra alteração foi o aumento das penas que também passaram a ser de reclusão, possibilitando, assim, a interceptação das comunicações telemáticas.

Mais estrutura
Apesar dos avanços promovidos pela lei em questão, a punição dos crimes cibernéticos depende não apenas de mudanças legislativas, mas também e, principalmente, de maiores investimentos nos setores de inteligência das polícias, já que estes crimes são praticados por pessoas capacitadas. Essa é a análise do defensor público Aldemar Monteiro, que considera a possibilidade de punição de atos preparatórios, impedindo que a conduta se desenvolva em crimes mais graves como o ponto mais relevante da Lei Carolina Dieckmann.

"Precisamos de mais estrutura por parte dos órgãos policiais, a parte pericial principalmente, e um pouco de velocidade na colaboração das plataformas", sugere Opice Blum.

Correndo atrás
A legislação brasileira, assim como as dos demais países, estará sempre a reboque dos avanços cibernéticos pela dinâmica da tecnologia e porque a fonte do Direito vem sempre das mudanças de cultura e hábitos da sociedade. "Portanto, os avanços cibernéticos serão sempre a engrenagem para o surgimento das novas regulamentações", explica Elaine Keller.

Já para Renato Opice Blum, "a legislação está acompanhando a evolução cibernética. Mas a grande dificuldade continua sendo quando a invasão acontece a partir de ataques externos".

"A eficácia das investigações está ligada ao investimento em tecnologias e capacitação dos agentes públicos", analisa Adelmar Nogueira.

Opice Blum informa que o Brasil acabou de validar, com a assinatura da Convenção de Budapeste junto a 54 países, o protocolo 14/7 de colaboração e transferência do sistema jurídico dos países signatários. A Convenção de Budapeste é do Conselho da Europa e trata-se de um arcabouço que ajuda no combate aos crimes cibernéticos.

Para **Nathália Gabriel, s**ócia da Área Cível na DD&L Associados, do Estado do Amazonas, especialista em Privacidade e Proteção de dados, a alteração dos tipos penais a partir da Lei Carolina Dieckmann promove evolução na legislação de combate aos crimes cibernéticos, como a Lei nº 14.155/2021, que a ltera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal). Tal evolução tornam mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato.

"Em que pese as modificações não tenham sido radicais, aumentou as penas de alguns crimes cibernéticos já existentes, como por exemplo o crime de estelionato contra idoso ou vulnerável, além de modificar a redação original do crime de invasão de dispositivo informático alheio, retirando a frase que especificava que o crime só se consumaria se ocorresse 'mediante violação indevida de mecanismo de segurança'. Deste modo, entende-se que mero acesso não autorizado já é passível de punição", afirma Nathália.

Rafael Braude Canterji, sócio do escritório Silverio Advogados, professor de Direito Penal da PUC-RS e conselheiro federal da OAB analisa que não se pode exigir da legislação em vigência a responsabilidade para resolver ou prevenir as condutas ilegais. "Não podemos incidir no erro de atribuir ao Direito Penal a responsabilidade de resolução ou prevenção de conflitos sociais e condutas desviadas dos comportamentos desejados. Ainda para aqueles que entendam que o propósito é este, sua prática resta dificultada pelos instrumentos tecnológicos da prática do crime", afirma.

Outro advogado do escritório Silverio Advogados, Rodrigo Azevedo, aponta que a Lei Carolina Dieckmann não está sozinha nesse combate aos crimes cibernéticos. "A ela se somam inúmeras outras disposições criminais e civis que podem ser aplicadas ao caso concreto", diz Azevedo ao destacar que a norma é um avanço importante.

A advogada Elaine Keller lembra que o combate aos crimes tipificados pela Lei Carolina Dieckmann, assim como os demais crimes, deve ser realizado através de políticas públicas. "Quando a questão chega ao Judiciário o que será feito é, dentro do devido processo legal, aplicar as sanções cabíveis. Nesse sentido, é papel do Judiciário criar jurisprudência sobre a matéria de modo a dar entendimento a algumas questões que não foram totalmente esclarecidas no texto normativo."

Apesar das dificuldades enfrentadas no setor cibernético como acompanhamento de novas tecnologias e as brechas na legislação vigente, o Brasil avança nesse combate, de acordo com avaliação dos dois especialistas do Silverio Advogados. "Os aperfeiçoamentos estão ocorrendo. O tema é complexo e os casos ocorrem em grande volume, dificultando o combate", diz Rafael Canterji. "O Judiciário vem abraçando as novas tecnologias e, junto com isso, naturalmente o combate aos desvios ocorridos por meio dela", afirma Rodrigo Azevedo.

Hoje, o crime está se digitalizando cada vez mais. O cibercrime, ou crime cibernético, é um negócio robusto. Somente em 2021, de acordo com relatório da Cybersecurity Ventures, os danos provocados por esses crimes chagaram à casa de US$ 6 trilhões em todo mundo. É o equivalente à terceira maior economia mundial, atrás apenas dos Estados Unidos e da China. Especialistas preveem que os custos globais do crime cibernético aumentem 15% ao ano nos próximos cinco anos. Segundo dados de uma empresa da área de segurança cibernética, a Fortinet, no ano passado o Brasil registrou mais de 88,5 bilhões de tentativas de ataques cibernéticos.