PROJETO DE LEI Nº DE 2020

(DO SR. DAVID SOARES)

Define os crimes cibernéticos e dá outras providências.

O CONGRESSO NACIONAL decreta:

Conceitos

Art. 1º.Para efeitos penais, considera-se:

I – "sistema informatizado": computador ou qualquer dispositivo ou conjunto de dispositivos, interligados ou associados, em que um ou mais de um entre eles desenvolve o tratamento automatizado de dados informatizados através da execução de programas de computador, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informatizados armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos;

II – "dados informatizados": qualquer representação de fatos, informações ou conceitos sob forma suscetível de processamento num sistema informatizado, incluindo programas de computador;

III – "provedor de serviços": qualquer entidade, pública ou privada, que faculte aos utilizadores de seus serviços a capacidade de comunicação ou processamento por meio de seu sistema informatizado, bem como qualquer outra entidade que trate ou armazene dados informatizados em nome desse serviço de comunicação ou processamento ou de seus usuários, incluindo servidores de aplicação e de conexão;

IV – “dados de tráfego”: dados informatizados relacionados com uma comunicação efetuada por meio de um sistema informatizado, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo de serviço subjacente;

V – “artefato malicioso”: sistema informatizado, programa ou endereço localizador de acesso a sistema informatizado destinados a permitir acessos não autorizados, fraudes, sabotagens, exploração de vulnerabilidades ou a propagação de si próprio ou de outro artefato malicioso;

VI – “credencial de acesso”: dados informatizados, informações ou características individuais que autorizam o acesso de uma pessoa a um sistema informatizado.

Acesso Indevido

Art. 2º. Acessar, indevidamente, por qualquer meio, direto ou indireto, sistema informatizado:

Pena – reclusão, de um a cinco anos, e multa.

Acesso indevido qualificado

§1º Se do acesso resultar:

I – prejuízo econômico;

II – obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais e industriais, arquivos, senhas, informações ou outros documentos ou dados privados;

III – controle remoto não autorizado do dispositivo acessado:

Pena – reclusão, de dois a cinco anos, e multa.

Causas de aumento de pena

§2º Nas hipóteses do § 1º, aumenta-se a pena de um a dois terços se:

I- houver a divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados, arquivos, senhas ou informações obtidas, se o fato não constituir crime mais grave;

II- o crime é cometido contra a Administração Pública Direta ou Indireta, qualquer um dos Poderes da União, Estado, Distrito Federal ou Município, ou contra empresa concessionária ou permissionária de serviços públicos.

Sabotagem informática

Art. 3º. Interferir sem autorização do titular ou sem permissão legal, de qualquer forma, na funcionalidade de sistema informatizado ou de comunicação de dados informatizados, causando-lhes entrave, impedimento, interrupção ou perturbação grave, ainda, que parcial:

Pena – reclusão, de um a cinco anos, e multa.

Parágrafo único. A pena é aumentada de um a dois terços se o crime é cometido contra a Administração Pública Direta ou Indireta, qualquer um dos Poderes da União, Estado, Distrito Federal ou Município, ou contra empresa concessionária ou permissionária de serviços públicos.

Dano a dados informatizados

Art. 4º. Destruir, danificar, deteriorar, inutilizar, apagar, modificar, suprimir ou, de qualquer outra forma, interferir, sem autorização do titular ou sem permissão legal, dados informatizados, ainda que parcialmente:

Pena – reclusão, de um a cinco anos, e multa.

Parágrafo único. Aumenta-se a pena de um a dois terços se o crime é cometido contra a Administração Pública Direta ou Indireta, qualquer um dos Poderes da União, Estado, Distrito Federal ou Município, ou contra empresa concessionária ou permissionária de serviços públicos.

Fraude Informatizada

Art. 5º. Obter, para si ou para outrem, em prejuízo alheio, vantagem ilícita, mediante a introdução, alteração ou supressão de dados informatizados, ou interferência indevida, por qualquer outra forma, no funcionamento de sistema informatizado:

Pena – reclusão, de um a cinco anos, e multa.

Parágrafo único. A pena aumenta-se de um terço se:

I - o agente se vale da utilização de identidade ou credencial de acesso falsa ou de terceiros para a prática do crime;

II – o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.

Obtenção indevida de credenciais de acesso

Art. 6º. Adquirir, obter ou receber, indevidamente, por qualquer forma, credenciais de acesso a sistema informatizado:

Pena – reclusão, de um a cinco anos, e multa.

Causa de Aumento

§1º Aumenta-se a pena de um a dois terços se:

I- houver a divulgação, comercialização ou transmissão a terceiro, a qualquer título, das credenciais de acesso;

II- o crime é cometido contra a Administração Pública Direta ou Indireta, qualquer um dos Poderes da União, Estado, Distrito Federal ou Município, ou contra empresa concessionária ou permissionária de serviços públicos

Artefato malicioso

Art. 7º. Constitui crime produzir, adquirir, obter, vender, manter, possuir ou por qualquer forma distribuir, sem autorização, artefatos maliciosos destinados à prática de crimes previstos neste Título, cuja pena será a prevista para o crime fim, sem prejuízo da aplicação das regras do concurso material.

Excludente de ilicitude

Parágrafo único. Não são puníveis as condutas descritas no caput quando realizadas para fins de:

I – investigação por agentes públicos no exercício de suas funções;

II - pesquisa acadêmica devidamente documentada e autorizada;

III – testes e verificações autorizadas de vulnerabilidades de sistemas; ou

IV – desenvolvimento, manutenção e investigação autorizadas visando o aperfeiçoamento de sistemas de segurança.

Art. 8º. Revogam-se os artigos 154-A e 154-B do Decreto-Lei no. 2.848, de 7 de dezembro de 1940, Código Penal.

Art. 9º. Esta lei entra em vigor na data da sua publicação.

JUSTIFICAÇÃO

O Brasil ainda não tem tipificação penal em diversas condutas criminais envolvendo crimes cibernéticos o que torna a legislação brasileira em descompasso com grande parte da comunidade mundial. O Brasil precisa acompanhar a evolução legislativa mundial e estar apto a tratar dos delitos que vêm sendo cometidos por meio dos sistemas informatizados e pela internet, muitos dos quais remanescem atípicos, pois além de dependermos de um arcabouço legal condizente com a atual realidade tecnológica, o processamento e a punição de tais delitos está no mais das vezes condicionada à cooperação internacional que é facilitada pela existência de tipos penais compatíveis.

O Projeto de Lei do Senado nº 236, de 2012, que trata da redação do Novo Código Penal está ainda em tramitação, aguardando designação do Relator, mas o relatório final do Anteprojeto de Lei apresentado pelo Relator, Senador Pedro Taques, traz um Título específico sobre os Crimes Cibernéticos.

Considerando ser de suma importância que o Brasil possua o quanto antes legislação apta a permitir que os operadores do direito coíbam as práticas de crimes cibernéticos que grassam, proliferam-se na atualidade, entendemos ser urgente a aprovação prioritária do conteúdo desse Título com relação aos crimes cibernéticos.

Dessa forma, considerando a magnitude da obra do Senado Federal em reformular o Código Penal como um todo e considerando que para tal tarefa certamente será dispendido um longo tempo, destacamos o Título VI do Projeto de Lei do Senado para que seja apreciado por essa Comissão de Ciência e Tecnologia, Comunicação e Informática sobre os Delitos Cibernéticos para que possa discutir desde logo a criação desses tipos penais.

Abaixo, transcrevemos as considerações postas no Relatório do Senador Pedro Taques a fim de subsidiar ao entendimento de Vossas Excelências:

"*Tratemos agora dos crimes cibernéticos (Título VI do Projeto de Código). Embora o CP, em regra, não seja diploma que traga conceitos, no caso de crimes cibernéticos, em razão dos aspectos técnicos envolvidos e o pouco conhecimento popular, entendemos ser essencial o estabelecimento de conceitos básicos, de modo a orientar a posterior interpretação, assim como diligentemente fez a Comissão de Juristas. Um Código não é escrito apenas para os operadores do Direito, mas para a sociedade como um todo. O art. 208 do Projeto traz os mesmos conceitos da Convenção de Budapeste, de 2004. A nossa proposta traz conceitos semelhantes, de modo a facilitar eventuais pedidos de cooperação internacional, mas inclui outros termos e conceitos mais modernos, suprindo lacunas já percebidas e criticadas em países que aderiram à Convenção. No art. 209, pune-se o acesso indevido. Hoje, há artigo semelhante em vigor, introduzido pela Lei nº 12.737, de 2012 (art. 154-A do CP). A redação do Projeto é melhor, porque fala em "acesso" e não em "invasão". Além disso, o art. 154-A exige dolo específico – finalidade de destruir, adulterar ou obter dados ou instalar vulnerabilidade para obter vantagem indevida. O art. 209 não exige essa finalidade. A redação do 203 Projeto exige, contudo, que o sistema informático seja "protegido". Tecnicamente, não faz diferença alguma se o sistema é ou não protegido. O desvalor reside no tipo de acesso, se devido ou indevido. A redação do art. 209 ainda traz o problema da "porta aberta" – o tipo exige que, do acesso, resulte exposição a risco de divulgação. Não sabemos como isso operaria na prática. Sugerimos retirar essa expressão, que pouco agrega. O § 2º foi deslocado de lugar. O § 3º reproduz o § 3º do artigo 154-A em vigor, o qual, oportuno acrescentar, esqueceu de punir também a pessoa que obtém dados privados que não sejam comunicações eletrônicas ou segredos industriais. Por isso, sugerimos a melhor organização do artigo. A sugestão também é de um maior intervalo entre as penas mínimas e máximas, permitindo a melhor adequação e individualização no caso concreto. Os §§ 1º e 2º do art. 153 do CP punem a divulgação de segredos contidos em sistemas de dados e qualificam a conduta se o banco de*

dados for de órgão público. As penas neles trazidas são bem maiores do que as do §§ 4º e 5º do art. 209, que punem aquele que acessa indevidamente e depois divulga as informações obtidas. A sugestão, aqui, é de readequação das penas, de modo que a conduta mais grave (acesso indevido, obtenção mais divulgação) seja punida de forma adequada. Por fim, o § 5º do Projeto (§ 2º na nossa proposta) é melhor do que o § 5º do art. 154-A do CP, que prevê causa de aumento se o crime é praticado contra determinadas pessoas. A proteção da Administração Pública parece ser mais adequada. Deslocamos os arts. 164 e 170 do Projeto para este Capítulo, por melhor adequação do bem jurídico tutelado. Propomos outros dois tipos penais. Primeiro, é necessária a punição da obtenção de credenciais, como senhas e impressões digitais, hoje utilizadas quase como documentos de identificação. Documentos servem para identificar pessoas no mundo real e credenciais no mundo virtual. Isso também é importante no caso mais comum de fraude bancária – atualmente, os e-mails trazem links que redirecionam para páginas falsas de bancos, onde são colhidas as informações a serem usadas posteriormente. Essa situação não é coberta por nenhum artigo (pois não há vírus, não há invasão). Daí a importância de se punir a obtenção, e, em outro artigo, o programador que faz o artefato. 204 Entendemos ser mais adequada e didática a reunião de todas as condutas do programador em um único artigo, com referência secundária aos demais, para evitar repetições. Foi incluída a excludente para evitar a punição de pesquisadores e desenvolvedores que trabalham para a criação de novas tecnologias de segurança e também das empresas que investigam os artefatos para aperfeiçoamento dos sistemas de segurança. Por fim, suprimimos o art. 211 do Projeto, em razão da dificuldade de processamento por ação penal privada. Algumas condutas descritas no Título poderiam gerar milhares de ações individuais, em vários estados da Federação, em razão da difusão dos danos decorrentes da ação criminosa. "

Note-se que desde a integração desta proposta ao Projeto de Lei nº 236, de 2012, já se passou tempo considerável e fatos novos ocorreram no cenário nacional, como os recentes ataques aos sistemas de diversos órgãos do Poder

Público Nacional, trazendo sérios riscos ao bom andamento dos serviços públicos e a sua prestação à população.

Assim, foi feita revisão sobre a proposta anterior para adequar a escala de aplicação das penas, possibilitando a resposta penal adequada à gravidade identificada em cada conduta. Para tanto, as penas máximas de cada delito foram fixadas em 5 anos, inclusive para permitir a utilização das técnicas especiais de investigação, essenciais para elucidar os complexos crimes cibernéticos cometidos com novas e diferentes tecnologias.

Sala de Sessões, em de ,2020

David Soares
(DEM/SP)
Deputado Federa

Deputado David Soares
DEM/SP