



INSTITUTO DOS ADVOGADOS BRASILEIROS

Comissão de Direito Penal

Comissão de Direito Digital

*APROVADO
UNÂNIME*

Referência: Indicação nº 061/2019

Autora: Dra. Fernanda Maibon Sauer

Matéria: Parecer sobre os Projetos de Lei nºs 4.719/2019 e 4.287/2019 - Alteram os artigos 141 e 154-A do Decreto-lei nº 2.848 de 07 de dezembro de 1940 (Código Penal), para alterar a disciplina dos crimes cibernéticos. Agravamento da pena.

Relatora: Dra. Marcia Dinis

Ementa: Crimes Contra a Honra. Rede Mundial de Computadores. Pena em Dobro. Crimes contra a Liberdade Individual. Invasão de Dispositivo. Reclusão. Endurecimento Penal. Propostas que não se adequam à função do Direito Penal. *Ultima ratio*. Necessária rejeição.

I) Retificação da Indicação nº 061/2019:

Inicialmente, cumpre destacar que a presente Indicação nº 061/2019 tem como matéria o “*Protejo Lei nº 4.719/2019 - Iniciativa do Senador Major Olímpio (PSL-SP) - Relatoria: Senador Rodrigo Pacheco – Altera os arts. 141 e 154-A do Decreto-lei nº 2.848 de 7 de dezembro de 1940 (Código Penal), para alterar a disciplina dos crimes cibernéticos. Agravamento da pena. Vista para considerações da Comissão de Direito Penal*”.

No entanto, o referido Projeto de Lei tem por objetivo a alteração do Código Penal Brasileiro para aumento das penas relativas somente ao crime de Invasão de dispositivo informático, previsto no artigo 154-A do referido diploma legal, sem qualquer alusão ao artigo 141 do Código Penal.

Em contrapartida, a íntegra da presente indicação faz referência ao Projeto de Lei nº 4.287/2019, o qual, por sua vez, propõe a alteração dos artigos 141 e 154-A do Código Penal, para alterar a disciplina dos crimes cibernéticos.

Considerando o possível erro material no qual a matéria da presente indicação incorreu, aliado a evidente similitude das proposições legislativas indicadas, esta Relatora entendeu por bem elaborar parecer sobre ambos os Projetos de Lei referidos, conforme fatos e fundamentos a seguir articulados.

II) Relatório:

O Projeto de Lei nº 4.719/2019 é de iniciativa do Senador Major Olímpio (PLS-SP) e de relatoria do Senador Rodrigo Pacheco (DEM), e visa agravar a pena cominada ao crime de invasão de dispositivo informático, previsto no artigo 154-A do Código Penal, ao qual atualmente é atribuída a seguinte sanção:

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: (Incluído pela Lei nº 12.737, de 2012).
Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa (Incluído pela Lei nº 12.737, de 2012).
[...] § 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: (Incluído pela Lei nº 12.737, de 2012).
Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. (Incluído pela Lei nº 12.737, de 2012)

A mencionada proposta legislativa visa tornar a pena de detenção do crime previsto no *caput* do supratranscrito dispositivo legal para reclusão, bem como aumentar a pena-base para 03 (três) anos e pena máxima para 06 (seis) anos.

Na hipótese do parágrafo 3º do artigo 154-A do Código Penal, o Projeto de Lei relatado propõe o aumento da pena para reclusão de 04 (quatro) a 08 (oito) anos.

Desde 27 de agosto de 2019 na Comissão de Constituição, Justiça e Cidadania (Secretaria de apoio à Comissão de Constituição, Justiça e Cidadania) do Senado, o referido Projeto de Lei foi redigido nos seguintes termos:

Art. 1º Esta lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal Brasileiro, para aumentar as penas relativas ao crime de Invasão de dispositivo informático previsto no art. 154-A do referido Decreto-Lei.

Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal Brasileiro passa a vigorar com as seguintes alterações:

“Art. 154-A.

Pena - reclusão, de 3 (três) a 6 (seis) anos, e multa.

[...] § 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: (Incluído pela Lei nº 12.737, de 2012)

Pena - reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a conduta não constitui crime mais grave.”

A justificativa apresentada para embasar a propositura do referido Projeto fundamenta-se na alegada necessidade de alteração do Código Penal como meio eficaz à proteção do direito à privacidade e de dados pessoais disponíveis em meio digital.

Foram citados casos emblemáticos amplamente veiculados pela mídia, como a suposta invasão a dispositivos informáticos de autoridades brasileiras e a invasão do dispositivo eletrônico da atriz Carolina Dieckmann e posterior divulgação de material íntimo encontrado no aparelho, que culminou na elaboração da Lei nº 12.737/2012, como exemplos que demonstrariam a necessidade do endurecimento penal para o aludido crime.

De acordo com o autor do Projeto, Senador Major Olímpio (PLS-SP), o apenamento previsto na legislação para o referido tipo penal seria brando, fazendo-se necessário



garantir a proteção da população com penas mais duras que, em tese, serviriam para intimidar os criminosos de cometerem esse tipo de crime:

JUSTIFICATIVA

Acompanhamos nos últimos dias diversas autoridades brasileiras sendo vítimas de invasão de seus dispositivos informáticos, cujo crime é previsto no art. 154- A do Código Penal Brasileiro.

Tal crime foi devidamente tipificado após diversos brasileiros terem sofrido invasões de suas privacidades e terem sido expostas, o caso mais polêmico à época foi o da atriz Carolina Dieckmann, cujo nome foi emprestado para a Lei nº 12.737 de 2012.

Ocorre que em que pese ter ocorrido a tipificação de tal crime o que se verifica é que o apenamento previsto na legislação vigente se tornou extremamente brando, o que incentiva criminosos a cometerem este tipo de crime.

Tal afirmação pode ser confirmada ao verificar o caso concreto em que criminosos invadiram celulares de diversas autoridades brasileiras, vazando assim informações que seriam de usos particulares e privados dessas pessoas.

Ora, o direito à privacidade do cidadão brasileiro é garantido por lei e aqueles que ferirem tal direito devem responder de forma correspondente ao prejuízo que causaram, o que, infelizmente, não ocorre na legislação atual.

Cumprе lembrar que recentemente o Senado Federal aprovou a Proposta de Emenda à Constituição – PEC nº 17/19 de autoria do senador Eduardo Gomes, que inclui a proteção de dados pessoais, disponíveis em meios digitais, na lista das garantias individuais da nossa Constituição Federal.

Ou seja, já restou reconhecido que a proteção de dados pessoais é um dos direitos fundamentais que devem ser protegidos, assim, é necessário garantir tal proteção com penas mais duras que intimidem os criminosos a cometerem este tipo de crime.

Não nos parece razoável que o delito de furto possua um apenamento previsto de um a quatro anos na sua forma simples, e nas suas formas qualificadas preveja penas que vão até dez anos, inclusive daqueles cometidos com destruição ou rompimento de obstáculos, mediante fraude, destreza e emprego de chave falsa, enquanto o crime de invasão de dispositivo informático prevê uma pena ínfima de três meses a um ano, na sua forma simples, e seis meses a dois anos, na sua forma qualificada.

A invasão de dispositivo de informática, na forma do tipo penal posto, vai além da subtração de um bem móvel, pois viola a própria intimidade e a vida privada, o que exige uma melhor adequação do quantum da pena, de forma que possa trazer resultado efetivo na reprimenda estatal, sendo uma das vias necessárias ao devido combate a esses crimes.

Dessa forma, é necessário que ocorra a alteração em nossa legislação para que o crime de invasão de dispositivos informáticos tenha uma pena equivalente ao dano cometido, o que, infelizmente, não ocorre hoje.

Portanto, peço o apoio dos nobres pares para a aprovação do presente Projeto de Lei. (grifamos)

O Projeto de Lei nº 4.287/2019, por sua vez, é de iniciativa do Senador Lasier Martins (PODEMOS/RS), e visa alterar o parágrafo único do artigo 141 do Código Penal para incluir a aplicação da pena em dobro para as hipóteses de crimes contra a honra praticados por meio da rede mundial de computadores, além de propor o aumento da pena cominada aos crimes previstos no artigo 154-A, *caput*, e § 3º, do mesmo diploma legal.

Atualmente, o Código Penal trata das matérias da seguinte forma:

Art. 141 - As penas cominadas neste Capítulo aumentam-se de um terço, se qualquer dos crimes é cometido:

(...) III - na presença de várias pessoas, ou por meio que facilite a divulgação da calúnia, da difamação ou da injúria. (...)

(...) Parágrafo único - Se o crime é cometido mediante paga ou promessa de recompensa, aplica-se a pena em dobro.

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: (Incluído pela Lei nº 12.737, de 2012).

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa (Incluído pela Lei nº 12.737, de 2012).

(...) § 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: (Incluído pela Lei nº 12.737, de 2012)

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. (Incluído pela Lei nº 12.737, de 2012)

Além de incluir a aplicação da pena em dobro para as hipóteses de crimes contra a honra praticados através da rede mundial de computadores no parágrafo único do artigo 141 do Código Penal, a referida proposição legislativa prevê o agravamento da pena cominada aos crimes previstos no artigo 154-A, *caput*, e § 3º, do mesmo diploma legal para, respectivamente, reclusão de 01 (um) a 04 (quatro) anos e multa, e reclusão de 02 (dois) a 05 (cinco) anos e multa, nos seguintes termos:

"Disposições comuns

Art. 141.

Parágrafo único. Se o crime é cometido mediante paga ou promessa de recompensa, ou através da rede mundial de computadores, aplica-se a pena em dobro." (NR)

"Invasão de dispositivo informático

Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena: reclusão, de 1 (um) a 4 (quatro) anos, e multa

(...) § 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: (Incluído pela Lei nº 12.737, de 2012)

Pena reclusão, de 2 (dois) a 5 (cinco) anos, e multa

A justificativa apresentada para embasar a propositura do mencionado Projeto de Lei se limitou à reprodução de trecho de artigo veiculado em portal jurídico¹, no qual se afirma que a alteração do Código Penal seria medida necessária para proteger o direito à privacidade e a proteção dos dados pessoais disponíveis em meio digital.

De acordo com o autor do Projeto, o apenamento previsto na legislação seria brando, fazendo-se necessária uma punição proporcional aos danos causados à sociedade

¹ Disponível em: <<https://jus.com.br/artigos/66527>>. Acesso em 06.11.2019.

pela prática de tais crimes, como uma forma de controlar a prática destes delitos, nos seguintes termos:

“JUSTIFICATIVA

A presente proposição é amplamente inspirada em trabalho dos Professores ADEMIR GASQUES SANCHES e ANA ELISA DE ANGELO sobre a insuficiência das leis em relação aos crimes cibernéticos no Brasil (disponível em <https://jus.com.br/artigos/66527>).

Segundo os citados autores:

‘A facilidade ao acesso à internet e os preços acessíveis na obtenção de aparelhos computacionais e móveis, faz com que o número de usufruidores do ambiente web cresça de forma intensa, por conseguinte, nas mesmas proporções, surgem os cybercrimes.

Os crimes que ocorrem com maior frequência em nosso país são: crimes contra a honra, divulgação de fotos sem autorização e a pedofilia e pornografia infantil. Os responsáveis pelo cometimento de tais ilícitos não são responsabilizados a proporção de suas condutas. Os sujeitos passivos sofrem consequências que vão além do campo virtual, muitas vezes, atingem sua vida íntima e trazem implicações que poderão perdurar por um longo período.

O Código Penal brasileiro tipifica diversas atuações que se enquadram ao ambiente web, porém, tem penas brandas e não suficientes para coibir a prática destes atos. Há também a lei Carolina Dieckman (Lei 12.737/2012), que modificou o Código Penal e inseriu artigos em seu corpo. Porém, apesar de especificar condutas praticadas na web, traz dúvidas interpretações e punições plácidas aos criminosos. Desta forma, a falta de uma legislação específica ao cyber crime intensifica a ideia de que a internet é uma terra sem lei.

Contudo, é necessária a produção de uma legislação que verse sobre crimes cometidos no ambiente virtual, uma vez que são comuns e trazem a suas vítimas prejuízos reais. A punição proporcional é uma forma de controlar a prática destes delitos, dado que, ao saber que poderá responder de forma penosa, o cracker, ou até mesmo uma pessoa comum, se policiará em seus atos. Desta forma, sabendo dos resultados advindos dos crimes virtuais, deve-se criar uma lei que não mais permita que a internet, melhor e mais ágil forma de comunicação/interação virtual, seja usada de forma prejudicial a seus usuários’.

Além disso, nos últimos tempos ficou evidente que esses crimes têm alcançado níveis de sofisticação e periculosidade consideráveis, que demandam uma responsabilização condizente com os danos causados à sociedade.

Com essas considerações, conclamamos os Nobres Pares à aprovação do presente projeto de lei”.



Frise-se que no mês de agosto de 2019, ambos os Projetos de Lei foram remetidos à CCJ para anexação ao PLS nº 236/2012, que trata da Reforma do Código Penal, e não mais tiveram movimentações.

III) Análise do conteúdo legislativo proposto:

O advento de novas tecnologias de informação culminou em modificações profundas na forma de pensar e se relacionar da sociedade contemporânea. Tal impacto é percebido em todos os espaços, inclusive na leitura do comportamento das instituições do Estado, que passa a considerar o acesso às novas tecnologias um direito dos cidadãos e incorporar ferramentas de inovação nos processos de gestão das funções estatais.

Nesse sentido, a Internet, cujo acesso é cada vez mais democratizado, se apresenta como uma ferramenta capaz de estabelecer conexões em escala global e de promover mudanças sociais, constituindo mais um espaço onde o Direito se faz necessário para, dentre outras coisas, coibir comportamentos legalmente reprováveis no ambiente virtual.

No Brasil, as primeiras normas a tratar da matéria foram as Leis nºs 12.735/2012 e 12.737/2012, que iniciaram a tipificação dos crimes cibernéticos e não foram precedidas de quaisquer legislações de matéria civil, optando desde logo o legislador pelo uso das sanções penais como primeira escolha e não como *ultima ratio*, em manifesta contrariedade ao princípio da intervenção mínima que rege o Direito Penal.

Posteriormente, outros ramos do direito passaram a tratar da matéria por meio da Lei nº 12.965/2014 e o chamado Marco Civil da Internet, que abordam os direitos e deveres dos usuários e protegem os dados pessoais e a privacidade destes. Em agosto de 2018, foi sancionada a Lei nº 13.709, conhecida como Lei Geral de Proteção de Dados Pessoais, que regulamenta o tratamento de dados pessoais por empresas e entrará em vigor em agosto de 2020.

Nota-se que existe uma preocupação em regulamentar o mundo digital por se mostrar como um campo fértil a conflitos, mas é necessário lembrar que os conflitos sociais devem ser preferencialmente solucionados por ramos alheios ao Direito Penal, sobretudo

por força do princípio da intervenção mínima, segundo o qual o processo de criminalização é limitado pela possibilidade de solução dos conflitos por outros meios menos gravosos².

Conforme contextualizado, normas penais foram elaboradas para tipificar crimes cibernéticos sem que antes houvesse a abordagem de tal matéria para tutela de bens jurídicos por outros ramos do direito.

Damásio de Jesus³ aponta para o fato de que, em sua maioria, os criminosos virtuais não praticariam crimes no mundo real, muitos são adolescentes, mas se aproveitam de fatores como a falsa sensação de anonimato, do conhecido despreparo das autoridades investigativas de ilícitos virtuais, e da ignorância dos usuários que muitas vezes cooperam sem saber para o cybercrime. Além disso, de acordo com o jurista, na maior parte dos crimes não há alta tecnologia, mas sim tecnologias de fácil aprendizagem disponíveis inclusive na Internet que podem ensinar e conduzir pessoas a praticarem invasões com certa facilidade.

A educação digital e a sofisticação do aparato de inteligência policial são as principais formas de se caminhar na direção de um espaço digital seguro e controlado nos excessos dos usuários.

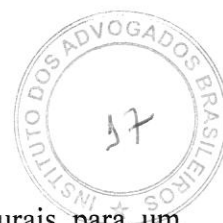
No entanto, a partir das justificativas apresentadas para as propostas de alteração legislativa ora analisadas, verifica-se que o legislador pretende se limitar a recorrer ao endurecimento penal como forma de intimidar possíveis autores de crimes a não praticarem determinadas condutas.

Embora tenha sido importante para o desenvolvimento do direito penal, a concepção de que o crime é unicamente um produto de um processo decisório do indivíduo sob a ótica da racionalidade foi superada, muitas vezes é ineficaz o aumento de penas para intimidar sujeitos com o intuito de diminuir a incidência de crimes. Além disso, ao considerar somente essa vertente para embasar as propostas de alteração legislativa, o legislador ignora que a função da pena não é somente a prevenção especial.

Tal posicionamento decorre da precipitação em apresentar soluções simples, genéricas e de fácil percepção da população para problemas que, em verdade,

² TAVAREZ, Juarez. **Fundamentos de Teoria do delito**. Florianópolis: Tirant to Blanch, 2018.

³ JESUS, Damasio de, MILAGRE, José Antônio. **Manual de crimes informáticos**. 1 ed. São Paulo: Saraiva, 2016.



demandam atenção contínua do Poder Público, com severas mudanças estruturais para um atendimento efetivo de políticas públicas de combate aos crimes cibernéticos.

A resposta estatal por meio de um simplório agravamento da intervenção penal, tornando as leis existentes mais rigorosas e incentivando a centralidade no cárcere, se presta apenas para que o Estado reafirme sua presença e força social perante a sociedade sem que, de fato, resolva os conflitos. Trata-se de manifesta expressão do Direito Penal de Emergência, que acaba por retirar ou restringir direitos e garantias fundamentais como tentativa de dar uma resposta ao populismo penal, que, direcionado pela mídia, insiste em aduzir uma suposta impunidade ocasionada pela alegada branda lei penal brasileira, ao arrepio das verdadeiras diretrizes do Direito Penal, que deve ser reservado como *ultima ratio* do sistema de justiça.

Neste diapasão, a análise sociológica de Marta Rodrigues de Assis Machado e Maíra Rocha Machado⁴ é precisa:

“O uso do termo ‘impunidade’, nessa linha, é perigoso, porque nos leva a dois tipos de redução: fecha a atuação do sistema de justiça na responsabilização individual com atribuição de pena e faz coincidir a ideia de pena com privação de liberdade por longos períodos. Esses diagnósticos partem de uma percepção de que algo está faltando para que possamos melhor lidar com um determinado problema social. E esse algo é sempre a prisão. Ainda que muitas vezes se esteja diante de problemas sérios na atuação do sistema de justiça, o discurso da impunidade nunca coloca em causa a resposta prisional e fecha o espaço para pensarmos sobre a melhor forma de resolver o problema. [...] **Isso tudo evidencia que a limitação do debate a esses termos – crime e pena aflictiva, de preferência prisão – exclui de saída uma série de mecanismos de prevenção potencialmente mais interessantes e eficazes e impede que avancemos na construção de políticas públicas.** E o que é pior: se avançarmos o nosso olhar sociológico para levar em consideração os efeitos da centralidade da prisão no debate sobre prevenção, veremos que seus

⁴ MACHADO, Marta Rodrigues, MACHADO Maíra Rocha. Manual de Sociologia Jurídica: O direito penal é capaz de conter a violência? 1ª ed., pg. 327, São Paulo: Saraiva, 2013.

resultados são ainda mais catastróficos, especialmente se o que se quer é diminuir a violência” (grifou-se - pgs. 344 e 345).

Além disso, os aumentos de pena previstos nos PLs ora analisados implicarão em uma sobrecarga do Poder Judiciário e em um aumento da população prisional. Uma vez que impossibilitarão a tramitação de alguns desses crimes perante os Juizados Especiais Criminais, restringirão a possibilidade de aplicação das medidas despenalizadoras previstas na Lei nº 9.099/1995 e poderão resultar no estabelecimento de um regime de cumprimento de pena mais gravoso e no impedimento da substituição da pena privativa de liberdade por pena restritiva de direitos.

O endurecimento penal e a inerente ideia da centralidade no cárcere vai de encontro à recente jurisprudência do Supremo Tribunal Federal, que nos autos da ADPF nº 347/DF (na qual o IAB participou como *amicus curiae*), declarou o Estado de Coisas Inconstitucional do sistema carcerário brasileiro, no qual se verificou a existência de um quadro de violação generalizada e sistêmica de direitos fundamentais, causado pela inércia e incapacidade reiterada e persistente das autoridades públicas em modificar tal conjuntura.

As ponderações do Supremo Tribunal Federal no bojo da referida ADPF deixaram evidente que o endurecimento penal também encontra obstáculos na superlotação e nas condições precárias e desumanas dos presídios, que não permitem uma política de encarceramento maciço e requerem transformações estruturais da atuação do Poder Público e a atuação de uma pluralidade de autoridades para modificar a situação inconstitucional.

Os pontos expostos acima evidenciam que não houve pesquisa para avaliar a real necessidade, adequação e impacto das propostas de alteração legislativa ora analisadas.

O Poder Público propôs mais uma vez o endurecimento das leis penais como única solução possível para problemas pontuais amplamente divulgados pela mídia, conforme consta nas justificativas dos PLs, em um notório Populismo Penal, sem cogitar a tutela dessas questões por outras esferas do direito, sem considerar que não adianta aumentar penas se as autoridades investigativas não possuem capacidade técnica para identificar os possíveis autores dos crimes e sem avaliar a sobrecarga do Poder Judiciário e o impacto desses aumentos de pena no sistema penitenciário brasileiro, que já conta com um déficit de quase 300 mil vagas.



IV) Conclusão:

Diante do exposto, sugere-se a rejeição das propostas contidas nos Projetos de Lei nºs 4.287/2019 e 4.719/2019, por manifesta afronta aos princípios que regem o Direito Penal, sobretudo o da intervenção mínima, a jurisprudência consolidada do Supremo Tribunal Federal e por não se verificar fundamentos legítimos que justifiquem o endurecimento penal.

Rio de Janeiro, 06 de novembro de 2019.

Marcia Dinis

Instituto dos Advogados Brasileiros

Comissão de Direito Penal

Comissão de Direito Digital

Relatora