Spencer Toth Sydow

CURSO DE DIREITO PENAL INFORMÁTICO

Partes Geral e Especial

4ª edição | revista, aumentada e atualizada de acordo com as Leis 14.133/21, 14.155/21 e 14.197/21, com considerações da Convenção sobre o Cibercrime e Investigação Defensiva

2023

EDITORA JusPODIVM
www.editorajuspodivm.com.br

Desenvolvimentos do Direito Penal Informático

Este capítulo tem por finalidade apresentar de modo mais completo possível os temas de Direito Penal Informático que, ao longo das duas últimas décadas mereceram reflexões mais detidas e que compõem o núcleo material deste ramo do Direito Penal.

Aqui apresentaremos o histórico desse segmento de estudo, as características do Direito Penal Informático que precisam ser compreendidas de modo basilar, a competência legislativa para delitos de tal natureza, a competência jurisdicional, a classificação dos delitos informáticos, e, em seguida, estudaremos os institutos do Direito Penal clássico que, para nós, merecem um novo colorido focado nesta área. Ao final, apresentaremos e analisaremos criticamente os mais relevantes delitos informáticos propriamente ditos.

A rede mundial e a tecnologia mostraram-se uma tendência irrefutável da sociedade. A evolução do novo meio socializante tem cada dia mais adeptos. Certamente, o crescimento de usuários levará a um consequente crescimento de ativos, ou seja, de informações com valor pecuniário direto ou indireto, seja no mercado, seja na criminalidade.

Como aprendemos nos bancos acadêmicos, Ulpiano no *Corpus Iuris Civilis* apresentou um brocardo que mesmo no ramo do Direito Penal é perfeito: "*Ubi homo ibi societas; ubi societas, ibi jus*", ou seja, onde há homem há sociedade e onde há sociedade há Direito. Como as pessoas físicas e jurídicas em sua maioria encontram-se representadas na virtualidade, é possível, sem sombra de dúvidas, dizer que a virtualidade é uma sociedade. E se é uma sociedade, ali há Direito a ser criado, estudado e compreendido.

Ousamos, ainda, acrescer uma complementação que faz com que esse brocardo esteja ainda mais em compasso com a realidade moderna: "*ubi societas, ibi crimen*" ou seja, onde há sociedade, há crime e, portanto, é preciso dentro do estudo do Direito, um estudo específico para as particularidades criminais. Em uma sociedade especial, com delitos especiais, é preciso um estudo especial.

É desiderato que o meio informático absorva e seja absorvido por todos os setores da sociedade no todo ou em parte, inclusive extinguindo algumas profissões. Segundo John PUGLIANO, autor de *The Robots are Coming: A Human's Survival Guide to Profiting in the Age of Automation*, médicos, advogados, arquitetos, contadores, pilotos de guerra, policiais e corretores de imóveis serão carreiras fortemente ameaçadas. Mas é impossível freiar esta imersão, posto que fulcral ao crescimento[1].

Por tal motivo, o uso da virtualidade como meio, ecossistema, ferramenta ou ainda ataque a ela em seus bens jurídicos informáticos geradores de vantagens e lucro tende a ser algo a ser estudado com afinco. É preciso estudar também o novo agente, a nova vítima, as novas especificidades, as técnicas, os ardis e assim sequencialmente.

Certamente por estar-se diante de uma sociedade de risco "*sui generis*" necessário se faz entender que tal conceito está diretamente relacionado com a falta de segurança frente à ideia de liberdade[2]. Por segurança, compreende-se a condição de algo ou alguém encontrar-se livre de perigo, perdas ou proteção.

1. ALOCAÇÃO DO DIREITO PENAL INFORMÁTICO NO DIREITO

O Direito Penal Brasileiro é ramo do Direito Público que essencialmente busca estudar os valores considerados fundamentais para uma determinada sociedade brasileira, considerada em um determinado momento histórico e

1. A rede foi denominada "*Triple A Engine*" ou mecanismo dos três "A´s" por conta de a Internet caracterizar-se por sua "*Acessibility*" (Acessibilidade), "*Anonimity*" (Anonimidade) e "*Affordability*" ("Arcabilidade" – possibilidade de se poder arcar com seus custos), conforme COOPER *et al* in Online sexual activity: An examination of potentially problematic behaviors. Sexual Addiction & Compulsivity. New York, 2004, pp.129-143 *apud* Crimes of the Internet (editado por Frank Schmalleger), Pearson Prentice Hall, New Jersey, 2008, p. 6.

2. Nas palavras de Ricardo M. Mata y Martín *apud* ROSSINI, op. cit, p. 132: *"(...) a expressão da liberdade do indivíduo e consiste no direito a utilizar lícita e livremente, com os limites constitucionais e legais, a tecnologia informática. De forma que os delitos informáticos podem ver-se como violação dessa mesma liberdade informática, como infração de distintas liberdades as que podem estender-se ao emprego destas tecnologias (intimidade, domicílio, livre circulação, associação etc.)".*

sob uma determinada legislação vigente. Tais valores são trazidos a estudo a partir de legislações federais aprovadas segundo um rito constitucional específico e consistem em análise de condutas que violam tais valores e um conjunto de normas jurídicas adjetivas que devem ser consideradas para tais avaliações. Uma vez identificado um fato penalmente relevante e respeitado o devido processo legal, aplicam-se medidas de segurança ou penas.

Uma vez que o Direito Penal Informático está incluso dentro do Direito Penal por ser um ramo dele, é possível dizer que se trata também de ramo do Direito Público.

Por tratar-se de um conjunto de normas que (i) influencia diretamente a forma de cometimento dos delitos, (ii) possui parcela de seu conteúdo definidor de infrações e gera imposição de consequências, (iii) traz novas formas de interpretação dogmática, (iv) modifica a forma como o Estado exerce seu direito de analisar provas, condutas, indícios e modifica a aplicação do *jus puniendi*, pode-se dizer que o Direito Penal Informático possui natureza mista de Direito Penal objetivo e subjetivo.

Ainda que os ciberdelitos estejam inseridos na categoria de Parte Especial, o Direito Penal Informático não se limita a novos tipos, mas sim possui inerentemente novos modos de análise e interpretação de praticamente todo o Direito Penal. Por possuir alçada de julgamento na Justiça Comum Estadual e Federal, aplica-se a todos os indivíduos e, portanto, pode ser classificado como Direito Penal Comum.

Também, por possuir parcela de influência no próprio Processo Penal, criando um verdadeiro Processo Penal Informático, pode tanto ser classificado como subjetivo, quanto como adjetivo.

No que se refere às fronteiras penais e à classificação usual da doutrina entre Direito Penal Internacional ou Direito Internacional Penal, há possíveis dilemas. A uma porque o Direito Penal Informático termina tratando tanto de direito produzido internamente cuja aplicação se dá sobre fatos ocorridos fora do Brasil (Direito Penal Internacional) quanto em situações de normas internacionais que vigoram dentro de nosso país (Direito Internacional Penal); a duas porque a virtualidade, em regra, não é território nacional, mas também não há tratado decretando nem regras especiais nem a internacionalidade desse ambiente, colocando, na realidade, a classificação desse ramo de direito em uma situação característica.

Em verdade, há muito declaramos que um dos maiores problemas do Direito Informático é seu caráter transbordante, posto que a escala da

virtualidade é global, aterritorial, ilimitada, transsoberânica, enquanto que o Direito (e seu caráter resolutivo) é regional, territorial, limitado e soberânico. Logo, problemas globais e multifacetados são julgados segundo soluções enviesadas, unilaterais e nacionais. Temos, pois, um Direito unilateral/unifacetado tratando de questões multilaterais/multifacetadas.

De toda a sorte, este é o modo como alocamos o ramo do Direito Penal Informático neste momento e até que o Brasil adira a um tratado internacional mais abrangente.

2. COMPETÊNCIA PARA LEGISLAR SOBRE DIREITO PENAL INFORMÁTICO

De acordo com o artigo 5º, inciso II da Constituição Federal, "*ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei*". Nessa lógica, os comportamentos apenas podem ser ditados e exigidos a partir de uma prévia existência de legislação. A isso, denominamos legalidade conforme já apresentamos previamente.

Na ótica penal, tal princípio ainda ganha conjugação de outro importante princípio, o da anterioridade, apresentando que, no que tange aos comportamentos penalmente considerados, segundo o artigo 5º, inciso XXXIX da Constituição Federal e o artigo 1º do Código Penal, "Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal".

Isso significa que leis penais não são suficientes para ditar comportamentos passados, limitando-se a produzir efeitos futuros quando geradoras de novas obrigações, novas regras que podem prejudicar acusados e, ainda no que tange à novos tipos penais e, portanto, novas condutas. A isso se chama "irretroatividade da lei penal maléfica" e seus efeitos são denominados *ex nunc*.

Contudo, normas penais que melhorem as condições dos acusados, beneficiem-nos ou extingam tipos penais possuem seus efeitos a partir de sua publicação, mas também devem ser aplicadas a para fatos passados (e para processos que, mesmo que já transitados em julgado, podem ser revistos a partir do recurso da Revisão Criminal), no que a ciência denomina "retroatividade da lei penal benéfica" e seus efeitos são denominados *ex tunc*.

Exemplificativamente, o surgimento da Lei nº 12.737/12 jamais poderia surtir efeitos na atriz que teve suas fotos expostas na rede algumas semanas antes pela irretroatividade de seus efeitos. Contudo, pessoas que outrora foram condenadas por delitos mais gravosos e que tivessem suas condutas enquadradas

nessa lei poderiam pedir revisão criminal, caso suas condenações tivessem sido mais gravosas do que a determinada no novo artigo 154-A, Código Penal.

No que toca à questão da competência legislativa em matéria penal informática, não há grandes dificuldades. Apesar de o Brasil ser uma Federação – o que em tese daria autonomias legislativas para os entes federativos, os Estados – nossa forma de Governo centralizou na esfera federal a competência para legislar sobre Direito Penal em geral. Assim, a competência para legislar sobre o Direito Penal Informática, está intocada:

> Artigo 22. Compete privativamente à União legislar sobre:
>
> I – direito civil, comercial, penal, processual, eleitoral, agrário, marítimo, aeronáutico, espacial e do trabalho; (grifo nosso)

No que tange à iniciativa, segundo o artigo 61 da Constituição Federal, podem propor a criação de leis penais (a) os membros do Congresso Nacional (qualquer membro ou Comissão da Câmara dos Deputados, do Senado Federal ou do Congresso Nacional), (b) ao Presidente da República, e (c) aos cidadãos, na forma de iniciativa popular do artigo 62, parágrafo 2º da Constituição Federal[3].

Não podemos deixar de apontar para o fato de que a EC 115/2022 trouxe ao artigo 22 um inciso XXX em que o tema "proteção e tratamento de dados pessoais" passa a ser também de competência privativa da União. Como defendemos uma proteção penal aos dados, possivelmente isso corrobora em duas frentes a competência aludida.

Finalmente, importante ressaltar que do mesmo modo como no Direito Penal comum, a lei é a fonte imediata e costumes e princípios gerais de Direito, fontes mediatas de interpretação legal.

3. COMPETÊNCIA JURISDICIONAL

A matéria de competência é pertinente ao Processo Penal Informático e não será abordada de forma exaustiva até mesmo porque o autor foca esforços especiais em análises materiais.

---

3. Nesse sentido, concordamos com NUCCI ao interpretar restritivamente o artigo 61, de modo que ao Supremo Tribunal Federal, aos Tribunais Superiores e ao Procurador-Geral da República apenas haveria a permissão de criação de leis de matéria de seu peculiar interesse, elencadas no artigo 96, II da Constituição Federal. NUCCI, Guilherme de Souza, Manual de Direito Penal – parte geral, parte especial – 7a edição revista, atualizada e ampliada, Revista dos Tribunais, São Paulo, p. 95.

Assunto de bastante dúvida e debate ainda hoje, a competência jurisdicional (e investigativa) depende, inicialmente, da lógica da natureza do delito. Assim, o primeiro raciocínio é no sentido de saber se o delito a ser analisado é de competência federal ou estadual. O raciocínio a se fazer é excludente: o que não for da competência de juízes federais o será residualmente de juízes estaduais. Para isso, mandamental a leitura do artigo 109 da Constituição Federal que preceitua:

> Artigo 109. Aos juízes federais compete processar e julgar: (…)
>
> IV – os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, excluídas as contravenções e ressalvada a competência da Justiça Militar e da Justiça Eleitoral;
>
> V – os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente;
>
> V-A as causas relativas a direitos humanos a que se refere o § 5º deste artigo; (…)
>
> IX – os crimes cometidos a bordo de navios ou aeronaves, ressalvada a competência da Justiça Militar;

Suprimimos alguns incisos que não nos parecem ter qualquer relevância quanto ao tema. E mantivemos alguns que parecem não ter relevância, mas que merecem algumas considerações.

Não há dúvidas de que sempre que a infração penal atingir a União, a competência será federal. Assim a violação a bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, excluídas as contravenções serão, pois, julgados por juízes federais.

O artigo 266 do Código Penal, em seu parágrafo primeiro, trata da interrupção de serviço telemático ou o impedimento de reestabelecimento. No caso, parece-nos que a Internet é serviço federal, gerido por um comitê federal (Comitê gestor da Internet Brasileira ou CGI.br) e, portanto, qualquer ataque em tal sistema atinge diretamente ou ao menos tangencia interesse da União[4]. Esposamos, assim, o entendimento de que este é um delito de competência federal nas situações de serviços telemáticos afetados dolosamente.

4. Observe-se algumas das atribuições do CGI.br, segundo o próprio site: (i) o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil; (ii) o estabelecimento de diretrizes para a administração do registro de Nomes de Domínio usando <.br> e de alocação

Porém, nos casos em que o segmento de serviço informático afetado seja limitado, por exemplo, uma VPN de uma empresa situada em um estado, entendemos que a competência deveria ser estadual por conta de sua abrangência.

Vale também relembrar que o art. 359-R do Código Penal já vigente aponta ideia semelhante que é a conduta típica de "destruir ou inutilizar meios de comunicação ao público, estabelecimentos, instalações ou serviços destinados à defesa nacional, com o fim de abolir o Estado Democrático de Direito". Nesse caso, entendemos que o elemento subjetivo específico forçaria a competência federal, novamente.

O inciso V do Art. 109, CF, fala em situações em haja tratado ou convenção internacional que preveja infração penal desde que a execução do delito tenha se iniciado no Brasil e o resultado tenha ocorrido no estrangeiro ou ali devesse ter ocorrido (casos de tentativa em que o evento é normativo).

O mesmo valeria para situações em que o delito tenha se iniciado no estrangeiro e o resultado tenha ocorrido no Brasil ou aqui devesse ter ocorrido. Obviamente, se o Brasil assinou e ratificou um tratado ou convenção, estará obrigado a julgar delitos ali abarcados. E é da competência da Justiça federal. Em especial, vale citar alguns desses tratados com implicações reais ou aparentes em nossa área, quais sejam:

a) Convenção Internacional de Repressão da Moeda Falsa – Decreto nº 3.074, de 14.09.1938.

b) Convenção Contra o Tráfico Ilícito de Entorpecentes e Substâncias Psicotrópicas – Decreto nº 154 de 26.06.1991.

c) Convenção das Nações Unidas Contra o Crime Organizado Transnacional Relativo à Repressão e Punição do Tráfico de Pessoas, Em Especial Mulheres e Crianças – Decreto nº 5.017, de 12.03.2004.

d) Convenção para a Repressão do Tráfico de Pessoas e do Lenocínio – Decreto nº 46.981, de 08.10.1959.

e) Convenção Interamericana para Prevenir e Punir a Tortura – Decreto nº 98.386, de 09.12.1989.

---

de endereços Internet (IPs); (iii) a promoção de estudos e padrões técnicos para a segurança das redes e serviços de Internet; (iv) a recomendação de procedimentos, normas e padrões técnicos operacionais para a Internet no Brasil; (v) a promoção de programas de pesquisa e desenvolvimento relacionados à Internet, incluindo indicadores e estatísticas, estimulando sua disseminação em todo território nacional.

f) Convenção Internacional Sobre a Eliminação de Todas as Formas de Discriminação Racial – Decreto nº 65.810, de 08.12.1969.

g) Convenção Sobre os Direitos da Criança Referente à Venda de Crianças à Prostituição e à Pornografia Infantil – Decreto nº 5.007, de 08.03.2004.

h) Convenção sobre o Cibercrimes (Convenção de Budapeste) – Decreto Legislativo nº 37, de 16 de dezembro de 2021.

Renato de Mello Jorge SILVEIRA, em extenso estudo, debateu a natureza jurídica das criptomoedas. Caso pudessem se equivaler a moedas propriamente ditas, tal convenção teria algum impacto na questão informática, afinal. Mas o professor assevera claramente que:

> Na realidade o bitcoin, bem como as dezenas de moedas virtuais, não se confunde com a noção de moeda eletrônica regulada pela Lei nº 12.865 de 09.10.2013. As moedas virtuais, na verdade, não podem ser vistas como moedas em si, e, portanto, não seriam sujeitas, nos dias de hoje, a nenhuma regulamentação dada à moeda em si[5]. (grifos nossos)

Por isso, excluem-se da competência federal, de imediato, questões relacionadas à falsificação de criptomoedas, restando-se, pois, competência estadual.

No caso, porém, de tais criptoativos serem utilizados para fins de evasão de divisa, a competência novamente deve ser a Federal, assim como nas situações em que for utilizada para questões atinentes à lavagem de capitais (art. 2º, III, Lei nº 9.613/98: a) quando praticados contra o sistema financeiro e a ordem econômico-financeira, ou em detrimento de bens, serviços ou interesses da União, ou de suas entidades autárquicas ou empresas públicas e b) quando a infração penal antecedente for de competência da Justiça Federal).

Recentemente, em sentido oposto, todavia, o HC nº 530.563-RS de relatoria do eminente Ministro Sebastião Reis Júnior no Superior Tribunal de Justiça reconheceu a Justiça Federal como competente para julgar crimes relacionados a contrato coletivo de investimento em bitcoins[6].

---

5. SILVEIRA, Renato de Mello Jorge. Bitcoin e suas fronteiras penais. Belo Horizonte: Editora D'Placido, 2018, pp. 118.

6. EMENTA HABEAS CORPUS. OPERAÇÃO EGYPTO. SUPOSTA INCOMPETÊNCIA DA JUSTIÇA FEDERAL. MANIFESTA IMPROCEDÊNCIA. CASO QUE OSTENTA CONTORNOS DISTINTOS DO CC N. 161.123/SP (TERCEIRA SEÇÃO). DENÚNCIA OFERTADA, NA QUAL É NARRADA A EFETIVA OFERTA DE CONTRATO COLETIVO DE INVESTIMENTO ATRELADO À ESPECULAÇÃO NO MERCADO DE CRIPTOMOEDA. VALOR MOBILIÁRIO (ART 2º, IX, DA LEI N. 6.385/1976). INCIDÊNCIA DOS CRIMES PREVISTOS NA LEI N.

O tráfico de substâncias entorpecentes e psicotrópicas, por sua vez, ocorre com enorme frequência através dos *sites* especializados na *Darkweb*, possuindo repercussões frequentes no Brasil, que deve investigar tais delitos por sua polícia federal e julgar na justiça de mesmo nome.

A Internet, também, continua sendo mecanismo atrativo para tráfico de seres humanos que buscam melhores condições de vida, inclusive com *sites* especializados em adoção e em noivas encomendadas. Tais competências, portanto, federais também, bem como as demais apontadas, sem grandes mistérios.

Das convenções apontadas, de longe a de repressão à Pornografia Infantil através da virtualidade é a que dá mais trabalho para a Justiça Federal[7].

7.492/1986. COMPETÊNCIA DA JUSTIÇA FEDERAL (Artigo 26 DA LEI N. 7.492/1986), INCLUSIVE PARA PROCESSAR OS DELITOS CONEXOS (SÚMULA 122/STJ). 1. A Terceira Seção desta Corte decidiu que a operação envolvendo compra ou venda de criptomoedas não encontra regulação no ordenamento jurídico pátrio, pois as moedas virtuais não são tidas pelo Banco Central do Brasil (BCB) como moeda, nem são consideradas como valor mobiliário pela Comissão de Valores Mobiliários (CVM), não caracterizando sua negociação, por si só, os crimes tipificados nos artigos 7º, II, e 11, ambos da Lei n. 7.492/1986, nem mesmo o delito previsto no artigo 27-E da Lei n. 6.385/1976 (CC n. 161.123/SP, DJe 5/12/2018). 2. O incidente referenciado foi instaurado em inquérito (não havia denúncia formalizada) e a competência da Justiça estadual foi declarada exclusivamente considerando os indícios colhidos até a instauração do conflito, bem como o dissenso verificado entre os Juízes envolvidos, sendo que nenhum deles cogitou que o contrato celebrado entre o investigado e as vítimas consubstanciaria um contrato de investimento coletivo. 3. O caso dos autos não guarda similitude com o precedente, pois já há denúncia ofertada, na qual foi descrita e devidamente delineada a conduta do paciente e dos demais corréus no sentido de oferecer contrato de investimento coletivo, sem prévio registro de emissão na autoridade competente. 4. Se a denúncia imputa a efetiva oferta pública de contrato de investimento coletivo (sem prévio registro), não há dúvida de que incide as disposições contidas na Lei n. 7.492/1986, notadamente porque essa espécie de contrato consubstancia valor mobiliário, nos termos do artigo 2º, IX, da Lei n. 6.385/1976. 5. Interpretação consentânea com o órgão regulador (CVM), que, em situações análogas, nas quais há oferta de contrato de investimento (sem registro prévio) vinculado à especulação no mercado de criptomoedas, tem alertado no sentido da irregularidade, por se tratar de espécie de contrato de investimento coletivo. 6. Considerando os fatos narrados na denúncia, especialmente os crimes tipificados nos artigos 4º, 5º, 7º, II, e 16, todos da Lei n. 7.492/1986, é competente o Juízo Federal para processar a ação penal (artigo 26 da Lei n. 7.492/1986), inclusive no que se refere às infrações conexas, por força do entendimento firmado no Enunciado Sumular n. 122/STJ. 7. Ordem denegada.

7. Apesar do normativo internacional, observe-se que o STJ já apontou incompreensivelmente no sentido oposto à Constituição Federal: 'CONFLITO NEGATIVO DE COMPETÊNCIA. PROCESSUAL PENAL. APURAÇÃO DO DELITO DO Artigo 241-A DO ESTATUTO DA CRIANÇA E DO ADOLESCENTE. SUPOSTA VEICULAÇÃO DE IMAGENS DE PORNOGRAFIA INFANTIL PELA INTERNET. COMPETÊNCIA FIRMADA PELO LUGAR DA INFRAÇÃO. ARTIGO 70 DO CÓDIGO DE PROCESSO PENAL. COMPETÊNCIA DE TERCEIRO JUÍZO, ESTRANHO AO CONFLITO. 1. A consumação do delito, que atualmente tem previsão no artigo 241-A do Estatuto da Criança e do Adolescente, 'ocorre no ato de publicação das imagens pedófilo-pornográficas, sendo indiferente a localização do provedor de acesso à rede mundial de computadores onde tais imagens encontram-se armazenadas, ou a sua efetiva visualização pelos usuários' (CC 29.886/SP, Rel. Ministra MARIA THEREZA DE ASSIS MOURA, TERCEIRA SEÇÃO, julgado em 12/12/2007, DJ 01/02/2008, p. 427). 2. A conduta delituosa a ser apurada, na hipótese, refere-se à veiculação de imagens de menores aliciadas para exposição em cenas obscenas, via webcam, por

Importante destacarmos que o Brasil ratificou a Convenção de Budapeste (Convenção sobre o Cibercrime) através do Decreto nº 37/2021. Ocorrido isso, nosso entendimento é o de que passam a ser de competência da Justiça Federal, também, os seguintes casos de Direito Material (aqui meramente elencados conforme o normativo aponta):

Título 1: Infrações contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos: (a) Acesso ilegítimo, (b) Intercepção ilegítima, (c) Interferência em dados, (d) Interferência em sistemas e (e) Uso abusivo de dispositivos

Título 2: Infrações relacionada com computadores: (a) Falsidade informática e (b) Burla informática

Título 3: Infrações relacionadas com o conteúdo: (a) – Infrações relacionadas com pornografia infantil

Título 4: Infrações relacionadas com a violação do direito de autor e direitos conexos.

Por tratar-se de legislação ainda não devidamente inserida no ordenamento jurídico brasileiro – ainda há a necessidade de publicação final pelo Gabinete da Presidência da República –, deixaremos de aprofundar-nos para evitarmos nos apressar e cometer eventuais equívocos. Porém, fica o registro de mudança de competência iminente a ser inserida neste Curso na próxima edição[8].

Resta ainda o inciso V-A do artigo 109 que a princípio parece fugir da temática Penal Informática.

Porém, como já apresentamos outrora, entendemos que o Princípio da Dignidade do Usuário deve ser inserido no ordenamento brasileiro, de

meio do MSN/ORKUT e TWITTER, além de hackeamento e utilização do perfil de uma delas, fazendo-se o agente passar por esta, para comunicar-se com terceiros. 3. Ausentes indícios de transnacionalidade do crime, a tanto não servindo o mero meio Internet, competente é o juízo estadual do local de indicada residência do suspeito, em Londrina/PR, na forma do artigo 70 do Código de Processo Penal. 4. Conflito conhecido para declarar competente o Juízo de Direito da Vara Criminal da Comarca de Londrina – TJ/PR, juízo estranho ao conflito.' (CC 136.257/PR, Rel. Min. NEFI CORDEIRO, TERCEIRA SEÇÃO, DJe 20/03/2015). Informativo nº 335 reinterpretou o tema, atualizando o Informativo nº 326: "Compete à Justiça Federal processar e julgar os crimes consistentes em disponibilizar ou adquirir material pornográfico envolvendo criança ou adolescente [artigos 241, 241-A e 241-B da Lei 8.069/1990] quando praticados por meio da rede mundial de computadores".

8. Vale relembrarmos que há posição no sentido de que a competência apenas seria da Justiça Federal se fosse identificada uma internacionalidade/transnacionalidade do delito. Assim, caso o espectro lesivo da conduta não envolvesse mais de um Estado soberano, há quem compreenda não ser competente a Justiça Federal. Em outro sentido, o fato de a arquitetura da rede sempre envolver mais de um Estado soberano e, pois, no sentido de que a competência seria sempre federal.

modo a reconhecermos, como alguns países já o fazem, a condição de Direito Humano àqueles direitos apontados como relacionados com a informática. Por isso, há tempos defendemos que todos os delitos informáticos próprios deveriam ser investigados e julgados pela Justiça Federal.

Entretanto, a Justiça Federal já se manifestou em algumas ocasiões em sentido diverso

> CONFLITO NEGATIVO DE COMPETÊNCIA. ARTIGOS 241-A E 241-B DO ECA. CRIMES PRATICADOS POR MEIO DA INTERNET. INDÍCIOS DE TRANSNACIONALIDADE. INEXISTÊNCIA. COMPETÊNCIA DA JUSTIÇA ESTADUAL. 1. Para firmar a competência da Justiça Federal, nos termos do artigo 109, inciso V, da Constituição Federal, faz-se necessária a presença de indícios da transnacionalidade do crime previsto em tratados ou convenções internacionais, não bastando a potencialidade do dano internacional. 2. Conflito conhecido para declarar a competência do Juízo Estadual, o suscitante. (CC 127.419/GO, Relatora p/ acórdão Ministra MARIA THEREZA DE ASSIS MOURA, TERCEIRA SEÇÃO, DJe 2/2/2015.)

Recentemente, a Lei nº 14.155/2021 acrescentou um parágrafo 4º ao artigo 70 do CPP e determinou que nos crimes previstos no art. 171 do Código Penal, quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção. De nossa alçada, a parte final[9].

Afora estes casos e feita a ressalva de nossa opinião pela competência da Justiça Federal para jurisdição de todos os delitos informáticos próprios, os demais delitos deverão ser julgados pela justiça estadual e investigados pelas polícias civis especializadas (se houver) dos Estados.

Não há, também, impedimento para que as polícias trabalhem em cooperação na averiguação para que se ganhe eficiência regional, especialmente quando há delegacia especializado ou quanto não há justiça federal na localidade.

9. Vale apontarmos que originalmente o PLS nº. 4554/2020, em sua redação final no Senado Federal, criava o capítulo II-A no Código de Processo Penal, inserindo um artigo 73-A em que se estabelecia que "quando o crime for cometido pela internet ou de forma eletrônica, a competência será determinada pelo lugar de domicílio ou residência da vítima". Essa disposição foi modificada na Câmara dos Deputados na apresentação de um substitutivo depois aprovado pelo Senado.

4. O SURGIMENTO E EVOLUÇÃO DO DIREITO PENAL INFORMÁTICO BRASILEIRO[10]

O Brasil inicia sua história legislativa no Direito Penal Informático de modo relativo no ano de 1997 com a promulgação da Lei nº 9.459/1997. Por conta de tal lei, o delito de preconceito de raça ou de cor passou a ter uma figura qualificada no parágrafo 2º do artigo 20, ao apresentar, ainda que de modo precário diante das tecnologias atuais e de modo indireto, que:

> Artigo 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.
>
> § 2º Se qualquer dos crimes previstos no caput é cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza[11]:
>
> Pena: reclusão de dois a cinco anos e multa.

Por certo, situações de divulgação de materiais preconceituosos através de redes sociais precárias, fóruns ou bate papos atingiam um número considerável de usuários e tinha seu potencial lesivo elevado, merecendo, portanto, maior reprimenda. De modo inteligente, o legislador produziu o dispositivo de modo amplo.

Contudo, apresentamos esse início na era penal informática como sendo algo relativo porque, conforme se observa, a Lei em tela, por imensa dificuldade em se prever o quanto a tecnologia se alastraria, previu como procedimento processual de contenção *a cessação das respectivas transmissões radiofônicas ou televisivas*[12] apenas, demonstrando que a questão informática era secundária.

Evoluamos até que cronologicamente haja a modificação (tardia) de tal norma.

---

10. Ainda que haja mudanças de caráter eminentemente processual em alguns casos, consideraremos tais mudanças para apresentar a história do Direito Penal Informático Brasileiro. Também, para fins de evolução histórica, consideramos as situações em que houve reconhecimento legislativo do caráter informático nas condutas, visto que praticamente todos os delitos comuns podem ser praticados de forma livre, inclusive pelo meio informático.

11. Importante ressaltar que o artigo 141, III do Código Penal também pode ser utilizado para questões informáticas por sua inteligente redação que faz abarcar genericamente qualquer meio facilitador. Na ocasião, o ano era 1940 e a redação ficou assim: *Artigo 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.* Assim, qualquer crime contra a honra que se utilize da virtualidade como propagadora tem a causa de aumento específica aplicada.

12. Artigo 20, parágrafo 3º, inciso II da Lei nº 7.716/1989.

A delinquência informática em espécie

Neste capítulo, objetivamos fazer algumas considerações importantes referentes ao que existe hoje acerca de Direito Penal Informático Brasileiro ou está prestes a surgir no ordenamento jurídico.

Focaremos nos delitos mais relevantes para a área, porém sem descuidarmos de que uma grande parte dos delitos comuns presentes em nosso Código Penal admite a modalidade informática como meio de execução da conduta (imprópria, portanto). É, por exemplo, o caso do homicídio, que pode ter sua execução através do desligamento de uma rede de suporte de um pronto socorro, da troca de remédios em um banco de dados informatizados de um hospital ou até mesmo a partir de uma sucessão de sustos e amedrontamentos feitos por VoIP em face de alguém cardíaco.

O foco, contudo, são os delitos que mais ocorrem ou os delitos que receberam tipificação legislativa por suas características eminentemente tecnológicas ou pelo vulto que tomaram especialmente nessa esfera.

Falaremos, portanto, da (a) invasão informática, (b) da exposição pornográfica não consentida, (c) do registro não autorizado de imagens de natureza íntima, (d) da alteração indevida de bancos de dados públicos, (e) do *scamming* (estelionato por meio virtual), (f) da sextorsão, (g) do *cyberstalking* (Delito de Perseguição), (h) da pornografia infanto-juvenil na virtualidade, e (i) de outros temas importantes do Direito Penal Informático.

Alguns dos temas já foram objeto de livros próprios. Por isso, a ideia é dar um apanhado compacto de cada tema, remetendo o leitor interessado em leituras mais detidas e a obras especiais.

1. AS LEIS Nºs 12.735/12 E 12.737/12

É de se destacar que existiam alguns projetos de lei em trâmite no Congresso Nacional sobre o tema e que, conforme é notório, a competência para legislar sobre Direito Penal é privativa da União, conforme o artigo 22, I, da Constituição Federal.

Também é importante que apresentemos liminarmente nossa preocupação acerca de um novo movimento legislativo precipitado, simbólico e pressionado por fatores midiáticos, capazes de fazer aprovar leis mal-acabadas e que não correspondem àquilo verdadeiramente necessitado pelo Direito Penal Brasileiro.

Em nossa ótica, deve o Princípio da Intervenção Mínima ser respeitado em elevado grau. A criação de novas legislações penais com aplicabilidade duvidosa termina por colocar o poder policial e o Judiciário em situação de ineficiência pragmática e o próprio Estado em posição de fragilidade, posto que não consegue aplicar a lei que criou e que permanece no ordenamento jurídico reafirmando tal fraqueza.

Na questão da informática, há ainda especial preocupação. Não é de hoje que se veem reivindicações das polícias civil, militar e federal por equipamentos melhores e mais modernos. Armas, munição, coletes à prova de balas e carros equipados são antigas demandas. O mesmo se diga acerca do exército e dos frequentes debates de seu sucateamento.

Delitos informáticos demandam pessoal altamente especializado e equipamentos de última geração; afinal é possivelmente com um agente munido da última geração de dispositivos que se terá que lidar.

Mais do que isso: é necessário conexão de alta qualidade e apoio de países de todo o mundo para que as investigações não esbarrem em formalidades e entraves burocráticos.

Não raro, o sistema responsável por registrar ocorrências em distritos policiais está fora do ar.

Em suma, o discurso antigo: de nada adianta o legislador gerar uma norma sem verificar se existe aplicabilidade e estrutura, assim como de nada adianta o político oferecer benesses sem verificar a previsão orçamentária.

O delito informático não é brasileiro. Nem o direito informático. Ele ocorre na virtualidade transsoberânica e a precisão do local em que as condutas ocorrem é difícil e etérea.

Os conceitos de territorialidade e exclusividade investigativa foram substituídos, nestes casos, pela cooperatividade e pela virtualidade, somadas à necessidade de velocidade e imaterialidade.

É delito de difícil contenção, de difícil previsão e de difícil visualização, em que muitas vezes o delinquente proficiente conhece todos os vestígios que deixa e sabe tratá-los melhor do que o próprio investigador em seu encalço.

Na criminalidade comum, consegue-se identificar o que é uma ação penalmente relevante, uma omissão própria e uma omissão imprópria, a partir de conceitos positivos de punição (proibição indireta) e deveres daqueles em posição de garantes.

Na delinquência virtual brasileira, ainda não se compreendeu ao certo quem é quem e quais os papéis exercidos e as responsabilidades com que cada um deve arcar, exceto nos limites traçados pelo Marco Civil da Internet.

É sabido que qualquer acesso à rede é feito via provedores, exclusivamente. Não existe acesso sem provedor. Logo, o provedor possui também papel fundamental.

O Marco Civil da Internet brasileira apresentou definições específicas a expressões usadas no Direito Informático, regrou as circunstâncias de atuação do provedor e dos usuários, limitou abusos eventuais do poder público e assegurou formalidades importantes para o novo estado democrático de direito na era digital. Conforme seu artigo 1º:

> Esta lei estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil e determina as diretrizes de atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Esta legislação, porém, data de 2014.

Na contramão da lógica, foram aprovados às pressas no Congresso Nacional o PL nº 2.793-C/2011 e o PL nº 84-G/99, ambos sancionados (no todo ou em parte) pela então Presidente da República Dilma Houssef. Portanto, invertendo paradigmas jurídicos, a norma de intervenção final foi aprovada antes da criação das normas elementares, e da definição de conceitos de natureza civil e administrativa.

2. O PL Nº 84/99 – LEI Nº 12.735/2012

Originalmente, o Projeto de Lei nº 84/99 era o PL nº 1.713/96, de autoria do deputado Cassio Cunha Lima. Foi retirado de pauta pelo fim da

legislatura e reproposto, com a numeração hoje conhecida, pelo Deputado Luiz Piauhylino, em 1999.

Recebeu como apensos o PL nº 2.557/2000, o PL nº 2.558/2000 e o PL nº 3.796/2000 do Deputado Alberto Fraga e o PL nº 6.983/2010 do Deputado Nelson Goetten.

Durante 5 anos, o Projeto de Lei nº 84/99 ficou parado e, em 2008, o Senado aprovou em revisão o projeto, apresentando substitutivo que alargava seu espectro original com o objetivo de aumentar as reformas e alterar o Decreto-lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 7.716, de 5 de janeiro de 1989, a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente) e a Lei nº 10.446, de 8 de maio de 2002.

Em 2010, recebeu no Senado Federal mudanças para tentar adequá-lo à Convenção de Budapeste ou Convenção do Cibercrime e, a partir dali, houve uma sucessão de substitutivos.

O PL original foi sendo retalhado até culminar no PL nº 84-G/99.

O projeto inicial – que buscava apresentar princípios, dar definições e criminalizar condutas de dano informático, acesso indevido, alteração de dados, obtenção indevida de dados, violação de segredo e produção de *malwares* em 18 (dezoito) artigos que alterariam o Código Penal – foi aprovado com apenas 6 (seis) artigos, sendo que apenas um deles modificou o Código Penal, um alterou o Código Penal Militar e um alterou a Lei nº 7.716/89 (lei que define os crimes resultantes de preconceito de raça ou de cor).

Houve um enorme desvirtuamento do objetivo inicial e deu-se atenção às mudanças no Código Penal Militar para delitos em tempo de guerra, geração de norma programática para adequação da polícia judiciária e modificações processuais cautelares para evitação de *periculum in mora* em delitos de preconceito.

Perdeu-se a maior parte dos tipos penais inovadores para se conseguir a aprovação de algum normativo na área de crimes informáticos, desperdiçando-se muitos anos de trabalho e fazendo o PL resumir-se nas seguintes alterações:

a) Acresceu ao artigo 298 do Código Penal um parágrafo único, com o *nomen iuris* de "falsidade de cartão", equiparando-se a documento particular o cartão de crédito ou de débito (redundante no que se refere ao PL n. 2.793-C/2011, artigo 3º, segunda parte);

b) Dentro do Código Penal Militar, no capítulo da traição, título "do favorecimento ao inimigo", tratando-se dos crimes militares em tempo de guerra, alterou o inciso II do artigo 356, acrescendo como favorecimento ao inimigo o prejuízo ou a tentativa de prejuízo, o comprometimento ou a tentativa de comprometimento, a entrega ou a exposição a perigo de dado eletrônico;

c) Dentro do Código Penal Militar, no capítulo da traição, título "do favorecimento ao inimigo", tratando-se de crimes militares em tempo de guerra, alterou o inciso III do artigo 356, acrescendo como favorecimento ao inimigo o prejuízo ou a tentativa de prejuízo, o comprometimento ou a tentativa de comprometimento, a perda, a destruição, a inutilização, a deterioração ou a exposição a perigo de perda, destruição, inutilização ou deterioração de dado eletrônico;

d) Alterou o inciso II do § 3º do artigo 20 da Lei nº 7.716/89, dando ao magistrado instrumento processual cautelar para cessação de prática, induzimento ou incitação a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional, permitindo que este determine a cessação das respectivas transmissões eletrônicas ou da publicação por qualquer meio;

e) Determinou que os órgãos da polícia judiciária estruturem setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado;

f) Determinou *vacatio legis* de 120 (cento e vinte) dias para a vigência da lei.

Ocorre, porém, que a maior parte das alterações propostas e apresentadas acima terminou por não ingressar em nosso ordenamento jurídico.

Vejamos.

Apesar de a legislação aprovada (porém modificada) ter passado por uma grande gama de debates e consulta pública, temos que há diversas críticas que devem a ela ser dirigidas.

Conforme apresentado, o projeto inicial foi sendo retalhado e terminou por ser aprovado no Congresso, visando alterar, conforme seu artigo 1º, somente o Código Penal, o Código Penal Militar e a Lei nº 7.716, de 5 de janeiro de 1989.

Ocorreu, porém, que a Mensagem nº 525, de 30.10.2012, apresentou veto presidencial aos artigos 2º e 3º, fazendo com que a proposta original,

que incluía alteração do Código Penal (CP) e do Código Penal Militar (CPM) constantes em parte do artigo 1º da Lei nº 12.735/12, restasse letra morta.

Assim, o artigo 1º ficou publicado conforme transcrito a seguir, sendo que os trechos grifados, na realidade, não correspondem verdadeiramente ao texto legal efetivo, visto que os artigos em vigor não tratam de alterações em todos os normativos apontados:

> Artigo 1º Esta Lei **altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 – Código Penal, o Decreto-Lei n. 1.001, de 21 de outubro de 1969 – Código Penal Militar**, e a Lei n. 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. (grifo nosso).

Destarte, o artigo 1º da Lei, por si, não representa corretamente o objetivo da legislação graças ao veto presidencial, estando, pois, a primeira parte tácita e indiretamente vetada também no que diz respeito ao Código Penal e ao Código Penal Militar.

Ainda no que se refere aos vetos, importante destacar que concordamos expressamente com a postura no que se refere ao artigo 2º da Lei nº 12.735/2012.

Isso porque corria-se um risco de se ter, no ordenamento jurídico, duas legislações datadas de 30 de novembro de 2012 que tratariam do mesmo assunto: a alteração do artigo 298 do Código Penal. Ambas acresciam um parágrafo único no delito de falsificação de documento privado para equiparar a tal o cartão de débito ou crédito.

A teratologia – impedida pelo veto – faria com que duas legislações de aprovação e publicação na mesma data tratassem de alteração de mesmo dispositivo legal. A maior gravidade do erro do legislador, ainda, restaria no fato de que os dispositivos davam redações **diferentes** ao mesmo parágrafo.

De todo modo, o veto ao artigo 2º da Lei nº 12.735/12 não impediu a alteração supramencionada, posto que a Lei nº 12.737/12, publicada na mesma data, teve sancionado seu artigo 3º, que fez acrescer o aludido mesmo parágrafo único.

No que se refere ao veto do artigo 3º da Lei nº 12.735/12, este foi justificado pelo fato de que a expressão "dado eletrônico" que se pretendia fazer constar nos incisos II e III do artigo 356 (no delito militar próprio de "Favor ao Inimigo") faria com que o Tipo Penal ficasse excessivamente abrangente,

violando princípios como o da taxatividade e fazendo com que a incidência da norma em si ficasse inviabilizada.

Restaram, assim, os artigos 4º, 5º e 6º da lei a serem analisados.

Curiosamente, o que deveria ser uma lei penal transformou-se em lei que não gerou qualquer impacto nessa esfera do direito. Isso porque o artigo 4º veio com a seguinte redação:

> Artigo 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Parece que a legislação tratou, nesse excerto, de norma regulamentar organizacional genérica das polícias judiciárias.

Em que pese ser a função do legislador federal apenas a regulamentação da polícia do Distrito Federal, conforme artigo 21, XIV da Constituição Federal, e que haja previsão constitucional que trate de norma geral para organização da polícia civil (artigo 24, inciso XVI da CF – competência concorrente), acreditamos que num futuro boa parte dos delitos de informática terminará por ser julgada pela Justiça Federal pelo potencial impacto mundializado e transestadual dos delitos. Também, verificamos que o Brasil proximamente ratificará o Tratado contra o ciberdelito.

Mas isso não exclui dos Estados a necessidade de especialização e treinamento de sua polícia investigativa no que se refere aos delitos circunscritos exclusivamente às suas regiões.

É fundamental ressaltarmos a fundamental necessidade de rigoroso treinamento das polícias para compreender linguagens específicas utilizadas pelos delinquentes virtuais (além da língua inglesa, predominante), técnicas utilizadas pelos infratores, bem como métodos para identificar, preservar e apreciar as provas informáticas. Já tratamos disse anteriormente, inclusive ao tratar da cadeia de custódia da prova digital.

Reitere-se a importância de peritos judiciais exclusivamente voltados para as investigações virtuais e informáticas, sob risco de elevado grau de impunidade e diminuta aplicação de quaisquer normativos no setor.

Resta, acerca desta lei, tratarmos de seu único artigo com repercussão processual penal significativa e imediata. Trata-se do artigo 5º, que diz:

> O inciso II do § 3º do artigo 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:

> "Artigo 20. (...)
> § 3º (...)
> II – a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio;
> (...)" (NR)

O que houve, em verdade, foi a alteração do inciso que dizia que o magistrado – uma vez ouvido o Ministério Público ou a pedido deste –, se verificasse que alguém praticou, induziu ou incitou a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional por intermédio dos meios de comunicação social ou publicação de qualquer natureza, poderia determinar a cessação das respectivas transmissões radiofônicas ou televisivas.

Por inexistência de previsão, estava ausente regra processual que permitiria medidas cautelares acerca dos meios eletrônicos. Assim, como tipo misto alternativo, a prática de qualquer dos núcleos apontados passa a poder contar com uma medida mais ampla para evitação da disseminação de delitos de ódio, posto que passa a poder determinar a cessação das respectivas transmissões radiofônicas, televisivas, **eletrônicas ou da publicação por qualquer meio**.

Desta forma, o meio de maior capacidade de difusão – que é a virtualidade hoje – passou a poder sofrer impactos constritivos para assegurar que os estragos causados por um movimento de ódio por raça, cor, etnia, religião ou procedência nacional sejam impedidos de se alastrar (em tese) com a velocidade proporcionada pela virtualidade.

O que nos preocupa nesse tipo de regulamentação processual é a forma como o magistrado fará tal cassação/proibição.

Isso porque há que se compreender que a decisão judicial pode gerar impactos em pessoas físicas ou jurídicas provedoras de serviços ou hospedagem situados no país – e nesse caso há formas de fazer cumprir efetivamente a lei –, mas também há possibilidade (mais provável, inclusive) de que a ordem almeje pessoas fora do país.

Como o delito de desobediência exige (a) ordem legal, (b) emanada por autoridade competente e (c) em face de pessoa que tenha obrigação de atendê-la, a situação se complica, a ameaça legislativa de o descumpridor sofrer processo-crime por desobediência fica praticamente inócua no segundo caso.

Isso porque, para se dar o cumprimento da cessação, será exigida carta rogatória do Brasil para o país (e a inexistência de acordo entre países, nesse

sentido, já seria um entrave formal) que, por si só, não pode ser considerada ordem, mas apenas pedido.

Há também a possibilidade de que o país rogado tenha legislação que permita a liberdade de expressão em grau elevado (como os EUA, por exemplo, por força da primeira emenda constitucional), mesmo preconceituosa, o que, por si só, faz com que a determinação judicial seja impraticável por incompatibilidade de legislações.

Neste sentido, o que resta para que haja praticidade do novel artigo é que torçamos para que o delito de ódio esteja armazenado em servidores brasileiros, em provedores hospedados no Brasil ou em serviços nacionais. Caso contrário, não bastará esta legislação para fazer impedir cautelarmente a permanência de tais atos.

Na maior parte dos países desenvolvidos, foram criadas espécies de agências internacionais para a cooperação de esforços entre países, no sentido de investigar e combater as violações cibernéticas ou que fazem uso da virtualidade e geram maior efetividade na aplicação da lei. Assim, não se perde tempo com a sistemática de cartas rogatórias burocráticas, geram-se grupos de trabalho dedicados e especializados em combate de delitos informáticos e consegue-se uma resposta jurisdicional verdadeira.

No mais, também se nota que não há mecanismo pecuniário explícito para exigir o cumprimento da obrigação, mas tão somente penal, numa ameaça de delito de desobediência que ainda passará necessariamente pela avaliação do Ministério Público para verificar seu cabimento. Ao judiciário, resta a alternativa dos *astreintes*.

Fundamental lembrarmos que o papel dos provedores e fornecedores de serviços virtuais em oferecer informações e retirar do ar conteúdos considerados abusivos encontra-se bem abalizado pelo Marco Civil da Internet, de modo mais efetivo do que o apresentado pela reforma da Lei nº 7.716/89. Reiteramos que as ordens necessariamente devem ser judiciais até o momento, exceto na questão da pornografia e intimidade que permitiriam ação proativa de *compliance* do provedor (baseada no artigo 21 do Marco Civil).

Finalmente, o artigo 6º da Lei deu *vacatio legis* de 120 (cento e vinte) dias para o seu ingresso no ordenamento jurídico. Por força do artigo 8º, § 1º, da Lei Complementar nº 95/98, a contagem se dá incluindo o *dies a quo* da publicação. Com isso, ironias à parte, a legislação entrou em vigor no território nacional no dia 1º de abril de 2013.

3. O PL Nº 2.793-C/2011 – LEI Nº 12.737/2012

Este normativo aproveitou-se da circunstância histórica de ter havido vazamento de fotos de uma atriz que foi fazer manutenção técnica de seu computador, e nele foram encontradas fotos íntimas dela. Por meio da obtenção ilegítima de tal mídia, houve um delito de extorsão, ocorrido graças ao acesso "indevido" aos dados pessoais da vítima.

Por conta desse fato ter sido amplamente divulgado na mídia, surgiu pressão sobre o legislador para que surgisse algum Tipo Penal que tutelasse os dados informáticos e, assim, restou aprovado o PL nº 35/2012 na Câmara dos Deputados, inicialmente originado pelo PL nº 2.793/2011.

Ao final, optou-se por manter o trâmite do PL nº 2.793/2011, que recebeu alterações e virou o substitutivo de letra "C" aprovado nas duas casas legislativas e que seguiu para sanção ou veto presidencial, nos seguintes moldes:

a) Criou o delito de invasão de dispositivo informático simples (artigo 154-A, Código Penal) com duas figuras;

b) Criou uma figura assemelhada à da invasão simples de dispositivo informático, com mesma pena do *caput* para o partícipe do delito principal (ou praticante do delito de meio), impedindo sua punição em menor grau (artigo 154-A, § 1º, Código Penal);

c) Criou uma causa de aumento específica para o delito de invasão simples em autoria ou participação, para o exaurimento com prejuízo econômico (artigo 154-A, § 2º, Código Penal);

d) Criou uma modalidade qualificada de invasão de dispositivo informático (artigo 154-A, § 3º, primeira parte, Código Penal) pela obtenção de conteúdo sigiloso dos dados obtidos;

e) Criou uma modalidade qualificada de invasão de dispositivo informático (artigo 154-A, § 3º, segunda parte, Código Penal) pela obtenção de controle remoto não autorizado;

f) Criou uma causa de aumento específica para a invasão de dispositivo informático qualificada, com a divulgação, comercialização ou transmissão a terceiros dos dados obtidos;

g) Criou uma causa de aumento geral para os delitos simples e qualificado pela especial qualidade da vítima imediata do delito (basicamente, os mais altos cargos públicos);

h) Determinou ser a ação penal pública condicionada a representação nos delitos com vítima comum e ação penal pública incondicionada, nos delitos com vítimas especiais, no que se refere aos delitos de invasão de dispositivo informático;

i) Alterou o *nomen iuris* do delito do artigo 266 do Código Penal para "Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública", aumentando o rol dos crimes contra os serviços públicos;

j) Acresceu o delito de interrupção ou perturbação de serviço informático, interrupção ou perturbação de serviço telemático e interrupção ou perturbação de informação de utilidade pública;

k) Modificou o parágrafo da figura qualificada nos delitos de "Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública", visto que determina que seja dobrada a pena caso a conduta ocorra em circunstância de calamidade pública;

l) Acresceu ao artigo 298 um parágrafo único, com o *nomen iuris* de "falsidade de cartão", equiparando-se a documento particular o cartão de crédito ou de débito.

A legislação em si não recebeu vetos e possuiu a mesma *vacatio legis* da anterior, ou seja, 120 (cento e vinte) dias. Isso fez com que esta norma também entrasse em vigor no ordenamento jurídico no dia 1º de abril de 2013.

Trata-se de lei com objetivo único de alterar os artigos 154, 266 e 298 do Código Penal, composta por apenas 4 (quatro) artigos, mas que gera implicações de ordem penal e processual penal também, posto que determina a espécie de ação penal cabível (no caso do artigo 154-A).

Em seu primeiro artigo, informa que disporá sobre a tipificação penal de delitos informáticos, no plural. Porém, o que se vê, na sequência (artigo 2º), é que somente houve criação legislativa de 1 (um) delito de tal natureza, denominado "invasão de dispositivo informático".

No terceiro artigo, o que se fez foi alargar a incidência do tipo do artigo 266, bem como o do artigo 298, ambos do Código Penal, sem inovação legislativa propriamente dita, mas sim abarcando situações que antes não poderiam gerar consequências penais pela inexistência específica de previsão (logicamente, portanto, limitado pelo princípio da legalidade) e pela proibição

da interpretação analógica *in malam partem* e ausência de permissão para extensão da interpretação no texto legal.

A Lei em comento sofreu alterações da Lei 14.155/2021, conforme apresentaremos em seguida.

4. A MUDANÇA NO ARTIGO 298 DO CÓDIGO PENAL

Diz o artigo:

> Artigo 298. Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
>
> Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.
>
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito. (NR)

Essencialmente, tratou-se de um esclarecimento legislativo, a fim de evitar que a tipicidade estrita do Direito Penal pudesse gerar circunstâncias de impunidade por atipicidade, trazendo, para a definição de documento particular, o cartão nas funções de débito ou de crédito.

É sabido que o legislador, ao tratar de falsificação de documentos, dividiu os tipos penais referindo-se aos documentos públicos e aos documentos privados.

Em certas situações, decidiu-se por equiparar certos documentos essencialmente privados (por serem emitidos/produzidos por pessoas jurídicas de direito privado) a documentos públicos, especialmente pela importância da documentação na sociedade e seu impacto. São, assim, documentos particulares com força de públicos para fins penais, como o testamento particular, os livros mercantis, as ações de sociedade comercial, o título ao portador transmissível por endosso e os documentos emanados por entidades paraestatais.

Cremos que, uma vez conhecida a definição de documento público original (emitido por funcionário público) ou por equiparação (§ 2º, artigo 297 do Código Penal), todos os outros documentos, por exclusão, encaixam-se na definição de documentos particulares.

Assim, a inclusão dos cartões como documentos privados no texto legal afasta qualquer dúvida acerca da aplicação do Código Penal nos casos em que há produção de cartões falsos, adulteração de numeração, data de validade, assinatura diversa da titularidade no campo traseiro, uso de numeração indevidamente, clonagem, entre tantas outras condutas.

Exposição da intimidade sexual

O objetivo deste tópico é fazer uma análise da Lei nº 13.772/18 que alterou o artigo 216 do Código Penal. A primeira apresentação deste tema se deu em artigo publicado, aqui revisto e atualizado.[1] O tipo penal não sofreu modificações pela Lei 14.155/21.

A lei em comento criou o Tipo Penal de "Exposição da Intimidade Sexual" inserindo uma letra "B" no referido artigo, além de criar um capítulo 1-A com título e subtítulo.

A análise aqui será focada na questão do tipo de "registro não autorizado de intimidade sexual" dentro do capítulo de "Exposição da Intimidade Sexual", mas também incluiremos alguns breves comentários sobre as mudanças pertinentes à temática.

O que se identifica no estudo da norma é que o legislador produziu uma lei descuidada do ponto de vista formal e com significativos defeitos técnicos e de aplicação, porém com alguma aplicação prática.

Os defeitos, porém, não necessariamente desqualificam a criação da legislação, que, por vezes, tenta cobrir penalmente uma lacuna comportamental de modo a criar na população e no meio legislativo a ideia de reprovabilidade.

O registro não autorizado, bem como a montagem multimídia eram, até dezembro de 2018, condutas sem tipo penal específico para retratar sua

1. SYDOW, Spencer Toth. Análise preliminar da Lei n. 13.772/18 e o novo delito de Exposição da Intimidade Sexual disponível em [https://meusitejuridico.editorajuspodivm.com.br/2019/01/31/analise-preliminar-da-lei-n-13-77218-e-o-novo-delito-de-exposicao-da-intimidade-sexual/]. Acesso em 30.03.2020 às 13:43h.

gravidade e, portanto, atípicas e exigiam esforço de adaptação aos tipos penais clássicos (como o constrangimento ilegal e a injúria).

Contudo, reitera-se argumento antigo: não há esforço legislativo no sentido de buscar especialistas na área e obras dedicadas ao tema para que a criação de um tipo penal seja adequada à realidade e à necessidade brasileira.

Tipos penais confusos e inadequadamente desenhados – no sentido do Princípio da Taxatividade – faz com que o Direito Penal não consiga aplicá-los em sua inteireza projetada e, portanto, isso enfraqueça a legitimidade estatal em seu poder-dever de punir.

Observemos as dificuldades da legislação.

1. QUESTÕES FORMAIS

1.1. Origem legislativa

A lei é de autoria do Deputado João Arruda – portanto é lei de origem da Câmara dos Deputados – e trata-se de evolução do PLC nº 18 de 2017, substitutivo ao PLC nº 5.555/13 (com 5 proposições apensadas).

Originalmente, tratava-se de projeto de lei com a finalidade de criminalizar a pornografia de vingança ou vingança pornográfica. Tanto é assim que tanto a justificativa do projeto de Lei quanto o Parecer SF nº 146 de 2017 apresentavam claramente a temática do PL:

> (…) consiste na divulgação de cenas privadas de nudez, violência ou sexo nos meios de comunicação, em especial nas mídias sociais, para causar constrangimento, humilhar, chantagear ou provocar o isolamento social da vítima[2].

e

> Entretanto, há uma dimensão da violência doméstica contra a mulher que ainda não foi abordada por nenhuma política pública ou legislação, que é a violação da intimidade da mulher na forma da divulgação na Internet de vídeos, áudios, imagens, dados e informações pessoais da mulher sem o seu expresso consentimento[3].

2. Disponível em [https://legis.senado.leg.br/sdleg-getter/documento?dm=7298197&ts=1545854780969&disposition=inline]. Acesso em 29.12.2021 às 10:58h.

3. [http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=ECB71A843300C0701607A89AD4191A79.proposicoesWebExterno2?codteor=1087309&filename=PL+5555/2013]. Acesso em 29.12.2021 às 10:59h.

No Senado Federal, o PL recebeu algumas emendas, dentre as quais interessante destacar a Emenda nº 2 do Senador Roberto Rocha, que sugeriu o título do capítulo 1-A como sendo "Da violação da Intimidade Sexual" e a Emenda nº 3 do mesmo legislador, sugerindo a criação do Tipo Penal de "registro não autorizado de intimidade sexual". Contudo, apesar de a Emenda nº 3 ter sido acolhida, a Emenda nº 2 foi rejeitada conforme verifica-se no excerto do parecer a seguir:

> Já o nome sugerido para o novo capítulo, "da violação da intimidade sexual", não deve ser acolhido, uma vez que o proposto pelo Substitutivo da CDH guarda maior proximidade com as condutas criminalizadas pelo projeto. Não obstante, nos parece importante suprimir a expressão "pública" do nome do novo Capítulo I-A adotado pelo Substitutivo da CDH, para, conforme bem assinalado pelo autor da Emenda nº 2-CCJ, deixar claro que a consumação do crime independe da exposição da intimidade para a população em geral, sobretudo porque o comportamento é claramente de natureza privada.

Fica, pois, cristalino que o PL tratava da conduta de exposição de conteúdo íntimo e sua lesividade, e que, conforme expresso no excerto anterior (e por nós já analisado em outro momento), independe de exposição ampla, servindo-se, para a tipicidade, a consecução de qualquer dos verbos, mesmo que praticamente ninguém tenha tido acesso ao material. Bastaria, portanto, que uma pessoa (terceiro) o tenha.

Ocorreu, porém, que a Lei nº 13.718/18 surgiu primeiro – quiçá pela anterioridade dos PLs nº 5.798/16 e nº 5.452/16 –, tornando inócua grande parte do objeto do PL em comento. Isso porque a referida Lei criou o artigo 218-C que estabeleceu – ou tentou estabelecer – o tipo penal de exposição pornográfica não consentida, abarcando, pois, a vingança pornográfica e demais formas de exposição.

Em verdade, entendemos que não há diferença prática alguma entre os rótulos "exposição pornográfica não consentida" e "exposição de intimidade sexual". Isso se dá porque os materiais referidos na expressão "exposição pornográfica", conforme artigo 218-C, são "cena de sexo, nudez ou pornografia" e os referidos no artigo 216-B são "cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado".

Entretanto o legislador não se preocupou em REVER o texto legal do PL nº 18 nem em estudar sua compatibilidade e adequação no cenário pós

promulgação da Lei nº 13.718/18. Assim, fez inserir um capítulo no Código Penal que se referia ao projeto ORIGINÁRIO.

Com isso, surgiu uma teratologia.

1.2. Uma teratologia na alocação do tipo

O capítulo denominado DA EXPOSIÇÃO DA INTIMIDADE SEXUAL não trata de nenhum tipo relacionado com exposição de intimidade sexual, mas apenas o tipo de "*registro não autorizado da intimidade sexual*" e também um equivalente relativo à montagem de material audiovisual da mesma natureza.

Isso porque "expor" é o ato de publicar (no sentido de dar acesso a qualquer terceiro não autorizado e, pois, tornar mais público do que aos relacionados) material e não o simples "registrar" de que trata o artigo.

Nessa bizarra toada, o verdadeiro tipo de e*xposição de intimidade* constante no artigo 218-C do Código Penal, encontra-se no capítulo DOS CRIMES SEXUAIS CONTRA O VULNERÁVEL, e não no capítulo DA EXPOSIÇÃO DA INTIMIDADE SEXUAL. Ademais, não trata de exposição de tipo que almeja apenas vítima vulnerável, mas qualquer espécie de vítima.[4]

Certamente o registro não autorizado é modalidade de VIOLAÇÃO de intimidade (conforme proposto da Emenda 2) mas evidentemente não trata de exposição. Expor, segundo o dicionário Michaelis, é "colocar em evidência, pôr à vista" e tais condutas estão diretamente relacionadas com os núcleos do tipo do artigo 218-C e não do artigo 216-B, CP.

Ressalte-se, entretanto, que não se está diminuindo a importância de um tipo incriminador para a conduta de registro não autorizado, mas apenas apontando o defeito formal de alocação do tipo, o que, por si só, prejudica uma adequada e séria exegese.

1.3. Desdobramentos do tipo e classificação

O artigo 216-B tem a seguinte redação:

> Produzir, fotografar, filmar ou registrar, por qualquer meio, conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado sem autorização dos participantes.

4. [https://meusitejuridico.editorajuspodivm.com.br/2018/10/05/exposicao-pornografica-nao-consentida-na-Internet-e-mudancas-da-lei-13-7182018/]. Acesso em 29.12.2021 às 11:10hs.

> Pena – detenção, de 6 (seis) meses a 1 (um) ano, e multa.
>
> Parágrafo único. Na mesma pena incorre quem realiza montagem em fotografia, vídeo, áudio ou qualquer outro registro com o fim de incluir pessoa em cena de nudez ou ato sexual ou libidinoso de caráter íntimo.

Assim, não se trata de um tipo de exposição, mas sim um tipo que visa punir o registro de material de natureza erótica ou pornográfica.

Consultando os dicionários, não identificamos uma boa tradução do verbo "registrar" que justificasse essa escolha do legislador. A menos inadequada seria a que aponta que tal conduta significa "colocar na memória", no sentido de que registrar significaria "capturar de modo perene".

Por certo os verbos "fotografar" e "filmar" tratam, até pela sua própria definição léxica, de registro[5]. Porém, o verbo "produzir" e "realizar montagem" não nos parece tratar de "registrar" mas sim de "violar" a intimidade a partir de uma produção não autorizada que impacta na imagem alheia. Mais uma razão para o título ter permanecido conforme a Emenda nº 2.

De todo o modo, por notoriedade, a expressão "registro por qualquer meio" parece-nos encerrar, via de regra, registros por áudio, por vídeo, por escultura (real ou 3D), por pintura, por avatar, por modelagem, por desenho, por grafite e tantos outros meios. A nosso ver, o que preocupa o legislador especialmente é o registro via *fotografia* e *filmagem*, dado o advento da tecnologia e a facilidade de tal prática, além da recorrência noticiada. Importante destacarmos que em uma sociedade que beira o ingresso na meta realidade, os avatares e a realidade virtual devem ser uma preocupação crescente.

Destaque importantíssimo: o tipo aqui debatido não trata de um crime informático próprio, mas sim *impróprio*. Isso porque o uso de mecanismos informáticos para captura/registro de material de intimidade sexual não necessita ser obrigatoriamente um meio digital (câmeras digitais, *webcams*, computadores, celulares etc.), podendo o agente cometer o delito de forma livre quanto ao método/meio escolhido[6]. Contudo, com a existência de uma crescente migração para a realidade artificial, os tipos desta natureza ali serão da modalidade *próprios*.

Por certo e dada a miniaturização de dispositivos de registro e a facilitação do uso de cognição automatizada (popularizada com o nome de

5. E até mesmo o "gravar via áudio", o "gravar por voz sobre IP" e assim sucessivamente.

6. Essa classificação já foi inúmeras vezes debatidas. Em especial, SYDOW, Spencer Toth. Crimes Informáticos e suas vítimas. 2ª Edição. São Paulo, Saraiva, 2016.

Inteligência Artificial ou IA), gerando *deep fakes* e *fake nudes*, a informática passa a ser a preocupação mais importante.

Da leitura atenta, depreende-se que o tipo penal buscou reprimir as seguintes 24 (vinte e quatro) condutas:

1) Produzir conteúdo com cena de nudez de caráter íntimo e privado sem autorização dos participantes;

2) Produzir conteúdo com cena de ato sexual de caráter íntimo e privado sem autorização dos participantes;

3) Produzir conteúdo com cena de ato libidinoso de caráter íntimo e privado sem autorização dos participantes;

4) Fotografar conteúdo com cena de nudez de caráter íntimo e privado sem autorização dos participantes;

5) Fotografar conteúdo com cena de ato sexual de caráter íntimo e privado sem autorização dos participantes;

6) Fotografar conteúdo com cena de ato libidinoso de caráter íntimo e privado sem autorização dos participantes;

7) Filmar conteúdo com cena de nudez de caráter íntimo e privado sem autorização dos participantes;

8) Filmar conteúdo com cena de ato sexual de caráter íntimo e privado sem autorização dos participantes;

9) Filmar conteúdo com cena de ato libidinoso de caráter íntimo e privado sem autorização dos participantes;

10) Registrar por qualquer meio conteúdo com cena de nudez de caráter íntimo e privado sem autorização dos participantes;

11) Registrar por qualquer meio conteúdo com cena de ato sexual de caráter íntimo e privado sem autorização dos participantes;

12) Registrar por qualquer meio conteúdo com cena de ato libidinoso de caráter íntimo e privado sem autorização dos participantes;

13) Realizar montagem em fotografia com o fim de incluir pessoa em cena de nudez de caráter íntimo;

14) Realizar montagem em vídeo com o fim de incluir pessoa em cena de nudez de caráter íntimo;

15) Realizar montagem em áudio com o fim de incluir pessoa em cena de nudez de caráter íntimo;

16) Realizar montagem em qualquer outro registro com o fim de incluir pessoa em cena de nudez de caráter íntimo;

17) Realizar montagem em fotografia com o fim de incluir pessoa em cena de ato sexual de caráter íntimo;

18) Realizar montagem em vídeo com o fim de incluir pessoa em cena de ato sexual de caráter íntimo;

19) Realizar montagem em áudio com o fim de incluir pessoa em cena de ato sexual de caráter íntimo;

20) Realizar montagem em qualquer outro registro com o fim de incluir pessoa em cena de ato sexual de caráter íntimo;

21) Realizar montagem em fotografia com o fim de incluir pessoa em cena de ato libidinoso de caráter íntimo;

22) Realizar montagem em vídeo com o fim de incluir pessoa em cena de ato libidinoso de caráter íntimo;

23) Realizar montagem em áudio com o fim de incluir pessoa em cena de ato libidinoso de caráter íntimo; e

24) Realizar montagem em qualquer outro registro com o fim de incluir pessoa em cena de ato libidinoso de caráter íntimo.

Trata-se de tipo com múltiplos núcleos sendo, pois, classificado como *tipo misto alternativo* em que o agente pode praticar qualquer dos verbos para que a conduta seja considerada praticada, aos olhos da justiça. Trata-se de delito instantâneo, posto que os verbos denotam o registro e não o armazenamento (que admitiria eventualmente a classificação de crime permanente)[7] ou a disseminação. Falaremos um pouco mais das outras classificações adiante.

Não há dúvida de que o tipo é apenas doloso, não existindo, no caso, o registro de intimidade sexual ou a montagem do mesmo gênero na modalidade culposa. Assim, não se pode praticar o tipo em situação de negligência ou de imprudência.

Dessa forma, alguém que deixasse imprudentemente um aparato gravando e terminasse por registrar tal material, não poderia ser acusado de

7. Em outro sentido está o delito do artigo 241-B da Lei 8.069/90 que fala em "Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente".

tal delito pela ausência de elemento subjetivo. Do mesmo modo aquele que, negligentemente deixasse de desligar um aparelho que tivesse o dever de cuidado de desligar. Como será visto adiante, tal particularidade será objeto de dificuldades probatórias para os órgãos acusatórios, bem como óbice para condenação.

Uma interessante questão está na lógica omissiva. O artigo 13, parágrafo 2º do Código Penal fala que o delito é praticado de forma omissiva do seguinte modo:

> § 2º – A omissão é penalmente relevante quando o omitente devia e podia agir para evitar o resultado. O dever de agir incumbe a quem:
>
> a) tenha por lei obrigação de cuidado, proteção ou vigilância;
>
> b) de outra forma, assumiu a responsabilidade de impedir o resultado;
>
> c) com seu comportamento anterior, criou o risco da ocorrência do resultado.

Nesse sentido, apesar de logicamente poder existir o tipo na modalidade omissiva (comissiva por omissão), parece-nos ilógico que, por exemplo, um segurança responsável pelas câmeras de vigilância, a polícia ou outro profissional que vise garantir o adequado comportamento de pessoas em ruas e ambientes possa ser obrigado a desligar as câmeras que estejam registrando uma nudez ou uma relação sexual em local impróprio visto que não há autorização para tal captura, pela clara colidência de bens jurídicos (segurança *versus* intimidade sexual) e quiçá, uma atipicidade conglobante.

Dessarte, o comportamento da potencial vítima (do art. 216-B, CP) de manter relação sexual ou expor nudez em local público ou local particular vigiado (que informe a condição de estar filmando o ambiente) não poderá servir de pauta para a realização de uma conduta, sob risco de haver grande inversão da lógica do Direito Penal: a conduta da potencial vítima seria *conditio sine qua non* para a realização do núcleo do tipo pelo agente.

Assim, a vitimodogmática deve se pronunciar no sentido de que o comportamento das pessoas registradas que, sabendo ou devendo saber que estão em um ambiente em que há registro de imagens e sons e ainda assim prosseguem com seu intento libidinoso, deve afastar a antijuridicidade a partir do exercício regular de um direito (vigiar patrimônio) ou do estrito cumprimento do dever legal (garantir segurança pública).

No sentido da máxima do processo penal de que a parte que causa a nulidade não pode argui-la, no Direito Penal a vítima (potencial) não pode, nesse caso, alegar ter sido vitimizada se ela mesma se colocou naquela posição.

Afora isso, o ato obsceno de natureza sexual ou libidinosa, previsto no artigo 233 do Código Penal, praticado por alguém diante de câmeras é punível pelas autoridades, que devem registrar tal prática sempre que possível para a garantia de materialidade e autoria delitivas. Possivelmente haverá situações em que essas duas condutas colidirão.

2. QUESTÕES MATERIAIS

2.1. Composição do bem jurídico "dignidade sexual"

Importante destacarmos que o bem jurídico "dignidade sexual" tem sofrido, desde 2009, importantes incrementos do ponto de visto ontológico.

No passado, a sexualidade humana em seus mais diversos aspectos era tratada por *delito contra os costumes*. Então, urgiu-se a necessidade de adaptação e construção da expressão *dignidade sexual*. Mas a informática especialmente trouxe à tona certos aspectos da dignidade sexual que não se idealizaram em 2009.

A exposição pornográfica não consentida na virtualidade configurava delito contra a honra e estava inserida no capítulo V do Código Penal. Hoje, a disseminação não autorizada da intimidade viola a dignidade sexual.

O tipo do artigo 216-B acrescenta a ideia de que registrar a intimidade também viola a dignidade sexual de alguém, assim como fazer montagem inserindo características identificadoras de alguém no intuito (lógico) de macular sua imagem.

Esse incremento, reputamos muito importante. Já há muito defendemos que violações dessa natureza deveriam estar alocadas na questão da violação da dignidade, que é o adjetivo relacionado ao autorespeito, ao amor-próprio e ao respeito que a sociedade dá a alguém.

Aquele que registra sorrateiramente a intimidade de alguém passa a ter consigo um poder injusto sobre o vitimizado. O agente do delito deixa o vitimizado em posição de fragilidade, posto que, em poder de material potencialmente violador de dignidade sexual, pode ameaçar, extorquir, violar a imagem, causar a perda de emprego e assim sucessivamente. Aliás, entendemos que em algum momento futuro o STJ será trazido para modificar o sentido da grave ameaça nesse sentido.

Ao Direito Penal coube enraizar a ideia de que a ninguém está permitido tomar sorrateiramente esse tipo de vantagem desonesta sobre o outro, identificando tal conduta como antijurídica.