I CONGRESSO DE TECNOLOGIAS APLICADAS AO DIREITO

PENAL, PROCESSO PENAL, CRIMINOLOGIA E NOVAS TECNOLOGIAS

P397
Penal, processo penal, criminologia e novas tecnologias [Recurso eletrônico on-line] organização I Congresso de Tecnologias Aplicadas ao Direito – Belo Horizonte;

Coordenadores: Guilherme Augusto Portugal Braga, Enio Luiz de Carvalho Biaggi e Lícia Jocilene das Neves – Belo Horizonte, 2017.

Inclui bibliografia
ISBN: 978-85-5505-663-5
Modo de acesso: www.conpedi.org.br em publicações
Tema: O problema do acesso à justiça e a tecnologia no século XXI

1. Direito. 2. Tecnologia. 3. Direito Penal. 4. Processo Penal. 5. Criminologia. I. I Congresso de Tecnologias Aplicadas ao Direito (1:2018 : Belo Horizonte, BH).

CDU: 34

I CONGRESSO DE TECNOLOGIAS APLICADAS AO DIREITO

PENAL, PROCESSO PENAL, CRIMINOLOGIA E NOVAS TECNOLOGIAS

Apresentação

É com imensa satisfação que apresentamos os trabalhos científicos incluídos nesta publicação, que foram apresentados durante o I Congresso de Tecnologias Aplicadas ao Direito nos dias 14 e 15 de junho de 2018. As atividades ocorreram nas dependências da Escola Superior Dom Helder Câmara, em Belo Horizonte-MG, e tiveram inspiração no tema geral "O problema do acesso à justiça e a tecnologia no século XXI".

O evento foi uma realização do Programa RECAJ-UFMG – Solução de Conflitos e Acesso à Justiça da Faculdade de Direito da UFMG em parceria com o Direito Integral da Escola Superior Dom Helder Câmara. Foram apoiadores: o Conselho Nacional de Pesquisa e Pós-graduação em Direito - CONPEDI, EMGE – Escola de Engenharia, a Escola Judicial do Tribunal Regional do Trabalho da 3ª Região, a Federação Nacional dos Pós-graduandos em Direito – FEPODI e o Projeto Startup Dom.

A apresentação dos trabalhos abriu caminho para uma importante discussão, em que os pesquisadores do Direito, oriundos de dez Estados diferentes da Federação, puderam interagir em torno de questões teóricas e práticas, levando-se em consideração a temática central do grupo. Foram debatidos os desafios que as linhas de pesquisa enfrentam no tocante ao estudo do Direito e sua relação com a tecnologia nas mais diversas searas jurídicas.

Na coletânea que agora vem a público, encontram-se os resultados de pesquisas desenvolvidas em diversos Programas de Pós-graduação em Direito, nos níveis de Mestrado e Doutorado, e, principalmente, pesquisas oriundas dos programas de iniciação científica, isto é, trabalhos realizados por graduandos em Direito e seus orientadores. Os trabalhos foram rigorosamente selecionados, por meio de dupla avaliação cega por pares no sistema eletrônico desenvolvido pelo CONPEDI. Desta forma, estão inseridos no universo das 350 (trezentas e cinquenta) pesquisas do evento ora publicadas, que guardam sintonia direta com este Grupo de Trabalho.

Agradecemos a todos os pesquisadores pela sua inestimável colaboração e desejamos uma ótima e proveitosa leitura!

CRIME CIBERNÉTICO COMO CRIME PERMANENTE: COMENTÁRIOS SOBRE O PROJETO DE LEI Nº 5.463/2016

CYBERCRIME AS A PERMANENT CRIME: COMMENTS ON LAW PROJECT Nº 5.463/2016

Felipe Otávio Moraes Alves [1]
Gustavo Lelles de Menezes [2]

Resumo

O objetivo do presente estudo é analisar o Projeto de Lei nº 5.463 de 2016, problematizando a inclusão na previsão de flagrante em infrações permanentes, os crimes cibernéticos cuja consumação se estendam no tempo. Buscar-se-á identificar se esta ou outras possíveis respostas – judiciais, legislativas ou executivas – são legítimas e eficazes, a fim de concretizar os preceitos da liberdade e privacidade na proteção ao usuário. Indaga-se a incidência da desnecessariedade de mandado judicial na busca e apreensão dos aparelhos dos cibercriminosos em flagrante delito. Adota-se, como método de procedimento, a pesquisa bibliográfica e, como método de abordagem, o dedutivo.

Palavras-chave: Cibercrime, Crime permanente, Internet, Mandado judicial, Direitos fundamentais

Abstract/Resumen/Résumé

The objective of the present study is to analyze the Project Law nº 5.463 of 2016, problematizing the inclusion in flagrant in permanent infractions, the cybercrimes whose consummation extends over time. It will be sought to identify if this or other possible answers are legit and effective, respecting the precepts of freedom and privacy by protecting the users. The incidence of the unnecessary judicial warrant is sought in the search and seizure of the devices of cybercriminals in flagrant crime. Are adopted, as a method of procedure, the bibliographical research and, as a method of approach, the deductive method.

Keywords/Palabras-claves/Mots-clés: Cybercrime, Permanent crime, Internet, Court order, Fundamental rights

---

[1] Bacharel em Direito pela UFG. Mestrando em Direito pela UNESP. Pesquisador pela UNESP em Direito Digital, correlacionando tecnologia, principalmente a Internet, ao Direito, nos problemas de violação dos direitos fundamentais

[2] Bacharel e Mestrando em Direito pela UNESP. Pesquisador pela UNESP em Direito Penal, nos problemas de violação dos direitos fundamentais

1 INTRODUÇÃO

Cada vez mais, a internet tem sido meio para condutas criminosas, sendo de mister importância a manutenção do Código Penal e do Código Processual Penal a fim de adequarem-se a essa nova tecnologia. Infelizmente, pela conduta do sujeito ativo dos delitos virtuais ser geralmente indireta, anônima e permanente, produzindo efeitos similares, ou até mais expressivos, que ações criminosas perpetradas no mundo não virtual, ainda há uma clara ineficácia do ordenamento jurídico e dos aparatos estatais de investigação policial em alcançar os cibercrimes.

Nesse sentido, se insere o Projeto de Lei nº 5.463 de 2016 que busca adaptar o instituto do flagrante à realidade da internet. Tal alteração legislativa, objetiva incluir dentro da previsão da prisão em flagrante no caso de infrações permanentes, constante no art. 303 do CPP, os crimes cibernéticos cuja consumação se estendam no tempo, seja pela permanência da publicação original em determinado sítio eletrônico, seja pela disseminação e replicação do conteúdo delituoso na rede mundial de computadores, ainda que haja exclusão, posterior ao flagrante, do conteúdo (ALVES, 2016). Assim, o flagrante digital realizar-se-ia quando se descobrisse, por investigação, a localização do suspeito através do endereço de *Internet Protocol*, ou qualquer outro meio de identificação de localidade da perpetração do crime, bastando a evidência de que o conteúdo ou ação delituosa ainda esteja disponível, de alguma forma, na internet.

Dessa forma, o advento de alterações legislativas que classifiquem os cibercrimes como delitos permanentes, resultaria em benefícios aos procedimentos investigativos tanto do Ministério Público quanto da polícia investigativa responsável. Por isso, deve ser discutido no presente estudo a legitimidade e benefícios mas também malefícios do enquadramento dos cibercrimes como delitos permanentes, a fim de elucidar as nuances de tal temática com vistas encontrar um meio termo na solução dos litígios sem abuso policial.

2 OBJETIVOS

Como objetivo geral, o trabalho busca problematizar e solucionar o problema central, sendo ele encontrar até que ponto deve o Direito ser eficaz, trazendo segurança às vítimas de cibercrimes, em detrimento de certas garantias jurídicas do acusado, ou seja, problematizar o Projeto de Lei nº 5.463/2016 que regulamenta o cibercriminoso como autor de crime permanente passível de prisão em flagrante delito. E como objetivos específicos, temos: a

análise da situação atual dos cibercrime, através da tecnologia – mais especificamente a Internet – e dos seus principais agentes sociais, econômicos e políticos envolvidos no meio cibernético, bem como seus respectivos interesses e lógicas de atuação; compreensão da realidade a partir da atuação do Estado; estudar a literatura, em geral, que trate destas novas formas de crimes e entender a relação entre a crime permanente e o cibercrime; fundamentar os critérios para as devidas adequações legislativas dos conflitos de direitos fundamentais, como a dignidade da pessoa humana, a partir do exame da legislação constitucional e infraconstitucional e críticas à regulamentação estatal.

3 METODOLOGIA

Para a construção deste presente estudo, é adotado o método teórico-dedutivo, com respaldo aos institutos e fundamentos da dignidade da pessoa humana, direito à liberdade e privacidade. As perguntas, a serem solucionadas durante o trabalho, são elucidadas com apoio de doutrinadores e pesquisadores e, mais ainda, de especialistas na área penal e digital, com comparações internacionais por doutrina, jurisprudência e legislação. O referencial teórico, consoante ao crime permanente, que deverá ser utilizado no decorrer do trabalho será o de Guilherme de Souza Nucci.

4 DESENVOLVIMENTO

Segundo o Código Penal, crime permanente é aquele de momento consumativo estendido temporalmente por domínio do criminoso sobre o momento de consumação do crime, já que o começo da execução incidiria em crime. Por exemplo, o crime de possuir pornografia infantil tem caráter permanente. O grande benefício para o processo investigativo deste tipo penal é a possibilidade da prisão em flagrante, ainda mais cabível pelo alcance da conduta criminosa em nível internacional, pela característica singular da internet, tratando-se na maioria das vezes de um crime plurilocal e à distância. Segundo Renato Lima (2013), crimes plurilocais são aqueles de cunho penal com ação e resultado ocorrendo em locais diferentes. E crimes à distância são infrações penais as quais acontecem dentro do Brasil mas o resultado se materializa no estrangeiro, ou vice-versa. Ademais, a determinação da competência prevista no artigo 70 do CPP, em caso de crime permanente, estará firmada pela prevenção, pelo art. 71 (CAPEZ, 2012).

Assim, o supracitado Projeto de Lei nº 5.463 de 2016 visa acrescentar aos §§ 1º e 2º ao art. 303 do CPP o denominado "flagrante digital", que estabelece como infração permanente delito cibernético de conteúdo permanente na internet (ALVES, 2016, p. 1):

> § 1º. Considera-se, também, como infração permanente o crime cibernético cujo conteúdo permaneça na internet, ainda que excluída a publicação original, mas, em razão de sua disseminação ou de qualquer outro motivo determinante, tenha havido a replicação e a permanência do conteúdo delituoso na rede mundial de computadores.
> § 2º Entende-se o agente em flagrante delito enquanto houver a permanência do conteúdo delituoso na internet, nos termos do parágrafo anterior. Art. 3° - Esta lei entra em vigor na data de sua publicação.

O deputado Roberto Alves (2016), autor do referido projeto de lei, fê-lo a fim de combater a disseminação da violência em redes de compartilhamento de vídeos na internet e aplicativos para telefonia móvel, após se sensibilizar com o caso de menor de 16 anos que teve imagens de violência sexual transmitidas nas redes sociais. Esta possiblidade de incidência do flagrante deverá alertar usuários a terem mais cuidado com o compartilhamento de conteúdo na internet, bastando a evidência de que o conteúdo ainda esteja disponível na internet; coibindo, por exemplo, o *cyberbulling*.

O crime permanente tem momento consumativo que se prolonga no tempo. Ou seja, a consumação continua ocorrendo enquanto perdurar o delito, como exemplo ao: portar conteúdo digital ilícito, manter conteúdo postado em rede sem permissão dos envolvidos, privar alguém de seu direito de liberdade e privacidade ou ocultar conteúdo protegido por força de lei. Esta associação se dá principalmente em relação aos crimes puros. Nisto, Guilherme Nucci (2014, p. 117) comenta que:

> Para identificação do crime permanente, oferece a doutrina duas regras: a) o bem jurídico afetado é imaterial (ex. saúde pública, liberdade individual etc.); b) normalmente é realizado em duas fases, a primeira, comissiva, e a segunda, omissiva (sequestra-se a pessoa através de uma ação, mantendo-a no cativeiro por omissão). Essas regras não são absolutas, comportando exceções.

E é neste momento que observamos justamente a possibilidade de aplicação do cibercrime como crime permanente. Vejamos que o bem jurídico, na maioria das vezes, será algum bem imaterial da pessoa, ferirá sua liberdade e em muitas vezes também a sua privacidade. E observa-se, em muitos casos, também as duas fases, já que o crime consolida-se em um momento através da ação do hacker ou quando o sujeito ativo do delito virtual divulga e mantém conteúdo ilícito, e em momento permanente posterior há a ação de atuação permanente e ilícita pelo meio virtual até eventual descobrimento da invasão, até o hacker tiver extraído todos benefícios de sua vítima ou descobrimento tardio da vítima do vazamento do seu

conteúdo privado.

A comparação torna-se ainda mais devida porque um dos núcleos do cibercrime é igualmente observável. Para o autor supramencionado, crimes permanentes seriam "aqueles que se consumam com uma única conduta, embora a situação antijurídica gerada se prolongue no tempo até quando queira o agente" (NUCCI, 2014, p. 117). Para Damásio Jesus (2009, p. 189-190), os crimes permanentes "são os que causam uma situação danosa ou perigosa que se prolonga no tempo. O momento consumativo se protrai no tempo, como diz a doutrina". Já para o professor Cézar Bitencourt (2010, p. 253-254), o "crime permanente é aquele crime cuja consumação se alonga no tempo, dependente da atividade do agente, que poderá cessar quando este quiser (cárcere privado e sequestro)."

De qualquer maneira, a base do conceito do crime permanente passa a ser a execução do fato típico e não, simplesmente, sua consumação, pois nos crimes instantâneos de efeitos permanentes – como ensina a doutrina – a consumação também se prolonga no tempo. Ora, os crimes permanentes são aqueles que quando consumados sua execução é realizada permanentemente pela vontade do agente ativo, no caso o hacker ou divulgador de conteúdo ilícito, como se fosse um ciclo de novas condutas com novos resultados, chegando a novas consumações, de forma contínua, e não uma só conduta com sua consumação prolongada no tempo. A distinção é importante pois haveria discussões sobre a aplicação da súmula 711 do Supremo Tribunal Federal, de aplicação da lei penal mais grave sobre o crime permanente.

E porque a comparação é importante? Pois para crimes permanentes, a busca e apreensão sem mandado judicial é possível em flagrante permanente. Além do novo efeito investigativo em si, do próprio flagrante delito auxiliar no combate a este supramencionado crime, haveria esta nova consequência jurídica. Tratando-se justamente de uma das soluções necessárias ao combate aos cibercrimes. Já que no caso de flagrante de crime permanente, é possível o combate mais célere com a realização de busca e apreensão sem mandado judicial, além da preocupação jurídica de cessá-lo imediatamente. Nesse caso, não se pode falar em ilicitude das provas obtidas. Isso porque, no caso de crime permanente, o momento consumativo do delito está sempre em execução. Que se trata da mesma lógica para os cibercrimes. Afinal, o momento consumativo do ato ilícito da prática de *hacking* ou divulgação de conteúdo ilícito na Internet está também sempre em execução, levando risco a sociedade em geral, e ao obter-se a informação de seu ato o crime está sendo praticado, ou seja, há o flagrante de crime permanente.

Em 2015, a decisão do STF no RE 603.616 discutiu se e quando policiais podem adentrar domicílios sem mandado judicial com o fito de buscar e apreender droga. Em síntese,

o STF definiu que o ingresso forçado em domicílios sem mandado judicial apenas se revela legítimo quando tiver suporte em razões devidamente justificadas pelas circunstâncias que indiquem que no interior da residência esteja a ocorrer situação de flagrante delito. A ilicitude do ingresso forçado na esfera domiciliar tem sido afastada pelo fato de que o tráfico de drogas (ou a posse de arma) configuram crime permanente, quando evidenciado o estado de flagrância. A princípio, estas razões devidamente justificadas têm de ser legitimamente evidenciadas; por não enxergar esses requisitos, no HC 138.565 em 2017, a 2ª Turma do Supremo Tribunal Federal concedeu *Habeas Corpus* para trancar ação penal contra um homem que teve sua residência vasculhada por policiais civis sem ordem da Justiça, encontrando drogas na residência. Ou seja, é uma incidência de flagrante a ser aplicada com a devida diligência.

Jéssica Picolo (2016) trata bem das características juridicamente relevantes do meio cibernético: a transnacionalidade, a deslocalização e a repetição automática. Esta a última é importante para julgarmos ser essa característica que torna o ato criminoso pela internet permanente, pois uma vez que instalado programa malicioso ou alterados os dados ou compartilhado conteúdo ilícito, a cada novo acesso no computador ou ao conteúdo compartilhado a ação criminosa é reiterada.

Assim, a possibilidade do flagrante delito poderia tornar desnecessária a ordem judicial, no caso de análise pela inviolabilidade e sigilo das comunicações do acusado pela Internet. Ora, como supramencionado, o problema da prova no meio informático é que ela é muito volátil. A investigação é mais complexa, porque envolve um caminho longo. É preciso preservar a prova para que ela se torne idônea. Para isso é necessário obter o endereço IP, que é a identidade virtual. Na maioria das vezes precisa-se recorrer à justiça para que o provedor forneça o IP, todo o processo é delongado, fazendo com que na maioria das vezes a vítima desista de procurar a polícia.

A busca e apreensão é medida coercitiva institucionalizada – procedida pelo próprio Estado – e que, naturalmente, violam direitos constitucionais, mas dentro dos próprios limites impostos pela Constituição Federal e legislação infraconstitucional. E por atingirem a liberdade individual do investigado, o emprego há de ser procedido com especial cuidado, devendo a autoridade violar o menos possível os direitos do indivíduo, no momento do cumprimento da diligência, agindo nada além do necessário para alcançar os fins perseguidos na persecução penal. Neste sentido, Cleunice Pitombo (2005, p. 91) já explicitava que "[...] o direito fundamental apenas poderá sofrer diminuição dentro da estrita legalidade", necessitando ter fins legítimos e justificativa socialmente relevante. O que é o caso quando a Polícia Federal investiga um cibercriminoso.

Nos Estados Unidos, a título de exemplo, as agências fiscalizadoras podem renunciar à permissão de um juiz local se um agente federal acredita provas criminais está prestes a ser destruído (NAKED SECURITY, 2015). O que é justamente o caso do hacker ou até do compartilhador de conteúdo ilícito, já que as evidências quase sempre estão na iminência de serem destruídas pelos mesmos, principalmente ao serem avisados ou souberem da Busca e Apreensão. E estes onerosos mandados de Busca e Apreensão, neste contexto, transformam os poucos casos de possíveis capturas de informações de cibercriminosos praticamente impossível.

Toda vez que o Estado deixa de dar uma resposta célere, especialmente em serviços essenciais também fere o direito fundamental dos indivíduos, pois, diminui no caso em questão, o acesso à segurança do usuário, deixa de administrar recursos de forma adequada – pela ineficácia de investigação desta espécie, enfim, trará prejuízo para a investigação, com prejuízo para a sociedade como um todo, cada dia mais exposta à crescente comunidade delinquente e irresponsável que têm sensação de impunidade por seus crimes cibernéticos.

A celeridade é o elemento mais importante na ação policial no meio virtual, em que a necessidade de ordem judicial e a não incidência do flagrante delito nestes crimes permanentes atrapalham rigorosamente este crucial elemento.

5 CONCLUSÃO

Dentro das hipóteses cabíveis, o estudo conclui que é legítimo ao Estado proteger as os direitos das vítimas de cibercrimes; todavia, é dever do Estado preservar a Internet como uma plataforma aberta, sem engessamentos por excesso de normas, devendo ter interferências mínimas mas pontualmente eficazes para solucionar e remediar os cibercrimes. Enseja-se aos cibercrimes os benefícios de um crime permanente, já que o bem jurídico na maioria das vezes será algum bem imaterial da pessoa, ferirá sua liberdade e em muitas vezes também a sua privacidade. Utilizando-se do Direito Comparado, conclui-se pela necessária efetividade das diretrizes doutrinárias para que a jurisprudência interna possa se embasar, complementarmente à lei. Pelas características singulares dos meios tecnológicos, mais especificamente da Internet, se observa a necessidade de uma real coercibilidade de normas visando a diminuição de práticas lesivas ao usuário. Com transparência, finalidade legítima e proporcionalidade, busca encontra-se a maximização dos efeitos positivos de uma liberdade de expressão e privacidade, com os devidos critérios para implicar o flagrante, e minimização dos efeitos negativos de violações dos cibercriminosos, como a associação do delito cibernético como crime permanente. E, por

causa das características singulares da Internet, certos direitos do cibercriminoso devem e podem ser afetados, como bem permite intrinsicamente o flagrante delito.

6 REFERÊNCIAS

ALVES, Roberto. Projeto de Lei nº 5463 de 2016. 01/06/2016. Acrescenta ao Código de Processo Penal o denominado "flagrante digital", que estabelece como infração permanente o delito cibernético. **Diário do Congresso Nacional**, Brasília, DF, 1 jun. 2016.

BITENCOURT, Cézar Roberto. **Tratado de Direito Penal**. São Paulo: Saraiva, 2010. p. 253-254.

CAPEZ, Fernando. **Curso de Processo Penal**. 19 ed. São Paulo: Saraiva, 2012. p. 277.

CARDOSO, Ismael. **Delegado da PF critica Marco Civil da Internet: "o crime agradece"**. 2012. Sem numeração. Disponível em: <https://tecnologia.terra.com.br/internet/delegado-da-pf-critica-marco-civil-da-internet-o-crime-agradece,e8dbfe32cdbda310VgnCLD200000bbcceb0aRCRD.html>. Acesso em: 20 abr. 2018.

JESUS, Damásio E. de. **Direito Penal**. 1 v. São Paulo: Saraiva, 2009. p. 189-190.

LIMA, Renato Brasileiro de. **Curso de Processo Penal**. Niterói: Impetus, 2013. p. 496.

NAKED SECURITY. **A aplicação da lei dos Estados Unidos precisa agora de um mandado de usar arraias.** Sem numeração. Disponível em: <https://nakedsecurity.sophos.com/pt/2015/09/04/us-law-enforcement-now-need-a-warrant-to-use-stingrays/>. Acesso em: 20 abr. 2018.

NUCCI, Guilherme de Souza. **Código Penal Comentado**. 14 ed. São Paulo: Editora Revista dos Tribunais, 2014.

_____. **Manual de direito penal**. 6 ed. São Paulo: Revista dos Tribunais, 2009.

PICOLO, Jessica de Freitas. Criminologia em torno do crime cibernético. In: **Âmbito Jurídico**, Rio Grande, XIX, n. 154, nov. 2016. Disponível em: <http://www.ambitojuridico.com.br/site/index.php/Paulo%20Leandro%20Maia?n_link=revista_artigos_leitura&artigo_id=18112>. Acesso em: 20 abr. 2018.

PITOMBO, Cleunice A. **Da Busca e da Apreensão no Processo Penal**. 2. ed. São Paulo: Revista dos Tribunais, 2005. p. 91.