II CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL

DIREITO PENAL E CIBERCRIMES

D597
Direito Penal e Cibercrimes [Recurso eletrônico on-line] organização Congresso Internacional de Direito e Inteligência Artificial: Skema Business School – Belo Horizonte;

Coordenadores: Fernando Henrique da Silva Horita; Fausto Santos de Morais; Camila Martins de Oliveira. – Belo Horizonte:Skema Business School, 2021.

Inclui bibliografia
ISBN: 978-65-5648-263-7
Modo de acesso: www.conpedi.org.br
Tema: Um olhar do Direito sobre a Tecnologia

1. Direito. 2. Inteligência Artificial. 3. Tecnologia. II. Congresso Internacional de Direito e Inteligência Artificial (1:2021 : Belo Horizonte, MG).

CDU: 34

II CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL

DIREITO PENAL E CIBERCRIMES

Apresentação

Renovando o compromisso assumido com os pesquisadores de Direito e tecnologia do Brasil, é com grande satisfação que a SKEMA Business School e o CONPEDI – Conselho Nacional de Pesquisa e Pós-graduação em Direito apresentam à comunidade científica os 12 livros produzidos a partir dos Grupos de Trabalho do II Congresso Internacional de Direito e Inteligência Artificial (II CIDIA). As discussões ocorreram em ambiente virtual ao longo dos dias 27 e 28 de maio de 2021, dentro da programação que contou com grandes nomes nacionais e internacionais da área em cinco painéis temáticos e o SKEMA Dialogue, além de 354 inscritos no total. Continuamos a promover aquele que é, pelo segundo ano, o maior evento científico de Direito e Tecnologia do Brasil.

Trata-se de coletânea composta pelos 255 trabalhos aprovados e que atingiram nota mínima de aprovação, sendo que também foram submetidos ao processo denominado double blind peer review (dupla avaliação cega por pares) dentro da plataforma PublicaDireito, que é mantida pelo CONPEDI. Os oito Grupos de Trabalho originais, diante da grande demanda, se transformaram em doze e contaram com a participação de pesquisadores de vinte e um Estados da federação brasileira e do Distrito Federal. São cerca de 1.700 páginas de produção científica relacionadas ao que há de mais novo e relevante em termos de discussão acadêmica sobre a relação da inteligência artificial e da tecnologia com os temas acesso à justiça, Direitos Humanos, proteção de dados, relações de trabalho, Administração Pública, meio ambiente, formas de solução de conflitos, Direito Penal e responsabilidade civil.

Os referidos Grupos de Trabalho contaram, ainda, com a contribuição de 36 proeminentes professoras e professores ligados a renomadas instituições de ensino superior do país, os quais indicaram os caminhos para o aperfeiçoamento dos trabalhos dos autores. Cada livro desta coletânea foi organizado, preparado e assinado pelos professores que coordenaram cada grupo. Sem dúvida, houve uma troca intensa de saberes e a produção de conhecimento de alto nível foi, mais uma vez, o grande legado do evento.

Neste norte, a coletânea que ora torna-se pública é de inegável valor científico. Pretende-se, com esta publicação, contribuir com a ciência jurídica e fomentar o aprofundamento da relação entre a graduação e a pós-graduação, seguindo as diretrizes oficiais. Fomentou-se, ainda, a formação de novos pesquisadores na seara interdisciplinar entre o Direito e os vários

campos da tecnologia, notadamente o da ciência da informação, haja vista o expressivo número de graduandos que participaram efetivamente, com o devido protagonismo, das atividades.

A SKEMA Business School é entidade francesa sem fins lucrativos, com estrutura multicampi em cinco países de continentes diferentes (França, EUA, China, Brasil e África do Sul) e com três importantes acreditações internacionais (AMBA, EQUIS e AACSB), que demonstram sua vocação para pesquisa de excelência no universo da economia do conhecimento. A SKEMA acredita, mais do que nunca, que um mundo digital necessita de uma abordagem transdisciplinar.

Agradecemos a participação de todos neste grandioso evento e convidamos a comunidade científica a conhecer nossos projetos no campo do Direito e da tecnologia. Já está em funcionamento o projeto Nanodegrees, um conjunto de cursos práticos e avançados, de curta duração, acessíveis aos estudantes tanto de graduação, quanto de pós-graduação. Em breve, será lançada a pioneira pós-graduação lato sensu de Direito e Inteligência Artificial, com destacados professores da área. A SKEMA estrutura, ainda, um grupo de pesquisa em Direito e Inteligência Artificial e planeja o lançamento de um periódico científico sobre o tema.

Agradecemos ainda a todas as pesquisadoras e pesquisadores pela inestimável contribuição e desejamos a todos uma ótima e proveitosa leitura!

Belo Horizonte-MG, 09 de junho de 2021.

Profª. Drª. Geneviève Daniele Lucienne Dutrait Poulingue

Reitora – SKEMA Business School - Campus Belo Horizonte

Prof. Dr. Edgar Gastón Jacobs Flores Filho

Coordenador dos Projetos de Direito da SKEMA Business School

DAS FERRAMENTAS TECNOLÓGICAS ÀS IMPOSSIBILIDADES PREDITIVAS QUANTO AOS CRIMES DIGITAIS

FROM TECHNOLOGICAL TOOLS TO PREDICTIVE IMPOSSIBILITIES AS TO DIGITAL CRIMES

Juliana Popolin Beretta [1]
Mauricio De Thomazi Oliveira Guedes [2]

Resumo

O advento das tecnologias trouxe aos criminosos uma nova ferramenta para a prática do cometimento de delitos. Nesse contexto, o presente trabalho apresenta dois pontos de vista: (i) expõe como a tecnologia pode ser utilizada em favor das investigações; e (ii) revela a dificuldade existente em predizer os crimes cibernéticos. Para tanto, aborda as transformações vivenciadas desde a Primeira Revolução Industrial até o momento presente, denominado de Indústria 4.0. Por fim, analisa, por meio de doutrinas e artigos, a natureza da Polícia Judiciária como sendo um órgão reativo, bem como a impossibilidade de atuação futura na repressão de crimes cibernéticos.

Palavras-chave: Direito penal, Policiamento preditivo, Crimes cibernéticos

Abstract/Resumen/Résumé

The advent of technologies has brought criminals a new tool for committing crimes. In this context, the current study presents two points of view: (i) it exposes how technology can be used in favor of investigations; and (ii) it reveals the existing difficulty in predicting cybercrimes. For this purpose, it addresses the transformations experienced from the First Industrial Revolution to the present moment, named Industry 4.0. Finally, it analyzes, by means of doctrines and articles, the nature of the Judiciary Police as being a reactive department, as well as the impossibility of future action in the repression of cybercrimes.

Keywords/Palabras-claves/Mots-clés: Criminal law, Predictive policing, Cybercrimes

[1] Graduanda no 4° ano de Direito pela Universidade Estadual de Londrina. (UEL0) Vinculada ao projeto de pesquisa sobre Policiamento Preditivo da Universidade Presbiteriana Mackenzie.

[2] Delegado de Polícia do Estado de São Paulo. Mestrando em Gestão e Políticas Públicas pela FVG. Vinculado ao grupo de pesquisa sobre Policiamento Preditivo da Universidade Presbiteriana Mackenzie.

1 INTRODUÇÃO

O processo civilizatório passou por grandes transformações ao longo dos anos. A evolução tecnológica e digital não foi diferente. A chamada Primeira Revolução Industrial, que ocorreu na Inglaterra entre os anos de 1760 e 1840, tem papel fundamental no início desse processo de evolução tecnológica e possibilitou à sociedade o desenvolvimento dos processos produtivos e das relações de trabalho.

Com o fim da Segunda Guerra Mundial, entre o final do século XIX e início do século XX, ocorreu a chamada Segunda Revolução Industrial, período no qual ocorreu a expansão do processo de industrialização da Inglaterra para outros países, entre eles França, Estados Unidos e Japão. Nesse período, houve um aprimoramento das indústrias elétricas e químicas, fomentando, assim, a produção em massa graças à eletricidade.

No início da década de 1960 houve a chamada Terceira Revolução Industrial, marcada pelo advento da computação e tecnologia digital, cujo objetivo principal era maior produção em menos tempo.

Atualmente o mundo experimenta a chamada Quarta Revolução Industrial, mais conhecida como Indústria 4.0, com grande desenvolvimento da *internet*, robótica, inteligência artificial e maior conexão global entre as pessoas. Novos produtos e serviços foram introduzidos no mercado como, por exemplo, a chamada "tecnologia disruptiva", responsável pelas novidades em uma ordem já existente, como a Netflix, Ifood, WhatsApp e Uber (FIGUEIREDO JÚNIOR, 2020, p. 122-123).

Nesse período nasceram os chamados "nativos digitais", indivíduos que desde os primeiros anos de vida já estão conectados aos meios eletrônicos, desenvolvendo assim grande habilidade na utilização dessa nova linguagem. Do outro lado estão os "imigrantes digitais", nascidos antes do advento da *internet*, que apresentam dificuldade de utilização dessas novas tecnologias e, portanto, demandam um processo de aprendizagem e de adaptação (FAVERO, 2021, p. 63-64).

2 OBJETIVOS E METODOLOGIA

O presente trabalho tem por objetivo destacar a importância do tema diante do vasto compartilhamento de dados no mundo contemporâneo e o consequente surgimento de novos delitos no ciberespaço, de modo a exigir o estudo da tutela penal específica ao tema. Além disso,

esse estudo analisa a possiblidade de se antever os espaços em que o crime cibernético pode acontecer.

Já no tocante à metodologia utilizada para desenvolver as molduras desta pesquisa, foram consideradas as doutrinas que abordam a matéria e a estrutura da Polícia Judiciária que é, em sua essência, um órgão de reação, tratando-se de uma pesquisa descritiva.

3 DESENVOLVIMENTO DA PESQUISA

O advento das novas tecnologias digitais, com sua arquitetura de negócios peculiar que prescinde o contato físico para a realização das transações, fez surgir o chamado "ciberespaço", que possibilita a interação das pessoas e a constituição de relações comerciais e sociais sem qualquer delimitação geográfica, o que inclui o acesso e pressupõe a troca, cada vez maior, de diversas informações.

Ao mesmo tempo, novos espaços virtuais constituem em um novo ambiente, não só para a circulação de informações, mas também para a circulação de riqueza na forma de moeda virtual, criando assim palco e novas possibilidades para o surgimento de fenômenos criminais em massa.

Se por um lado as plataformas eletrônicas são verdadeiras cidades e praças digitais onde circula a riqueza mediante o comércio virtual, transferência de valores e troca de informações, esse mesmo ambiente serve como cenário para uma nova espécie de crimes, denominados "crimes digitais".

Portanto, os chamados crimes digitais consistem, na realidade, no grupo heterogêneo de atividades criminosas que engloba uma série de diferentes tipos criminais, alguns contra o patrimônio ou financeiros, outros contra a dignidade sexual ou a honra. Todos esses tipos criminais, contudo, exibem a mesma característica, que é a imprescindibilidade dos meios digitais (JUSTIFICANDO, 2018, online).

Uma análise detida da cronologia dos delitos digitais, assim delimitados, revela inicialmente sua compartimentação em três fases distintas: (i) primeira geração, em que os computadores são utilizados como instrumento para a prática do crime que, sem o computador, não seria possível; (ii) segunda geração, a dos crimes híbridos, em que os criminosos se utilizam do computador para praticar delitos já existentes; e (iii) terceira geração, em que há os "crimes *stricto sensu*", ou seja, crimes que só existem em razão da *internet* (LEITÃO JUNIOR, 2020, p. 208 e 209).

Além disso, os crimes cibernéticos podem ser divididos em duas classificações, quais sejam: (i) crimes digitais próprios ou puros, os quais ameaçam bens informáticos; e (ii) crimes digitais impróprios ou mistos, aqueles que atingem bens jurídicos tutelados pela própria lei (MARCELO XAVIER DE FREIRAS CRESPO, 2017, p. 416).

Nesse contexto, o novo cenário formado pelo advento da *internet* desencadeou situações inéditas que o Direito Penal ainda procura alcançar, regulamentando o dever objetivo de cuidado no ambiente virtual.

A arquitetura das redes sociais estimula o usuário à exposição de sua rotina, hábitos de consumo, dados pessoais, vida privada e convicções ideológicas, construindo um conjunto cada vez mais rico e detalhado de informações.

Como o modelo de negócio adotado pelas empresas controladoras das redes sociais é exatamente a utilização do acervo construído como ferramenta de inteligência de mercado, o usuário das redes passa a ser o verdadeiro produto comercializado. Assim sendo, é constantemente estimulado a se expor na rede sem qualquer cuidado ou preocupação com os riscos associados.

Naturalmente, a atividade criminosa encontra facilidades na ausência de limites bem estabelecidos no mundo informático e alimenta uma tecnologia criminosa, dispondo desse manancial de informações que possibilita uma série de novas modalidades criminosas. Não obstante, no mundo ideal, seria esperado que a tutela penal acompanhasse essa evolução, entretanto, analisando o comportamento dos mais diversos modelos de reação legal e esse novo fenômeno, constata-se que "o nosso Direito Penal claudica, num passo cansado, falto de fôlego, longe de poder sincronizar a velocidade de caminhada com a evolução cultural humana (que não se pode antever onde findará" (FAVERO, 2021, p. 12).

Apesar desse descompasso entre as novas tecnologias e a tutela penal, o campo da Segurança Pública não pode se omitir diante da atividade cada vez mais especializada dos criminosos, exigindo-se dela a atualização de seus métodos de atuação, o planejamento e a execução de políticas eficientes em resposta aos novos crimes da era digital. Em essência, a segurança é um direito fundamental e deve ser assegurado mediante ações efetivas de defesa, proteção social e proteção perante terceiros (FABRETTI, 2014, p. 113). Assim, a revisão e o aperfeiçoamento da tutela penal no campo cibernético passam a ter extrema importância, tendo em vista a exposição dos bens jurídicos tutelados no meio digital.

A Polícia Judiciária, que é essencialmente reativa pela natureza de sua atividade, já utiliza ferramentas digitais como forma de enfrentamento ao crime digital, tais como a

infiltração virtual de agentes, “geolocalização” por meio dados de estação rádio base e *softwares*, capazes de recuperar conversas enviadas nos aplicativos dos celulares.

Contudo, se por um lado os criminosos viram, no ambiente digital, um espaço para expandir suas práticas delituosas, por outro lado a força policial encontrou um novo meio para diligenciar e planear a obtenção de provas que podem auxiliar na identificação de criminosos (SILVA, 2020, p. 190).

Apesar dos vários desafios na condução de uma investigação criminal pelos meios digitais, quais sejam, a falta de investimento, a deficiência da estrutura policial e o aumento do volume de dados a serem analisados pelos policiais em tempo exíguo, a grande vantagem da obtenção de provas pelo meio digital é a garantia de sua integridade e, consequentemente, a segurança na sua utilização.

A garantia da integridade do material coletado durante a investigação exige cuidados para a efetividade e adequação da aplicação da cadeia de custódia da prova digital, ou seja, “o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte” (artigo 158-A, *caput*, do Código de Processo Penal). Em termos processuais, apesar de o mencionado artigo não ter mencionado a prova digital, sua aplicação é possível diante da analogia autorizada pelo Direito Processual Penal, no artigo 3° do referido diploma legal.

Assim, superado o desafio da coleta e da autorização processual para a utilização da prova digital, outra preocupação emerge, qual seja, a implementação de uma inteligência policial capaz de sistematizar o fluxo de informações e integrar os vestígios e fragmentos levantados no meio digital.

Nesse contexto, há três formas de prevenir os delitos digitais: a primeira diz respeito ao combate à cogitação delitiva, mediante a educação e abordagem dos aspectos intrínsecos à prática dos delitos; a segunda recai sobre uma análise da sociedade para se identificar o tempo e o espaço nos quais esses crimes são passíveis de ocorrer; e a terceira, tradicionalmente conhecida como repressão estatal, que é atuação direta depois da prática delitiva (SYDOW, 2020, p. 640 e 641).

Entretanto, em todas as hipóteses mencionadas, no ambiente atual dificilmente se conseguiria aplicar a predição da prática desse tipo de delito. O delito informático não apresenta um padrão estruturado enquanto fenômeno criminal, fugindo da forma tradicional do delito tal qual costuma se apresentar na sociedade. Essa particularidade cria dificuldades adicionais para os juristas adequarem a lógica do Direito Penal ao desafio de estruturar uma atividade preditiva.

4 CONCLUSÃO

O problema de predição criminal se fundamenta nos próprios cânones do Estado Democrático de Direito e nos fins do Direito Penal e da pena. A possibilidade de imposição de uma pena criminal fundamenta-se na ideia de que a intervenção estatal pode recuperar o criminoso prevenindo a ocorrência de novos crimes.

A sistemática do direito penal e da investigação criminal, portanto, parte do pressuposto do efetivo cometimento do crime. Esse raciocínio impacta todos os institutos penais de forma fundamental, inclusive o próprio conceito de crime, uma vez que exige a efetiva prática dos atos executórios do crime, na sua tipicidade.

Nesse contexto, o movimento de predição criminal fica abalado em sua própria essência, por consistir numa atividade "preparatória", circunscrita num tempo anterior ao acontecimento do tipo penal.

Entretanto, tendo em vista as peculiaridades dos crimes cibernéticos, é possível tecer algumas considerações sobre a atividade de predição criminal nesse cenário. A própria atuação –essencialmente repressiva – da Polícia Judiciária leva a tal questionamento, pois os crimes cibernéticos, enquanto fenômeno, dependem de uma série de atos preparatórios e arranjos de informação dispostos num ambiente aberto, cujos dados são de fácil acesso. O "*modus operandi*" peculiar dos crimes cibernéticos depende dessa "ausência de cuidado" com o tratamento das informações *on line*.

Além disso, em termos de avanços institucionais, é notória a ausência de um órgão internacional de controle e organização das formas de tratamento do referido fenômeno.

Por derradeiro, em razão de sua natureza difusa, a identificação do local de perfazimento e consumação desse tipo de delito são fatores que dificultam o "policiamento preditivo" no ambiente virtual, tanto para efeito de classificação processual penal como para a estruturação de possíveis meios de enfrentamento.

REFERÊNCIAS

CASTRO, Henrique Hoffmann Monteiro de Castro. **Lei 13.441/17 instituiu a infiltração policial virtual.** Disponível em: https://www.conjur.com.br/2017-mai-16/academia-policia-lei-1344117-instituiu-infiltracao-policial-virtual. Acesso em: 03 de maio de 2021.

CRESPO, Marcelo Xavier de Freitas. **História dos crimes digitais no Brasil**. In: PRIORI, Mary Del; MULLER, Angélica. (Org.). História dos crimes e da violência no Brasil. São Paulo: Unesp, 2017. P.407-431.

FABRETTI, Humberto Barrionuevo. **Segurança pública: fundamentos jurídicos para uma abordagem constitucional**. São Paulo: Atlas, 2014.

FAVERO, Bruno de Oliveira. **Cibercriminologia:** os meios eletrônicos e o policiamento em ambientes digitais. Jundiaí [SP]: Paco Editorial, 2021.

JORGE, Higor Vinicius Nogueira. **Tratado de Investigação Criminal Tecnológica**/ coordenador Higor Vinicius Nogueira Jorge e vários autores - Salvador: Editora JusPodivm, 2020.

JUSTIFICANDO. **Crimes digitais: quais são, quais leis os definem e como denunciar.** Disponível em: https://www.justificando.com/2018/06/25/crimes-digitais-quais-sao-quais-leis-os-definem-e-como-denuncia. Acesso em: 03 maio de 2021.

MACHADO, Leonardo Marcondes. **Aplicação da cadeia de custódia da prova digital.** Disponível em: https://www.conjur.com.br/2020-mar-31/academia-policia-aplicacao-cadeia-custodia-prova-digital. Acesso em: 03 de maio 2021.

SYDOW, Spencer Toth. **Curso de Direito Penal Informático.** Spencer Toth Sydow – Salvador: JusPodivm, 2020.

TUTIDA, Daniel. **Você sabe o que é tecnologia disruptiva? Descubra e confira 4 exemplos.** Disponível em: https://encontreumnerd.com.br/blog/o-que-e-tecnologia-disruptiva. Acesso em: 03 de maio de 2021.