XI CONGRESSO RECAJ-UFMG

CRIMINOLOGIA E CYBERCRIMES

C929
Criminologia e cybercrimes [Recurso eletrônico on-line] organização XI Congresso RECAJ-UFMG: UFMG – Belo Horizonte;

Coordenadores: Marco Antônio Alves, Thiago Dias de Matos Diniz e Viviane Vidigal de Castro – Belo Horizonte: UFMG, 2020.

Inclui bibliografia
ISBN: 978-65-5648-251-4
Modo de acesso: www.conpedi.org.br em publicações
Tema: Desafios, travessias e potencialidades para o direito e o acesso à justiça face aos algoritmos, ao big data e à inteligência artificial.
1. Criminologia. 2. Cybercrimes. 3. Tecnologia. I. XI Congresso RECAJ-UFMG (1:2020: Belo Horizonte, MG).

CDU: 34

XI CONGRESSO RECAJ-UFMG

CRIMINOLOGIA E CYBERCRIMES

Apresentação

É com imensa satisfação que o Programa RECAJ-UFMG – Acesso à Justiça pela Via dos Direitos e Solução de Conflitos da Faculdade de Direito da Universidade Federal de Minas Gerais e o CONPEDI – Conselho Nacional de Pesquisa e Pós-graduação em Direito tornam público à comunidade científica o conjunto dos oito livros produzidos a partir dos Grupos de Trabalho do XI Congresso RECAJ-UFMG: Desafios, travessias e potencialidades para o Direito e o Acesso à Justiça face aos algoritmos, ao big data e à inteligência artificial. As discussões ocorreram em ambiente virtual ao longo dos dias 18, 19 e 20 de novembro de 2020, dentro da programação que contou com grandes nomes nacionais e internacionais da área, além de cento e sessenta e três pesquisadoras e pesquisadores inscritos no total, provenientes de quatorze Estados da federação (AC, AM, BA, CE, MG, PA, PE, PR, RJ, RO, RS, SC, SE e SP). Os livros compõem o produto deste congresso, que há mais de uma década tem lugar cativo no calendário científico nacional.

Trata-se de coletânea composta pelos cento e oito 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 geraram cerca de seiscentas páginas de produção científica relacionadas ao que há de mais novo e relevante em termos de discussão acadêmica sobre diversos temas jurídicos e sua relação com a tecnologia: Acesso à Justiça e tecnologias do processo judicial; Direito do Trabalho no século XXI; Estado, governança, democracia e virtualidades; tecnologias do Direito Ambiental e da sustentabilidade; formas de solução de conflitos, educação e tecnologia; Direitos Humanos, gênero e tecnologias da contemporaneidade; inteligência artificial, startups, lawtechs e legaltechs; e Criminologia e cybercrimes.

Os referidos Grupos de Trabalho contaram, ainda, com a contribuição de vinte e quatro proeminentes pesquisadores ligados a renomadas instituições de ensino superior do país, dentre eles alguns mestrandos e doutorandos do próprio Programa de Pós-graduação em Direito da UFMG, que indicaram os caminhos para o aperfeiçoamento dos trabalhos dos autores. Cada livro desta coletânea foi organizado, preparado e assinado pelos professores e pós-graduandos que coordenaram os trabalhos. Sem dúvida, houve uma troca intensa de saberes e a produção de conhecimento de alto nível foi, certamente, o grande legado do evento.

Nesta esteira, a coletânea que ora se apresenta é de inegável valor científico. Pretende-se, com esta publicação, contribuir com a ciência jurídica e com o aprofundamento da relação entre a graduação e a pós-graduação, seguindo as diretrizes oficiais da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES. Importante lembrar, ainda, da contribuição deste congresso com a formação de novos pesquisadores na seara interdisciplinar entre o Direito e a tecnologia, uma vez que o número de graduandos que apresentaram trabalhos de qualidade foi expressivo.

O Programa RECAJ-UFMG existe desde 2007 e foi criado poucos meses após o Conselho Nacional de Justiça ter iniciado o Movimento pela Conciliação. Durante a I Semana Nacional de Conciliação, em 2006, a Faculdade de Direito da UFMG, por meio de seu então diretor, Professor Doutor Joaquim Carlos Salgado, firmou o compromisso, em 4 de dezembro de 2006, de envidar esforços para incluir disciplina sobre as formas de solução de conflitos na grade curricular da faculdade.

De forma pioneira no país e observando a necessidade de estudo e aprofundamento dos temas do acesso à justiça e das formas de solução de conflitos complementares ao Poder Judiciário, a Professora Doutora Adriana Goulart de Sena Orsini passou a ofertar a disciplina “Formas de Resolução de Conflitos e Acesso à Justiça” no período de 2007-2017, em todos os seus semestres na Faculdade de Direito da UFMG.

Nesse contexto, o Programa RECAJ-UFMG atua desde o início em atividades de ensino, pesquisa e extensão em acesso a justiça pela via dos direitos e soluções de conflitos. Reúne grupos de alunos e ex-alunos da graduação e da pós-graduação stricto sensu que, sob orientação da Prof. Adriana, passaram a estudar de forma aprofundada os temas nucleares do Programa e aqueles que lhes são correlatos. Desenvolvendo uma série de projetos, tais como grupo de estudos, disciplinas optativas, seminários, pesquisas, cursos de formação, atividades de extensão, dentre outras, o Programa RECAJ-UFMG honra a sua vocação para ações variadas em seus temas de forma responsável, séria, atualizada, científica e contemporânea. No RECAJ-UFMG, a indissociabilidade entre o ensino, pesquisa e a extensão é uma marca distintiva.

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

Belo Horizonte-MG, 26 de novembro de 2020.

Profª. Drª. Adriana Goulart de Sena Orsini - Coordenadora do Programa RECAJ-UFMG

Prof. Dr. Caio Augusto Souza Lara - SKEMA Business School/ESDHC/CONPEDI

Prof. Dr. José Eduardo Resende Chaves Júnior - SKEMA Business School/PUC Minas

CRIMES CIBERNÉTICOS

CYBER CRIMES

Eduardo Soares Da Silva
Najah Jamal Daakour Barakat

Resumo

Os avanços técnicos na área da informática aumentam o risco de abuso, pois agora é possível atacar longe e com a possibilidade relativa do anonimato oferecido pela rede de computadores. Logo, demonstrando a evolução pandêmica do cibercrime as autoridades estão encarando a luta contra esses crimes cibernéticos com leis como a Lei de Geral de Proteção de Dados Pessoais para que a sociedade continue contando com o bom funcionamento dos sistemas de informação e com novas tecnologias que são alvo de ataques de criminosos cibernéticos, a segurança desses sistemas é de importância estratégica particular.

Palavras-chave: Direito, Cibercrime, Tecnologia

Abstract/Resumen/Résumé

Technical advances in the field of information technology increase the risk of abuse, as it is now possible to attack from afar and with the relative possibility of anonymity offered by the computer network. Therefore, demonstrating the pandemic evolution of cybercrime, the authorities are facing the fight against these cyber crimes with laws such as the General Law for the Protection of Personal Data so that society continues to rely on the smooth functioning of information systems and new technologies that are the target of attacks by cyber criminals, the security of these systems is of particular strategic importance.

Keywords/Palabras-claves/Mots-clés: Law, Cybercrime, Technology

INTRODUÇÃO

Apresente pesquisa aborda os crimes cibernéticos e tem como elemento principal analisar o crescimento do acesso à internet nos últimos anos junto a um rápido desenvolvimento devido a conectividade computacional e os smartphones. O advento da globalização tomando conta das comunicações através da rede mundial de computadores, assim como o crescimento exponencial da tecnologia digital, trouxeram enormes benefícios, mas juntamente com eles vieram os maiores riscos internos e externos ultrapassando as fronteiras, por este motivo o estudo sobre crimes cibernéticos torna-se imprescindível.

As novas oportunidades criadas no "ciberespaço" aumentaram a capacidade dos delinquentes individuais e das redes criminosas que surgiram para encontrar brechas nas vulnerabilidades na "nova" economia. Assim é essencial discutir: qual o papel das tecnologias digitais? Isto significa que os novos riscos associados a essas mudanças exigem atenção em todas as frentes: nacional, regional e internacional.

Logo, deve-se analisar o processo de globalização que continua crescendo sobremaneira, sendo que uma resposta universal aos problemas da segurança na era digital ainda tem que sugerir novos esforços para garantir a segurança e isto tem sido reativo, em vez de proativo.

O objetivo principal é fomentar a discussão acerca do direito frente as novas tecnologias, perpassando por temas artificiais, de modo a colaborar na disseminação e nos debates sobre os referidos temas de forma atualizada, como o acesso à justiça, a Lei Geral de Proteção de Dados, os algoritmos, o big data e a inteligência, seguido por objetivos específicos buscando demonstrar os crimes cibernéticos e a cooperação jurídica sobre o sistema de justiça brasileiro e a perspectiva do acesso à justiça na atualidade.

O estudo se dará com pesquisas bibliográficas em livros acadêmicos, revistas científicas e sites confiáveis que mencionam crimes cibernéticos. Como critério de inclusão serão observados sites em português que busquem sobre o tema, como critério de exclusão quaisquer materiais que não envolvam o assunto.

Sob esse estudo de crimes cibernéticos pode-se analisar como países desenvolvidos lidam com o tema e com o crescente número de pessoas que se tornam alvos pelo simples motivo de compartilhar informações tais quais: fotos, filmagens, ou mesmo *Fake News*, ocorrendo assim o crime virtual. Contudo pode se observar a precariedade de leis envolvendo o assunto no Brasil, tendo como consequência por vezes a banalização de muitos crimes cibernéticos.

1 CRIMES CIBERNÉTICOS E O SISTEMA DE JUSTIÇA BRASILEIRO E A PERSPECTIVA DO ACESSO À JUSTIÇA NA ATUALIDADE

Crimes cibernéticos possuem uma noção ampla que inclui todas as ofensas criminais cometidas através de redes de computadores e, mais especificamente, através da Internet. Com o governo, indústrias, mercados e consumidores cada vez mais dependentes de conectividade, eles são propensos a uma série de ameaças (CABETTE, 2013).

O âmbito das atividades criminosas e as suas consequências sociais podem ser resumidas por uma tipologia de crimes virtuais como pornografia infantil, furto de propriedade intelectual, ataques a redes de computadores e criminosos convencionais como nos casos em que existem evidências em formato digital.

De acordo com Rocha (2013) alguns tipos de criminalidade abrangem a seguinte lista:

• Interferência no uso legal de um computador: cibervandalismo e terrorismo; negação de serviço; inserção de vírus, *worms* e outros códigos maliciosos;

• Divulgação de materiais ofensivos: pornografia/pornografia infantil; conectados a jogos apostas; conteúdo racista; conteúdo traiçoeiro ou de ódio;

• Ameaçar Comunicações: extorsão; *cyber-stalking*;

• Falsificação: roubo de identidade; Ofensas de IP; software, pirataria de CDs e DVDs; violações de direitos autorais etc;

• Fraude: fraude de cartão de pagamento e fraude de transferência de e-fundos; roubo de Internet e serviços telefônicos; fraude em leilões; fraude contra o consumidor e vendas diretas; fraude de valores mobiliários online;

• Outros: interceptação ilegal de comunicações; comercial/corporativo espionagem; comunicações em promoção de conspirações criminosas; lavagem de dinheiro.

Muitos desses riscos parecem imitar a exploração criminosa tradicional, embora executado com facilidade, velocidade e impacto sem precedentes em todas as jurisdições e, portanto, a resposta apropriada é guiada por novas disciplinas tecnológicas. As tarefas de identificar os cibercriminosos e levá-los à justiça representam desafios formidáveis para agências de aplicação da lei em todo o mundo, e exigem um grau e oportunidade de cooperação que até há pouco tempo era considerada difícil, se não impossível, alcançar.

No entanto, a intrusão de computadores é agora mais provável um predicado para ofensas mais graves. Computação forense e protocolos de preservação de evidências são essenciais para investigação e acusação eficazes, especialmente tendo em conta a natureza transfronteiriça.

Consequentemente, como em outros tipos de crime, a ênfase está seguindo as regras tradicionais da cadeia de provas e assegurando que o comando e controle atribui prontamente os especialistas relevantes à tarefa em questão. Os principais estudiosos de prevenção ao crime fornecem uma revisão de prevenção do crime no contexto do comércio eletrônico. Na "situação" online, o furto de informação e manipulação de identidade e confiança são os personagens principais e as armas mais utilizadas (NARTINS et al., 2007, p.79).

Um fator crucial para o sucesso do cometimento dos crimes é como a confiança é adquirida e mantida quando os comerciantes devem ser mais intrusivos sobre suas identidades e o risco de crédito dos clientes, além da aparente facilidade em que a confiança é manipulada por fraudadores e outros que operam na situação online. Há de se ter grande atenção aos riscos colocados na fase pós-transação (ou seja, entrega de bens ou serviços encomendados), um assunto muitas vezes negligenciado nas discussões de cibercrime.

2 A RESPEITO DA LGPD - LEI GERAL DE PROTEÇÃO DE DADOS

A relativa novidade do crime informático significou que a maioria das agências de policiamento apenas recentemente desenvolvessem medidas específicas para registrá-las. O advento de legislação relacionada com computadores e processos conexos e o estabelecimento de resposta a emergências informáticas e unidades dedicadas ao crime tecnológico dentro das delegacias, juntamente com o desenvolvimento da conscientização das vítimas de crimes e defesa do consumidor, levaram as jurisdições à frente do mercado digital revolução para começar a registrar a incidência da ilegalidade no ciberespaço (CASTRO, 2003, p.36).

No entanto, no Brasil o marco da internet também denominada Lei N° 12.965/14, que regula princípios e garantias que quem utiliza a internet podem servir como base para a elaboração de estatísticas policiais sobre crimes denunciados e que frequentemente dizem mais sobre as atividades e prioridades da polícia do que sobre a extensão do crime. Isso porque em muitos crimes tradicionais, as vítimas não as reportam às autoridades. A natureza transnacional do crime cibernético reflete o processo de globalização, que se intensificou nas últimas duas décadas (BRASIL, 2014).

O surgimento do comércio eletrônico, bem como a dimensão social da Internet e os crimes cibernéticos associados chegam juntamente com os desafios à capacidade independente dos Estados para regular a ordem social e econômica dentro de seus territórios. Versões radicais da globalização vão mais adiante e sugerem que o sistema de relações internacionais do Estado não fornece uma metodologia eficaz para regulamentar os mercados domésticos ou

transnacionais, em especial o comércio internacional. Com o advento da Lei Geral, o Brasil se insere na lista das centenas dos países que atualmente são considerados adequados na proteção da privacidade dos usuários, bem como a utilização de dados. Da mesma forma a GPDR (*General Data Protection Regulation*) um regulamento de dados pessoais europeu, que abrange toda a União e Espaço Econômico Europeu, a LGPD produzirá uma mudança de paradigmas na gestão de informação de dados, corroborando a indispensabilidade de adequação interna e da edificação da cultura de amparo de dados no Brasil. Em qualquer versão da globalização, tais como grandes instituições comerciais, desempenham um papel crucial no surgimento de um sistema de estado transnacional (BRASIL, 2018).

As perspectivas de segurança dos brasileiros aumentaram com as normas gerais contidas na Lei Geral de Proteção de dados a qual é uma disciplina que abarca a proteção de dados pessoais tem como fundamento lidar com ameaças complexas colocadas pelo cibercrime argumentam o que o garante uma confiança no Estado e um desenvolvimento eficaz ao que diz respeito os meios tecnológicos, a polícia vem cada vez mais se especializando, para resolver questões de segurança cibernética que sem leis de proteção poderia expor diversos dados originando conflitos sociais na Internet.

Embora agora existam convenções e tratados internacionais expressamente destinadas a inibir redes criminosas sérias ou infratores que operam através das fronteiras, o alcance desses instrumentos é limitado pela velocidade e escala da ratificação interna e o advento de leis habilitadoras. Ao lidar com crimes de TI, a aplicação da lei está em desvantagem por causa da notável velocidade em que os crimes cibernéticos se desdobram para a típica cooperação de baixa velocidade oferecida pelas formas tradicionais de assistência.

O papel das agências multinacionais, como a Interpol e as Nações Unidas nunca foram tão essenciais. Em diversos países os resultados ficam muito aquém de criar uma teia sem emenda de acordos bilaterais ou multilaterais e de fiscalização, isso garantiria um ambiente hostil para os criminosos cibernéticos. A compatibilidade de atividade criminosa com essas mudanças globais é ilustrada pela expansão e convergência dos negócios rentáveis do contrabando de seres humanos, da pornografia, narcóticos ou outras mercadorias ilícitas com o desenvolvimento da comunicação, infraestrutura e comércio.

3 ASPECTOS ATUAIS DO DIREITO FACE AOS ALGORITMOS, AO BIG DATA E INTELIGÊNCIA ARTIFICIAL

A circulação de informação na *Web* está sujeita ao que é conhecido como uma bolha de filtros cuja própria existência contradiz a visão de uma democracia digital baseada no acesso igual para todos ao conhecimento e uma habilidade compartilhada para discutir publicamente e racionalmente tópicos de interesse geral.

Embora aparentemente a massa de informação nunca tenha sido tão vasta e rapidamente disponível, a informação não filtrada por algoritmos torna-se uma mercadoria mais rara do que as escolhas pessoais anteriores na *Web* isolam as pessoas por causa de uma lógica cumulativa característica do círculo vicioso característica da inteligência artificial. Se às vezes eles recebem muito poder, mecanismos de seleção algorítmica operam diariamente, anonimamente, durante e fora dos períodos eleitorais.

Um usuário do Google que deseja saber mais sobre a situação da Turquia em julho de 2016, com base em seu histórico de pesquisas e, portanto, em seu perfil, será exibido nos sites turísticos da primeira página, enquanto outro será direcionado para últimas notícias da repressão neste país (BARROSO, 2010, p.56).

Mas os algoritmos também têm uma ligação direta com as notícias falsas, na medida em que estes últimos não são de interesse para o remetente se não forem capazes de compartilhá-los em grande escala por meio de programas capazes de automatizar a transmissão de notícias e de conteúdo, criando artificialmente uma onda de popularidade, uma tendência que lhes permitirá entrar no fluxo de atualizações do *Facebook*.

Para chegar o público alvo, é suficiente que apenas um dos amigos o tenha validado, integrando-o em seu segmento de notícias, enquanto a viralidade dessa informação se baseia em uma máquina de venda automática baseada nos trabalhadores pagos pelo clique. Além disso, o efeito de bolha dos filtros pode ser combinado com o efeito de câmara de eco que acentua o viés de confirmação: Os amigos pensam iguais.

A informação compartilhada em determinado perfil fortalece as predisposições, expondo o usuário à propaganda inequívoca. Não obstante, não basta estar satisfeito com uma explicação do suporte técnico, neste caso a Internet, mas de colocar essa ferramenta no contexto de uma economia de atenção em si dependente do “tecnocapitalismo” neoliberal.

REFERÊNCIAS

BARROSO, Luis Roberto. **Curso de direito constitucional contemporâneo.** 2.ed. São Paulo: Saraiva, 2010.p.78- 82.

BRASIL. **Lei nº. 12.965, de 24 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em 4 de nov. de 2020.

CABETTE, Eduardo Luiz Santos. **O novo crime de invasão de dispositivo informático.** Conjur, 2013, p.26- 30. Disponível em: < http://www.conjur.com.br/2013-fev-04/eduardo-cabette-crime-invasao-dispositivo-informatico>Acesso em:05 nov. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Redação dada pela Lei nº 13.853, de 2019. Brasília, DF: Senado Federal, 2018. Diponivel em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm Acesso em: 4 de nov. de 2020.

NARTINS, Adalberto et al. **O Direito na sociedade da informação**. 1. São Paulo: Atlas, 2007, p.79- 83.

ROCHA, Carolina Borges**. Evolução dos crimes cibernéticos**. Revista Jus Navigandi, Teresina,ano 18,n. 3706, 23 ago 2013, p.56- 60.