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

CRIME VIRTUAL: O PERIGO DA EXPOSIÇÃO COMPARTILHADA NA INTERNET.

VIRTUAL CRIME: THE DANGER OF SHARED EXPOSURE ON THE INTERNET.

Marlene Aparecida Alves Pedrosa [1]

Resumo

Este estudo objetiva discutir os crimes cibernéticos empreendendo-se uma análise sobre o perigo da exposição compartilhada na internet e a necessidade de uma norma penal especial destinada aos crimes digitais. Para tanto, como metodologia, emprega a revisão literária em doutrinas e legislações que se dedicam ao estudo do tema em análise demonstrando que tendo em vista a proliferação dos crimes cibernéticos, é importante uma análise criteriosa e ética sobre o tema cibercriminalidade sabendo-se que o delito cibernético provoca enormes prejuízos financeiros, pessoais e morais à sociedade e, a maioria das condutas ilícitas na internet, continua sem previsão legal.

Palavras-chave: Ambiente cibernéticos, Condutas ilícitas, Cibercrimes, Legislação

Abstract/Resumen/Résumé

This study aims to discuss cyber crimes, the danger of shared exposure on the internet and the need for a special criminal law aimed at digital crimes. As a methodology, it employs literary revision of doctrines and legislation dedicated to the study of this theme, demonstrating that in view of the proliferation of cyber crimes, it is important to carry out a careful and ethical analysis on the cybercrime theme, knowing that this crime causes enormous financial losses. , personal and moral to society and, most of the illicit conduct on the internet, remains without legal provision.

Keywords/Palabras-claves/Mots-clés: Cyber environments, Illicit conduct, Cybercrimes, Legislation

[1] Centro universitário UNA ,Belo Horizonte ,Minas Gerais (Brasil) ,graduanda.E-mail:marpedrosa10@hotmail.com.

CRIME VIRTUAL: O PERIGO DA EXPOSIÇÃO COMPARTILHADA NA INTERNET.

Nome do autor[1]

INTRODUÇÃO

Não restam dúvidas de que a vida, tanto no aspecto privado, como profissional e social, está totalmente conectada ao universo informático. Conectada, não somente no sentido de interligada *online*, mas também no sentido de submissão a uma nova dominação global do meio de comunicação. Houve a integração e a sujeição. Do mesmo modo estão conectadas as instituições financeiras, empresas de energia, de transportes terrestres, marítimos e aéreos, instituições de ensino, toda a administração pública, instituições religiosas, empresas privadas e estabelecimentos comerciais. A essa dominação imputa-se não apenas a necessidade de arquivamento e processamento de informações, mas inclusive, a tomada automática de decisões realizadas pelos computadores e seus programas. Difundiu-se globalmente essa nova tecnologia de informação simplificadora e amplificadora das relações interpessoais privadas, profissionais e negociais que encanta e ao mesmo tempo agrilhoa todas as pessoas à rede mundial de computadores.

É bem verdade também que a revolução digital e a nova tecnologia de informação encurtaram as distâncias entre as pessoas e países, democratizou a intercomunicação e o acesso às informações, trouxe mais praticidade e agilidade para as atividades humanas. Todavia, essa praticidade e agilidade passaram a ser desfrutadas também pelos infratores e organizações criminosas em âmbito mundial. A facilitação e o estreitamento nas relações pessoais possibilitaram aos criminosos o ingresso em ambientes até então inacessíveis, reduziram os obstáculos para as empreitadas ilícitas, permitiram a milhões, que mesmo de suas residências, violem direitos autorais, e viabilizaram uma expansão ainda maior no tráfico de produtos proibidos, como armas, drogas, animais silvestres, órgãos do corpo humano, peças arqueológicas etc.

Apresentados estes entendimentos iniciais, este artigo objetiva discutir os crimes cibernéticos empreendendo-se uma análise sobre o perigo da exposição compartilhada na internet e a necessidade de uma norma penal especial destinada aos crimes digitais.

O interesse pelo tema surgiu frente à constatação de que a lei penal existente ainda não

[1]Inserir num único parágrafo (máximo 3 linhas) o minicv.

se mostra eficaz para enfrentar os crimes cometidos pela internet havendo ainda muitas dificuldades na equiparação das leis específicas destinadas a normatizar a internet com a legislação comum. Ademais, o Marco Civil da internet não traz em seu texto todas as possibilidades de crimes praticados pela internet tornando necessário o uso da analogia para fazer frente aos crimes cometidos pela rede mundial de computadores.

O Direito – é forçoso insistir – está sempre a reboque das inovações científicas e tecnológicas, de sorte que a solução penal para as violações digitais pode chegar tarde aos seus destinatários que, talvez, já tenham encontrado a solução técnica, extrajurídica, para o problema ou já tenham criado uma nova forma de violação, tornando as questões aqui pontuadas temas deveras superados.

FUNDAMENTAÇÃOTEÓRICA

Atualmente são muitos os crimes cometidos pela internet, especialmente nas redes sociais, dentre os quais se destacam: furto de senhas, *bulling* e *cyberbullyng*, exposição da intimidade de terceiros, chantagens e muitas outras situações que implicam em invasão de privacidade, extorsão, crimes contra a honra, *revenge porn* (pornografia da vingança), estupro virtual, pedofilia, extorsão sexual, entre outros (CANEDO, 2010).

E os problemas não cessam por aí: vírus em aparelhos celulares, clonagem de *smartphones*, fraudes em TV por assinatura, violação de correspondência eletrônica, perseguição digital, clonagem de cartões magnéticos, pirataria virtual, crimes contra o sistema financeiro, invasão de sistemas, entre outros (MÈLO, 2019). Nem os órgãos governamentais estão livres dos criminosos hodiernos e não raro sofrem com a sabotagem informática ao ter seus sistemas invadidos.

Os crimes podem ser classificados em próprios, impróprios e mistos conforme será visto a seguir.

Pode-se dizer que os crimes próprios começaram com a evolução tecnológica. São novas categorias, que facilitadas pela evolução da informática, atingem bens juridicamente protegidos. Dito de outra forma, são os crimes cometidos com o objetivo de obter dados, informações, e também aqueles que interferem no funcionamento do sistema. São exemplos de cibercrimes próprios: o acesso indevido ou abusivo a sistemas; a interceptação de dados informáticos; a interferência em sistemas informáticos; a instalação de vulnerabilidades; a violação de medidas de segurança dos sistemas; a produção, a oferta, a distribuição, a venda ou difusão de dispositivo ou programa informacional que tornem possível o acesso, a

interceptação, a violação e a interferência em sistemas e dados informáticos (MORAES; SANTORO, 2015).

Os cibercrimes impróprios, também denominados impuros, são identificados a partir dos crimes clássicos que passam a ser perpetrados também pela internet, isto é, o computador e a rede são empregados apenas como instrumentos para a execução criminosa. Nesta categoria estão arroladas: as fraudes, quando o agente utiliza-se de recursos informacionais, criando subterfúgios para levar as vítimas a erro; as falsificações de documentos, englobando, de acordo com a atual redação do art. 298 do CP, a contratação de cartões; o dano a dados ou sistemas informacionais; a espionagem e o boicote, além de outros crimes contra a segurança nacional; a reprodução não autorizada de programas ou produtos; a falsificação de softwares; as ameaças, os crimes contra a honra; os delitos de opinião etc. (MORAES; SANTORO, 2015).

Na internet, os crimes contra a honra são cometidos com grande frequência, pois, na maioria das vezes, o crime é motivado pela falsa ideia de anonimato.

Breves e Sampaio (2014) relatam uma experiência real vivida por uma das autoras numa rede social. Breves foi acusada de maltratar gatos num prédio onde morava em Copabacana. A "denúncia" foi postada na internet e ela relata: "ao sofrer agressões pela rede social, eu visualizei minha vida, minha profissão, os meus projetos, os meus sonhos, tudo destruído" (BREVES; SAMPAIO, 2014, p. 13). Durante dez dias, mais de mil postagens fizeram-na conhecer o ódio gratuito lançado pelas pessoas. Segundo Breves e Sampaio,

> [...] a humilhação experimentada a fez querer sumir, pois acreditava que aquele turbilhão de ódio, medo, raiva, pânico, desamparo, desespero, vergonha, solidão e ansiedade jamais iriam passar. Segundo relata, as mensagens eram alimentadas diariamente com juízos de valor que a condenavam, inclusive, à morte. Ela chegou a ser ameaçada de morte pela internet e tinha medo até de sair de casa e ser pega na porta do prédio. Passou a comparar a experiência a uma versão moderna do Coliseu de Roma, no qual as pessoas iam para assistir, aplaudir e torcer para que os gladiadores fossem assassinados cruelmente, num grande espetáculo. Nessa versão do Coliseu do século XXI, as pessoas vão assistir, aplaudir e participar de falatórios na rede social, que podem culminar em morte (BREVES; SAMPAIO, 2014, p. 17).

O caso de Breves foi levado ao Juizado Especial do Rio de Janeiro. No âmbito criminal, ele aceitou a proposta de transação penal, lançada pelo Ministério Público, e pagou a importância de mil reais a uma entidade de proteção aos animais. A ação civil ainda está em trâmite, segundo relata a autora.

Já o Tribunal de Justiça do Paraná, quando julgou o *Habeas Corpus* nº 1329408-5, referente a queixa-crime oferecida por suposta prática do crime capitaneado no art. 138 do Código Penal por publicação e realização de comentários ofensivos no *Facebook*, reconheceu que não existiu ultraje ao princípio da indivisibilidade da ação penal, pois não obstante a acusada tenha sido realmente a autora da primeira publicação, que deu origem a comentários ofensivos, estes foram realizados em momentos distintos, configurando, portanto fatos diversos.

Também, nesse julgado, é importante destacar que não havia necessidade de oferecer queixa-crime individualmente a todos aqueles que realizaram comentários hostis, cabendo ao querelante optar por apresentar somente em face da autora do *post* e de um dos autores dos comentários, não havendo coautoria nesse caso.

Ao contrário do que se pensa, segundo Breves e Sampaio (2014), é fácil identificar aquele que praticou um crime pela internet. Todo computador ou dispositivo móvel ligado à internet possui um IP, que é um registro numérico que o computador ou roteador recebe ao entrar na internet. Pelo IP é possível encontrar o local de onde partiu a ofensa.

Dependendo da situação em que foi publicado e da gravidade do seu conteúdo, um comentário maldoso pode ser interpretado como difamatório. Assim, podem ser imputadas ao ator as penas previstas em lei. Ainda que não exista no Brasil legislação específica para crimes digitais, a Justiça brasileira julgará do mesmo modo como se os comentários fossem feitos em qualquer outra circunstância e/ou lugar (VANCIM; NEVES, 2015).

Muitas vezes crimes graves são praticados sem que seus autores tenham conhecimento disto. Mesmo não existindo a intenção de causar dano a terceiros, o responsável pela inserção de um comentário poderá ficar sujeito à acusação pelo crime. A título de exemplificação, uma empresa ainda pode ser figurada como corresponsável por um delito se o funcionário o cometeu durante o seu período de trabalho valendo-se da infraestrutura disponibilizada pela empresa (VANCIM; NEVES, 2015).

A criminalidade organizada também existe na Internet. Existem muitos criminosos que valem-se de computadores para agir, invadindo e atacando sistemas. As quadrilhas no meio eletrônico não usam armas e nem ameaçam usuários pessoalmente, a maior arma destes criminosos é o alto conhecimento em informática e outros dispositivos relacionados. As quadrilhas geralmente são departamentalizadas, ou seja, divididas em setores, a citar: o primeiro grupo são os usuários que invadem sistemas; o segundo são pessoas que roubam dados e informações importantes de empresas, se passando por pessoas que ali trabalham; o terceiro setor é formado por vendedores de informações privilegiadas, ou seja, de posse das

informações, os criminosos conseguem lucrar vendendo dados pessoais (CPF, RG, etc) e informações chaves de empresas (VANCIM; NEVES, 2015).

Por fim, citam-se os crimes de informática mistos, que englobam todas aquelas ações em que o agente tem como alvo um bem juridicamente protegido diferente da informática, no entanto, o sistema informacional é ferramenta indispensável para a sua consumação (VANCIM; NEVES, 2015).

De tempos em tempos surgem alguns "crimes da moda". Como resposta, o policiamento é incrementado e inibe certos tipos de delitos. Assim, os criminosos praticam um novo tipo de crime e o ciclo continua.

Diante da nova realidade, que admite a interligação massiva de pessoas ao redor do mundo, à velocidade da luz, descortina-se aos profissionais do Direito um vasto campo, desconhecido e repleto de incertezas.

METODOLOGIA

Como metodologia, empregou-se a revisão de literatura realizada por meio de doutrinas, legislações e jurisprudências, de acesso físico e virtual, que ajudam a enfrentar o problema proposto neste estudo.

RESULTADOS E DISCUSSÃO

A sociedade humana caminha através do Século XXI, estruturando-se progressivamente como a Sociedade da Informação, experimentando os benefícios decorrentes dos avanços tecnológicos e das novas descobertas científicas que proporcionam a comodidade e o conforto do acesso rápido e integral às informações, trazendo diversas conquistas sociais que vão desde a sofisticada pesquisa acadêmica até os mais inusitados serviços disponibilizados pelo comércio eletrônico, conforme foi discutido e explicitado ao longo desta pesquisa.

Os inúmeros obstáculos vencidos com a informatização e o advento das novas TICs elevaram um grave contraste com os deletérios problemas daí oriundos. A migração de diversas atividades sociais desenvolvidas na sociedade tradicional para a sociedade cibernética, conduzindo para essa dimensão, os criminosos virtuais.

Essa radical e gradativa mudança de hábitos dos indivíduos e das comunidades trouxe como consequência mais gravosa os referidos crimes virtuais concentrando a atividade dos

cibercriminosos, esses especialistas em TICs, que acompanharam o êxodo social cibernético e por intermédio de um aprendizado veloz e transbordante de genialidade maléfica, criaram e aprimoraram um *modus operandi* próprio, moderno, extremamente sofisticado, direcionando seus incríveis conhecimentos técnicos para o cometimento de delitos virtuais.

Desta forma, referidos infratores, fazendo uso de estações móveis (*notebook*, celular, *palm top*, *tablet*, *iPod* etc.), estações fixas (*workstation*) interligadas em redes locais ou computadores pessoais instalados no conforto de suas residências, conectam-se a milhares de outros sistemas informatizados e atravessam com a velocidade dos sinais digitais todo o *backbone* internacional na Internet, que se transformou nesse magnífico advento cultural e tecnológico da humanidade na transposição desse último século.

A utilização de novas tecnologias e avanços científicos demanda planejar também os efeitos daí decorrentes. Do ponto de vista criminal, deve-se pensar na ponderação de princípios frente à preocupante constatação de que os cibercrimes têm natureza complexa e são extremamente voláteis.

Não se admite mais que a internet seja vista como um "território sem lei", porque nesse mencionado ambiente, atualmente, desenvolve-se ampla diversidade de serviços e atividades financeiras, sendo um espaço aberto de interação da sociedade civil.

Portanto, mesmo muitas infrações cometidas na internet se assemelhando ou incidindo no tipo penal tradicional, o cibercrime impróprio, excetuadas as nuances direcionadas para o elemento do tipo, há uma lacuna que deve ser preenchida por legislação especial que demanda criar nova classificação, sancionando o delito cibernético próprio, posto que as pequenas reformas penais e processuais penais efetuadas recentemente não foram suficientes para suprir a demanda exigida pela delinquência cibernética emergente.

CONCLUSÕES

Em linha de conclusão, percebe-se que o delito cibernético provoca enormes prejuízos financeiros, patrimoniais, pessoais e morais à sociedade e, até o presente momento, a ampla maioria das condutas ilícitas na internet, continua sem previsão legal e, desta feita, são condutas atípicas.

Esse novíssimo fenômeno criminoso campeia sem obstáculos pelo sistema jurídico, enquanto não cessam de surgir novos "tipos penais cibernéticos" que surpreendem os operadores do direito e deixam a sociedade assustada e perplexa, diante dos legisladores que

se quedam vagarosos e silentes a observarem o flagelo social cibernético. É de fundamental importância uma análise criteriosa, responsável e ética a respeito do tema cibercriminalidade, posicionando-se urgentemente pela estruturação do sistema normativo, conforme foi amplamente discutido e debatido nesta pesquisa.

REFERÊNCIAS BIBLIOGRÁFICAS

BREVES, Beatriz; SAMPAIO, Virgínia. **A Maldade Humana**: como detonar uma pessoa no facebook – baseado em uma história real. Rio de Janeiro: Mauad X, 2014.

CANEDO, Edna Dias et al. Social Networks: Security and Privacy. **The Fifth International Conference on Forensic Computer Science**, Brasília, v. 1, n. 5, 2010.

MÈLO, Augusto. **Proteção de Dados Pessoais na Era da Informação**. Curitiba: Juruá Editora, 2019.

MORAES, Alexandre Rocha Almeida; SANTORO, Luciano de Freitas. **Direito Penal Avançado**. Curitiba: Juruá Editora, 2015.

VANCIM, Adriano Roberto; NEVES, Fernando Frachone. **Marco Civil da Internet**. 2. São Paulo: Editora Mundo Jurídico, 2015.