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

STALKERWARE: O FENÔMENO DE ESPIONAGEM NO CIBERESPAÇO E O SEU IMPACTO NOS RELACIONAMENTOS ABUSIVOS

STALKERWARE: THE SPYING PHENOMENON IN CYBER SPACE AND ITS IMPACT ON ABUSIVE RELATIONSHIPS

Camilla Rafael Fernandes [1]

Resumo

Este projeto de pesquisa pretende analisar as lacunas nas regulações éticas e legais sobre o uso recente de aplicativos que permitem a espionagem, relacionado com a Lei nº 14132 que tipifica o crime de perseguição, associando esses aspectos no contexto virtual. Irá ser tratado como esses aplicativos atuam no ambiente cibernético e corroboram em relacionamentos abusivos. Assim, fundamentará as consequências práticas do stalkerware e suas implicações jurídicas. A pesquisa que se propõe, na classificação de Gustin, Dias e Nicácio (2020), pertence à vertente metodológica jurídico-social. No tocante ao tipo genérico de pesquisa desenvolvido na pesquisa, foi adotada a pesquisa teórica.

Palavras-chave: Relacionamentos tóxicos, Crime de perseguição, Segurança virtual, Regulamentação, Stalkerware

Abstract/Resumen/Résumé

This research project will analyze the gaps in the ethical and legal regulations on the use of applications that allow espionage, related to Law nº 14132 that typifies the crime of persecution, and how these are associated in the virtual context. Also, will be treated how these applications act in the cyber environment and corroborate in abusive relationships. It will substantiate the practical consequences of stalkerware and its legal implications. The proposed research, in the classification of Gustin, Dias and Nicácio (2020), belongs to the juridical-social methodological aspect. Regarding the generic type of research, theoretical research was adopted.

Keywords/Palabras-claves/Mots-clés: Toxic relationships, Persecution crime, Virtual security, Regulations, Stalkerware

[1] Estudante na Escola Superior Dom Helder Câmara na modalidade integral.

1. CONSIDERAÇÕES INICIAIS

A presente pesquisa trata sobre os preceitos legais e jurídicos relativos ao fenômeno do stalkerware no ambiente virtual. Nesse sentido, é notório uma presença cada vez maior da tecnologia no cotidiano dos indivíduos, seja de forma a auxiliar nas tarefas simples e fundamentais ou simplesmente como veículo de entretenimento e lazer. Contudo, por mais importante que seja o papel da tecnologia atualmente, esta possui uma faceta negativa a qual está relacionada com práticas ilegais e crimes cibernéticos.

Sob esse viés, é possível diferenciar os mais diversos tipos de condutas desse gênero que integram a realidade virtual como também identificar diretamente como tais padrões de comportamentos possuem impacto na vida das milhares de vítimas desses crimes. Assim sendo, por mais que seja uma situação urgente é impossível e utópico pensar na segregação entre o mundo concreto e a realidade virtual como a principal solução dessa problemática. Desse modo, é imprescindível expender as ferramentas jurídicas e tecnológicas disponíveis a fim de que se chegue a um meio viável e eficiente de combate a tais infrações.

Conquanto, há inúmeros entraves legais e lacunas jurídicas os quais impedem que tal problema seja enfrentado de forma eficaz e rápida. Dessa maneira, com a tipificação do crime de perseguição tem-se um avanço essencial como ferramenta de combate ao stalkerware. Entretanto, deve ser ressaltado que a existências de aplicativos de dispositivos celulares os quais estão disponíveis a todos e sem nenhuma restrição, legal ou não, constitui umas das adversidades mais vigente dentro desse cenário.

A pesquisa que se propõe, na classificação de Gustin, Dias e Nicácio (2020), pertence à vertente metodológica jurídico-social. No tocante ao tipo genérico de pesquisa desenvolvido na pesquisa, foi adotada a pesquisa teórica. O raciocínio desenvolvido na pesquisa será predominantemente dialético. Por consequência, a pesquisa tem a finalidade de identificar as lacunas da problemática e investigar ferramentas jurídicas e tecnológicas que irão auxiliar nas soluções adequadas referentes à problemática.

2. O CONFLITO ENTRE A EVOLUÇÃO TECNOLÓGICA E A LEGALIDADE

A modernidade tem como característica marcante a conjunção entre a vida privada e a pública, envolvendo, dessa maneira, a tecnologia no processo de exposição através das mídias sociais e meios eletrônicos. Por conseguinte, tal contexto em aliança aos massivos incentivos de permanecer constantemente conectados leva os indivíduos a se exibirem de forma excessiva

e sem restrições no ambiente virtual o que, na grande maioria das vezes, corrobora para que crimes cibernéticos aconteçam. À vista disso, eis o entendimento de Zygmunt Bauman:

> Os adolescentes equipados com confessionários eletrônicos portáteis são apenas aprendizes treinando e treinados na arte de viver em uma sociedade confessional – uma sociedade notória por eliminar a fronteira que antes separava o privado e o público, por transformar o ato de expor publicamente o privado em uma virtude e em um dever público. (BAUMAN, 2008, p. 103)

Nesse viés, é possível realizar uma correlação entre o exposto e os ideais propostos pelo filósofo sul coreano Byung-Chul Han (2019). Este abarca que o corpo social nos dias de hoje presencia a "Era da Informação", visto que o ciberespaço abre a possibilidade de os indivíduos terem a liberdade de criar, acessar e compartilhar informações, dados e conteúdo de forma literal e ágil. Contudo, tal liberdade possui ressalvas a serem feitas em detrimento do dano causado tanto de forma implícita como explícita, a aos usuários da tecnologia.

Consequentemente, é fundamental destacar que o direito à privacidade (art. 5°, X, CF/88) e da dignidade da pessoa humana (art.1°, III), são colocados em pauta dentro dessa contextualização. Dessarte, por mais que haja aspectos os quais foram criados a fim de tornar o ambiente virtual o mais seguro possível, como, por exemplo, a Lei Geral de Proteção de Dados, ainda é possível ver tais direitos sendo desrespeitados uma vez que o sentimento de impunidade é extremamente forte e, dessa maneira, torna-se um incentivo para os crimes. Isso ocorre em função da sensação de super segurança e autorização irrestrita de se manifestar plenamente, as quais se combinam para concretizar a desordem.

Ademais, há a pauta da mentalidade predominante dentro desse panorama. A sociedade evoluiu tecnologicamente de tal forma que a divisa entre o que deve ser resguardado em detrimento da vida íntima e que pode ser apresentado tornou-se mínima. Coloca-se em exibição com tal intensidade que a tentativa de construção de uma rede de seguridade no meio virtual não chega em seu potencial. Logo, os indivíduos influenciados por tal atitude em conjunto ao imenso número de estímulos que os incentivam a perpetuar com tal posicionamento faz com que se agrave o problema.

Em face disso, esses são instigados dentro da coletividade a se exporem de maneira incessante e sempre ficarem à procura de que os outros sujeitos, dentro do círculo em que se encontram, também o façam. Deste modo, tem-se dois fenômenos acontecendo ao mesmo tempo: o da exposição permanente e o da observação desta. Isso sobrevém em detrimento de que tal conduta é uma das características principais para se sentir pertencido dentro da

comunidade uma vez que “na era da informação, a invisibilidade é equivalente à morte” (BAUMAN, 2008, p. 21). Diante disso, Thompson expõe:

> Além de sonhar com a fama, outro sonho, o de não mais se dissolver e permanecer dissolvido na massa cinzenta, sem face e insípida das mercadorias, de se tornar uma mercadoria notável, notada e cobiçada, uma mercadoria comentada, que se destaca da massa de mercadorias, impossível de ser ignorada, ridicularizada ou rejeitada. Numa sociedade de consumidores, tornar-se uma mercadoria desejável e desejada é a matéria de que são feitos os sonhos e os contos de fadas (THOMPSON, 2011, p. 22).

Não obstante, dentro dessa contextualização percebe-se uma imenso artificio o qual possui a finalidade de consagrar um mercado ilícito dentro do meio virtual. Em consideração a isso, é notório o aumento de casos de venda de informações pessoais sem a autorização do titular como também a própria ação de hackers. Por outro lado, um novo problema tem surgido ao haver a possibilidade, não de pessoas com habilidades e conhecimentos notórios sobre tecnologia, mas sim, cidadãos comuns, acessarem tais informações privadas.

Sob essa perspectiva, ganha destaque o stalkerware o qual pode ser conceituado como um software, disponibilizado diretamente para indivíduos, que possibilita que o usuário remoto monitore as atividades do dispositivo de outra pessoa sem consentimento e sem notificação persistente ou explícita de tal usuário para que o primeiro possa vigiar o seu parceiro (COALITION, 2019). Dessa forma, tal aplicativo abre espaço não apenas para parceiros ciumentos e abusivos como também pais controladores (LOUBAK, 2019).

Portanto, esses aplicativos permitem vigilância da vida de determinado indivíduo ao ter a capacidade de providenciar a localização do aparelho celular, histórico de navegação, mensagens de texto, conversas em redes sociais além de permitir a gravação de vídeos ou áudios. Segundo o relatório da empresa de cibersegurança Kaspersky, as tentativas de espionagem aumentaram em 228% nos últimos anos, um número de 37.532 usuários (LOUBAK, 2019). Outrossim, houve mais de 26.619 amostrar de programas de stalkerware sendo os mais famosos os MobileTool, iSpyoo, Talklog, Spy Phone App, FlexiSpy e Reptilucus.

Com essa onda enorme de stalkerware várias organizações sem fins lucrativos se organizaram a fim de mobilizar um movimento para diminuir e tentar solucionar esse novo entrave. Assim, a ONG White Ring afirmou que “as vítimas raramente buscam ajudam porque se sentem envergonhadas” (COALITION, 2019), o que faz com que seja mais uma barreira a descontruir. Desse modo, intensificando o problema, houve vários casos em que as próprias

empresas de segurança estavam tendo os seus próprios relatórios hackeados e vazados (FREEDMAN, 2018).

3. OS APLICATIVOS DE ESPIONAGEM E A SUA RELAÇÃO DIRETA COM OS RELACIONAMENTOS ABUSIVOS

Em primeiro plano, a nomenclatura stalking tem origem da língua inglesa a qual a palavra stalk tem o sentido de perseguir, o ato de aproximação silenciosa, no intuito de caça e atacar à espreita (DELITTI, 2010). Dessa forma, esse evento implica as ação de determinado indivíduo invadir a privacidade de outro, podendo coagir, exercer influência emocional e até mesmo, em casos extremos, restringir a liberdade da vítima (DELITTI, 2010). A sua característica mais marcante é a repetição e a insistência de maneira incessante.

Diante disso, a nova lei nº 14.132 de 31 de março de 2021 trouxe uma inovação dentro desse contexto de stalking. Acrescentou o art. 147-A o qual tem a finalidade de prevenir o crime de perseguição e colocando como pena a reclusão, de seis meses a dois anos, e multa. Apesar de ser um instrumento de importantíssima relevância, percebe-se que esse possui diversas lacunas referentes ao uso de tecnologias e ao espaço virtual em si em relação ao crime de stalking.

Em consequência, os aplicativos de stalkerware são vendidos normalmente por meio de empresas as quais são legalmente registradas sob fachadas diferentes mas que utilizam como cenário a proposta de solução de rastreamento de funcionário como também monitoramento de crianças, uma função dos controles dos pais (COALITION, 2019). Por mais que esses softwares tenham sido criticados diversas vezes e apontando como um problema sério, grande maioria dos países a legislação direta sobre o assunto ainda permanece extremamente vaga.

No cenário atual, por mais que as leis ainda sejam precárias é possível afirmar que o stalkerware em si é ilegal mesmo ainda que a venda de sus aplicativos e programas sejam legal. Por esse motivo, caso alguém seja flagrado utilizando uma dessas tecnologias poderá ser criminalizado, contudo, será pelos crimes de espionagem, assédio e escuta. Além do mais, não há nenhum recurso legal ou ferramenta jurídica a qual seja feita diretamente sobre as consequências que um possível desenvolvedor do programa poderá sofrer (COALITION, 2019).

Como sequela de tal impunidade os programas disponíveis facilitam para que os abusos contra mulher aconteçam de forma ampliada. A maioria dos alvos de stalkers são mulheres, constituindo uma porcentagem de 70% e estabelecendo uma conexão direta com a

violência doméstica (COLAITION, 2019). Por mais que tenhamos como auxilio a Lei nº 11.340/2006 conhecida como Lei Maria da Penha a qual disponibiliza em seus artigos quinto e sétimo uma proteção ampliada às mulheres em relacionamentos ela ainda se torna falha e ineficiente por não abordar as condutas no meio digital e referentes ao stalkerware (DELITTI, 2010).

Por esse motivo é fundamental estabelecer ditames específicos sobre esse assunto. Prova disso encontra-se caso o parceiro decida divulgar informações, imagens íntimas ou até mesmo vídeos da vítima sem a sua permissão. Embora o art. 19 da Lei n° 12.965/2014 (Marco Civil da internet) possibilitar que o conteúdo violador dos direitos da personalidade seja retirado pelo titular, os danos causados às vítimas já foram concretizados bem como a violência por si só. Dessa maneira, outra problemática é criada.

Sob um outro olhar, o relacionamento torna-se um vínculo constante de agressão e brutalidade, o que pode levar a graves casos de feminicídio. Dessa forma, a vítima passa a ser enganada por um parceiro o qual passa demonstrar uma faceta a qual antes não era conhecida e sem que ela possua qualquer meios de se proteger. Isso ocorre em face de que "a identidade passa a ser um item a venda que o indivíduo pós-moderno adquiri e realiza seus contos e fantasias de ser e criar tornando fácil o descarte de troca desta máscara" (LOUREIRO JUNIOR, 2018, p. 36).

Em suma, a pauta fundamental é como melhorar essa situação visto que o Brasil se tornou o segundo pais com mais vítimas de stalkerware em 2020. Há ainda muitos recursos a serem concretizados e colocados em prática bem como uma maior proteção e prevenção da principal vítima desse fenômeno que é a mulher. Logo, é notório que o problema é extremamente complexo e cheio de variáveis.

Assim, observa-se que o debate vai além de como resolver esses empasses, mas também de como trazer ferramentas legislativas efetivas e atualizadas sobre essa nova realidade. Dessa maneira, verifica-se a dificuldade de decisão em relação a esse tópico.

4. CONSIDERAÇÕES FINAIS

A partir das reflexões anteriores sobre o tema, observou-se que na sociedade globalizada as informações são compartilhadas de maneira efêmera e sem responsabilidade firme. Nesse cenário, a probabilidade da remoção de um conteúdo já publicado é quase nula. Assim, muito se discute sobre quais seriam as melhores soluções em detrimento dos crimes cibernéticos.

Entretanto, a discussão principal rotaciona em como a Lei nº 14.132 ainda não é suficiente em relação ao crime de stalkerware e como isso tem um efeito colateral direto com o aumento de relacionamentos abusivos e casos de feminicídios. Dessa maneira, é necessário revisar as soluções possíveis e as formas de diminuir os casos. Assim, observa-se que o debate vai além de como resolver esses empasses, mas também de como trazer ferramentas legislativas efetivas e atualizadas sobre essa nova realidade.

Afinal, verifica-se a gigantesca contrariedade de decisão em relação a esse tópico. O fenômeno do stalkerware apesar de ser relativamente novo tem se tornado cada vez mais presente e implica consequências jurídicas extremas as quais devem ser observadas atentamente. Para culminar, ainda não há nada de específico em relação á problemática o que acarreta ainda mais dificuldade de ver a situação claramente e chegar a um desenlace conclusivo e indubitável.

5. REFERÊNCIAS

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 2 nov. 2020.

BRASIL. Lei n° 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**, Brasília 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 2 nov. 2020.

BRASIL. Lei n° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 2 nov. 2020.

BRASIL. Lei nº 14.132, de 31 de março de 2021. Acrescenta o art. 147-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal, para prever o crime de perseguição; e revoga o art. 65 do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). **Diário Oficial da União**, Brasília 31 de março de 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14132.htm. Acesso em: 2 de maio de 2021.

BAUMAN, Zygmunt. **Vida para o consumo: a transformação das pessoas em mercadoria**. Rio de Janeiro: Zahar, 2008.

DELITTI, Luana Souza. O que se entende por stalking e como é abordado pela lei?. **Jusbrasil**, 2010. Disponível em: https://lfg.jusbrasil.com.br/noticias/2191085/o-que-se-entende-por-stalking-e-como-e-abordado-pela-lei-luana-souza-delitti. Acesso em: 2 de maio de 2021.

FREEDMAN, Linn Foster. Millions of Sensitive Records Leaked by Another Sypware Maker. **Lexblog**, 2018. Disponível em: https://www.lexblog.com/?s=Spyware+Company+Hacked. Acesso em: 2 de maio de 2021.

GUSTIN, Miracy Barbosa de Sousa; DIAS, Maria Tereza Fonseca; NICÁCIO, Camila Silva. **(Re)pensando a pesquisa jurídica: teoria e prática**. 5ª. ed. São Paulo: Almedina, 2020.

HAN, Byung-Chul. **A sociedade da Transparência.** Tradução de Enio Paulo Giachini. Rio de Janeiro: Vozes, 2019.

LOUBAK, Ana Letícia. O que é stalkerware? Uso de app espião para vigiar parceiro cresce no Brasil. **Techtudo**, 2019. Disponível em: https://www.techtudo.com.br/noticias/2019/12/o-que-e-stalkerware-app-espiao-de-parceiros-gera-polemica.ghtml. Acesso em: 02 de maio de 2021.

LOUREIRO JUNIOR, Leonardo Godóes. **A modernidade líquida e o comportamento do consumidor na era digital**. Cuiabá: 2018. Disponível em: https://bdm.ufmt.br/bitstream/1/832/1/TCC_2018_Leonardo%20Godoes%20Loureiro%20Junior.pdf. Acesso em: 2 de maio de 2021.

O QUE É STALKERWARE?. **Coalition Against Stalkerware**, 2019. Disponível em: https://stopstalkerware.org/pt/o-que-e-stalkerware/. Acesso em: 27 de abril de 2021.

THOMPSON, John B. **A mídia e a modernidade. Uma teoria social da mídia**. Petrópolis, RJ: Vozes, 2011.