II CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL

TECNOLOGIAS DISRUPTIVAS, DIREITO E PROTEÇÃO DE DADOS II

T255
Tecnologias Disruptivas, Direito e Proteção de Dados - II [Recurso eletrônico on-line] organização Congresso Internacional de Direito e Inteligência Artificial: Skema Business School – Belo Horizonte;

Coordenadores: Caio Augusto Souza Lara; Wilson de Freitas Monteiro; José Luiz de Moura Faleiros Júnior. – Belo Horizonte:Skema Business School, 2021.

Inclui bibliografia
ISBN: 978-65-5648-269-9
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

TECNOLOGIAS DISRUPTIVAS, DIREITO E PROTEÇÃO DE DADOS II

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

VIOLAÇÃO DO DIREITO DA PRIVACIDADE DE DADOS POR ESPIONAGEM DIGITAL: STALKERWARE

VIOLATION OF THE RIGHT TO DATA PRIVACY BY DIGITAL ESPIONAGE: STALKERWARE

Bernardo Cabral Filgueiras [1]
Moisés Ferreira Nunes [2]

Resumo

Este projeto de pesquisa discorre sobre a prática do stalking, realizado por stalkerwares, suas implicações legais e consequências para os indivíduos atacados. Além disso, deseja-se entender como a legislação brasileira pode punir adequadamente os stalkers. Será utilizada a vertente jurídico-sociológico, a técnica da pesquisa teórica, já o raciocínio desenvolvido na pesquisa será predominantemente o dialético. Dessa forma, constata-se que o stalkerware é realizado em um alvo selecionado previamente por um indivíduo próximo tendo como intuito o controle das informações pessoais do alvo. Ademais, o stalker não é julgado adequadamente devido à ausência de uma legislação específica ao uso dos stalkerwares.

Palavras-chave: Stalkerware, Stalking, Espionagem digital, Violação de privacidade, Perseguição digital

Abstract/Resumen/Résumé

This research project will discuss the practice of stalking, through stalkerwares, its legal implications and consequences for attacked individuals. Besides that, it’s desired to understand how Brazilian law can adequately punish stalkers. For this, the legal-sociological aspect, the theoretical research technique, will be used, and the reasoning developed in the research will be predominantly dialectical. Therefore, it’s preliminarily verified that stalkerware is carried out on a target previously selected by a close individual to control the target's personal information. Moreover, the stalker is not judged properly on account of the absence of specific legislation for the use of stalkerwares.

Keywords/Palabras-claves/Mots-clés: Stalkerware, Stalking, Digital espionage, Breach of privacy, Digital chase

[1] Graduando em Direito, modalidade Integral, pela Escola Superior Dom Helder Câmara.

[2] Graduando em Direito, modalidade Integral, pela Escola Superior Dom Helder Câmara.

1. CONSIDERAÇÔES INICIAIS

A presente pesquisa tem como objetivo analisar a questão da violação do direito do indivíduo que tem sua privacidade de dados violada, por meio da espionagem, com o uso do *stalkerware*. O problema da violação da privacidade digital, por meio do *stalkerware*, está atrelado à infração da prerrogativa da privacidade individual. A partir da violação, o *stalker*, pode usar de sua vantagem para vender informações ou causar terror, chantagem, desconforto, controle ou, até mesmo, o início de uma relação violenta com a vítima. Portanto, é preciso conhecer essa nova forma de invasão da privacidade digital do usuário, de modo que o indivíduo saiba agir perante a ela.

Nos dias atuais, estão sendo registrados um enorme volume de infrações de privacidade de dados por meio dos *stalkerwares*, o que pode ser comprovado com o aumento de usuários individuais afetados por *stalkerware* globalmente. Sob essa ótica, é dado como fato que houve um aumento de 34,09%, entre 2018 e 2020, do número de indivíduos lesados pelo *software* (KASPERSKY, 2021). Além disso, de acordo com o Código Penal Brasileiro, a prática do *stalking* infringe a lei nº 14.132, de 31 de março de 2021, art. 147-A "perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade" (BRASIL, 2021). Visto isso, o presente estudo é necessário para que estratégias possam ser criadas para coibir a venda do *software*, que é feita por empresas que se beneficiam de lacunas da legislação brasileira.

Além disso, embora, na legislação brasileira, haja a Lei Geral de Proteção de Dados (BRASIL, 2018), ela não abrange a questão da espionagem dos dados por meio de *stalkerwares*, apenas que os dados dos indivíduos devem ser armazenados e protegidos. Nesse sentido, esta legislação não coíbe a prática da espionagem digital por meio de *softwares*, por isso o art. 147-A (BRASIL, 2021), incorporado recentemente ao Código Penal, se faz necessário para que a segurança seja efetiva no meio particular digital. Ademais, os indivíduos que têm sua privacidade violada, e são acometidos pelo *stalking*, sofrem inúmeras lesões psicológicas como "como transtorno de ansiedade, pânico, ansiedade generalizada e depressão" (MARQUES, 2020).

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, foi escolhido o tipo jurídico-projetivo. O raciocínio desenvolvido na pesquisa foi predominantemente dialético e quanto ao gênero de pesquisa, foi adotada a pesquisa teórica.

2. *STALKERWARE* NA ESPIONAGEM DIGITAL

A tecnologia e, consequentemente, as redes sociais trouxeram inúmeras vantagens para a sociedade, que vão desde a comunicação em tempo real entre indivíduos até a troca de informações por todo globo terrestre. Porém, assim como todas as coisas, trouxe desvantagens como a falta de privacidade e segurança de dados, por exemplo. Desse modo, a sociedade deve ter, como ponto principal, a prerrogativa de que a segurança não deve ser negligenciada, visto que os perfis virtuais são considerados uma extensão da realidade.

O desrespeito no ciberespaço ocorre de diversas maneiras e atinge pessoas de diferentes condições sociais, nacionalidades, gêneros e etnias, por exemplo. Alguns exemplos de violência que ocorrem no meio virtual são: crimes contra a honra – como difamação ou injúria – ameaças, discursos de ódio ou *stalking*. Assim, dentre os citados, o *stalking* vem se popularizando com o aumento da acessibilidade do acesso à tecnologia.

O termo *stalking* é originado da palavra *stalker*, da língua inglesa, e tem por significado "seguir uma pessoa o mais próximo possível sem ser visto ou ouvido, geralmente para capturar ou matar"[1], além disso, o dicionário sugere, também, a seguinte definição "seguir e observar ilegalmente alguém por um período de tempo"[2] (STALK, 2021) (tradução nossa). Sob essa ótica, a partir do significado do termo, ele também pode ser aplicado no ambiente virtual com iguais riscos à segurança do usuário do que na realidade.

A partir da prática do *stalking*, no ambiente virtual, foi desenvolvido o *stalkerware*, que é um *software* que fica em segundo plano no *gadget* do indivíduo espionando e, consequentemente, obtendo os dados da vítima, que é escolhida previamente pelo *stalker*. Segundo a definição dada pelo site da organização Coalition Against Stalkerware, Stop Stalkerware:

> É um *software*, disponibilizado diretamente para indivíduos, que possibilita que o usuário remoto monitore as atividades do dispositivo de outro usuário sem consentimento e sem notificação persistente ou explícita de tal usuário para que o primeiro possa, intencionalmente ou não, facilitar a vigilância de seu parceiro, assédio, abuso, espionagem e/ou violência (STOP STALKERWARE, 2019).

A Kaspersky (2021), empresa internacional de segurança virtual, divulgou dados referentes à ocorrência da prática do *stalking* por meio do *stalkerware*. Segundo tais dados, o Brasil, em 2020, esteve entre as primeiras colocações em um ranking de países mais afetados

[1] No original: To follow an animal or person as closely as possible without being seen or heard, usually in order to catch or kill them.
[2] No original: To illegally follow and watch someone over a period of time.

pelo *software*, além disso, mais de 6,5 mil indivíduos foram afetados, o que corresponde a 12% de todos os ataques do mundo. Dessa forma, fica evidente que parte da sociedade brasileira, com a popularização do meio virtual, é vítima de um problema de âmbito internacional.

As empresas que desenvolvem os *stalkerwares*, como Mobile Tracker Free ou TheTruthSpy, alegam em suas políticas de privacidade que os *softwares* devem ser usados com um fim que não seja o monitoramento sem consentimento de um indivíduo. Um exemplo disso é um informe legal que pode ser visto no site do Mobile Tracker Free "o usuário do dispositivo deve ter conhecimento de que você está vendo seus dados pessoais [...] a empresa do Mobile Tracker Free não será, em nenhum caso, responsabilizada por suas ações" (MOBILE TRACKER FREE, 2021). Nesse sentido, é visível que as empresas aproveitam de brechas legais encontradas nas legislações e vendem um produto que pode ser usado para outro fim que não seja o designado.

A legislação brasileira proíbe que essas empresas vendam o *software* para o fim de espionar os indivíduos sem consentimento prévio. No entanto, é permitida, pela lei, a venda do *software*, capaz de roubar dados, para fins de controle parental ou monitoramento de empresas, desde que haja aviso prévio aos monitorados. Com essa permissão, dada pela lei, as empresas vendem o produto sem qualquer tipo de verificação do intuito do uso e, com isso, o *stalker* não encontra desafios para adquirir a ferramenta necessária para o monitoramento ilegal.

Atualmente, no mercado, existem várias opções de *softwares* espiões, como os já citados TheTruthSpy ou Mobile Tracker Free. Diante desse amplo mercado, os consumidores podem escolher inúmeros pacotes de serviço que monitoram mensagens, localização geográfica, ligações e, até mesmo, fazem capturas de tela por preços acessíveis a qualquer indivíduo. Assim, basta o *stalker* ter acesso ao aparelho do alvo e instalar o *software*, que fica e segundo plano de modo quase imperceptível, dessa forma, ele pode monitorar a atividade da vítima de maneira remota.

Conclui-se, portanto, que o *stalkerware* pode ser obtido, instalado e utilizado de maneira simples, o que influencia diretamente no grande número de casos registrados de *stalking* com o uso do *stalkerware*, visto no relatório emitido pela Kaspersky (2021). Infere-se que a privação desse tipo de *software* pode ser realizada de maneira análoga a burocratização feita para a obtenção do porte de armas, que rege no Estatuto do Desarmamento (BRASIL, 2003). Com esse Estatuto houve uma redução expressiva do número de homicídios registrados e, de modo semelhante, poder-se-ia deduzir que o número de ocorrências de *stalking* por *softwares* sofreria uma redução. Logo, burocratizar a obtenção do *stalkerware* se faz necessária.

3. O *STALKERWARE* E A LEGISLAÇÃO BRASILEIRA

O Código Legislativo Brasileiro não abrange alguns casos que envolvem o mundo cibernético, com isso, muitos crimes virtuais não são julgados de maneira justa. Uma vez que esses são condenados com base em uma legislação não específica. No entanto, o poder legislativo brasileiro deu início ao desenvolvimento de mecanismos mais específicos para inibir a prática do stalking que, de acordo com o Código Penal Brasileiro, infringe a lei nº 14.132, de 31 de março de 2021, art. 147-A "perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade" (BRASIL, 2021).

Além disso, o stalkerware invade a privacidade do indivíduo, de acordo com o Código Penal Brasileiro, violando a lei nº 12.737, de 30 de novembro de 2012, art. 154-A:

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita (BRASIL, 2012).

Dessa forma, o indivíduo que pratica o *stalking*, por meio do *stalkerware*, está sujeito a sanções estabelecidos pelo Código Legislativo Brasileiro.

Ademais, os sistemas operacionais, como Android ou IOS, por exemplo, desenvolveram barreiras contra os *stalkerwares*. Nesse sentido, a empresa Google estabelece uma Política de Desenvolvimento de Programas que proíbe a comercialização dos *softwares* de espionagem que atuam sem consentimento prévio na sua loja oficial de aplicativos para o Android, a Play Store, "não é permitido usá-los para monitorar outras pessoas, mesmo com conhecimento ou permissão delas e independentemente de os apps exibirem uma notificação contínua" (SUPPORT GOOGLE, 2020).

Portanto, de modo semelhante, o Código Legislativo Brasileiro deve proibir qualquer tipo de uso do *software*, independentemente se for para controle parental ou gerenciamento de empresas com aviso prévio. A partir dessa medida as empresas que se beneficiam da lacuna na legislação brasileira para a comercialização dos *stalkerwares* serão restringidas e o *software* não poderá ser utilizado para fins de invasão de privacidade digital. Desse modo o número de vítimas acometidas pelo *stalking* digital será vertiginosamente reduzido.

4. CONSIDERAÇÕES FINAIS

A partir do exposto, infere-se que a prática do *stalking*, por meio de *stalkerwares*, é um perigo evidente para a preservação da privacidade individual no meio digital. É por esse motivo que a legislação brasileira precisa criar mecanismos para coibir a espionagem digital, uma vez que as leis vigentes apresentam lacunas que são aproveitadas pelas empresas, desenvolvedoras dos *stalkerwares*, e pelos *stalkers*.

Além disso, o tema deve ser exposto e debatido a fim de que a população brasileira tenha conhecimento de como agir perante a uma ameaça de *stalkerware* e identificar a presença dele em seus *gadgets*. Nesse sentido, os dados e informações individuais estarão mais seguros de ameaças no meio virtual e na realidade. Assim, não haverá possibilidade de que ocorram chantagens, extorsões, vendas ou até mesmo divulgações feitas a partir dos dados de algum indivíduo.

Dessa forma, conclui-se preliminarmente que para evitar a propagação da espionagem digital, feita por *stalkerwares*, devem existir mais mecanismos que sejam eficientes na mitigação dos *softwares* espiões. Embora recentemente o artigo 147-A, da lei nº 14.132, de 31 de março de 2021, tenha sido promulgado, ele não combate integralmente o *stalking*. É por essa razão que o Poder Legislativo deve elaborar uma lei que seja mais restritiva, não deixando espaços para a alegação de controle parental ou monitoramento empresarial como justificativa para o uso de *softwares* como os *stalkerwares*. Desse modo, conclui-se que com a ação governamental sugerida o número de casos de espionagem digital por *stalkerwares* será reduzido.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. *Lei nº 10.826*, de 22 de dezembro de 2003. Dispõe sobre registro, posse e comercialização de armas de fogo e munição e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2003/l10.826.htm. Acesso em: 1 maio 2021.

BRASIL. *Lei nº 12.737*, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 1 maio 2021.

BRASIL. *Lei nº 13.709*, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 01 maio 2021.

BRASIL. *Lei nº 14.132*, de 31 de março de 2021. Atualiza e consolida a legislação sobre o crime de perseguição e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14132.htm. Acesso em: 01 maio 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.

KASPERSKY. *O Estado do Stalkerware em 2020*, 2021. Disponível em: https://media.kasperskycontenthub.com/wp-content/uploads/sites/100/2020/03/25175214/PT_BR_The-State-of-Stalkerware-2020.pdf. Acesso em: 01 maio 2021.

MARQUES, Carlos Henrique Alvarenga Urquisa. Stalking: o assédio da modernidade. *Barroso e Coelho Advocacia*, 2020. Disponível em: https://www.barrosoecoelho.com.br/blog/2020/2/14/stalking-o-assdio-da-modernidade#:~:text=A%20persegui%C3%A7%C3%A3o%20promovida%20atrav%C3%A9s%20do,necessidade%20de%20repara%C3%A7%C3%A3o%20desses%20danos.. Acesso em: 01 maio 2021.

MOBILE TRACKER FREE. *Informe legal*, 2021. Disponível em: https://br.mobile-tracker-free.com/. Acesso em: 01 maio 2021.

STALK. *In: Cambridge Advanced Learner's Dictionary & Thesaurus*. Cambridge: Cambridge University Press, 2021. Disponível em: https://dictionary.cambridge.org/pt/dicionario/ingles/stalk. Acesso em: 01 maio 2021.

STOP STALKERWARE. *O que é stalkerware?*, 2019. Disponível em: https://stopstalkerware.org/pt/o-que-e-stalkerware/. Acesso em: 01 maio 2021.

SUPPORT GOOGLE. *Políticas do programa para desenvolvedores: comunicado do dia 16 de setembro de 2020*, 2020. Disponível em: https://support.google.com/googleplay/android-developer/answer/10065487?hl=pt-BR. Acesso em: 01 maio 2021.