

II CONGRESSO DO CONHECIMENTO

CRIMES CIBERNÉTICOS

C929

Crimes cibernéticos [Recurso eletrônico on-line] organização II Congresso do Conhecimento – Belo Horizonte;

Coordenadores: Camila Martins de Oliveira e Tarcísio Maciel Maciel Chaves de Mendonça – Belo Horizonte, 2019.

Inclui bibliografia

ISBN: 978-85-5505-877-6

Modo de acesso: www.conpedi.org.br em publicações

Tema: Empreendedorismo e inovação

1. Conhecimento. 2. Empreendedorismo. 3. Inovação. I. II Congresso do Conhecimento (1:2019 : Belo Horizonte, BH).

CDU: 34



II CONGRESSO DO CONHECIMENTO

CRIMES CIBERNÉTICOS

Apresentação

É com imensa satisfação que apresentamos os trabalhos científicos incluídos nesta publicação. Eles foram apresentados durante a programação do II Congresso do Conhecimento, nos dias 11 a 14 de setembro de 2019, em Belo Horizonte-MG. O evento proporcionou importante debate sobre a educação na era tecnológica como um dos grandes desafios enfrentados pelos profissionais do século XXI. A temática se coloca em evidência no ensino superior, em que as metodologias tradicionais ainda ocupam lugar importante nas salas de aula, contrastando com o perfil do aluno cada vez mais jovem e conectado.

Como vencer esse desafio e construir um ensino superior de excelência e que atenda às necessidades impostas pela tecnologia? A busca por esta resposta foi o que motivou a primeira edição do Congresso do Conhecimento, no ano de 2017. A temática específica escolhida para a segunda edição do evento, neste ano, foi empreendedorismo e inovação. A partir do tema, o congresso buscou debater questões como empreendedorismo de carreira, programação neurolinguística, empreendedorismo social, inteligência artificial, dentre outros temas. Além das palestras e oficinas, a segunda edição do Congresso contou também com a participação mais ativa dos congressistas, que puderam submeter trabalhos científicos para apresentação em oito grupos temáticos.

O II Congresso do Conhecimento foi uma realização conjunta da Dom Helder - Escola de Direito e da EMGE – Escola de Engenharia, tendo como apoiadores o Conselho Nacional de Pesquisa e Pós-graduação em Direito (CONPEDI), a Secretaria de Educação do Governo do Estado de Minas Gerais, a Neo Ventures, o SEBRAE, a Cozinha Vitrine e a Estrutura da Mente.

A apresentação dos trabalhos abriu caminho para uma importante discussão, em que os pesquisadores, oriundos de cinco Estados diferentes da Federação, puderam interagir em torno de questões teóricas e práticas, levando-se em consideração a temática central de cada grupo. Foram debatidos os desafios que as linhas de pesquisa enfrentam no momento e sua relação com a tecnologia e o tema geral do evento.

Na coletânea que agora vem a público, encontram-se os resultados de pesquisas desenvolvidas em diversas instituições de nível superior, notadamente as pesquisas oriundas dos programas de iniciação científica, isto é, trabalhos realizados por graduandos em Direito

e seus orientadores. Os trabalhos foram rigorosamente selecionados, por meio de dupla avaliação cega por pares no sistema eletrônico desenvolvido pelo CONPEDI. Desta forma, estão inseridos no universo das 75 (setenta e cinco) pesquisas do evento ora publicadas, que guardam sintonia direta com este Grupo de Trabalho.

Agradecemos a todos os pesquisadores pela sua inestimável colaboração e desejamos uma ótima e proveitosa leitura!

SOBERANIA EM RISCO: A AMEAÇA DO BIG DATA À MANUTENÇÃO DA PAZ LA SOUVERAINETÉ EN DANGER: LA MENANCE DU BIG DATA CONTRE LA PAIX

Lucas Tabanez Murta de Souza

Resumo

Este projeto de pesquisa pretende analisar do ponto de vista do Direito Internacional Público e da sociologia como o monitoramento de informações, impulsionado pelo big data, pode provocar instabilidade entre os Estados mediante a violação de direitos humanos e atentados contra a soberania dos demais membros da sociedade internacional. Pela análise de obras doutrinárias conclui-se que, enquanto o desenvolvimento tecnológico ultrapassou os limites concebidos, isso não pode ser dito sobre o desenvolvimento da discussão ética na utilização das tecnologias. Quanto a investigação, pertence a classificação de Witker (1985) e Gustin (2010), o tipo jurídico-projetivo. Predominará o raciocínio indutivo.

Palavras-chave: Soberania, Direito internacional, Big data, Direitos humanos, Crimes cibernéticos

Abstract/Resumen/Résumé

Ce projet de recherche veut analyser du point de vue du Droit International et de la sociologie comment surveillance des informations, intensifié pour le big data, provoque instabilité entre les États avec la violation du droits de l'homme et des attaques contre les membres de la société internationale. Avec l'analyse des œuvres doctrinales on conclut, pendant le développement de technologie a dépassé les limites conçus, mais ça ne peut pas dire sur la discussion éthique par sa utilisation. Sur la investigation, il appartenant à la classification de Witker (1985) et Gustin (2010), le type juridique-projetif. Il predominera le raisonnement inductif.

Keywords/Palabras-claves/Mots-clés: Souveraineté, Droit international, Big data, Droits de l'homme, Cyber-crime

1. COSIDERAÇÕES INICIAIS

A presente pesquisa origina-se no estudo do caso Snowden de exposição do aparelhamento de espionagem norte-americano e britânico em diversos membros da sociedade internacional. Nesse sentido, torna-se notório o impasse de como os Estados podem abusar de sua soberania e dos direitos humanos a fim de obter acesso a informações de indivíduos e membros da sociedade internacional.

Dessa forma, é lícito ponderar que o desenvolvimento da internet é, sem dúvidas, notável, principalmente em relação ao armazenamento de dados proporcionado posteriormente. No entanto, enquanto o desenvolvimento tecnológico ultrapassou os limites esperados pelo homem, isso não pode ser dito sobre o desenvolvimento da discussão ética de sua utilização. No cenário atual, a exposição do abuso da soberania de países no uso de dados oriundos de empresas privadas para proteger interesses unilaterais das potências mundiais, como demonstrado no caso Snowden, colocam em risco a soberania e a paz na sociedade internacional.

Com isso, o objetivo do trabalho é analisar do ponto de vista do Direito Internacional Público e da sociologia como o aparelhamento de monitoramento de informações, impulsionado pelo *big data*, pode provocar instabilidade entre os Estados soberanos mediante a violação de direitos humanos e atentados contra a soberania dos demais membros da sociedade internacional.

A pesquisa que se propõe pertence à vertente metodológica jurídico-sociológica. No tocante ao tipo de investigação, foi escolhido, na classificação de Witker (1985) e Gustin (2010), o tipo jurídico-projetivo. O raciocínio desenvolvido na pesquisa será predominantemente indutivo. Por fim, a pesquisa visa esclarecer o problema correlacionado a espionagem de dados e possíveis alternativas que possibilitem a resolução sem a burocratização de contato entre pessoas de todo o globo, próprio da internet.

2. DO PANOPTISMO REAL

O panótico de Bentham é a figura abordada por Paul-Michel Foucault a fim de explicar a nova lógica de controle moderna. Em sua obra “Vigiar e Punir”, o autor explica a inversão da lógica da masmorra pela lógica vigilante do panótico. Além disso, ele descreve a arquitetura da prisão e indica como ela estaria inteiramente focada em mostrar ao detento que cada um de

seus passos está sendo monitorado, a fim de controlar cada um de seus movimentos (FOUCAULT, 1975, p. 215-216)

A despeito disso, Foucault nunca chegara a efetivamente experienciar o aprimoramento dessa lógica com a rede mundial de computadores. No panoptismo real, os indivíduos, pelas facilidades proporcionadas pelos aplicativos de comunicação, são incentivados a trocarem informações e, muito embora a intenção daqueles seja somente demonstrar momentos de felicidade para sua família e amigos, o monitoramento a serviço da guerra cibernética por informações não cessa.

Nesse sentido, pode-se depreender uma compatibilidade analógica ao ambiente da internet que, apesar de ser considerada livre, ainda sofre a incidência dos vigias. No entanto, torna-se difícil esclarecer quem exatamente são eles. Ora, o acesso de informações promovido pelo desenvolvimento da armazenagem massiva de dados, o big data, pode interessar a diversas instituições, inclusive aos governos das potências internacionais.

Indubitavelmente, as tentativas de espionagem das potências não tardariam em serem expostas. No caso Snowden, divulgado pelo jornalista Glenn Greenwald, revelam que a Agência de Segurança Nacional¹, dos Estados Unidos, e o Quartel General de Comunicação do Governo², do Reino Unido, seriam os principais responsáveis. Primeiramente, as agências iniciaram o projeto denominado *Bullrun*, que tinha o objetivo de colocar falhas de segurança escondidas em aplicativos comerciais, essas falhas eram chamadas de *backdoor* ou *trapdoor*, com isso, as instituições tinham acessos à dados fornecidos pelos aplicativos diretamente. Em segundo plano, a NSA e a GCHQ também utilizavam seus supercomputadores para quebrar a segurança dos dados pela “força bruta” (THE GUARDIAN, 2014).

Dessa forma, é possível notar, em primeira análise, um abuso do poder concedido pela soberania dos países quando utilizam de sua verba milionária para extrair informação de seus cidadãos e empresas. Não obstante, o abuso torna-se ainda mais notório ao passo que a Microsoft, em uma declaração, afirma ter sido obrigada a cooperar com o programa PRISM da NSA. De acordo com a reportagem:

As empresas de tecnologia mantem a declaração de trabalharem com a agência de inteligência somente quando legalmente obrigada. O The Guardian previamente reportou que a Microsoft cooperava com a NSA para contornar a criptografia do Outlook.com email e serviços de conversa. A empresa insistiu que ela foi obrigada a cumprir com a "existência de demandas da lei", quando concebia seu produto (THE GUARDIAN, 2014, tradução nossa).

¹ Nacional Security Agency (NSA).

² Government Communication Headquarters (GCHQ)

É fácil acreditar que a espionagem norte-americana afeta somente os cidadãos do país. No entanto, Lyon explica que o programa da NSA, PRISM, além de dar acesso direto aos dados das grandes empresas envolvidas com o armazenamento de dados e internet, salientando Apple, Facebook, Google, Microsoft, Skype, Yahoo e YouTube, também dispunha do programa denominado “Co- Traveller”. Nessa iniciativa, a agência poderia buscar alvos estrangeiros por meio de dados de cidadãos americanos e, uma vez alcançando alvos estrangeiro, poderia coletar dados da rede por meio de dados anteriormente coletados, criando uma escala gigante de coleta de informação. Por conseguinte, com a violação de informações de cidadãos estrangeiros, é gerado uma responsabilidade internacional. (LYON, 2014).

A despeito de consequências, é possível ponderar que a espionagem é uma questão de segurança nacional e comum a todos os países, todavia, o novo tipo de espionagem, promovido pelo panoptismo real, insere civis em meio a uma iminente guerra cibernética, na qual há uma disputa para o controle da sociedade internacional. Todavia, faz-se claro outro limite claramente violado por essa prática, os Direitos Humanos. O documento de 1948 dispõe em seu artigo 12 que ninguém será submetido a interferências arbitrárias com sua privacidade, família, casa e correspondência, ironicamente as práticas da NSA fere cada um desses bens jurídicos (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1948).

3. A regulação da internet em equivalência ao surgimento dos Direitos Humanos

A internet, como é notável, é o expoente máximo da globalização iniciada com as expedições marítimas europeias. Não é possível, porém, olvidar que a relação entre homens é a própria fonte matriz do Direito. E, embora fora criado alguns direitos para os povos conquistados, por muito tempo foi difícil compreender de fato a existência de uma única espécie de seres humanos no planeta, mais difícil ainda desenvolver respeito para com a vida de outrem. O primeiro ponto crítico, deu-se início após o fim da primeira grande guerra, a qual ceifou milhares de vida e arrasou o antigo império alemão. Em segundo plano, devido a negligência ao primeiro ponto, deu-se origem a conhecida Segunda Guerra Mundial.

Em ambos os cenários, como Hannah Arendt explica, ocorreram grandes migrações e, essa população errante, não tinha direitos, estava inserida em uma guerra maior do que poderia reger o direito nacional. Segundo a própria autora: “Uma vez fora do país de origem, permaneciam sem lar; quando deixavam o seu Estado [...] perdiam todos os direitos: eram o refugio da terra” (ARENDT, 1951, p. 300). Desse modo, não eram dignos de nenhum respeito, estranhos que deveriam ser tratados de acordo com a misericórdia do Estado no qual estavam

dispostos. Por consequência, após o fim da segunda grande guerra, houveram diversas atrocidades em que a tecnologia humana, tão exaltada até então, foi utilizada para a destruição da própria espécie. Em resposta a isso, as nações deram origem ao tribunal de Nuremberg e, posteriormente, a Declaração Universal dos Direitos Humanos.

Em uma linha similar, salienta-se que a globalização cresceu com a progressão geométrica das tecnologias de informação. Nesse sentido, houve um crescimento de relações interpessoais e, logo, a necessidade de novos direitos. Assim como a globalização criou adventos catastróficos para a humanidade, a internet tem efeito semelhante, primeiramente o já citado caso Snowden e, em segundo o caso da Cambridge Analytica. A partir desse momento, os dados gerados pelas redes sociais, como destacado no panoptismo real, foram transformados nas commodities mais valorizadas. Com isso, partindo de testes de personalidades empresas se especializaram no uso dessas informações. Segundo Lara (2019, p. 102):

Como produto de seu trabalho antiético e ilegal, restou claro que a empresa Cambridge Analytica passou a possuir um rico acervo de dados sobre 50 milhões de pessoas, como revelou o The Guardian, podendo manipular o conteúdo da campanha e direcionar toda sua produção de conteúdo, favorável ao candidato Trump [...].

Dessa maneira, os dados obtidos pela Cambridge Analítica, explica Lara, foram utilizados para controle social e, por conseguinte subverter a lógica democrática de diversos membros da sociedade internacional. Primeiramente, é explicitado a ligação clara e efetiva da empresa na campanha de Trump nos Estados Unidos da América, no Brexit e outros (LARA, 2019). Teme-se, portanto, o surgimento de Estados e empresas que controlem os dados promovidos pela internet ao ponto de suprimirem a soberania e dos demais países. Portanto, considera-se a solução mais viável, como apontado por Brito, a criação de uma declaração em *soft law*, objetivando a defesa dos Estados sem enfraquecer o Direito Internacional (BRITO, 2014).

4. Considerações Finais

Diante do exposto, verifica-se uma política de negligência aos perigos promovidos pela falta de regulação na internet. Nesse sentido, a soberania e os princípios democráticos fundamentais para a manutenção dos direitos humanos põem-se em risco iminente de derrocada, uma vez que Estados cada vez mais inserem seus cidadãos e estrangeiros a uma guerra por dados, a qual inicia um processo de retrocesso a evolução das relações entre seres humanos.

Com isso, faz-se necessário a atuação crítica dos órgãos internacionais para defender a paz e a privacidade dos seres humanos. E, embora a guerra por informação em um mundo conectado seja inevitável, uma declaração de princípios não vinculante de como deve ser a conduta de empresas e Estados em relação aos dados de cidadãos, próprios do país ou estrangeiros, deve ser o primeiro passo para a resolução do problema e indução de uma tendência à proteção da soberania não somente de seu país, mas a livre determinação de todos os povos.

REFERÊNCIAS

AREDT, Hannah. *As origens do totalitarismo*. 7. ed. San diego: Harcourt Brace Jovanovich, Inc, 1979. Disponível em: <https://bit.ly/1M0mclq>. Acesso em: 24 ago. 2019.

BRITO, Adriane Sanctis. *O regime internacional da internet: construção argumentativa de sua especialidade*. 2014. Monografia (obtenção do título de Mestre em Direito) - Universidade de São Paulo, São Paulo, 2014. Disponível em: <https://bit.ly/2HokVJK>. Acesso em: 25 ago. 2019.

FOUCAULT, Paul-Michel. *Vigiar e Punir: nascimento da prisão*. Tradução de Raquel Ramallete. 20. ed. Petrópolis: Editora Vozes, 1999. Disponível em: <https://bit.ly/2KUm0eA>. Acesso em: 25 ago. 2019.

GREENWALD, Gleen. Revealed: how US and UK spy agencies defeat internet privacy and security. *The Guardian*. Disponível em: <https://bit.ly/2ovkbuj>. Acesso em: 24 ago. 2019.

GUSTIN, Miracy Barbosa de Sousa; DIAS, Maria Tereza Fonseca. *(Re)pensando a pesquisa jurídica: teoria e prática*. 3ª. ed. Belo Horizonte: Del Rey, 2010.

LARA, Caio Augusto Souza. *O acesso tecnológico à justiça: por um uso contra-hegemônico do do big data e dos algoritmos*. 2019. Monografia (obtenção do título de Doutor em Direito) – Universidade Federal de Minas Gerais, Belo Horizonte, 2019.

LYON, David. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big data & Society*, Kingston v.2, ed. 7, p. 1-13. 2014. Disponível em: <https://bit.ly/2KUwVEZ>. Acesso em: 25 ago. 2019.

UNITED NATIONS. *Universal Declaration of Human Rights*. Paris: UN, 1948. Disponível em: <https://bit.ly/2FDJSix>. Acesso em: 25 ago. 2019.

WITKER, Jorge. *Como elaborar uma tesis en derecho: pautas metodológicas y técnicas para el estudiante o investigador del derecho*. Madrid: Civitas, 1985.