UNIVERSIDADE FEDERAL DE SANTA CATARINA
CAMPUS REITOR JOÃO DAVID FERREIRA LIMA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

JULIANA DANTAS LIMA

Discurso de ódio em ambiente virtual:

contribuições da gestão da informação para aumento da eficiência na investigação policial

FLORIANÓPOLIS
2020

JULIANA DANTAS LIMA

Discurso de ódio em ambiente virtual:
contribuições da gestão da informação para aumento da eficiência na investigação policial

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Informação da Universidade Federal de Santa Catarina para a obtenção do título de Mestre em Ciência da Informação como parte dos requisitos necessários à obtenção do título de mestrado.

Orientador: Dr. William Barbosa Vianna

Florianópolis

2020

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Lima, Juliana Dantas
Discurso de ódio em ambiente virtual : contribuições da Gestão da Informação para aumento da eficiência na investigação policial / Juliana Dantas Lima ; orientador, William Barbosa Vianna, 2020.
119 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro de Ciências da Educação, Programa de Pós Graduação em Ciência da Informação, Florianópolis, 2020.

Inclui referências.

1. Ciência da Informação. 2. Crime de ódio. 3. Racismo. 4. Internet. 5. Investigação policial. I. Vianna, William Barbosa. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Ciência da Informação. III. Título.

Juliana Dantas Lima

Discurso de ódio em ambiente virtual:
contribuições da gestão da informação para aumento da eficiência na investigação policial

O presente trabalho em nível de mestrado foi avaliado e aprovado por banca examinadora composta pelos seguintes membros:

Prof. Dr. Cezar Karpinski
Universidade Federal de Santa Catarina – UFSC

Prof. Dr. Rogério, da Silva Nunes
Universidade Federal de Santa Catarina – UFSC

Prof. Dr. Rodrigo Eduardo Botelho Francisco
Universidade Federal do Paraná – UFPR

Prof. Dr. Marcio Matias - suplente
Universidade Federal de Santa Catarina - UFSC

Prof. Dr. Maurício Floriano Galimberti - suplente
Universidade Federal de Santa Catarina - UFSC

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para obtenção do título de mestre em Ciência da Informação.

Documento assinado digitalmente
Adilson Luiz Pinto
Data: 10/05/2020 10:54:55-0300
CPF: 184.218.848-83

Prof. Dr. Adilson Luiz Pinto
Coordenação do Programa de Pós-Graduação em Ciência da Informação

Prof. Dr. William Barbosa Vianna
Orientador

Documento assinado digitalmente
William Barbosa Vianna
Data: 11/05/2020 01:23:42-0300
CPF: 456.660.911-15

Florianópolis, 2020.

Dedico este trabalho aos meus pais, base de tudo; aos meus irmãos e cunhada, parceiros de todas as jornadas e às minhas sobrinhas, Clarice e Manuela, as alegrias da família. Dedico ainda à Polícia Federal pela oportunidade de trabalhar em uma instituição norteada por valores nos quais acredito e aos meus colegas policiais federais que compartilham da crença de que juntos podemos contribuir para a construção de um país melhor.

AGRADECIMENTOS

Agradeço a Deus pela oportunidade de aprender, pelas inspirações e orientações e por nunca me deixar só. Aos meus pais, Marcos Rutênio e Clerisa, por todo amor que recebi e pelo esforço no investimento em minha educação. Em especial, agradeço a minha mãe, por ser exemplo de mulher batalhadora, que me fez crescer consciente de que a liberdade e a independência estão no trabalho e nos estudos.

Agradeço à Polícia Federal pela oportunidade de estudar e contribuir com novos conhecimentos para a instituição. À Universidade Federal de Santa Catarina por proporcionar um ambiente de estudo confortável e acolhedor.

Agradeço aos professores do Programa de Pós-Graduação em Ciência da Informação pelos conhecimentos ministrados, pelo acolhimento e dedicação. Em especial, agradeço ao meu orientador, Prof. Dr. William Barbosa Vianna, por ter acreditado no potencial deste trabalho e por ter conduzido a pesquisa com toda a sua experiência, conhecimento e dedicação.

Agradeço aos meus colegas de mestrado, pelos momentos de descontração e pela amizade construída ao longo da convivência. Em especial, agradeço a amiga Rejane Haltenburg pelo carinho, parceria e incentivo nos momentos difíceis, amizade para a vida toda que o mestrado me proporcionou; a Débora Campos pelas dicas e momentos de boas risadas; a Paula Dora pelo acolhimento e pelos momentos alegres de boas conversas e ao amigo Marcelo Moreira pelo apoio e incentivo.

Por fim, agradeço a minha cachorrinha Nana, companheira inseparável, abdicando de passeios e de algumas madrugadas de sono, mas mantendo sempre a mesma alegria e o mesmo amor.

Ninguém nasce odiando outra pessoa pela cor de sua pele, ou por sua origem, ou sua religião. Para odiar, as pessoas precisam aprender, e se elas aprendem a odiar, podem ser ensinadas a amar, pois o amor chega mais naturalmente ao coração humano do que o seu oposto. A bondade humana é uma chama que pode ser oculta, jamais extinta (MANDELA, 1995).

RESUMO

O presente trabalho tem como objetivo identificar formas de aumentar a eficiência da Polícia Federal na investigação de crimes de ódio na Internet, com o apoio da Gestão da Informação. Os crimes de ódio são crimes de caráter coletivo e suas vítimas comumente fazem parte das chamadas minorias sociais. A pesquisa aborda o estudo dos crimes de ódio na Internet, contextualizando-o à luz da legislação brasileira e das atribuições da Polícia Federal, a qual compete a investigação do crime de racismo cometido pela Rede Mundial de Computadores, previsto no art. 20 da Lei nº 7.716/1989. Trata-se de uma pesquisa exploratória cujo tema ainda é pouco tratado em estudos científicos, não tendo sido encontrado nas pesquisas bibliográficas realizadas nenhuma obra com abordagem idêntica. No que tange aos procedimentos metodológicos, foram utilizadas técnicas de pesquisa bibliográfica e documental, recorrendo à análise de livros, artigos, teses, dissertações, legislação nacional e internacional assim como jurisprudências nacionais que tratam do objeto estudado. A seguir, foram realizados levantamentos técnicos entre especialistas em investigação de crimes cibernéticos, visando analisar a aplicabilidade de ferramentas usadas na investigação de outros crimes na apuração dos casos de racismo na Internet. Procedeu-se ainda à pesquisa no site da Polícia Federal sobre operações policiais já realizadas relacionadas ao racismo na internet bem como buscas sobre dados quantitativos de inquéritos policiais relacionados ao tema. São abordadas questões como a importância da atuação do Estado na regulamentação de condutas praticadas na Internet; a investigação de crimes cibernéticos no Estado Informacional; os ilícitos praticados pela propagação de discursos de ódio na Internet; a atuação da Polícia Federal na investigação de crimes de racismo na Internet e o uso de conhecimentos oriundos das investigações de outros crimes cibernéticos para apurar os crimes de ódio cometidos em ambiente virtual. Como resultado, constatou-se a relevância da formação de parcerias com instituições governamentais e não-governamentais para a criação de redes de colaboração e intercâmbio de informações a fim de combater o racismo na internet. Verificou-se ainda a necessidade da adoção de medidas para o esclarecimento da população sobre os discursos de ódio na internet, os casos em que estes configuram crimes, quais os tipos penais a eles relacionados e a que instituições se deve recorrer. Verificou-se ainda que o desenvolvimento ou aquisição de software para varredura na internet pela busca por palavras-chave, utilizando técnicas de mineração de texto contribuiria para a eficiência das investigações. Neste contexto, propõe-se a adoção de ferramentas da Gestão da Informação para aprimorar a eficiência da investigação de crimes relacionados à discriminação e ao racismo na Internet, analisando estratégias para aprimorar a coleta de informações sobre tais fatos. Vários são os caminhos e não seria possível adotar uma solução única para equacionar demandas tão diversificadas e dotadas de especificidades. Uma possibilidade a ser explorada em estudos futuros é a criação de ferramentas de mineração de texto aplicadas ao monitoramento de discursos discriminatórios e racistas na Internet para dar suporte às investigações deste tipo de crime.

Palavras-chave: Crime de ódio. Racismo. Internet. Investigação policial. Gestão da Informação.

ABSTRACT

This paper aims to identify ways to increase the efficiency of the Federal Police in investigating hate crimes on the Internet, with the support of Information Management. Hate crimes are crimes of a collective nature and their victims are commonly part of the so-called social minorities. The research addresses the study of hate crimes on the Internet, contextualizing it in the light of Brazilian legislation and the competency of the Federal Police, which is responsible for investigating the crime of racism committed by the World Wide Web, provided for in art. 20 of Law No. 7,716 / 1989. It is an exploratory research whose theme has not been explored enough in scientific studies, and no other papers with an identical approach have been found in the bibliographic researches. Regarding methodological procedures, bibliographic and documentary research techniques were used, through the analysis of books, articles, theses, dissertations, national and international legislation as well as national jurisprudence dealing with the object studied. Next, technical surveys were carried out among experts in the investigation of cybercrimes, aiming to analyze the applicability of tools used in the investigation of other crimes when dealing with cases of racism on the Internet. There was also research on the Federal Police website about police operations already carried out related to racism on the internet, as well as searching for quantitative data from police inquiries related to the topic. Topics such as the importance of the State's role in the regulation of Internet conduct are addressed; the investigation of cybercrimes in the Informational State; the illicit acts practiced by the propagation of hate speech on the Internet; the role of the Federal Police in investigating crimes of racism on the Internet and the use of knowledge from investigations of other cybercrimes to investigate hate crimes committed in a virtual environment. As a result, it was detected how important it is to form and strengthen partnerships with governmental and non-governmental institutions to form collaborative networks and exchange information to combat racism on the internet. There was also a need to adopt measures to inform the population about hate speech on the internet, about when these constitute crimes, which are the related criminal types and to which institutions one should contact. It was also found that the development or acquisition of software for scanning the internet by searching for keywords, using text mining techniques, would contribute to the efficiency of the investigations. In this context, it is proposed to adopt Information Management tools to improve the efficiency of investigating crimes related to discrimination and racism on the Internet, analyzing strategies to improve the collection of information on such facts. There are several paths and it would not be possible to adopt a single solution to address such diverse and specific demands. One possibility to be explored in future studies is the creation of text mining tools applied to the monitoring of discriminatory and racist discourses on the Internet to support investigations of this type of crime.

Keywords: *Hate crime. Racism. Internet. Police investigation. Information management.*

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ADO	Ação Direta de Inconstitucionalidade por Omissão
ARPA	*Advanced Research Projects Agency Network*
CF	Constituição Federal
CGPFAZ	Coordenação-Geral de Polícia Fazendária
CI	Ciência da Informação
CPS	*Child Protection Sistem*
CRFB	Constituição da República Federativa do Brasil
DICOR	Diretoria de Investigação e Combate ao Crime Organizado
DUDH	Declaração Universal dos Direitos do Homem
ECA	Estatuto da Criança e do Adolescente
GI	Gestão da Informação
GRCC	Grupos de Repressão a Crimes Cibernéticos
GRI	Gestão de Recursos de Informação
HC	Habeas Corpus
IP	*Internet Protocol*
KDD	*Knowledge Discovered Databases*
KDT	*Knowledge Discovered in Texts*
LGBT	Lésbicas, Gays, Bissexuais, Travestis, Transexuais e Transgêneros
NCMEC	*National Center for Missing & Exploited Children*
ONG	Organização não governamental
ONU	Organização das Nações Unidas
P2P	*Peer-to-peer,* ou ponto-a-ponto
PF	Polícia Federal
PI	Pornografia infantil
PNL	Programação Neurolinguística
SRCC	Serviço de Repressão a Crimes Cibernéticos
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
TI	Tecnologia da Informação
TIC	Tecnologias da Informação e Comunicação
TLD	*Top Level Domain* ou Domínio de Nível Superior
URCC	Unidade de Repressão a Crimes Cibernéticos

URCOP	Unidade de Repressão aos Crimes de Ódio e Pornografia Infantil na Internet
URL	*Uniform Resource Locator* ou Localizador Padrão de Recursos

SUMÁRIO

1 INTRODUÇÃO

A evolução tecnológica, ocorrida sobretudo a partir da segunda metade do século passado, proporcionou um notável desenvolvimento das tecnologias relacionadas à informação e comunicação, tornando-as acessíveis a milhares de pessoas. Impulsionada pelo avanço tecnológico, a comunicação tornou-se extremamente veloz, permitindo a circulação massiva de conteúdo em meio digital de uma forma praticamente instantânea, com grande repercussão social e forte impacto no relacionamento interpessoal e coletivo (CASTELLS, 2016).

Importa destacar que o ciberespaço é definido por Pierre Lévy como "o espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores" (LÉVY, 1999, p. 92). Já os crimes cibernéticos, ou crimes digitais, são aqueles em que um agente utiliza a informática ou a telemática para praticar condutas definidas em lei como ilícitas. Em tais situações, a tecnologia é utilizada como ferramenta ou instrumento para o cometimento de ilícitos penais (CRESPO, 2011).

Considerando a legislação como um produto da sociedade em que está inserida, é natural que as mudanças nas relações sociais repercutam no ordenamento jurídico. À medida em que tais relações se tornam mais complexas, faz-se necessário criar novas leis para regulamentá-las (BARRETO; BRASIL, 2016), ao mesmo tempo em que é preciso encontrar estratégias e mecanismos para garantir a aplicação dessas leis. Desse modo, as normas jurídicas aplicadas aos crimes cibernéticos e ao regramento das condutas relativas à circulação de informações no ciberespaço são fruto da adaptação do mundo jurídico às mudanças decorrentes da revolução nas tecnologias de informação e comunicação. Nesse ambiente onde seres humanos e organizações interagem, o Estado deve exercer legitimamente seu poder de regulamentar essas relações.

O presente trabalho tem como objeto de estudo a investigação dos crimes de ódio praticados por meio da Rede Mundial de Computadores. Tal denominação se aplica aos delitos que de alguma forma expressam discriminação ou intolerância contra uma coletividade. De acordo com Mason (2005), utiliza-se a expressão "crime de ódio" para definir os crimes motivados por alguma espécie de preconceito. Tal classificação pode decorrer de fatores como raça, cor, religião, etnia, sexualidade, deficiência ou gênero.

O termo "crime de ódio" não existe na legislação penal brasileira, pois não há, na legislação pátria, um tipo penal que o descreva. Embora não haja uma definição legal, a doutrina entende que tais crimes consistem em atos ilícitos motivados por ideias discriminatórias contra

determinados grupos sociais. Contudo, a falta de um tipo penal claramente definido dificulta tanto a investigação como a punição deste tipo de crime.

Existem tipos penais previstos no Brasil cuja motivação pelo preconceito é expressa em lei. A principal lei penal vigente criada para tipificar e punir condutas motivadas pelo preconceito contra grupos sociais é a Lei nº 7.716/1989, conhecida como "Lei de Racismo" (BRASIL, 1989). Segundo o artigo 1º da citada lei, "serão punidos, na forma desta Lei, os crimes resultantes de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional". O art. 20, §2º aponta como hipóteses de racismo "praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional [...] cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza", atribuindo a tais hipóteses pena de reclusão de dois a cinco anos e multa. Já o art. 20, § 3º, inciso III, prevê que o juiz, após ouvido o Ministério Público, poderá determinar "a interdição das respectivas mensagens ou páginas de informação na Rede Mundial de Computadores" – deixando claro, portanto, que o Direito Penal pátrio criminaliza a propagação de conteúdos racistas pela Internet.

Sobre a relação da Polícia Federal com o tema do racismo na Internet, nos termos da Lei nº 10.446/2002, art. 1º, inciso III, uma de suas atribuições é investigar infrações penais "relativas à violação a direitos humanos, que a República Federativa do Brasil se comprometeu a reprimir em decorrência de tratados internacionais de que seja parte", que tenham repercussão interestadual ou internacional e que exijam repressão uniforme (BRASIL, 2002). Tal violação aos direitos humanos ocorre no caso do racismo, conforme previsto na Convenção Internacional sobre a Eliminação de todas as Formas de Discriminação Racial, da qual o Brasil é signatário.

Na hipótese do art. 20, §3º, inciso III da Lei de Racismo, uma vez que o conteúdo é passível de ser acessado em qualquer parte do planeta via Internet, fica estabelecida sua repercussão internacional[1] – evidenciando, deste modo, a atribuição da Polícia Federal de investigar casos de racismo na Internet. Contudo, embora seja caracterizado o dever da PF de investigar situações de racismo, cabe atentar para o fato de que o termo "crime de ódio" é mais abrangente, pois envolve outras hipóteses de discriminação não contempladas na Lei nº 7.716/1989, como, por exemplo, as decorrentes de gênero ou orientação sexual. A ausência de

[1] Há julgados do STF e STJ que entendem que, além de existir a publicação do conteúdo via Rede Mundial de Computadores, para que sua investigação seja atribuição da Polícia Federal, é preciso que haja acesso por usuários da Internet em outros países, configurando assim a repercussão internacional.

uma tipificação penal que contemple as diversas hipóteses de crimes de ódio faz com que muitas situações de discriminação permaneçam impunes.

Em recentes julgados, o STF declarou a omissão do Congresso Nacional em regulamentar atos de discriminação contra grupos LGBT (lésbicas, gays, bissexuais, transexuais e travestis), determinando que tais situações fossem enquadradas no tipo penal do racismo até que haja futura regulamentação[2]. Outra tentativa de evitar a impunidade relacionada a crimes de ódio não previstos no ordenamento jurídico foi a criação da Lei nº 13.642/2018, que atribuiu à Polícia Federal o dever de investigar crimes de "ódio contra a mulher na Internet" (BRASIL, 2018).

Segundo a Lei nº 13.642/2018, o caput do art. 1º da Lei nº 10.446/2002 passa a vigorar acrescido do inciso VII: "quaisquer crimes praticados por meio da Rede Mundial de Computadores que difundam conteúdo misógino, definidos como aqueles que propagam o ódio ou a aversão às mulheres". Contudo, mais uma vez, a ausência de norma que defina o tipo penal de "propagar ódio", descrevendo como se caracteriza tal conduta e definindo uma pena, dificulta a aplicação da citada lei pela Polícia Federal.

Constata-se que existe uma tendência de reconhecimento pela legislação penal das diversas hipóteses de crimes de ódio, ampliando o rol de situações discriminatórias. Importa destacar que, ao se abordar o tema do racismo e do discurso de ódio de forma geral, muito já se escreveu sobre as origens sociais e históricas das diversas formas de discriminação e preconceito. Contudo, no caso do presente estudo, tem-se como foco a investigação policial do racismo na Internet e nas contribuições da Gestão da Informação (GI) para o aprimoramento dessas investigações.

Valentim e Gelinski (2005, p. 18) definem a Gestão da Informação como "um conjunto de atividades para prospectar/monitorar, selecionar, filtrar, agregar valor e disseminar informação, bem como para aplicar métodos, técnicas, instrumentos e ferramentas que apoiem esse conjunto de atividades". As atividades apontadas pelos autores guardam semelhança com a coleta, processamento e análise da informação realizados no curso de uma investigação policial. Assim, o presente estudo busca elaborar estratégias para melhorar a eficiência da investigação policial dos casos de racismo na Internet, por meio da análise dos processos relacionados à apuração de crimes de ódio e das contribuições fornecidas pela Gestão da Informação.

---

[2] Ação Direta de Inconstitucionalidade por Omissão nº 26 (BRASIL, 2019a) e Mandado de Injunção nº 4.733 (BRASIL, 2019b).

O referencial teórico está estruturado em cinco tópicos principais. O primeiro tem como tema central o Estado informacional e o poder de polícia no combate ao uso criminoso da informação. Nele são analisados: a informação na era digital, as diferentes concepções de informação, o papel estatal na Sociedade da Informação e o poder de polícia no Estado informacional. Este capítulo visa contextualizar a pesquisa no âmbito das temáticas envolvendo a Sociedade da Informação e os desafios que as novas tecnologias da informação e comunicação impõem ao Estado.

O segundo tópico aborda a questão da investigação de crimes cibernéticos. Este tema abrange o estudo das investigações criminais no Estado informacional, os crimes cibernéticos e suas características, culminando no estudo do crime de ódio no ordenamento jurídico brasileiro. Tem-se como objetivo situar a questão do crime de ódio no contexto dos crimes cibernéticos em geral, analisando suas peculiaridades e as limitações da atuação estatal para seu combate.

No terceiro capítulo do referencial, é abordada a atuação da Polícia Federal no combate a crimes de ódio na Internet. Partindo da análise das atribuições da PF para a investigação do racismo e de outras formas de ódio não previstas expressamente na Lei nº 7.716/1989, são analisados dados referentes à ação do órgão no combate ao racismo na Internet. Esta sessão visa fazer um recorte mais específico sobre ao papel da Polícia Federal no enfrentamento aos crimes de ódio em ambientes virtuais.

No quarto tópico, aborda-se a contribuição da Gestão da Informação para aprimorar a investigação de crimes cibernéticos. Nesse momento, é tratada a questão da GI como ferramenta para aprimorar a fase de coleta de informações sobre casos de racismo na Internet, analisando as formas como a PF costuma tomar conhecimento desses crimes, bem como refletindo sobre alternativas para a informação sobre o fato criminoso chegue aos responsáveis pela investigação.

Nesse contexto, a GI pode contribuir com a criação de estratégias relacionadas ao posicionamento do órgão perante outras instituições (públicas ou particulares). Assim, analisa-se a relevância de se firmar parcerias a fim de ampliar o acesso a informações sobre crimes de ódio na Internet. A visão estratégica sobre formas de consecução dos objetivos institucionais na investigação policial pode ser analisada sob os fundamentos da Gestão da Informação.

Tarapanoff (2006) corrobora o entendimento acerca de uma visão estratégica da GI como ferramenta para manutenção e evolução de uma organização. O autor entende que a finalidade primordial da Gestão da Informação é o acompanhamento de processos, o suporte às

decisões estratégicas e a obtenção de vantagens competitivas sobre a concorrência. Trata-se, portanto, de uma ferramenta de preservação institucional, pois permite que a organização se mantenha eficiente e competitiva em relação a outras instituições.

Por fim, o quinto capítulo do traz a comparação de técnicas investigativas utilizadas em outras espécies de crimes. Assim, por meio da comparação com um software utilizado na investigação da propagação de conteúdo de pornografia infantil na Internet, procura-se verificar se a adoção de ferramentas de tecnologia da informação poderia contribuir para obtenção de melhores resultados na investigação de casos de racismo na Internet.

1.1 PROBLEMATIZAÇÃO E QUESTÃO DE PESQUISA

Conforme Dumont, Ribeiro e Rodrigues (2006), o termo Tecnologia da Informação, em sentindo amplo, abrange toda tecnologia aplicada à coleta, armazenamento, processamento, uso, comunicação, transmissão e atualização de qualquer forma ou espécie de informação. O aprimoramento dessas tecnologias foi responsável pela criação e expansão da Internet, conectando milhares de pessoas.

Nos anos de 1990, a Internet se disseminou por praticamente todo planeta. A velocidade dessa expansão é assim retratada: “Para se ter uma ideia da pujança desta chamada Nova Era ou Sociedade da Informação, para atingir 50 milhões de usuários o rádio levou 38 anos, o computador pessoal, 16, e a televisão, 13, enquanto nos EUA a Internet levou apenas 4 anos” (DUMONT; RIBEIRO; RODRIGUES, 2006, p. 29).

Para Alvin Toffler, em seu livro “A terceira onda”, ao longo de sua história, a humanidade passou por três grandes “ondas” de mudanças. A primeira onda foi com a invenção da agricultura, que fez com que os indivíduos não precisassem mais ser nômades. A segunda onda, para o autor, foi a Revolução Industrial, que fez com que muito do trabalho humano passasse a ser realizado por máquinas, dando origem a uma forma de produção massificada. A terceira onda, por sua vez, foi a transição de uma sociedade industrial para uma Sociedade da Informação, na qual a tecnologia conecta produtores e consumidores. Após a terceira onda, a informação tornou-se o insumo mais relevante, sendo esse período denominado “era da informação” (TOFFLER, 1980, *apud* DUMONT; RIBEIRO; RODRIGUES, 2006, p. 144).

O intercâmbio massificado de informações e a interconexão de indivíduos em nível global também trouxeram aspectos negativos. A Internet virou um campo fértil para o cometimento de crimes, entre os quais as injúrias raciais e o racismo.

A cada onda de mudanças, a humanidade precisa se adaptar, reorganizar seus sistemas normativos e as estruturas produtivas e governamentais, a fim de adequar a realidade já existente ao novo. O presente estudo se encaixa no contexto de adaptação do aparato repressivo punitivo estatal a novos tipos de crimes, viabilizados pelas novas tecnologias da informação e comunicação.

Entre as várias modalidades de crimes cibernéticos surgidos com o advento da Era da Informação, o presente trabalho pretende se ater aos "crimes de ódio" praticados na Internet. Na legislação brasileira, não existe um conceito de crime de ódio ou um tipo penal definindo uma conduta que caracterize tal crime e imputando-lhe uma pena.

Segundo Meyer-Pflug (2009, p. 97), o discurso de ódio consiste na manifestação de "ideias que incitem a discriminação racial, social ou religiosa em determinados grupos, na maioria das vezes, as minorias". Seria o caso do crime de racismo, tipificado pela a Lei nº 7.716/1989; dos atos de discriminação contra grupos LGBT, enquadrados no tipo penal do racismo por entendimentos recentes do STF, e dos conteúdos misóginos, definidos pela Lei nº 13.642/2018 como aqueles que propagam o ódio ou a aversão às mulheres (BRASIL, 1989; 2018; 2019a; 2019b).

A presente pesquisa tem como recorte a investigação pela PF dos casos de ódio na Internet que são tipificados como crime pela legislação penal brasileira (Lei nº 7.716/1989). Em face do exposto, tem-se por objetivo responder a seguinte questão de pesquisa: como é possível aumentar a eficiência da Polícia Federal na investigação de crimes de ódio na Internet, utilizando a Gestão da Informação para auxiliar na identificação de conteúdo ilícito?

1.2 MOTIVAÇÕES E JUSTIFICATIVA

Os crimes de ódio praticados pela Internet implicam em agressões que atentam contra a dignidade humana, afetando milhares de pessoas. São crimes de caráter coletivo e suas vítimas comumente fazem parte das chamadas minorias sociais. É importante estudar formas de se combater tal conduta, de modo a evitar a impunidade e a sensação de impotência da vítima diante de situações de dor e humilhação.

No que tange à criminalidade praticada na Internet, existe um sentimento de impunidade em decorrência da sensação de anonimato em função da distância entre autor e vítima. Os criminosos informáticos, em regra, são indivíduos que percebem a Internet como um escudo e que não costumam cometer crimes fora do espaço cibernético. Em algumas situações,

há ainda uma ausência de percepção da ilegalidade da conduta, dos riscos assumidos e do dano causado à vítima (BARRETO; BRASIL, 2016).

No que tange aos dados quantitativos sobre casos de racismo na Internet, vale atentar para os indicadores da Central Nacional de Denúncias de Crimes Cibernéticos, extraídos do site mantido pela SaferNet (2019, s\n), associação civil de direito privado, sem fins lucrativos, que atua na promoção e defesa dos Direitos Humanos na Internet no Brasil[3]. Importa mencionar que tal instituição já firmou acordos de cooperação com a Polícia Federal e o Ministério Público Federal, visando colaborar com o combate a crimes cibernéticos relacionados violações a direitos humanos na Internet.

A Central de Denúncias mantida pela SaferNet traz os seguintes dados quantitativos sobre casos de racismo na Internet, referentes ao período de 2006 a 2018[4]:

> Em 13 anos, a Central de Denúncias recebeu e processou 574.873 denúncias anônimas de Racismo envolvendo 98.851 páginas (URLs) distintas (das quais 32.682 foram removidas) escritas em 7 idiomas e hospedadas em 7.002 domínios diferentes, de 110 diferentes TLDs e conectados à Internet através de 11.830 números IPs distintos, atribuídos para 62 países em 5 continentes. As denúncias foram registradas pela população através dos 3 *hotlines* brasileiros que integram a Central Nacional de Denúncias de Crimes Cibernéticos.

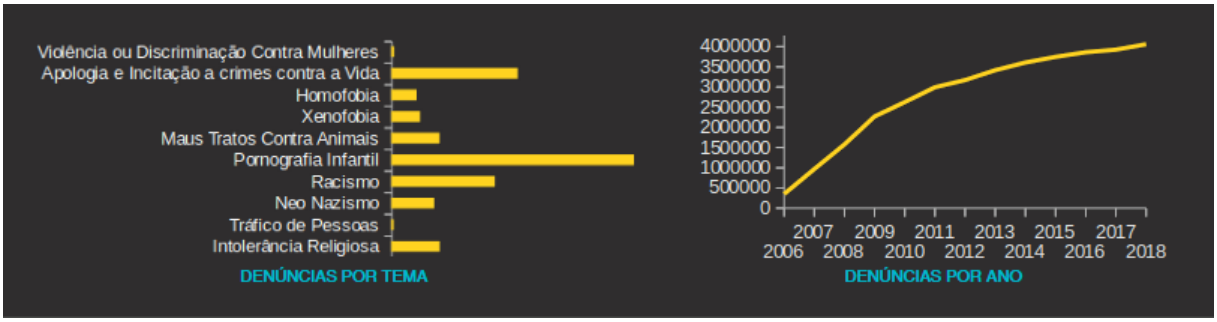
Cabe esclarecer que os dados acima estão em constante atualização, sendo provável que haja alterações quantitativas dos resultados em função da data em que a pesquisa for realizada. Ressalta-se ainda que as informações supratranscritas são extraídas com o uso de uma legenda dinâmica e que os valores foram obtidos por meio da seleção do critério "racismo"[5] na opção da legenda referente ao tipo de conteúdo.

A Figura 1 mostra a evolução do número de denúncias à ONG nos últimos anos, bem como a estratificação das denúncias por tema.

---

[3] Disponível em: https://new.safernet.org.br/content/institucional#. Acesso em: 27 out. 2019.
[4] Disponível em: http://indicadores.safernet.org.br#. Acesso em: 23 nov. 2019.
[5] Os conceitos para os termos usados na pesquisa estão disponíveis em https://new.safernet.org.br/denuncie#, por meio da seleção na legenda dinâmica do tema a ser tratado. Nesse contexto, o termo racismo refere-se a "Material escrito, imagens ou qualquer outro tipo de representação de ideias ou teorias que promovam e/ou incitem o ódio, a discriminação ou violência contra qualquer indivíduo ou grupo de indivíduos, baseado na raça, cor, religião, descendência ou origem étnica ou nacional". Acesso em: 23 nov. 2019.

Figura 1 – Projeção sobre denúncias de ódio na Internet[6]



Fonte: SaferNet (2019).

Analisar a questão do racismo na Internet é relevante para encontrar mecanismos que auxiliem em sua prevenção e punição. O combate a qualquer forma de discriminação é necessário, pois só assim é possível promover a construção de uma sociedade mais justa e igualitária.

1.3 OBJETIVOS

1.3.1 Objetivo geral

Identificar formas para aumentar a eficiência da Polícia Federal na investigação do racismo na Internet com o apoio da Gestão da Informação.

1.3.2 Objetivos específicos

- Analisar a necessidade da interferência estatal sobre condutas e relações travadas por meio da Rede Mundial de Computadores;
- Avaliar a questão dos crimes de ódio na Internet no contexto da Sociedade da Informação, a partir das jurisprudências dos tribunais superiores (STF e STJ) e de operações e investigações já realizadas pela Polícia Federal;
- Identificar estratégias para aprimorar a coleta de informações sobre discursos de ódio que configurem racismo na Internet, utilizando conhecimentos da Gestão da Informação;

[6] Disponível em: https://new.safernet.org.br/denuncie#. Acesso em: 23 nov. 2019.

- Comparar elementos relevantes da investigação de casos de pornografia infantil com as técnicas utilizadas para investigar crimes de ódio.

2 MÉTODOS E MATERIAIS

2.1 CARACTERIZAÇÃO DA PESQUISA

O presente trabalho consiste em uma pesquisa exploratória, com a finalidade de identificar elementos da Gestão da Informação capazes de aumentar a eficiência da Polícia Federal na investigação e combate aos crimes de ódio praticados pela Rede Mundial de Computadores. A pesquisa exploratória visa proporcionar ao pesquisador uma maior familiaridade com o objeto pesquisado e costuma ser aplicada ao estudo de temas ainda pouco explorados (GIL, 2010, p. 27).

Recorre-se à pesquisa exploratória quando há finalidade de aprofundar as informações relativas ao assunto investigado, colaborando para a definição e o desenvolvimento das questões que serão abordadas. Por meio dela, é possível delimitar e direcionar o tema da pesquisa, orientar seus objetivos, formular hipóteses e desenvolver novos enfoques (PRODANOV; FREITAS, 2013, p. 51-52).

Quanto à abordagem, a pesquisa pode ser classificada como de caráter qualitativo. Considera-se que a pesquisa qualitativa busca entender o mundo utilizando uma abordagem interpretativa e naturalista. Nessa abordagem, os fatos são estudados dentro do seu contexto natural, partindo do significado que as pessoas lhes atribuem. Entre as características da pesquisa qualitativa está a multiplicidade de métodos, tais como análise de documentos, entrevistas e observações (CRESWELL, 2014, p. 49-50).

O presente trabalho utiliza as técnicas de pesquisa bibliográfica e documental, visto que recorre à análise de livros, artigos, teses, dissertações e documentos que tratem do objeto estudado. A pesquisa bibliográfica refere-se ao estudo da contribuição de diversos autores sobre o tema. Já a pesquisa documental faz uso da análise de documentos para a extração de dados relevantes (LAKATOS; MARCONI, 2010).

No que tange à pesquisa bibliográfica, foram analisadas publicações que tratam sobre a questão dos crimes de ódio praticados pela Internet. O tema abordado é multidisciplinar, envolvendo conteúdos afetos às Ciências Policiais, Direito, Criminologia e Ciência da Informação. Nesse contexto, optou-se por realizar uma revisão bibliográfica narrativa da literatura. Nas palavras de Rother (2007, p. 5), “os artigos de revisão narrativa são publicações amplas, apropriadas para descrever e discutir o desenvolvimento ou o ‘estado da arte’ de um determinado assunto, sob ponto de vista teórico ou contextual”.

Por fim, foram realizados levantamentos técnicos, respondidos por especialistas em investigação de crimes cibernéticos, selecionados entre policiais federais com experiência neste tipo de investigação. A seguir, realizou-se uma comparação entre os resultados obtidos em tais levantamentos.

2.2 REVISÃO BIBLIOGRÁFICA E DOCUMENTAL

2.2.1 Revisão bibliográfica da literatura

Foi realizada uma pesquisa bibliográfica, aplicando técnicas de seleção de dados para realizar uma análise sobre os temas pesquisados. Segundo Gil (1999), a pesquisa bibliográfica é indicada para se chegar a uma solução sobre um determinado problema de pesquisa. Assim, é necessário que o tema estudado seja colocado em termos de um problema, ou seja, um questionamento a ser solucionado pelo estudo.

Os artigos científicos utilizam informações bibliográficas ou eletrônicas com a finalidade de obter resultados de pesquisas de outros autores para fundamentar teoricamente um determinado objetivo. Segundo Boccato (2006),

> A pesquisa bibliográfica busca a resolução de um problema (hipótese) por meio de referenciais teóricos publicados, analisando e discutindo as várias contribuições científicas. Esse tipo de pesquisa trará subsídios para o conhecimento sobre o que foi pesquisado, como e sob que enfoque e/ou perspectivas foi tratado o assunto apresentado na literatura científica.

A pesquisa bibliográfica costuma ser aplicada para o desenvolvimento de estudos exploratórios ou descritivos, nos quais o objeto do estudo ainda é pouco conhecido, o que dificulta a formulação de hipóteses precisas e operacionalizáveis. Nesses casos, utiliza-se a pesquisa bibliográfica como caminho para a aproximação com o tema estudado por meio das fontes bibliográficas, proporcionando um amplo alcance de informações bem como possibilitando o uso de dados dispersos em inúmeras publicações. Assim, tal pesquisa auxilia na construção ou no aprimoramento da definição do quadro conceitual relacionado ao tema do estudo (GIL, 1999; LIMA; MIOTO, 2007).

No presente trabalho, as principais fontes para a revisão bibliográfica foram bases de dados sobre Sociedade da Informação, crimes cibernéticos, racismo, investigação policial, Ciência da Informação e Gestão da Informação, em língua portuguesa e língua inglesa. A fim

de apresentar uma visão panorâmica das referências utilizadas, em um aspecto geral, foram elencados alguns dos principais referenciais teóricos utilizados.

Assim, no item 3.1, foram analisadas questões relativas aos poderes de Estado e o papel do Estado na Sociedade da Informação, adotando-se como principais referenciais teóricos Pierre Lévy (1999), Jorge Werthein (2000), Sandra Braman (2006), Marta Pinheiro (2012), Yuval Harari (2015), André Lemos (2015), Manuel Castells (2016) e Luiz Carlos Bresser Pereira (2017).

Nos itens 3.2 e 3.3, foram utilizadas referências na área de crimes cibernéticos, mais especificamente temas relacionados ao racismo praticado pela Internet. As principais referências utilizadas foram as obras de Christiano Santos (2010), Marcelo Crespo (2011), Emerson Wendt (2013) e Higor V. N. Jorge (2013). Foram ainda utilizados referenciais teóricos para extração de conceitos jurídicos usados na pesquisa, entre eles, Helly Lopes Meirelles (2002), Dalmo de Abreu Dallari (2003), Pedro Lenza (2017) e Cezar Roberto Bittencourt (2018).

No item 3.4, foram analisados conceitos relacionados à Gestão da Informação e à contribuição que os conhecimentos proporcionados por esta disciplina podem proporcionar à investigação de crimes cibernéticos, notadamente aos crimes de racismo perpetrados pela Internet. Foi abordada ainda a questão da semelhança entre tipos penais que utilizam termos e expressões discriminatórias para a sua perpetração e o uso da informação como ferramenta de esclarecimento e conscientização do usuário sobre a relevância de notificar as autoridades acerca dos crimes cibernéticos dos quais tomem conhecimento. Foram utilizados como referenciais autores como Dobrica Savic (1992), Chun Wei Choo (1995) (1998), Thomas H. Davenport (1998) (2002), Marcelo Crespo (2011), Maria Cristina V. Freitas e William B. Vianna (2019) e Luiz Miguel N. Corujo e Carlos G. Silva (2019) e o Roteiro de Atuação Crimes Cibernéticos, publicado pelo Ministério Público Federal (2016).

Já no item 3.5, realizou-se uma análise de técnicas investigativas adotadas em outras espécies de crimes a fim de verificar a aplicabilidade dos seus recursos na investigação do crime de racismo na Internet. Entre os referenciais teóricos foram adotados Rodrigo Lange e Célia Ralha (2011), Claudia Peersman *et al* (2014) e Felipe B. Caiado e Marcelo Caiado (2018).

No que concerne à amostragem para a realização da pesquisa, buscou-se obter uma amostra dos principais artigos, teses e dissertações sobre o tema por meio de buscas nos seguintes sites acadêmicos: Google Acadêmico, *Scopus* e *Web of Science*. Assim, quanto aos aspectos específicos da pesquisa bibliográfica, foram realizadas buscas com os termos *racismo*,

crime de ódio e *Internet*, optando pela utilização das aspas a fim de que os resultados fossem mais precisos.

Entre os critérios para a seleção dos arquivos, o principal foi a acurácia em relação ao objeto de estudo do presente trabalho. Também foi considerada a qualidade acadêmica dos resultados das buscas.

O repositório que apresentou um maior número de resultados foi o Google Acadêmico. Ao se pesquisar por *racismo* AND *Internet* para páginas em português, sem qualquer outro filtro, surgiram aproximadamente 32.000 resultados. Diante da magnitude do número de resultados, optou-se por restringir a pesquisa aos anos de 2015 a 2019, tendo sido obtidos aproximadamente 15.500 resultados. Considerando que a última pesquisa também apresentou resultados elevados, optou-se por acrescentar o termo *investigação* às buscas, deixando os demais parâmetros (páginas e português e lapso temporal) inalterados. Nesta última busca foram apresentados 10.300 resultados, número ainda bastante elevado. Por fim, optou-se por acrescentar o termo *policial* aos mesmos parâmetros de busca utilizados anteriormente, chegando-se ao número de 3.750 resultados. Assim, a pesquisa nesta base de dados não se mostrou viável devido ao grande volume de resultados positivos, dificultando a seleção de documentos alinhados aos objetivos centrais da pesquisa.

Ato contínuo, foi realizada pesquisa na base de dados da Scopus, na qual, utilizando os argumentos "*Internet"* AND "*racismo"* entre os anos de 2015 a 2019, a busca resultou em 100 resultados, sendo 21 destes de *"Open Access"*. Foram lidos os resumos *(abtracts)* dos 21 artigos de acesso aberto. Observou-se que os documentos tinham como foco a abordagem de questões sociais relacionadas ao racismo na Internet. Não foram encontrados documentos focados na perspectiva das investigações policiais.

Por fim, ao se pesquisar pelos termos *racismo*, *Internet* e *crime*, utilizando o booleano AND na plataforma Web of Science e restringindo a busca aos últimos 5 anos, foram encontrados apenas 11 resultados, os quais não apresentaram aderência ao foco dado pela pesquisa, qual seja, o estudo dos crimes de racismo na Internet à luz da investigação policial.

Importa observar que o fato de a pesquisa bibliográfica não ter encontrado referências que tratassem especificamente sobre o tema da investigação policial de casos de racismo na Internet gerou a necessidade de fazer aproximações e reflexões, partindo de outras vertentes ou perspectivas, bem como de outros estudos de caso. Assim, em algumas situações, os temas abordados nesse trabalho, tais como racismo, crimes cibernéticos, Ciência da Informação, Gestão da Informação, Direito Digital e tecnologias da informação, foram estudados

individualmente, sendo necessário fazer reflexões para se chegar a uma perspectiva ampla e proporcionar uma visão mais abrangente sobre o problema de pesquisa.

2.2.2 Revisão documental

No tocante à pesquisa documental, foram utilizadas legislações nacionais e internacionais, bem como jurisprudências nacionais do STF e STJ sobre racismo praticado pela Rede Mundial de Computadores e temas conexos. Considerando que o objeto central do estudo é a investigação pela Polícia Federal do racismo praticado pela Rede Mundial de Computadores, optou-se por centralizar a análise documental (legislação e jurisprudência) em fontes nacionais.

A pesquisa documental foi realizada de forma suplementar à pesquisa bibliográfica. Na construção da pesquisa em referência, procedeu-se à análise dos documentos de natureza jurídica listados a seguir.

2.2.2.1 Documentos nacionais

- Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal (BRASIL, 1940);
- Lei nº 5.172, de 25 de outubro de 1966 (Código Tributário Nacional). Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios (BRASIL, 1966);
- Constituição da República Federativa do Brasil de 1988 (BRASIL, 1988);
- Lei nº 7.716, de 5 de janeiro de 1989 (Lei de Racismo). Define os crimes resultantes de preconceito de raça ou de cor (BRASIL, 1989);
- Lei nº 10.446, de 8 de maio de 2002. Dispõe sobre infrações penais de repercussão interestadual ou internacional que exigem repressão uniforme, para os fins do disposto no inciso I do § 1o do art. 144 da Constituição (BRASIL, 2002);
- Lei nº 11.340, de 7 de agosto de 2006 (Lei Maria da Penha). Cria mecanismos para coibir a violência doméstica e familiar contra a mulher, nos termos do § 8º do art. 226 da Constituição Federal, da Convenção sobre a Eliminação de Todas as Formas de Discriminação contra as Mulheres e da Convenção Interamericana para Prevenir, Punir e Erradicar a Violência contra a Mulher;

dispõe sobre a criação dos Juizados de Violência Doméstica e Familiar contra a Mulher; altera o Código de Processo Penal, o Código Penal e a Lei de Execução Penal; e dá outras providências (BRASIL, 2006);

- Lei nº 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências (BRASIL, 2012a).
- Lei nº 12.737, de 30 de novembro de 2012 (Lei Carolina Dieckman). Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências (BRASIL, 2012b);
- Lei nº 13.104, de 9 de março de 2015. Altera o art. 121 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, para prever o feminicídio como circunstância qualificadora do crime de homicídio, e o art. 1º da Lei nº 8.072, de 25 de julho de 1990, para incluir o feminicídio no rol dos crimes hediondos (BRASIL, 2015a);
- Lei nº 13.105, de 16 de março de 2015. Código de Processo Civil (BRASIL, 2015b);
- Lei nº 13.185, de 6 de novembro de 2015. Institui o Programa de Combate à Intimidação Sistemática (*Bullying*) (BRASIL, 2015c);
- Lei nº 13.642, de 3 de abril de 2018. Altera a Lei nº 10.446, de 8 de maio de 2002, para acrescentar atribuição à Polícia Federal no que concerne à investigação de crimes praticados por meio da rede mundial de computadores que difundam conteúdo misógino, definidos como aqueles que propagam o ódio ou a aversão às mulheres (BRASIL, 2018);
- Projeto de Lei nº 2496/2019 (BRASIL, 2019c).

2.2.2.2 Documentos internacionais

- Convenção de Budapeste ou Convenção sobre o Cibercrime (CONSELHO DA EUROPA, 2001);

- Declaração Universal dos Direitos do Homem (ONU, 1948);
- Convenção Internacional sobre a Eliminação de todas as Formas de Discriminação Racial (ONU, 1965; BRASIL, 1969);
- Declaração sobre a Raça e os Preconceitos Raciais (UNESCO, 1978).

2.2.2.3 Jurisprudências nacionais dos STF e STJ

No que tange ainda à revisão documental, foi realizada uma pesquisa nos *sites* do STF[7] e STJ[8], os quais foram escolhidos por se tratarem das últimas instâncias no sistema recursal pátrio, propiciando uma visão panorâmica da opinião do Poder Judiciário sobre o tema. Inicialmente foi feita pesquisa no site do STF, sendo utilizado o termo *crime de ódio*, sem limitação de data, na aba "Jurisprudências", não sendo encontrado nenhum resultado. Em seguida, foi feita busca pelo termo *racismo* nas mesmas condições, sendo encontrados 27 acórdãos e 3 decisões da presidência.

Com o intuito de especificar as buscas para adequá-la ao objeto do presente estudo, foram feitas duas novas pesquisas, uma adotando-se a palavra *racismo* com o booleano "e" adicionado à palavra *Internet,* sem restrições de data, sendo encontrados apenas dois acórdãos. Nas mesmas condições, foi pesquisada a palavra *racismo* juntamente com o booleano "e" juntamente à expressão (sem aspas) *Rede Mundial de Computadores*, tendo como resultado 4 acórdãos sobre o tema. Cabe esclarecer que, ao se colocar a expressão *Rede Mundial de Computadores* entre aspas, a busca não apresentou resultados.

Foi realizada ainda busca no site do STJ, em condições idênticas. Inicialmente foi feita pesquisa utilizando o termo *crime de ódio*, sem limitações de qualquer natureza, na aba Jurisprudências, sendo encontradas 4 decisões monocráticas. Em seguida, foi feita busca pelo termo *racismo* nas mesmas condições, sendo encontrados 58 acórdãos, 564 decisões monocráticas e 4 informativos de jurisprudência.

A fim de especificar as buscas para adequá-las ao tema estudado, foram feitas duas novas pesquisas, uma adotando-se a palavra *racismo* com o booleano "e" adicionada à palavra *Internet*, sem restrições de datas, sendo encontrados 12 acórdãos, 101 decisões monocráticas e 2 informativos de jurisprudência. Nas mesmas condições foi pesquisada a palavra *racismo*, juntamente com o booleano "e" somada à expressão (entre aspas) *Rede Mundial de*

[7] Disponível em: https://portal.stf.jus.br/jurisprudencia/. Acesso em: 21 nov. 2019.
[8] Disponível em https://scon.stj.jus.br/SCON/. Acesso em: 23 nov. 2019.

Computadores, tendo resultado idêntico à busca anterior, qual seja, 12 acórdãos, 101 decisões monocráticas e 2 informativos de jurisprudências.

Considerando a quantidade de julgados e a adequação ao tema da pesquisa, foram analisados apenas as hipóteses em que os termos *racismo* ou *crime de ódio* estavam acompanhados da palavra *Internet* ou da expressão *Rede Mundial de Computadores*. Foi feita a leitura das respectivas emendas das decisões resultantes das buscas, observando-se que muitas delas versam sobre a análise da competência para julgamento do crime de racismo praticado na Internet e sobre outras questões direta ou indiretamente relacionadas ao tema. Assim, foi possível obter uma visão panorâmica sobre o posicionamento dos tribunais superiores acerca do assunto. Alguns textos da jurisprudência analisada, selecionados por apresentarem maior aderência ao tema da pesquisa, foram utilizados no estudo em tela.

Entre as jurisprudências analisadas foram selecionados, por terem maior aderência ao objeto da pesquisa, os seguintes julgados:

- BRASIL. Supremo Tribunal Federal. Ação direta de inconstitucionalidade por omissão n.º 26. Relator: Min. Celso de Mello. Brasília, 13/06/2019.

- BRASIL. Supremo Tribunal Federal. Embargos de declaração em *Habeas Corpus* n.º 121.283 – DF. Relator: Min. Roberto Barroso. Brasília, 10/06/2014.

- BRASIL. Supremo Tribunal Federal. Mandado de Injunção n.º 4733 – DF. Relator: Min. Edson Fachin. Brasília, 13/06/2019. 2019b.

- BRASIL. Superior Tribunal de Justiça. Conflito de competência n.º 146.983 – RJ (2016/0147383-6). Relator: Min. Felix Fischer. Brasília, 24/05/2017.

2.3 LEVANTAMENTO TÉCNICO

Com o intuito de analisar a possibilidade de criação de *software* capaz de realizar varreduras na Internet em busca de conteúdo de ódio, mais especificamente aqueles voltados à propagação do racismo na Internet, foi realizado um levantamento técnico com dois grupos de especialistas compostos por policiais federais com experiência nas temáticas abordadas. O primeiro grupo era constituído por quatro especialistas que atuam ou já atuaram em investigações que utilizam a ferramenta CPS *(Child Protection System)*; o segundo, por quatro especialistas que atuam ou já atuaram na investigação de crimes envolvendo propagação de conteúdo de ódio ou de racismo na Internet.

A quantidade reduzida de especialistas consultados deve-se à especificidade do tema abordado e ao número restrito de policiais com experiência nos campos de interesse para a pesquisa. Contudo, importa ressaltar que, para fins da análise comparativa pretendida, o número de levantamentos técnicos se mostrou suficiente, visto que as respostas obtidas nos respectivos grupos apresentaram alto grau de similitude, sendo possível identificar as características necessárias para a comparação pretendida.

Para comparar as técnicas de investigação de diferentes crimes, sendo uma em que existe um software específico para varredura automática (CPS) e outra na qual não se utiliza essa funcionalidade, foram estruturados dois modelos de levantamentos técnicos, ambos abordando sete temas, quais sejam: conexão via servidor central, uso de redes sociais, identificação de IPs, compartilhamento em rede P2P, *stop words*, compartilhamento de imagens e vídeos, e uso de bibliotecas de *hash* como comparativos.

Segundo Gil (1999, p. 128), questionário é a "técnica de investigação composta por um número mais ou menos elevado de questões apresentadas por escrito às pessoas, tendo por objetivo o conhecimento de opiniões, crenças, sentimentos, interesses, expectativas, situações vivenciadas, etc." No caso da presente pesquisa, substituiu-se o termo *questionário* por *levantamento técnico*, uma vez que os consultados são especialistas no assunto estudado.

Nos levantamentos podem ser utilizadas questões abertas ou fechadas. No material elaborado para a presente pesquisa, em regra, optou-se pela realização de perguntas abertas, com o intuito de acessar mais profundamente o conhecimento dos especialistas. De acordo com Chaer, Diniz e Ribeiro. (2011, p. 262),

> As perguntas abertas são aquelas que permitem liberdade ilimitada de respostas ao informante. Nelas poderá ser utilizada linguagem própria do respondente. Elas trazem a vantagem de não haver influência das respostas pré-estabelecidas pelo pesquisador, pois o informante escreverá aquilo que lhe vier à mente. Um dificultador das perguntas abertas é também encontrado no fato de haver liberdade de escrita: o informante terá que ter habilidade de escrita, de formatação e desconstrução do raciocínio. Já as perguntas fechadas trarão alternativas específicas para que o informante escolha uma delas. Têm como aspecto negativo a limitação das possibilidades de respostas, restringindo, pois, as possibilidades de manifestação do interrogado.

As questões utilizadas na pesquisa foram estruturadas em quadros e separadas por tema para facilitar sua contextualização no campo de estudo. Cabe esclarecer que, em que pese os temas e a apresentação serem idênticos nos dois modelos, algumas questões foram acrescentadas no levantamento técnico aplicado aos especialistas com experiência em

investigações relacionadas ao ódio/racismo na Internet, tendo em vista que este é o foco central da pesquisa em tela, no qual se pretende contribuir para o aprimoramento da investigação.

O Quadro 1 e o Quadro 2, abaixo elencados, apresentam as questões contidas nos levantamentos técnicos encaminhados para cada um dos especialistas, conforme o grupo para o qual foi selecionado. Tal seleção foi feita adotando como critério a experiência nos respectivos tipos de investigação.

Quadro 1 – Questões para especialistas no uso da ferramenta CPS

Temas	**Questões para especialistas no uso da ferramenta CPS**
Conexão via servidor central	•Como a PF toma conhecimento do fato a ser investigado? •O conteúdo criminoso costuma ser compartilhado por meio de conexões via servidor?
Redes sociais	•As redes sociais costumam ser utilizadas como ambiente para a prática de delitos em que se utiliza a ferramenta CPS como recurso de investigação? •Os detentores das redes sociais colaboram para a identificação dos autores de crimes por meio delas praticados?
Identificação de IPs	•Como são identificados os IPs referentes aos conteúdos criminosos compartilhados? •São utilizados códigos IPs previamente catalogados como parâmetros de busca na investigação?
Compartilhamento P2P	•São utilizadas conexões ponto-a-ponto (P2P) como meio de compartilhamento de arquivos com conteúdo ilícito?
Stop words	•A prática do delito se dá pelo compartilhamento de textos? •É comum a utilização de palavras-chave como referencial para a investigação?
Compartilhamento de imagens e vídeos	•A prática do delito se dá pelo compartilhamento de imagens e vídeos? •São utilizadas palavras-chave como referencial para a identificação arquivos ilícitos compartilhados na Internet?
Uso de bibliotecas de *hash* como comparativos	•São utilizados códigos *hash* previamente identificados e catalogados como parâmetros de busca na investigação?

Fonte: Elaborado pela autora (2019).

Quadro 2 – Questões para especialistas em crimes de ódio na Internet

Temas	Questões para especialistas em crimes de ódio na Internet
Conexão via servidor central	•De que forma a prática de racismo na Internet costuma chegar ao conhecimento da PF? •Você sabe se há um monitoramento constante da Internet para identificar a propagação de conteúdos racistas? •O conteúdo criminoso costuma ser compartilhado por meio de conexões via servidores? •Tem conhecimento se existem softwares específicos para a investigação de conteúdo de ódio na Internet? •Você acredita que softwares específicos poderiam auxiliar investigação de crimes de ódio na Internet?
Redes sociais	•As redes sociais costumam ser utilizadas como meio para a prática de delitos de ódio na Internet? •Você tem conhecimento se os detentores das redes sociais colaboram para a identificação dos autores de crimes por meio delas praticados? •Quais as principais dificuldades encontradas para a identificação da autoria e materialidade?
Identificação de IPs	•Como são identificados os IPs referentes aos conteúdos criminosos compartilhados? •São utilizados códigos IPs previamente catalogados como parâmetros de busca na investigação?
Compartilhamento P2P	•São utilizadas conexões ponto-a-ponto (P2P) como meio de compartilhamento de arquivos com conteúdo ilícito?
Stop words	•A prática do delito se dá pelo compartilhamento de textos? •É comum a utilização de palavras-chave como referencial para a investigação?
Compartilhamento de imagens e vídeos	•A prática do delito se dá pelo compartilhamento de imagens e vídeos? •São utilizadas palavras-chave como referencial para a identificação arquivos ilícitos compartilhados na Internet?
Uso de bibliotecas de *hash* como comparativos	•São utilizados códigos *hash* previamente identificados e catalogados como parâmetros de busca na investigação?

Fonte: Elaborado pela autora (2019).

Após uma síntese das respostas obtidas para cada grupo de questões, procedeu-se um estudo comparativo dos resultados no âmbito dos respectivos tópicos. Tal estudo analisou as respostas obtidas nos questionários em relação à cada um dos temas. A comparação entre os resultados no âmbito respectiva área temática foi feita de forma manual, mediante a leitura e averiguação das diferenças e similitudes, tema a tema, dos quatro questionários relacionados ao quadro 1, seguida do mesmo procedimento em relação aos quatro questionários do quadro 2.

3 REFERENCIAL TEÓRICO

3.1 ESTADO INFORMACIONAL E O PODER DE POLÍCIA NO COMBATE USO CRIMINOSO DA INFORMAÇÃO

3.1.1 A informação na era digital

Consideráveis avanços tecnológicos marcaram as últimas décadas do século XX e geraram um novo paradigma denominado de "revolução da tecnologia da informação". Segundo Castells (2016), as revoluções tecnológicas são marcadas por sua penetração em todos os domínios da atividade humana, não como uma fonte externa de impacto, mas como o tecido no qual a própria atividade é exercida. Contudo, a revolução da tecnologia da informação tem uma característica especial, que consiste no fato de estar fundamentada em tecnologias de processamento de informação e comunicação.

No entender do autor, a atual revolução tecnológica caracteriza-se por aplicar os conhecimentos e informações que produz para gerar novos conhecimentos e dispositivos de processamento e comunicação da informação. Desse modo, ela cria um ciclo de realimentação entre as novas tecnologias, seus usos e seus desdobramentos, aplicando-os na criação de novos domínios. Ocorre, portanto, uma amplificação da difusão tecnológica, visto que usuários contribuem para o aprimoramento da inovação a que tiveram acesso. Assim, nas palavras de Castells: "As novas tecnologias da informação não são simplesmente ferramentas a serem aplicadas, mas processos a serem desenvolvidos. Usuários e criadores podem tornar-se a mesma coisa. Dessa forma, usuários podem assumir o controle da tecnologia, como no caso da Internet" (CASTELLS, 2016, p. 88).

Na sociedade moderna, a revolução na comunicação digital tem repercutido em várias áreas como na cultura, na filosofia e na religião. A difusão de conteúdo digital e a preocupação com seu processamento tem sido de tal relevância que, segundo Harari (2015), o universo seria um fluxo de dados e o valor dos fenômenos ou entidades seria definido com base na sua contribuição para o seu processamento.

Existe uma dificuldade humana em lidar com as mudanças causadas pela revolução das tecnologias de informação e comunicação, devido à quantidade de dados e informação e ao sentimento de incapacidade de assimilar e processar todo o conteúdo a que se tem acesso. Tal dificuldade também se reflete na morosidade estatal em administrar as consequências geradas

por um enorme volume de informações digitais, pois os Estados, em regra, não têm estrutura organizacional, tecnológica e legislativa suficientemente dinâmicas e eficientes para se adaptarem às constantes inovações proporcionadas pela revolução digital (HARARI, 2015).

No que tange propriamente ao conteúdo digital, embora as expressões "dados", "informação" e "conhecimento" sejam frequentemente empregadas como sinônimos, tratam-se de conceitos distintos. Para Buckland (1991 p. 351), partindo da ideia da informação como um fenômeno ou processo cujo nível de complexidade aumenta progressivamente, haveria um caminho que parte dos dados até chegar ao conhecimento. Nesse caminho, os "dados" seriam o patamar menos dotado de significação, a "informação" seria uma conexão de dados com uma agregação de sentido, e "conhecimento", a assimilação propriamente dita do significado, possibilitando uma compreensão lógica dos fatos.

O conceito de conhecimento, portanto, adota uma perspectiva voltada para o ser humano, segundo a qual seria fruto de um trabalho intelectual sobre as informações assimiladas. Assim, a informação é a matéria-prima para a produção de novos conhecimentos. Neste sentido, De Sordi (2008) esclarece que o conhecimento é um novo saber, fruto da análise e reflexões sobre a informação, conforme os valores e modelo mental de quem o desenvolve.

A revolução da tecnologia da informação está fundada na análise, processamento e transmissão da informação e do conhecimento que circulam em meio digital. Graças a ela, a comunicação passou a se dar em um ambiente denominado por alguns autores como "ciberespaço". Para Lemos (2015, p. 128), o ciberespaço pode ser entendido sob duas perspectivas: "como o lugar onde estamos quando estamos em um ambiente simulado (realidade virtual) e como um conjunto de redes de computadores, interligadas ou não, em todo o planeta, a Internet".

O autor esclarece ainda que há uma tendência de fusão entre ambas as concepções de ciberespaço, haja vista que as redes e as realidades virtuais tendem a se unirem. Lemos complementa: "o ciberespaço é assim uma entidade real, parte vital da cibercultura planetária que está crescendo sob nossos olhos. Ele não é desconectado da realidade, mas um complexificador do real" (LEMOS, 2015, p. 128).

Para efeito deste estudo, optou-se, por interpretar e utilizar o termo "ciberespaço" como sendo o conjunto de redes de computadores por meio da qual circula a informação em todo o planeta. Tal interpretação tem maior afinidade com o objeto da pesquisa, o qual analisa a circulação da informação por redes computacionais com o intuito de propagar conteúdo discriminatório em relação a determinados grupos.

As inovações trazidas pelo desenvolvimento das tecnologias de informação e comunicação fomentaram um profundo e complexo debate de ideias. A Ciência da Informação (CI) surgiu com o intuito de assimilar e analisar as mudanças geradas pela revolução informacional. De acordo com Borko (1968), "Ciência da Informação é a disciplina que investiga as propriedades e o comportamento informacional, as forças que governam os fluxos de informação, e os significados do processamento da informação, visando à acessibilidade e à usabilidade ótima".

Observa-se que o conceito de Borko (1968), embora datado de meados do século passado, permanece atual, pois transmite a magnitude do campo de estudo da Ciência da Informação. Segundo o autor, é preciso analisar não só as questões relacionadas à informação propriamente dita, mas também ao comportamento informacional e às forças que governam o fluxo da informação. O autor entende que a informação possui um "comportamento" próprio dentro de um ambiente, não podendo ser vista como algo isolado, mas como parte de um "fluxo".

Considerando a complexidade e dimensão do campo de estudo da CI, Saracevic (1995) conclui que a interdisciplinaridade que a caracteriza resulta da diversidade de questões que pretende solucionar. Assim, a Ciência da Informação dialoga com várias disciplinas, justamente pelo fato de buscar solução para problemas diversos, gerando a necessidade de recorrer a subsídios de outros campos.

Cabe à CI analisar de forma ampla os fatores relacionados à informação. Entre tais fatores estão o estudo da transferência da informação (comunicação) no contexto das novas tecnologias, e a análise das conjunturas sociais e culturais relacionadas à informação digital.

O campo de estudo da CI está intimamente conectado à questão da disseminação criminosa de conteúdo de ódio pela Internet. O procedimento de investigação de um conteúdo racista pela Internet envolve o estudo das propriedades da informação e a investigação do comportamento informacional. A investigação criminal do ódio na Internet consiste em coletar um conteúdo informacional, analisar sua licitude, verificar sua fonte e o meio utilizado para sua propagação.

Observa-se que o campo de estudo da Ciência da Informação guarda grande semelhança com a coleta, processamento e análise feitos pelo investigador. No caso da investigação, a acessibilidade e usabilidade ótima pretendidas pela CI também se aplicam, posto que estão presentes no acesso eficiente ao conteúdo informacional ilícito e no sucesso do seu processamento, chegando à autoria do propagador e à punição dos responsáveis.

Todo o contexto relacionado ao surgimento de novas tecnologias de informação e comunicação na Era Digital impactou diretamente na criminalidade. Os conteúdos ofensivos veiculados na presença de uma pessoa ou de um grupo passaram a ser disseminados pela Internet, ganhando uma magnitude antes inimaginável. A própria atribuição da Polícia Federal para investigar os casos de racismo na Internet deve-se à internacionalidade desse veículo de comunicação – ou seja, a PF só investiga porque o meio utilizado para propagação gera a internacionalização do crime, sendo a repercussão internacional um dos requisitos previstos em lei para a definição de competência investigativa relacionada a tais espécies de delito.

Entende-se, portanto, que os conceitos referentes à Sociedade da Informação e à informação na era digital estão conectados ao campo de estudo dos crimes cibernéticos, os quais também são frutos dessa nova era. Observa-se ainda que o manejo e estudo da informação digital pelos investigadores guarda grande semelhança com o trabalho realizado por cientistas da informação, distinguindo-se pela finalidade específica de combate à impunidade no uso ilícito da informação digital.

3.1.2 A informação e suas diferentes concepções

Na sociedade moderna, a revolução gerada pela criação de novas tecnologias, notadamente na área da comunicação, interferiu fortemente nas relações pessoais e sociais. As mudanças causadas pelas inovações tecnológicas foram de tal relevância que ensejaram a criação do termo "Sociedade da Informação" para contemplar a ideia de um novo modelo de sociedade. Segundo Werthein (2000), tal expressão surgiu no final do século passado, em substituição ao conceito de "sociedade pós-industrial", para referir-se ao conteúdo específico do "novo paradigma técnico-econômico". Nas palavras do autor:

> A realidade que os conceitos das ciências sociais procuram expressar refere-se às transformações técnicas, organizacionais e administrativas que têm como "fator-chave" não mais os insumos baratos de energia – como na sociedade industrial – mas os insumos baratos de informação propiciados pelos avanços tecnológicos na microeletrônica e telecomunicações (WERTHEIN, 2000, p. 71-72).

Assim, a informação está no centro da revolução da tecnologia e consiste na sua matéria-prima, sendo a fonte por meio da qual a realidade é interpretada, debatida e assimilada. Observa-se ainda que o conceito de informação é complexo, pois pode ser interpretado considerando diferentes pontos de vista.

Diversas formas de se abordar o estudo da informação também são apresentadas por Sandra Braman. Segundo a autora, o conceito de informação se modifica em função da perspectiva em que é concebida, afirmando que ela pode ser compreendida como recurso, mercadoria, dados padronizados, agente, repositório de possibilidades ou força constitutiva. A partir da perspectiva adotada, a ideia de informação assume características distintas (BRAMAN, 2006).

Segundo Braman (2006), a informação é tida como um recurso quando é tratada como algo que uma entidade (pessoa, organização ou comunidade) necessita possuir para funcionar. Seria vista, portanto, como uma entrada em um processo de tomada de decisão. Neste caso, a busca da informação decorreria da necessidade de preencher um vazio de conhecimento.

A informação é percebida como *commodity* quando é tratada como algo que é comercializável. Essa abordagem é criticada sob o argumento de que desconsidera a função social da informação. Já a definição de informação como percepção de um padrão (conhecimento) considera o contexto em que as informações são produzidas. Essa abordagem reconhece que a informação faz parte de um contexto de tempo e espaço, afetando e sendo afetada pelo meio. A informação é considerada uma base para inovação, para modificação na estrutura social ou para introdução de novas tecnologias (BRAMAN, 2006).

A autora apresenta ainda a possibilidade de percepção da informação como um agente, pois, em algumas situações, ela é capaz de tomar decisões por si só e assim interferir na realidade. Seria o caso da informação contida nas máquinas e sistemas informatizados. Esta perspectiva reconhece o poder realizador da informação, sendo incentivada pelas recentes inovações tecnológicas, nas quais *softwares* passam a ser utilizados para suplementar e até substituir a tomada de decisão humana (BRAMAN, 2006).

A informação pode ser vista como uma gama de possibilidades (ou repositório de possibilidades), considerando que é praticamente impossível haver uma exata correspondência entre um fato narrado e seu respectivo conteúdo informativo. Desse modo, ainda que frequentemente tratada como fato, a informação não seria concretamente descritiva, acabando por se referir a probabilidades (BRAMAN, 2006).

Por fim, a autora aponta para o estudo da informação como uma força constitutiva na sociedade. Observa-se que os papéis constitutivos e constitucionais da informação estão intimamente relacionados. Os princípios constitucionais descrevem um ideal, enquanto forças constitutivas têm um efeito empírico que pode ou não aproximar a sociedade do objetivo

constitucional. Segundo a autora, a informação teria o poder de modificar o contexto por meio do efeito cumulativo de fluxos informacionais, afetando o ambiente (BRAMAN, 2006).

Em relação ao contexto da informação utilizada para propagar conteúdo de ódio, ou seja, para incitar discriminação e preconceito contra determinados grupos sociais, observa-se que há uma preocupação com o conteúdo informativo e com sua força constitutiva. Existe uma percepção de que o conteúdo informacional trazido por ideias dessa natureza pode gerar efeitos nocivos na sociedade. A criminalização do racismo na Internet reflete uma preocupação estatal em garantir a prevalência de princípios constitucionais.

Importa ressaltar que a República Federativa do Brasil tem a dignidade da pessoa humana como um de seus fundamentos (art. 1º, inciso III da Constituição da República Federativa do Brasil), bem como traz a "prevalência dos direitos humanos" e o "repúdio ao terrorismo e ao racismo" como princípios que regem suas relações internacionais (art.4º, incisos II e VIII da CRFB). Já no caput do art. 5º, a CRFB prevê a igualdade de todos perante a lei sem distinção de qualquer natureza, e o inciso VIII, também do art. 5º, dispõe que "ninguém será privado de direitos por motivo de crença religiosa ou de convicção filosófica ou política, salvo se as invocar para eximir-se de obrigação legal a todos imposta e recusar-se a cumprir prestação alternativa, fixada em lei" (BRASIL, 1988).

Todos os dispositivos acima mencionados traduzem um ideal traçado pela Constituição Federal brasileira que é diametralmente oposto aos discursos de ódio e às ideias racistas estudadas neste trabalho. A preocupação em tipificar penalmente o racismo na Internet reflete um reconhecimento da informação como uma força constitutiva e uma preocupação em evitar a propagação de ideologias contrárias aos valores constitucionais.

A definição de informação enquanto força constitutiva aparece em diversas literaturas, sendo usada para apoiar uma ampla variedade de posições políticas. Para os psicólogos sociais, a criação de informação e os fluxos informacionais literalmente constroem a realidade. Já os sociólogos da mídia operacionalizam essas ideias quando elas se manifestam em situações específicas de criação de fatos (BRAMAN, 2006).

As definições mais complexas são dirigidas por uma preocupação com a construção do significado e se concentram no contexto (semiótica); na tomada de sentido por parte dos receptores de mensagens (estudos culturais); e no impacto cultural, econômico, político e social das arquiteturas de conhecimento (ciência da informação e sociologia do conhecimento). Tais abordagens têm em comum o respeito pela forma, aliado à consciência de que o conteúdo é

importante, notadamente quando reúne informações úteis para direcionar condutas e orientar decisões (BRAMAN, 2006).

Segundo a autora, as definições de informação apresentadas se aplicam a toda a gama de fenômenos e processos nos quais ela está envolvida, podendo ser utilizadas em estruturas sociais de qualquer grau de articulação e complexidade. A escolha da definição de informação a ser adotada acaba, de certo modo, sofrendo uma interferência política. A percepção da informação como uma força constitutiva é a abordagem que tem a maior amplitude, pois atinge o maior número de preocupações fundamentais para os gestores políticos. Com base em tal concepção, identifica-se toda uma gama de valores que devem ser considerados no processo de tomada de decisões (BRAMAN, 2006).

Os conceitos trazidos por Sandra Braman refletem a compreensão da informação como elemento inserido em um contexto social. No caso dos crimes cibernéticos, a percepção da informação como uma força constitutiva reforça o alinhamento entre o tema estudado na presente pesquisa e o campo de estudo da CI. Tal perspectiva traz ainda a importância da informação para os gestores públicos, cabendo-lhes, no que tange à disseminação de conteúdo de ódio na Internet, implementar medidas de gestão para combater o uso criminoso da informação, tendo em vista sua reconhecida lesividade e seu desajuste em relação aos princípios constitucionais brasileiros.

3.1.3 O papel do Estado na Sociedade da Informação

A Sociedade da Informação comtempla uma nova conjuntura que abrange a sociedade e suas instituições. O Estado também faz parte dessa conjuntura e deve, portanto, se adaptar aos novos desafios. Para refletir sobre o papel do Estado nesse contexto, é interessante partir de seu conceito. Segundo Dallari (2003, p. 118), Estado é "a ordem jurídica soberana que tem por fim o bem comum de um povo situado em determinado território".

O Estado é constituído por três elementos: povo, território e governo soberano. O povo são os indivíduos que têm um vínculo de cidadania com o Estado – diferindo de população, que é um conceito meramente demográfico, correspondente ao número de pessoas que habitam um determinado espaço. Já o território seria a base geográfica, a dimensão espacial do Estado. O governo é a instância diretiva máxima do Estado (LENZA, 2017).

As nações, por sua vez, são moldadas por características culturais. Assim, existe um poder simbólico que fortalece e caracteriza a nação. O conceito de Estado não contempla esse

poder simbólico, pois está centrado nas características de suas organizações burocráticas e não em termos culturais. Sua maior força está no exercício do poder estrutural. Já o Estado-nação moderno representa o esforço para reunir os modos culturais e burocráticos de organizar a sociedade (BRESSER-PEREIRA, 2017).

Os Estados-nação tiveram sua origem no absolutismo monárquico, que se constituiu na Europa, notadamente na França e na Inglaterra, depois da revolução comercial e da emergência de uma burguesia associada ao monarca. Como esclarece Bresser-Pereira (2017, p. 158),

> o *estado-nação* ou *país* é um tipo de sociedade político-territorial soberana, formada por uma nação, um Estado e um território. É a forma de poder territorial que se impôs nas sociedades modernas a partir da revolução capitalista em substituição aos feudos e principalmente aos *impérios antigos*.

O surgimento do Estado informacional ocorreu dentro de uma longa história de formas sucessivas de Estado. Braman (2006) afirma que Estado burocrático e a nação cultural têm histórias separadas; algumas nações estão espalhadas por vários estados e também é comum que Estados tenham dentro de si mais de uma nação. Observa ainda que é possível que os Estados, no que concerne a suas formas de governo, sofram mudanças, pois são sistemas adaptativos e complexos. Tais sistemas são produzidos por interações entre hábitos culturais, leis formais, discurso e modos de organização dentro de um campo de possibilidades em constante modificação. Como outros sistemas adaptativos complexos, os Estados respondem a modificações nos recursos disponíveis bem como em seus ambientes.

O Estado informacional surgiu após a Segunda Guerra Mundial, com a instalação e crescimento das empresas que exerciam atividades fora de seus países de origem. Na década de 1970, as corporações multinacionais e transnacionais buscaram maximizar suas operações e minimizar a sujeição às restrições impostas por qualquer Estado-nação. As empresas multinacionais ganharam importância no cenário econômico internacional. Alguns cientistas políticos começaram a falar sobre a perda do poder do Estado em relação a outras entidades, tais como as grandes multinacionais, chegando a sugerir a possibilidade do seu completo desaparecimento (BRAMAN, 2006).

As redes e as tecnologias da informação permitiram o desenvolvimento de repositórios, servidores e bancos de dados, advindos de múltiplos centros de informação, coexistindo sem princípios diretores. Para se posicionar nesse cenário, o Estado informacional precisa integrar as ações de diferentes ministérios, ligando um conjunto de informações que

componha à identidade nacional. Faz-se necessário utilizar o poder e infraestrutura estatal para unir diferentes redes de informação (BRAMAN, 2006).

O desenvolvimento de meta-tecnologias e a crescente intensidade da circulação da informação aumentaram a importância do uso de técnicas políticas para manipular o poder informacional. Os governos que perceberam tal contexto e maximizaram sua capacidade de usar o poder informacional fizeram a transição da forma política conhecida como "Estado de bem-estar social" para o Estado informacional (BRAMAN, 2006).

Nesse contexto o Estado informacional é caracterizado por múltiplas interdependências com entidades estatais e não-estatais, que exigem o uso da infraestrutura global de informações para criação, processamento, fluxo e uso de dados. Assim, ele utiliza o controle sobre as informações para produzir áreas de influência dentro do ambiente de rede (PINHEIRO, 2012).

Harari (2015) afirma que o Estado, marcado por suas características burocráticas, não consegue acompanhar a velocidade da evolução tecnológica do ciberespaço. Desse modo, existe uma grande dificuldade das estruturas democráticas atuais em colher e processar dados relevantes numa velocidade que lhes permita ter controle sobre fatos e formar visões significativas de futuro. Há um descompasso entre a velocidade de regulamentação estatal e o espaço virtual em constante mutação. Segundo o autor, é possível que nas próximas décadas ocorram mais revoluções, como a causada pela Internet, nas quais a tecnologia se antecipará à política.

O autor explica que a revolução digital proporcionou um acréscimo no número de informações e conhecimentos muito maior do que a sociedade pode assimilar. O Estado, tradicionalmente considerado o ente responsável pela tomada de decisões e por direcionar a sociedade, tem demonstrado impotência, em algumas situações, diante de dilemas apresentados pela Sociedade da Informação. Assim, independentemente do regime de governo adotado, seja democrático ou ditatorial, a dificuldade em lidar como um grande volume de informações é um ponto comum. As variáveis apresentadas pelo grande fluxo de informações tornam a tomada de decisões um processo cada vez mais complexo (HARARI, 2015).

À medida em que o Estado demonstra uma fragilidade em lidar com a revolução digital, a dimensão do seu poder é questionada e outras forças, como o mercado ou a mídia, são apresentadas como detentoras de poder decisório. Em que pese não existir uma aferição precisa da dimensão do poder do Estado na Sociedade da Informação, há um reconhecimento quanto à necessidade do exercício de seu poder enquanto ente comprometido com os valores da

coletividade. Não seria prudente uma omissão do Estado que viabilizasse a concentração do poder informacional nas mãos de instituições movidas unicamente por interesses particulares (HARARI, 2015).

Braman (2006) entende que a necessidade de uma atuação proativa do Estado vai ao encontro do ideal que propõe uma ênfase na organização política do uso do poder informacional. Ao se analisar as características do Estado informacional percebe-se que ele nasce da transformação de uma economia "globalizada" e utiliza as capacidades tecnológicas e informacionais anteriormente inexistentes, num hibridismo de responsabilidades dos setores público e privado.

Desse modo, a utilização do poder informacional por parte do Estado significa uma atuação alinhada com as mudanças de paradigma geradas pela revolução digital. O Estado, enquanto ente responsável pela defesa dos interesses de uma coletividade, necessita manter-se atualizado e conectado aos valores e desafios do contexto social no qual está inserido.

Considerando que a criação da Internet se deu na década de 1960, observa-se que seu surgimento é um fato bastante recente à vista do impacto das mudanças socioeconômicas por ela proporcionadas. De acordo com Crespo (2011), a Internet surgiu com o desenvolvimento da *Advanced Research Projects Agency Network* (ARPA) por algumas universidades americanas. Quando de sua criação, essa rede era de uso exclusivo das Forças Armadas norte-americanas. O mundo vivia o contexto histórico da Guerra Fria, ensejando a preocupação em criar uma ferramenta de comunicação que funcionasse de forma contínua e que não fosse interrompida em casos de calamidades como uma guerra nuclear. Um dos principais objetivos, quando da elaboração dessa rede de comunicação, era que não houvesse um comando central que pudesse ser alvejado e causar a interrupção do fluxo da comunicação (CRESPO, 2011).

A partir da década de 1990, ocorreu um grande aumento da convergência da informática e das telecomunicações, bem como a disseminação do uso dos computadores domésticos e crescimento da utilização da Internet e serviços eletrônicos no cotidiano das pessoas. Assim, o desenvolvimento e a difusão do acesso à tecnologia contribuíram para a formação da Sociedade da Informação, caracterizada, entre outras coisas, pela valorização de bens imateriais (CRESPO, 2011).

A informação passou a ser cada vez mais percebida não apenas como um valor econômico, mas também como uma ferramenta de poder e fonte de perigos potenciais. Assim, os Estados investem em tecnologia para obter acesso a tal fonte de poder. Os sistemas de defesa

também se tornaram cada vez mais dependentes da informática, gerando uma preocupação com a manipulação e o uso estratégico da informação (CRESPO, 2011).

Observa-se, portanto, que a interferência do Estado no ciberespaço é inevitável. A tecnologia e a conexão digital fazem parte de todos os setores da sociedade, gerando no Estado e nos agentes políticos que o representam a necessidade de manter toda a estrutura estatal atualizada a fim de atender às novas demandas sociais. Tal atualização pode se dar de diversas formas, tais como investimentos em tecnologia, adaptação da estrutura legislativa e capacitação de servidores.

As novas modalidades de crimes que resultaram das inovações nas tecnologias de informação e comunicação geram no Estado a necessidade de elaborar estratégias de adaptação. O fato de um crime ser praticado pela Internet ou por outras ferramentas de comunicação digital não reduz o poder-dever estatal de investigá-los e puni-los, mas acrescenta novos desafios ao enfrentamento da criminalidade.

O Estado informacional, para atender aos desafios da Sociedade da Informação, inclusive no que tange ao combate à propagação de conteúdo de ódio pela Internet, pode firmar parcerias com outras entidades, estatais ou não. Assim, considerando que tais ilícitos costumam ter repercussão internacional, devido à conectividade proporcionada pela Rede Mundial de Computadores, a colaboração entre instituições se faz necessária, pois não é viável combater de forma isolada um fenômeno que ocorre em escala global.

3.1.4 Poder e poder de polícia no Estado informacional

Para Braman (2006), os cientistas políticos costumam classificar o poder de três formas: instrumental, estrutural e simbólico. Todavia, a informatização da sociedade aumentou consideravelmente a importância de uma quarta forma de poder: o informacional.

O poder instrumental molda os comportamentos humanos, manipulando o mundo material por meio da força física. Esse é o modo mais contundente e familiar de poder, que costuma ser exercido por forças militares e policiais, por meio do uso de armas. O poder instrumental foi de importância central para o Estado moderno desde que este começou a surgir, no século XVI. O poder estrutural molda os comportamentos humanos manipulando o mundo social por meio de regras e instituições, as quais limitam a gama de escolhas disponíveis e determinam como as atividades específicas serão realizadas, sistematizando comportamentos de modo que haja menos incerteza e mais confiança em relação às expectativas. Já o poder

simbólico afeta os comportamentos humanos, manipulando o mundo material, social e simbólico por meio de ideias, palavras e imagens. Tal poder também tem raízes antigas e seu exercício externo ao Estado costuma ser mencionado como "propaganda" ou "diplomacia pública". Segundo a autora, os Estados exercem poder simbólico internamente por meio de campanhas, tentativas de direcionamento da opinião pública e até mesmo pelo sistema educacional (BRAMAN, 2006).

O poder informacional ganhou maior notoriedade no contexto da Sociedade da Informação. Ele age moldando os comportamentos humanos por meio da manipulação das bases informacionais do poder instrumental, estrutural e simbólico. O poder informacional atua ainda sobre as outras formas de poder, modificando o seu exercício e alterando a natureza de seus efeitos. Ele pode ser descrito como "genético", porque aparece na gênese (nas origens informacionais) dos demais poderes. Está presente no mundo material, nas estruturas sociais e nos símbolos, que são a essência do poder em suas outras formas (BRAMAN, 2006).

Observa-se que as diversas formas de poder costumam se relacionar de múltiplos modos. Assim, elas não são excludentes, podendo interferir cumulativamente em um determinado fato. Braman aponta como exemplo de exercício cumulativo de espécies distintas de poder o crescimento de grandes empresas de armas, durante a era industrial, fortemente alinhadas com governos específicos, demonstrando uma ligação entre o poder instrumental ao poder estrutural (BRAMAN, 2006).

O poder também pode ser classificado como atual, potencial ou virtual – classificação decorrente da revolução digital. O poder atual ocorre no momento que é exercido. Já o potencial representa uma fase em que o poder é exigível, porém, ainda não foi efetivado. O processamento, a distribuição e o uso da informação são frequentemente necessários para a transformação do poder potencial em real (BRAMAN, 2006).

O poder virtual, por seu turno, costuma ser aferido a partir da base de conhecimento a qual seu titular tem acesso. O conhecimento é tão central para o poder em sua fase virtual que toda expansão da base de conhecimento de um Estado-nação provoca, concomitantemente, um crescimento no domínio do poder disponível para ele (BRAMAN, 2006).

No âmbito interno, sob a ótica do Direito, uma das formas tradicionais de exercício do poder por parte do Estado é o poder de polícia. Segundo Hely Lopes Meirelles, ele consiste numa faculdade da Administração Pública de condicionar e restringir o uso e gozo de bens, atividades e direitos individuais (MEIRELLES, 2002).

O poder de polícia é definido pelo Código Tributário Nacional nos seguintes termos:

> Art. 78. Considera-se poder de polícia atividade da administração pública que, limitando ou disciplinando direito, interesse ou liberdade, regula a prática de ato ou abstenção de fato, em razão de interesse público concernente à segurança, à higiene, à ordem, aos costumes, à disciplina da produção e do mercado, ao exercício de atividades econômicas dependentes de concessão ou autorização do Poder Público, à tranquilidade pública ou ao respeito à propriedade e aos direitos individuais ou coletivos (BRASIL, 1966).

Portanto, o poder de polícia se refere a limitações ao exercício das liberdades individuais em prol de um bom convívio coletivo. As formas de exercício de poder já mencionadas demonstram que o Estado tem instrumentos legais para exercer legitimamente sua vontade. O exercício do poder estatal deve ocorrer inclusive no ciberespaço, ambiente no qual muitas relações inerentes à Sociedade da Informação são travadas, não podendo esse ambiente ficar à margem da legislação.

A necessidade de um comportamento responsável referente ao uso da informação digital é narrada por Werthein (2000). Segundo o autor,

> em alguns outros casos, como a perda da privacidade, a sociedade tem-se mobilizado para promover o que Leal identifica como o "comportamento normal responsável" inclusive por meio de legislação adequada para proteger os direitos do cidadão na era digital. A perda do sentimento de controle sobre a própria vida e a perda da identidade são temas que continuam preocupantes e que estão ainda por merecer estratégias eficientes de intervenção (WERTHEIN, 2000, p. 76).

No que tange ao controle estatal, Braman (2006) esclarece que, na história da Sociedade da Informação, as tecnologias industriais foram substituídas por meta-tecnologias, as organizações mudaram de forma, novas arquiteturas de conhecimento foram desenvolvidas bem como ocorreram mudanças na economia. Assim, o Estado precisou se adaptar a esta nova realidade e os governos também passaram a usar informação e tecnologias da informação em novos caminhos. Essas práticas levaram a mudanças na natureza do poder e seu exercício via política de informação. Logo, é comum que haja modificações nas leis para adaptação política à nova realidade, refletindo a necessidade de adaptação do sistema jurídico.

As quatro formas de poder elencadas por Braman (2006) – estrutural (força física), instrumental (instituições), simbólico (ideias, palavras e imagens) e informacional (bases informacionais) – estão a serviço do Estado para realização dos seus objetivos institucionais. Refletir sobre as formas de poder estatal é relevante para compreender por que o Estado, apesar de todas as mudanças trazidas pela Sociedade da Informação, ainda se apresenta como ente mais apto para reger e organizar a sociedade. A autora esclarece ainda que o Estado tem se

adaptado ao longo do tempo para atualizar suas formas de exercício de poder às demandas sociais. Assim, as mudanças decorrentes das novas tecnologias não excluem o poder estatal, gerando apenas novas demandas por adaptações.

As reflexões sobre o poder de polícia trazem um conceito jurídico acerca do dever do Estado de promover o bem comum. Cabe esclarecer que as ponderações sobre o poder trazidas por Braman (2006) partem de uma perspectiva distinta do conceito legal de poder de polícia. Contudo, ambas apontam para um entendimento de que o Estado continua sendo o ente mais apto para exercer poder na Sociedade da Informação, sendo relevante que ele o exerça também no enfrentamento às novas formas de criminalidade surgidas na era digital.

Conforme se observou, as bases teóricas e históricas nas quais o Estado foi moldado remontam a uma evolução secular. Por conta dessa evolução, o Estado tem se adaptado com a finalidade de permanecer como a instituição mais apta a garantir a estabilidade do convívio social e a promoção do bem comum.

3.2 A INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS

3.2.1 As investigações criminais no Estado informacional

Na Sociedade da Informação, a ausência de fronteiras e o surgimento de novas formas de comunicação, notadamente digitais, modificaram a percepção de tempo e de espaço. Tais mudanças também repercutiram nas normas de Direito Penal. Muitos delitos já previstos em lei ganharam um novo *modus operandi* e foram facilitados pelo pretenso anonimato proporcionado pela Internet. Ofensas contra a honra, *bullying*, delitos sexuais e econômicos passaram a ser cometidos também na Rede Mundial de Computadores, em decorrência da informatização e da comunicação instantânea. A criminalidade, portanto, encontrou novas formas se de fazer presente, o que levou à constatação da existência de lacunas na lei penal, uma vez que diversas condutas prejudiciais ainda não são tipificadas como delito (CRESPO, 2011).

O uso da tecnologia para cometer crimes tem demandado adaptação do Estado para coibir o crescimento da criminalidade no ciberespaço. Essa adaptação se dá por meio da regulamentação estatal, pelo aparelhamento dos órgãos policiais e pela readequação e inovação nas técnicas de investigativas.

A Convenção de Budapeste define cibercrime como os “atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados

informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados" (CONSELHO DA EUROPA, 2001, S.I.).

A situação do cibercrime no Brasil é extremamente preocupante: além de os lucros das atividades ilícitas no campo virtual serem altíssimos, deve-se ressaltar que, diante de leis brandas e da impunidade, condutas ilícitas na Internet estão atraindo quadrilhas que antes atuavam em crimes como roubo a bancos e tráfico de drogas. Uma característica peculiar dos cibercriminosos brasileiros é que eles concentram suas fraudes contra pessoas e empresas brasileiras. Uma das razões para isso seria justamente a legislação vaga, que não pune esses criminosos de forma eficaz, com os bandidos virtuais passando pouco ou nenhum tempo presos (BARRETO; BRASIL, 2016).

O ciberespaço é considerado vulnerável em decorrência de características como a capacidade de processar, guardar e circular uma grande quantidade de informação digital de diversos formatos (fotos, filmes, sons) em tempo real, cujo controle é dificultado em virtude da estrutura descentralizada e não hierarquizada da Internet. A vulnerabilidade também se dá devido o número elevado de usuários com liberdade para acessar, transferir, enviar e difundir informações. Tais usuários tanto podem utilizar o ambiente digital de forma responsável, como podem usá-lo para a prática de crimes. Além disso, as próprias características físicas, técnicas e lógicas das Tecnologias da Informação e Comunicação (TIC) que permitem que estas venham a ser acessadas de maneira ilegítima ou ter seu conteúdo alterado. Por fim, um outro fator que contribui para a vulnerabilidade do ciberespaço é a enorme potencialidade de multiplicação das ações ilícitas ocorridas na Internet, decorrente da facilidade na comunicação (CRESPO, 2011).

A necessidade de aprimoramento da investigação justifica-se pelo crescimento e complexidade dos crimes digitais, caracterizados por uma dinâmica social extremamente veloz e dotada de novos meios de comunicação. Nas palavras de Santos (2018),

> com o mundo tornando-se cada vez mais interligado por meio de dispositivos eletrônicos, não é surpreendente que os crimes que utilizam a tecnologia como meio ou como fim também estejam em crescimento exponencial (tanto em termos de quantidade, quanto em termos de variedade).

A finalidade da investigação policial é produzir provas acerca da autoria e materialidade de um crime. As provas são elementos levados ao processo com o objetivo de fornecer subsídios ao juiz na busca da verdade real, permitindo que este possa formar sua opinião. Todos os meios lícitos podem ser utilizados para comprovar os fatos e argumentos alegados no processo. No caso dos crimes digitais, muitas dessas provas estão disponíveis em

meios eletrônicos ou pela Internet, sendo necessário o uso de procedimentos adequados para sua coleta e preservação (SANTOS, 2018).

A questão da legalidade dos meios de obtenção de provas deve nortear o trabalho de investigação policial. As provas digitais necessitam observar o mesmo rigor técnico e legal para sua produção que as demais. Para Barsoti (2018), tais provas formam uma nova modalidade, pois o fato de serem produzidas, armazenadas ou transmitidas por meio digital, a partir de um computador ou de qualquer dispositivo eletrônico, faz com que tenham características peculiares, exigindo profissionais especializados e a adoção de procedimentos específicos para a sua obtenção. Assim esclarece a autora sobre as singularidades da prova digital:

> A prova produzida em ambiente digital tem como características a portabilidade (que pode se dar por meio eletrônico ou via Internet), reprodutibilidade (pode ser copiada e compartilhada inúmeras vezes podendo ser facilmente alterada) e a volatilidade (veremos mais a diante que alguns meios de prova se estabelecem por meio de vestígios e indícios que podem desaparecer rapidamente), tais características dificultam em muitos casos sua coleta e análise, bem como a identificação de autenticidade. Existem inúmeros tipos de provas digitais, entre eles, os mais comuns são arquivo de áudio e vídeo, imagens digitais, mensagens eletrônicas cujo produto final é considerado para fins judiciais um documento eletrônico (BARSOTI, 2018, S.I.).

Cabe destacar que a variedade de crimes e de tecnologias gera uma grande dificuldade em estabelecer uma padronização para a produção, coleta e preservação dos meios probatórios utilizados para investigar ilícitos digitais. Nesse contexto, é relevante que o policial tenha conhecimentos sobre o ambiente virtual, novas tecnologias e crimes conexos a essa área.

O art. 384 do Novo Código de Processo Civil (Lei nº 13.105/2015) prevê como meio para garantir a autenticidade da prova digital o seu registro em Ata Notarial. Tal procedimento tem o objetivo de viabilizar a comprovação em juízo de fatos ocorridos em ambiente digital. Assim prevê o citado dispositivo:

> Art. 384. A existência e o modo de existir de algum fato podem ser atestados ou documentados, a requerimento do interessado, mediante ata lavrada por tabelião.
> Parágrafo único. Dados representados por imagem ou som gravados em arquivos eletrônicos poderão constar da ata notarial (BRASIL, 2015b).

Quanto às provas produzidas para instruir processos criminais, Barsoti (2018) esclarece:

> No âmbito criminal, quando se tratar de prova digital - ao ser lavrado um boletim de ocorrência -, é necessário solicitar ao escrivão que acesse o dispositivo eletrônico ou site da Internet (registre o endereço eletrônico acessado), em que se encontre a prova

> do alegado, afim de que seja registrada a sua existência e assegurada a veracidade do meio probatório, visto que o escrivão de polícia é dotado de fé pública, dispensando assim a necessidade da ata notarial em casos criminais.

Os dispositivos legais mencionados demonstram a preocupação do Estado com as informações que circulam em ambiente digital e evidenciam a necessidade de regulamentação do ciberespaço. Essa necessidade de estruturação e especialização decorre das características e peculiaridades dos crimes cibernéticos. Para Kummer (2017, S.I.),

> no caso de investigação de crimes informáticos, existem particularidades que a tornam singular em relação à investigação dos demais tipos de crimes: em primeiro lugar, o anonimato que a rede possibilita; em segundo lugar, a fugacidade das provas, efêmeras que são, pois podem desaparecer ou serem apagadas da rede muito rapidamente.

Numa demonstração de atualização do Direito para regulamentar as novas demandas sociais, o art. 20 da Lei nº 7.716/1989 (BRASIL, 1989), conhecida como Lei de Racismo, teve sua redação modificada, passando a trazer providências a serem adotadas pelo Estado nas hipóteses em que o racismo é praticado por meios digitais. Com a nova redação, o inciso II do parágrafo 3º prevê que o juiz poderá determinar "a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio" (BRASIL, 1989). Já o inciso III do mesmo parágrafo traz a possibilidade de decretação judicial da "interdição das respectivas mensagens ou páginas de informação na Rede Mundial de Computadores".

Entre as inovações legais necessárias para capacitar o Estado a atender as demandas sociais referentes ao combate à criminalidade em ambiente digital, pode-se citar a Lei nº 12.735/2012, que determinou que os órgãos de polícia judiciária (as Polícias Civis e a Polícia Federal) deverão estruturar "setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado" (BRASIL, 2012a).

Em que pese o esforço de regulamentação já realizado, muito ainda necessita ser feito, notadamente no que tange aos meios legais para propiciar o combate à criminalidade na Rede Mundial de Computadores. Exemplificando as necessidades legais nessa seara, pode-se citar o alerta apresentado por Kummer (2017, p. S.I.):

> Falta, portanto, uma norma que regulamente a obrigatoriedade específica de colaboração das empresas e provedores de acesso à Internet nesse sentido, como forma de agilizar o combate ao crime informático, independentemente de ordem judicial.

Observa-se que as alterações normativas acima citadas têm como característica comum o fato de terem sido implementadas na última década. A produção legislativa nacional nos assuntos ligados ao ciberespaço é bastante recente e representa um esforço do Direito para atender a necessidade de regulamentação das relações decorrentes das novas tecnologias, contudo, ainda há um longo caminho a ser percorrido.

3.2.2 Os crimes cibernéticos e suas características

Marcelo Crespo (2011) ressalta que o Direito é um fenômeno cultural e acompanha a realidade temporal e geográfica em que se desenvolve. As normas necessitam ter capacidade de adaptação para regulamentar as constantes mudanças sociais, políticas e econômicas, uma vez que tais mudanças interferem diretamente na seara jurídica.

Entre as recentes modificações ocorridas na sociedade, o autor destaca o impacto da informática como instrumento de informação e seu consequente valor econômico. Neste cenário, o Direito tem sido chamado a regulamentar as diversas questões ocorridas em ambiente digital. Da demanda social, surgiu o Direito da Informática, definido como o ramo do Direito que estuda e busca soluções para conflitos jurídicos decorrentes da evolução tecnológica. O direito da informática, na visão de Crespo, não seria um novo ramo do Direito, mas uma releitura das normas jurídicas à luz da Sociedade da Informação (CRESPO, 2011).

Observa-se que o desenvolvimento da tecnologia e da comunicação digital tem sido usado tanto de forma positiva, conectando pessoas em todo mundo e possibilitando a transmissão de informação, como de forma negativa, servindo de meio para o cometimento de delitos. A Internet tem demonstrado ser um ambiente favorável à criminalidade, tendo em vista que os delitos praticados pela Rede Mundial de Computadores são bastante lucrativos e envolveriam baixos riscos para os criminosos. Estudiosos afirmam que existe uma tendência de aumento da criminalidade por meios eletrônicos. De acordo com Santos (2018, p. S.I.),

> Cameron Brown, expert em segurança aplicada à defesa cibernética e pesquisador independente de tendências criminosas no ciberespaço, adverte que as oportunidades de ganhar a vida através do crime cibernético "impulsionarão os hipossuficientes e demais indivíduos de baixa renda a perseguir uma vida de crime na Web, dado o baixo risco e potenciais altos rendimentos", e, segundo seus estudos, a IA (inteligência artificial) cometerá mais crimes por meios eletrônicos do que os seres humanos por volta dos anos 2040, deixando um alerta aos governos e organizações quanto aos inimigos que terão que enfrentar em condições mais e mais desiguais (as tecnologias não dormem e nem param para se alimentar, muito embora tornem-se mais ágeis e poderosas com o passar do tempo).

Inicialmente, importa esclarecer que não há uma unanimidade quanto à utilização do termo “crimes digitais” ou “crimes informáticos”. Crespo (2011) prefere não tratar as duas expressões como sinônimos. O autor defende que a denominação “crimes digitais” é a mais adequada, visto que pretende referir-se a situações que envolvam o uso da informática ou da telemática para a prática de crimes.

No que tange aos crimes digitais, numa primeira impressão, seriam considerados delitos de meio, ou seja, seriam crimes que já estão previstos em lei e que apenas passaram a ser praticados também pela via tecnológica. Contudo, passou-se a reconhecer a existência de condutas ilícitas praticadas por meio da informática contra bens jurídicos diversos daqueles tradicionalmente já protegidos pelo Direito. Assim, não só tipos penais já regulamentados como a vida, a integridade física, o patrimônio, a fé pública, mas, também outros surgidos na era digital, como as informações armazenadas (dados), a segurança dos sistemas de redes informáticas ou de telecomunicações são protegidos pelo Direito Penal. Desse modo, quanto à classificação dos crimes digitais, estes podem ser divididos em próprios ou impróprios. Os próprios seriam aqueles em que o agente visa atingir o computador, o sistema de informática ou os dados e as informações neles utilizadas; os impróprios, por seu turno, seriam condutas perpetradas contra bens jurídicos já tradicionalmente previstos em lei, nas quais a Internet é usada apenas como ferramenta (CRESPO, 2011; DARÓS MALAQUIAS, 2015).

São exemplos de crimes digitais próprios as condutas de acesso não autorizado a sistemas informáticos, as ações destrutivas nesses sistemas, a interceptação de comunicações e as modificações de dados. Já os crimes digitais impróprios são aqueles praticados contra bens jurídicos tradicionais, podendo serem exemplificados pelos crimes contra a honra (injúria, calúnia e difamação), racismo e ameaça quando praticados por meios eletrônicos (CRESPO, 2011).

Wendt e Jorge (2013), por outro lado, adotam a denominação “crimes cibernéticos”, fazendo a distinção entre “abertos” e “exclusivamente cibernéticos”:

> Com relação aos crimes cibernéticos “abertos”, são aqueles que podem ser praticados da forma tradicional ou por intermédio de computadores, ou seja, o computador é apenas um meio para a prática do crime, que também poderia ser cometido sem o uso dele. Já os crimes “exclusivamente cibernéticos” são diferentes, pois eles somente podem ser praticados com a utilização de computadores ou de outros recursos tecnológicos que permitem o acesso à Internet (WENDT; JORGE, 2013, S.I.).

Conforme mencionado, existem diversas modalidades de crimes cibernéticos. Com o intuito de facilitar a percepção destes ilícitos, foi incluído o Quadro 3, no qual constam os crimes cibernéticos mais frequentes na Rede Mundial de Computadores.

Quadro 3 – Principais crimes cibernéticos e usas tipificações

Crime	**Tipificações**
Estelionato e furto eletrônicos (fraudes bancárias)	arts. 155, §§ 3º e 4º, II, e 171 do CP
Invasão de dispositivo informático e furto de Dados	art. 154- A do CP
Falsificação e supressão de dados	arts. 155, 297, 298, 299, 313-A, 313-B do CP
Armazenamento; produção; troca; publicação de vídeos e imagens contendo pornografia infanto-juvenil	arts. 241 e 241-A, do ECA (Lei nº 8.069/1990)
Assédio e aliciamento de crianças	art. 241-D, do ECA (Lei nº 8.069/1990)
Ameaça	art. 147 do CP
Cyberbullying (veiculação de ofensas em blogs e comunidades virtuais)	arts. 138, 139, 140 do CP
Interrupção de serviço	art. 266, parágrafo 1º, do CP
Incitação e apologia de crime	arts. 286 e 287 do CP
Prática ou incitação de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional	art. 20 da Lei nº 7.716/1989
Crimes contra a propriedade intelectual artística e de programa de computador	art. 184 do CP e Lei nº 9.609/1998
Venda ilegal de medicamentos	art. 273 CP

Fonte: Caiado e Caiado (2018).

O Quadro 3 demonstra a diversidade de crimes comumente praticados pela Internet. A ampliação do uso da Internet tem impactado na esfera criminal em relação ao aumento dos meios digitas para a prática de ilícitos.

Devido ao dinamismo que caracteriza a área da tecnologia de informação e comunicação, novos produtos estão sempre sendo criados, paralelamente, a incidência de crimes cibernéticos tem aumentado. Assim, observa-se que as novas tecnologias vêm sendo utilizadas como instrumento para praticar crimes.

A regulamentação estatal, entretanto, é bem menos dinâmica que o constante processo de inovação tecnológica e a consequente onda de criminalidade que costuma acompanhá-lo. Tal lentidão pode se dar tanto pela dogmática jurídica quanto pela complexa estrutura burocrática que lhe serve de fundamento (KUMMER, 2017).

A demanda pela investigação de crimes cibernéticos é crescente, gerando para os órgãos encarregados da persecução penal a necessidade de atualização das técnicas utilizadas na investigação. Tal atualização passa pelo uso de estratégias eficientes, levando em conta as peculiaridades de cada crime, investimentos em novas tecnologias e capacitação de servidores. Cabe ressaltar que, em que pese a multiplicidade de ilícitos cibernéticos, no caso do presente trabalho, será analisado especificamente o crime de racismo na Internet, com previsão no art. 20 da Lei nº 7.716/1989 e em entendimentos do STF.

3.2.3 O crime de ódio no ordenamento jurídico brasileiro

Na Sociedade da Informação, alguns utilizam a tecnologia positivamente, para propagar valores como igualdade, fraternidade e inclusão; outros usam as mesmas ferramentas de comunicação digital para incitar o ódio e a violência. Nesse contexto, novos desafios são impostos ao Estado, que necessita se adaptar e regulamentar as condutas praticadas por meio da Internet, evitando seu mau uso – sem, todavia, restringir arbitrariamente as liberdades individuais. Assim, tecnologia, criminalidade, ciberespaço e Direito nunca estiveram tão inter-relacionados.

No cenário dos crimes cibernéticos, encontram-se os crimes de ódio praticados por meio da Rede Mundial de Computadores. Deve-se ressaltar que o termo "crimes de ódio" não existe na lei penal brasileira. Tal denominação se aplica os delitos motivados pela discriminação ou intolerância contra determinadas coletividades.

Apesar da expressão não constar na legislação brasileira, os chamados "crimes de ódio" estão previstos no Brasil por meio da Lei nº 7 716, de 5 de janeiro de 1989, conhecida como Lei do Racismo. Segundo o artigo 1º da citada lei, "serão punidos, na forma desta Lei, os crimes resultantes de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional" (BRASIL, 1989).

Conforme se observa, a lei que define o tipo penal do racismo trata de diversas formas de discriminação além da racial. Contudo, considerando que as discriminações dessa natureza são bastante frequentes, entendeu-se relevante trazer reflexões sobre o conceito de racismo. Conforme o art. 2º da Declaração sobre a Raça e os Preconceitos Raciais da UNESCO,

> O racismo engloba as ideologias racistas, as atitudes fundadas nos preconceitos raciais, os comportamentos discriminatórios, as disposições estruturais e as práticas institucionalizadas que provocam a desigualdade racial, assim como a falsa ideia de que as relações discriminatórias entre grupos são moral e cientificamente justificáveis;

> manifesta-se por meio de disposições legislativas ou regulamentárias e práticas discriminatórias, assim como por meio de crenças e atos antissociais; cria obstáculos ao desenvolvimento de suas vítimas, perverte a quem o põe em prática, divide as nações em seu próprio seio, constitui um obstáculo para a cooperação internacional e cria tensões políticas entre os povos; é contrário aos princípios fundamentais ao direito internacional e, por conseguinte, perturba gravemente a paz e a segurança internacionais (UNESCO, 1978, S.I.).

Já o art. 1º da Convenção Internacional sobre a Eliminação de todas as Formas de Discriminação Racial traz a seguinte definição:

> Na presente Convenção, a expressão "discriminação racial" significa qualquer distinção, exclusão, restrição ou preferência fundadas na raça, cor, descendência ou origem nacional ou étnica que tenha por fim ou efeito anular ou comprometer o reconhecimento, o gozo ou o exercício, em igualdade de condições, dos direitos humanos e das liberdades fundamentais os domínios, político, econômico, social, cultural ou em qualquer outro domínio da vida pública (BRASIL, 1969).

No ordenamento jurídico brasileiro, o racismo abrange outras espécies de discriminação que vão além dos preconceitos de raça ou de cor. Tal norma tipifica penalmente uma série de condutas motivadas por discriminação ou preconceito. No seu art. 20, a Lei nº 7.716/1989 prevê como crime a conduta de "praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional" (BRASIL, 1989).

Este dispositivo trata ainda de diversas formas de propagação de conteúdo racista, entre os quais se inclui a Rede Mundial de Computadores, conforme prevê expressamente o art. 20, § 3º, III:

> Art. 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.
> Pena: reclusão de um a três anos e multa.
> §1º Fabricar, comercializar, distribuir ou veicular símbolos, emblemas, ornamentos, distintivos ou propaganda que utilizem a cruz suástica ou gamada, para fins de divulgação do nazismo.
> Pena: reclusão de dois a cinco anos e multa.
> §2º Se qualquer dos crimes previstos no caput é cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza:
> Pena: reclusão de dois a cinco anos e multa.
> §3º No caso do parágrafo anterior, o juiz poderá determinar, ouvido o Ministério Público ou a pedido deste, ainda antes do inquérito policial, sob pena de desobediência:
> I - o recolhimento imediato ou a busca e apreensão dos exemplares do material respectivo;
> II- a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio;
> III- a interdição das respectivas mensagens ou páginas de informação na Rede Mundial de Computadores.
> §4º Na hipótese do § 2º, constitui efeito da condenação, após o trânsito em julgado da decisão, a destruição do material apreendido (BRASIL, 1989).

Na hipótese do delito previsto no art. 20 da Lei nº 7.716/1989, o sujeito ativo do crime deve referir-se a uma coletividade. É a menção ao coletivo que evidencia o preconceito contra um grupo em virtude de sua uma raça, cor, etnia, religião ou procedência.

Observa-se que a Lei nº 7.716/1989 é de grande importância, pois nela está a tipificação legal em relação ao discurso de ódio de cunho discriminatório. Nesse contexto, Santos (2010) esclarece que, para efeito da Lei do Racismo, será configurado crime sempre que houver qualquer espécie de discriminação ou segregação, comissiva ou omissiva, adotada contra alguém em decorrência de sua raça, cor, etnia, religião ou de sua procedência nacional, e que vise atrapalhar, limitar ou tolher o exercício regular do direito da pessoa discriminada, contrariando o princípio constitucional da isonomia.

Além da regulamentação trazida pela Lei do Racismo, a questão atinente à propagação de conteúdo discriminatório deve ser observada à luz da Constituição Federal, visto que tal norma, enquanto lei maior do ordenamento jurídico brasileiro, prevê expressamente a proteção ao princípio da dignidade humana (art. 1º, inciso III da CRFB/1988), a igualdade perante a lei (art. 5º, caput da CRFB/1988), e a não submissão a tratamento desumano ou degradante (art. 5º, inciso III do texto constitucional). Ressalta-se que a igualdade é um pressuposto inerente ao reconhecimento da dignidade humana. Nesse contexto, os direitos essenciais são reconhecidos a todos.

A Constituição Federal prevê ainda como um de seus objetivos fundamentais "promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação" (art. 3º, inciso IV da CRFB/1988) (BRASIL, 1988). Tais diretrizes também devem ser aplicadas às interações sociais ocorridas no ciberespaço.

A vedação ao racismo também é corroborada por tratados internacionais de direitos humanos dos quais o Brasil é signatário. Tais tratados são aplicáveis ao ordenamento jurídico brasileiro, formando um bloco de constitucionalidade que vem ampliar e consolidar direitos para combater a discriminação e o preconceito (art. 5º, §§ 1º e 2º da CRFB/1988).

Diferentemente dos demais tratados internacionais, que apresentam força hierárquica infraconstitucional, os tratados internacionais de proteção dos direitos humanos detêm natureza de norma constitucional (art. 102, inciso III "b" da CRFB/1988). Assim, a interpretação da Lei nº 7.716/1989, no que tange aos crimes de racismo, deve ser a da proteção do que materialmente pode considerado como bem jurídico fundamental integrante do bloco de constitucionalidade.

Cabe destacar que, ao longo do tempo, houve uma ampliação das situações criminalizadas pelo Direito Penal como racismo. A Lei nº 1.390/1951 (Lei Afonso Arinos) considerava ilícitas apenas as ofensas fundadas em preconceito de raça ou de cor. O preconceito era tido como uma contravenção penal, com pena máxima de 1 ano. A Lei nº 7.437/1985 acrescentou à Lei Afonso Arinos as hipóteses de preconceito em baseado no sexo e estado civil, permaneceu tratando-as, contudo, como contravenções penais, e não como crimes.

Em 1989, a Lei 7.716 tipificou o racismo como crime, porém continuou penalizando apenas condutas preconceituosas fundamentadas na raça ou na cor. Somente em 1997, por meio da Lei nº 9.459, foram incluídas na Lei 7.716/1989 as hipóteses de discriminação ou preconceito decorrentes da etnia, religião ou procedência nacional, aumentando a pena para de 1 a 3 anos. Ressalta-se, todavia, que o preconceito e a discriminação em função do sexo ou estado civil permaneceram sendo contravenções penais, tendo em vista a ausência de sua previsão na Lei 7.716/1989.

3.3 ATUAÇÃO DA POLÍCIA FEDERAL NO COMBATE AO RACISMO NA INTERNET

3.3.1 Atribuições da Polícia Federal na investigação do racismo

No que tange à atribuição de investigar os crimes de ódio praticados pela Internet, a Constituição Federal prevê, no art. 109 e incisos, as hipóteses de competência da Justiça Federal em razão da matéria. Entre tais hipóteses, considerando o objeto do presente trabalho, vale atentar para os seguintes trechos:

> Art. 109. Aos juízes federais compete processar e julgar:
> [...]
> IV – os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, excluídas as contravenções e ressalvada a competência da Justiça Militar e da Justiça Eleitoral;
> V – os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no país, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente;
> [...]
> Art. 144. A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos:
> I - Polícia Federal;
> [...]
> § 1º A Polícia Federal, instituída por lei como órgão permanente, estruturado em carreira, destina-se a:

> I – apurar infrações penais contra a ordem política e social ou em detrimento de bens, serviços e interesses da União ou de suas entidades autárquicas e empresas públicas, assim como outras infrações cuja prática tenha repercussão interestadual ou internacional e exija repressão uniforme, segundo se dispuser em lei (BRASIL, 1988)

Tratam-se, portanto, de situações que atentem contra bens, serviços e interesses da União e suas entidades autárquicas ou empresas públicas e de crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no país, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente.

A Lei nº 10.446/2002, ao dispor sobre atribuições investigativas da PF, prevê em seu art. 1º, inciso III que o órgão tem a atribuição de investigar infrações penais em que haja repercussão interestadual ou internacional que exija repressão uniforme "relativas à violação a direitos humanos, que a República Federativa do Brasil se comprometeu a reprimir em decorrência de tratados internacionais de que seja parte".

Os crimes de racismo previstos na Lei nº 7.716/1989, quando praticados por meio da Internet, são julgados pela Justiça Federal, pois satisfazem os requisitos previstos em lei quanto à proteção por tratados ou convenção internacional, visto que o Brasil é signatário da Convenção Internacional sobre a Eliminação de todas as Formas de Discriminação Racial[9]. A internacionalidade da conduta criminosa decorre da possibilidade de acesso ao conteúdo informacional por um usuário conectado à Internet em qualquer lugar do planeta.

Quanto à competência da Justiça Federal, vale atentar para o seguinte trecho do Roteiro de Atuação: Crimes Cibernéticos, elaborado pelo Ministério Público Federal:

> Quando praticados de forma individualizada, como a simples troca de e-mails entre pessoas residentes no Brasil, a competência será da Justiça estadual, visto que, nesse caso, não há repercussão internacional, não se enquadrando nas hipóteses do inciso V do art. 109 da Constituição.
> Porém, nos casos em que o crime seja praticado com utilização de sites, blogs ou redes sociais, tais como Facebook, Twitter, Instagram, SnapChat, Vine, Pinterest e outras, a competência será da Justiça Federal, a teor do inciso V do art. 109 da Constituição, visto que o Brasil é signatário da Convenção Internacional sobre a Eliminação de Todas as Formas de Discriminação Racial, de 7 de março de 1966, aprovada pelo Decreto Legislativo nº 23, de 21 de junho de 1967, que entrou em vigor no País em conformidade com o disposto em seu artigo 19, 1º, a 4 de janeiro de 1969, consoante o Decreto nº 65.810, de 8 de dezembro de 1969, aplicando-se aqui mutatis mutandis o quanto exposto com relação aos crimes de pornografia infanto-juvenil praticados por meio da Internet (BRASIL, 2016).

[9] O Decreto nº 65.810, de 8 de dezembro de 1969, promulgou a Convenção Internacional sobre a Eliminação de todas as Formas de Discriminação Racial, assinada pelo Brasil em 07 de março de 1966 (BRASIL, 1969).

Os julgados abaixo transcritos tratam da competência da Justiça Federal para a investigação do racismo praticado pela Internet.

> PENAL E PROCESSUAL PENAL. CRIME DE RACISMO. INDUZIMENTO E INSTIGAÇÃO ATRAVÉS DA INTERNET. INTERNACIONALIDADE. CONVENÇÃO INTERNACIONAL SOBRE ELIMINAÇÃO DE TODAS AS FORMAS DE DISCRIMINAÇÃO RACIAL. COMPETÊNCIA DA JUSTIÇA FEDERAL. (ARTS. 109, INCISOS III E V, DA CF). (...)
> Hipótese de crime perpetrado por meio da Rede Mundial de Computadores (Internet), tendo o acusado criado uma comunidade de cunho racista, intitulada 100% BRANCO, no site de relacionamento denominado ORKUT, isso através de IP localizado no Brasil, o que possibilitou a propagação de textos racistas além das fronteiras do território nacional, vez que o acesso pode se dar prontamente no estrangeiro.
> Uso de um site de relacionamentos de acesso mundial para divulgação de textos de conteúdo racista, sendo indiscutível a competência da Justiça Federal, pela previsão da repressão em convenção internacional, assim como pela inegável marca da internacionalidade. Incidência do art. 109, inciso V, da CF/88, na previsão que estabelece a competência da Justiça Federal em situações de crimes previstos em tratados ou convenção internacional, quando, iniciada a execução no país, o resultado tenha ou devesse ter ocorrido no estrangeiro. (...)
> (PROCESSO: 200881000016774, ACR7738/CE, RELATOR: DESEMBARGADOR FEDERAL MANOEL ERHARDT, Primeira Turma, JULGAMENTO: 16/02/2012, PUBLICAÇÃO: DJE 24/02/2012 - Página 140)

> PENAL. CONFLITO DE COMPETÊNCIA. CRIME DE RACISMO PRATICADO POR INTERMÉDIO DE MENSAGENS TROCADAS EM REDE SOCIAL DA INTERNET.USUÁRIOS DOMICILIADOS EM LOCALIDADES DISTINTAS. CONEXÃO INSTRUMENTAL. EXISTÊNCIA. COMPETÊNCIA FIRMADA PELA PREVENÇÃO EM FAVOR DO JUÍZO ONDE AS INVESTIGAÇÕES TIVERAM INÍCIO.
> A competência para processar e julgar o crime de racismo praticado na Rede Mundial de Computadores estabelece-se pelo local de onde partiram as manifestações tidas por racistas. Precedente Seção. 2. No caso, o procedimento criminal (quebra de sigilo telemático) teve início na Seção Judiciária de São Paulo e culminou na identificação de alguns usuários que, embora domiciliados em localidades distintas, trocavam mensagens em comunidades virtuais específicas, supostamente racistas. O feito foi desmembrado em outros treze procedimentos, distribuídos a outras seções judiciárias, sob o fundamento de que cada manifestação constituía crime autônomo. 3. Não obstante cada mensagem em si configure crime único, há conexão probatória entre as condutas sob apuração, pois a circunstância em que os crimes foram praticados - troca de mensagens em comunidade virtual - implica o estabelecimento de uma relação de confiança, mesmo que precária, cujo viés pode facilitar a identificação da autoria. 4. Caracterizada a conexão instrumental, firma-se a competência, no caso, em favor do Juízo Federal de São Paulo - SJ/SP, onde as investigações tiveram início. Cabendo a este comunicar o resultado do julgamento aos demais juízes federais para onde desmembrados foram remetidos, a fim de que restituam os autos, ressalvada a existência de eventual sentença proferida (art. 82 do CPP). 5. Conflito conhecido para declarar a competência do Juízo Federal da 9ª Vara Criminal da Seção Judiciária de São Paulo, o suscitante.
> (STJ - CC: 116926 SP 2011/0091691-2, Relator: Ministro SEBASTIÃO REIS JÚNIOR, Data de Julgamento: 04/02/2013, S3 - TERCEIRA SEÇÃO, Data de Publicação: DJe 15/02/2013)

> CONFLITO DE COMPETÊNCIA. PROCESSUAL PENAL. RACISMO PRATICADO ATRAVÉS DE PUBLICAÇÃO DE MENSAGENS RACISTAS EM SÍTIO DE RELACIONAMENTO. INTERNET. IDENTIFICAÇÃO DOS AUTORES. NECESSIDADE. LOCAL DO CRIME. LUGAR DE ONDE FORAM

> ENVIADOS OS TEXTOS OFENSIVOS. AUSÊNCIA DE DADOS APTOS A PROVAR A ORIGEM DAS OFENSAS.CONTINUIDADE DO PROCEDIMENTO INVESTIGATÓRIO. PREVENÇÃO. COMPETÊNCIA DAQUELE JUÍZO QUE PRIMEIRO CONHECEU DA INVESTIGAÇÃO.
> A competência para processar e julgar os crimes praticados pela Internet, dentre os quais se incluem aqueles provenientes de publicação de textos de cunho racista em sites de relacionamento, é do local de onde são enviadas as mensagens discriminatórias. 2. Na espécie, mesmo após recebidas as informações da empresa proprietária do sítio, não houve como identificar, por enquanto, os autores das ofensas, o que impõe, obviamente, a manutenção do feito no âmbito daquele juízo que primeiro tomou conhecimento da investigação. 3. Conflito conhecido para declarar a competência do JUÍZO FEDERAL DA 4A VARA CRIMINAL DA SEÇÃO JUDICIÁRIA DO ESTADO DO RIO DE JANEIRO, o suscitado.
> (CC 107.938/RS, Rel. Ministro JORGE MUSSI, TERCEIRA SEÇÃO, julgado em 27/10/2010, DJe 08/11/2010).

Importa destacar que há julgados do STF e STJ que entendem que, além da publicação do conteúdo na Rede Mundial de Computadores, é preciso que haja acesso por usuários da Internet em outros países para que seja configurada a repercussão internacional – caracterizando, assim, a competência da Justiça Federal. Conforme tal entendimento, sem que haja acessos do conteúdo fora do Brasil, a competência para julgamento do crime se manteria na esfera da Justiça estadual. As diferentes interpretações quanto à competência para julgamento dos crimes de racismo pela Internet podem ser exemplificadas pelos julgados abaixo:

> STF – HABEAS CORPUS 121.283
> [...] 2. É da Justiça estadual a competência para processar e julgar o crime de incitação à discriminação racial por meio da Internet cometido contra pessoas determinadas e cujo resultado não ultrapassou as fronteiras territoriais brasileiras (BRASIL, 2014).
> STJ – CC 146.983 / RJ – CONFLITO DE COMPETENCIA
> [...] 7. Esta Corte, interpretando o disposto no art. 109, V, da CF, tem entendido, como regra geral, ser competência da Justiça Federal o julgamento de infrações penais que apresentem fortes indícios de internacionalidade da conduta e/ou de seus resultados e que estejam previstas em tratado ou convenção internacional, como é caso do racismo, previsto na Convenção Internacional sobre a Eliminação de todas as Formas de Discriminação Racial, da qual o Brasil é signatário (BRASIL, 2017).

No caso da investigação dos discursos de ódio e racismo na Internet, a Polícia Federal costuma investigar sempre que tem notícia da propagação de tal espécie de conteúdo na Rede Mundial de Computadores. Os fatos relacionados, induzimento ou incitação à discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional pela Internet costumam chegar ao conhecimento da Polícia Federal por meio de informações oriundas de terceiros – pessoas que tomem conhecimento do fato ou instituições públicas ou particulares. Não costuma haver um monitoramento constante da Internet para rastrear a propagação do conteúdo de ódio.

O volume incalculável de informações que circulam na Internet impossibilita o monitoramento contínuo de seu conteúdo. Além disso, não existe uma ferramenta investigativa voltada especificamente para a busca de discursos de ódio na Internet. Assim, considerando o volume informacional envolvido, a fim de que haja um aprimoramento da investigação de crimes de racismo na Internet, faz-se necessário recorrer ao uso da Gestão da Informação para facilitar a identificação de discurso de ódio no ciberespaço.

3.3.2 Outras formas de discurso de ódio não previstas expressamente na Lei do Racismo

Conforme analisado, a Rede Mundial de Computadores tem sido utilizada como meio para a propagação de conteúdos ofensivos e discriminatórios. O caráter criminoso dessas condutas está previsto na Lei nº 7.716/1989. Importa esclarecer que o rol de possíveis vítimas previsto na lei não contempla todos os casos de discriminação, como ocorre com preconceito em função do gênero, o qual não conta com previsão no tipo penal do racismo. Todavia, as mulheres estão entre as vítimas frequentes de situações discriminatórias na Internet.

No contexto dos crimes de ódio praticados pela Internet, merecem especial atenção as inovações trazidas pela Lei nº 13.642/2018, que alterou a Lei nº 10.446/2002 para acrescentar às atribuições da Polícia Federal a investigação de crimes praticados por meio da Rede Mundial de Computadores que consistam na difusão de conteúdos misóginos, definidos pela lei como "aqueles que propagam ódio ou aversão contra às mulheres" (BRASIL, 2018).

No Direito brasileiro, antes da Lei nº 13.642/2018, algumas normas já demonstravam uma preocupação em combater a violência contra a mulher. Entre tais normas, destaca-se a Lei nº 11.340/2006, popularmente conhecida como Lei Maria da Penha, que trouxe inovações para promover maior efetividade no combate à violência contra a mulher no contexto das agressões relacionadas à convivência doméstica ou familiar – ou seja, aquelas em que o agressor tem relação afetiva ou familiar com a vítima (BRASIL, 2006). Também pode-se mencionar a Lei nº 13.104/2015, que alterou o art. 121 do Código Penal Brasileiro e incluiu o feminicídio como uma das circunstâncias qualificadoras do homicídio, definindo-o como homicídio qualificado contra a mulher "por razões da condição de sexo feminino" (BRASIL, 2015a).

Já a Lei nº 12.737/2012 (BRASIL, 2012b), conhecida como Lei Carolina Dieckmann promoveu alterações no Código Penal Brasileiro (Decreto-Lei nº 2.848 de 7 de dezembro de 1940), tipificando os chamados delitos ou crimes informáticos. Entre os dispositivos trazidos

por tal norma, chama a atenção a tipificação da invasão do dispositivo informático, prevista no art. 154 –A, qual seja:

> 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: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa (BRASIL, 2012b).

Observa-se que a Lei Carolina Dieckmann não se restringe a hipóteses em que a vítima do crime seja do sexo feminino, em que pese seu surgimento ter sido inspirado pela agressão sofrida por uma mulher. Já a Lei nº 13.642/2018 tem a particularidade de trazer expressamente tanto a questão do combate a crimes praticados na Internet quanto à situação específica de a vítima ser do sexo feminino.

O principal impacto da Lei nº 13.642/2018 seria ampliar a quantidade de crimes investigados pela Polícia Federal. Contudo, a ausência de descrição quanto a condutas típicas caracterizadoras de crimes de atos de misoginia na Internet dificulta sua aplicabilidade. A Lei nº 13.642/2018 amplia formalmente a atribuição investigativa do Polícia Federal, porém, a efetividade prática da ampliação desta atribuição investigativa esbarra na ausência de previsão de condutas específicas que tipifiquem os crimes de ódio contra mulher na Internet.

O Brasil, enquanto Estado Democrático de Direito, é regido com base em leis criadas por representantes do povo eleitos de forma democrática. Assim, pode-se dizer que um dos princípios máximos o Estado brasileiro é o Princípio da Legalidade que determina que todos, inclusive o próprio Estado, devem obediência às leis. A Constituição Federal determina em seu artigo 5º, inciso II que: "Ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei".

Na esfera do Direito Penal, tal princípio também é previsto no art. 5º, inciso XXXIX, da Constituição (BRASIL, 1988). Segundo tal dispositivo: "Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal". Desse modo, segundo tal princípio, o Estado só pode punir crimes tipificados em lei e aplicar sanções nela previstas.

Sobre o princípio da legalidade, Bitencourt (2018) esclarece:

> Em termos bem esquemáticos, pode-se dizer que, pelo princípio da legalidade, a elaboração de normas incriminadoras é função exclusiva da lei, isto é, nenhum fato pode ser considerado crime e nenhuma pena criminal pode ser aplicada sem que antes da ocorrência desse fato exista uma lei definindo-o como crime e cominando-lhe a sanção correspondente. A lei deve definir com precisão e de forma cristalina a conduta proibida.

No âmbito penal, a legalidade está amparada ainda em uma máxima originada do Direito Romano, que prevê que "*Nullum crimen sine lege. Nulla poena sine lege*", ou seja, não há crime nem pena sem lei – sendo denominada Princípio da Reserva Legal, da Legalidade Estrita ou da Tipicidade.

A Tipicidade é, portanto, uma consequência direta do Princípio da Legalidade. Desse modo, no âmbito da previsão legal acerca da descrição das condutas consideradas criminosas, aplica-se no Brasil o Princípio da Reserva Legal, que consiste numa aplicação mais restrita do princípio da legalidade, pois exige lei formal para a regulamentação de determinadas matérias.

> Quanto ao princípio de reserva legal, este significa que a regulação de determinadas matérias deve ser feita, necessariamente, por meio de lei formal, de acordo com as previsões constitucionais a respeito. Nesse sentido, o art. 22, I, da Constituição brasileira estabelece que compete privativamente à União legislar sobre Direito Penal. A adoção expressa desses princípios significa que o nosso ordenamento jurídico cumpre com a exigência de segurança jurídica postulada pelos iluministas. Além disso, para aquelas sociedades que, a exemplo da brasileira, estão organizadas por meio de um sistema político democrático, o princípio de legalidade e de reserva legal representam a garantia política de que nenhuma pessoa poderá ser submetida ao poder punitivo estatal, se não com base em leis formais que sejam fruto do consenso democrático (BITTENCOURT, 2018).

A Lei nº 13.642/2018, ao prever a atribuição da Polícia Federal para investigar crimes de "ódio contra a mulher na Internet", concentrou-se na questão da investigação criminal e no combate à impunidade. Tal norma conta apenas com dois artigos, e traz a seguinte disposição:

> Art. 1º O caput do art. 1º da Lei nº 10.446, de 8 de maio de 2002, passa a vigorar acrescido do seguinte inciso VII:
> [...]
> VII - quaisquer crimes praticados por meio da Rede Mundial de Computadores que difundam conteúdo misógino, definidos como aqueles que propagam o ódio ou a aversão às mulheres.
> (NR)
> Art. 2º Esta Lei entra em vigor na data de sua publicação (BRASIL, 2018).

Já o Caput do art. 1º da Lei nº 10.446/ 2002 dispõe:

> Art. 1º. Na forma do inciso I do § 1o do art. 144 da Constituição, quando houver repercussão interestadual ou internacional que exija repressão uniforme, poderá o Departamento de Polícia Federal do Ministério da Justiça, sem prejuízo da responsabilidade dos órgãos de segurança pública arrolados no art. 144 da Constituição Federal, em especial das Polícias Militares e Civis dos Estados, proceder à investigação, dentre outras, das seguintes infrações penais:
> [...]

> quaisquer crimes praticados por meio da Rede Mundial de Computadores que difundam conteúdo misógino, definidos como aqueles que propagam o ódio ou a aversão às mulheres.
> Parágrafo único. Atendidos os pressupostos do caput, o Departamento de Polícia Federal procederá à apuração de outros casos, desde que tal providência seja autorizada ou determinada pelo Ministro de Estado da Justiça.

Observa-se que a Lei nº 13.642/2018 não alterou as atribuições já existentes da Polícia Federal, mas apenas incluiu uma nova atribuição, que, assim como as previstas nos demais incisos, deve se pautar pelas restrições trazidas no *caput*. Ou seja, a investigação criminal se dará nas hipóteses em que "houver repercussão interestadual ou internacional que exija repressão uniforme". A questão da repercussão interestadual e da repressão uniforme está prevista no art. 144 da própria Constituição Federal:

> Art. 144. A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos:
> I - polícia federal;
> II- polícia rodoviária federal; III - polícia ferroviária federal; IV - polícias civis;
> V - polícias militares e corpos de bombeiros militares.
> §1º A polícia federal, instituída por lei como órgão permanente, estruturado em carreira, destina-se a:
> I - apurar infrações penais contra a ordem política e social ou em detrimento de bens, serviços e interesses da União ou de suas entidades autárquicas e empresas públicas, assim como outras infrações cuja prática tenha repercussão interestadual ou internacional e exija repressão uniforme, segundo se dispuser em lei (BRASIL, 1988).

A Lei nº 10.446/2002, portanto, em seu art. 1º, traz uma lista de crimes que podem ser investigados pela Polícia Federal, ainda que não haja agressão direta a bens, serviços ou interesses da União. Nesse contexto, os delitos que se enquadram na hipótese seu do art. 1º poderão ser investigados pela Polícia Federal, ainda que a competência para seu julgamento seja da Justiça estadual.

A Lei nº 10.446/2002 faz também uma ressalva quanto à preservação das atribuições para outros órgãos de segurança pública, ao dispor que a investigação pela PF se dará "sem prejuízo da responsabilidade dos órgãos de segurança pública arrolados no art. 144 da Constituição Federal, em especial das Polícias Militares e Civis dos Estados, proceder à investigação, dentre outras, das seguintes infrações penais [...]" (BRASIL, 1988).

Cabe destacar que a lista de crimes previstos no art. 1º da Lei 10.446/2002 é meramente exemplificativa, pois o parágrafo único deste mesmo dispositivo prevê que a Polícia Federal poderá investigar outras infrações penais que não estejam em seu rol, desde que sejam atendidos os pressupostos do *caput* – ou seja, que o fato tenha repercussão interestadual ou internacional

e exija repressão uniforme, e que tal providência seja autorizada ou determinada pelo Ministro de Estado da Justiça.

A Lei nº 13.642/2018, ao atribuir à Polícia Federal a competência para investigar crimes associados à propagação de conteúdo de ódio ou misógino praticados pela Internet, trouxe uma relevante inovação jurídica. Tal alteração normativa refletiu a preocupação social com a impunidade nos casos de violência contra mulheres praticadas pela Rede Mundial de Computadores. Assim, a busca de uma investigação eficiente pode ser entendida como parte de um processo de conscientização quanto à necessidade de se combater a misoginia na sociedade moderna.

No que tange à inovação trazida pela Lei nº 13.642/2016, observa-se que existe uma dificuldade em relação a sua aplicabilidade em virtude da ausência de tipificação penal quanto à sua hipótese de incidência. Nesse contexto, para proporcionar uma maior efetividade ao combate à propagação de conteúdo de ódio contra a mulher na Internet, entende-se como relevante a inclusão da discriminação de gênero no tipo penal trazido pela Lei de Racismo.

Outra questão não prevista na Lei de Racismo seria a discriminação em decorrência da orientação sexual. Em julgados proferidos no dia 13 de junho de 2019, o Supremo Tribunal Federal (STF) considerou a homofobia uma modalidade de racismo, passando a criminalizá-la. O Supremo declarou a omissão do Congresso Nacional em regulamentar as condutas racistas praticadas contra o grupo definido como LGBT (lésbicas, gays, bissexuais, transexuais e travestis) e determinou que tais condutas fossem enquadradas no tipo penal do racismo até sua futura regulamentação.

Segundo o STF, a necessidade de combate às condutas discriminatórias está prevista Constituição Federal, não podendo a omissão do Poder Legislativo ser uma causa para a impunidade. Assim, a Corte Suprema ressaltou que, com a decisão, não estaria legislando, mas garantindo o cumprimento da Constituição. A utilização da Lei do Racismo como parâmetro para a equiparação de outras formas de discriminação foi analisada na Ação Direta de Inconstitucionalidade por Omissão (ADO) nº 26 (BRASIL, 2019a) e no Mandado de Injunção nº 4.733 (BRASIL, 2019b), protocoladas pelo Partido Popular Socialista (PPS) e pela Associação Brasileiras de Gays, Lésbicas e Transgêneros (ABGLT). Tais entidades entendem que a minoria LGBT deve ser incluída no conceito de "raça social" e os agressores punidos na forma do crime de racismo. Seguem abaixo trechos das citadas decisões:

Ação Direta de Inconstitucionalidade por Omissão (ADO) nº 26:

> d) dar interpretação conforme à Constituição, em face dos mandados constitucionais de incriminação inscritos nos incisos XLI e XLII do art. 5º da Carta Política, para enquadrar a homofobia e a transfobia, qualquer que seja a forma de sua manifestação, nos diversos tipos penais definidos na Lei nº 7.716/89, até que sobrevenha legislação autônoma, editada pelo Congresso Nacional, seja por considerar-se, nos termos deste voto, que as práticas homotransfóbicas qualificam-se como espécies do gênero racismo, na dimensão de racismo social consagrada pelo Supremo Tribunal Federal no julgamento plenário do HC 82.424/RS (caso Ellwanger), na medida em que tais condutas importam em atos de segregação que inferiorizam membros integrantes do grupo LGBT, em razão de sua orientação sexual ou de sua identidade de gênero, seja, ainda, porque tais comportamentos de homotransfobia ajustam-se ao conceito de atos de discriminação e de ofensa a direitos e liberdades fundamentais daqueles que compõem o grupo vulnerável em questão (BRASIL, 2019a).

Mandado de Injunção nº 4.733:

> O Tribunal, por maioria, conheceu do mandado de injunção, vencido o Ministro Marco Aurélio, que não admitia a via mandamental. Por maioria, julgou procedente o mandado de injunção para (i) reconhecer a mora inconstitucional do Congresso Nacional e; (ii) aplicar, com efeitos prospectivos, até que o Congresso Nacional venha a legislar a respeito, a Lei nº 7.716/89 a fim de estender a tipificação prevista para os crimes resultantes de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional à discriminação por orientação sexual ou identidade de gênero, nos termos do voto do Relator, vencidos, em menor extensão, os Ministros Ricardo Lewandowski e Dias Toffoli (Presidente) e o Ministro Marco Aurélio, que julgava inadequada a via mandamental (BRASIL, 2019b).

A preocupação com o conteúdo das informações que circulam na Internet e a tendência de surgimento de novas leis que ampliem o número de vítimas de crimes de ódio no ciberespaço pode ser percebida ainda por meio da apresentação do Projeto de Lei (PL) nº 2496/2019, apresentado em 24 de abril de 2019. Conforme prevê em sua ementa, o projeto

> Altera as Leis nº 10.446, de 8 de maio de 2002, e nº 12.965, de 23 de abril de 2014, para incluir no rol das infrações de repercussão interestadual ou internacional que exigem repressão uniforme os crimes, praticados ou planejados por meio da Internet, que se caracterizem pela difusão de conteúdo de preconceitos de origem de raça, cor, sexo, idade e quaisquer formas de discriminação; nos quais haja apresentação de violação aos direitos humanos; que sejam classificados como inafiançáveis e insuscetíveis de graça; ou que difundam conteúdo misógino; e para estabelecer mecanismos de cooperação internacional na investigação de tais crimes (BRASIL, 2019c).

O PL foi apresentado na Câmara dos Deputados e será submetido ao trâmite legislativo, podendo futuramente vir a ser convertido em lei. Em que pese a questão ainda estar sujeita a debates e não ter força de lei, é possível constatar uma preocupação com a circulação de conteúdos discriminatórios na Internet, havendo uma tendência de se abranger um número maior de possíveis vítimas, bem como uma intenção do legislador de ampliar as hipóteses de investigação dessa modalidade de crime cibernético pela Polícia Federal.

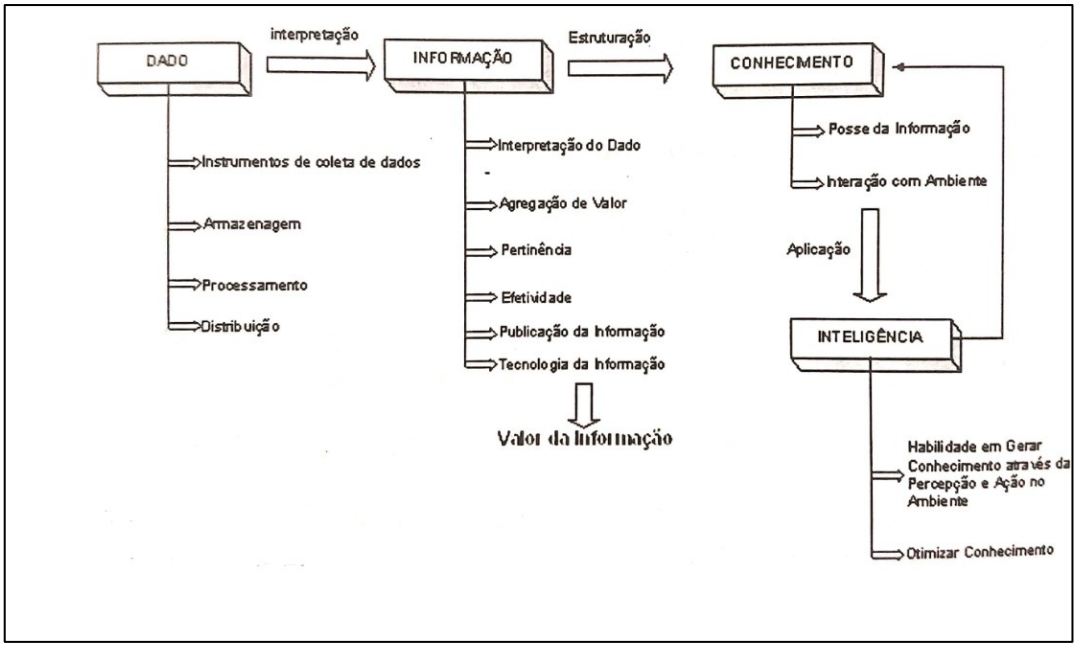
3.4 O USO DA GESTÃO DA INFORMAÇÃO PARA APRIMORAR A INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS

3.4.1 Ferramentas de Gestão da Informação como caminho para o aumento da eficiência

Segundo Dumont, Ribeiro e Rodrigues (2006), o grande desafio enfrentado por governantes na atualidade é como melhorar e modernizar a inteligência pública diante da imensa quantidade de informações e da escassez de conhecimento. Os instrumentos de acesso à informação tornaram-se ágeis por meio de redes de comunicação e sistemas de informação. Os gestores necessitam tomar decisões rapidamente, numa realidade extremamente mutável e com um grande volume de informações disponíveis. Nesse cenário, torna-se cada vez mais imprescindível dominar técnicas e ferramentas que permitam a geração e a aplicação do conhecimento.

Os autores definem informação como "mensagem transmitida da interpretação de um ou mais dados". Já o conhecimento seria a "a coleção de informações situadas no interior de um agente que o habilita a atuar no meio ambiente com eficácia maior do que se esse agente não dispusesse dessa informação". Inteligência, por sua vez, seria "a capacidade de um agente gerar conhecimento através da percepção e da ação no ambiente em que vive" (DUMONT; RIBEIRO; RODRIGUES, 2006, p. 34-35). A Figura 2 descreve as etapas de desenvolvimento da inteligência e geração do conhecimento em qualquer instituição.

Figura 2 – Etapas de geração do conhecimento



Fonte: Dumont, Ribeiro e Rodrigues (2006, p. 35).

Sob o aspecto epistemológico, não existe um consenso acerca do conceito de Gestão da Informação nem sobre o campo do conhecimento no qual ela se situa. Na Ciência da Informação, a GI ora é vista como uma disciplina, ora como como uma área de conhecimento. Ainda que haja diversos estudos sobre o tema, não há uma unanimidade quanto a sua definição conceitual. No Brasil, a Tabela de Áreas do Conhecimento da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes) costuma classificar a GI no âmbito da grande área das Ciências Sociais Aplicadas, que também contempla a CI. Em Portugal, por sua vez, a tabela utilizada pela Fundação para a Ciência e a Tecnologia (FCT) não aponta um enquadramento específico para a GI, que pode ser incluída na área das Ciências Sociais e na subárea Economia e Gestão ou na subárea Ciências da Comunicação, mais especificamente no âmbito das Ciências Documentais e da Informação (FREITAS; VIANNA, 2019).

A Gestão da Informação pode ser compreendida como subdisciplina da gestão e como disciplina da Ciência da Informação. Nas palavras de Corujo e Silva (2019),

> a Gestão da Informação (GI) como disciplina é uma questão ainda em debate. É, por um lado, amplamente aceite quer como subdisciplina da gestão, quer como disciplina da ciência da informação, quer como campo intimamente relacionado com os sistemas de Informação, posicionando-se estes na perspectiva da tecnologia da informação (TI).

Ainda segundo os autores, embora a GI comumente seja contextualizada na área empresarial, o capital informacional também está diretamente ligado à origem de qualquer instância estatal e/ou militar, pois estas também necessitam de um esforço para medir, contar, avaliar e conhecer o capital informacional com o objetivo de estimar e gerir recursos. Destaca-se que a utilização da GI no aprimoramento da eficiência organizacional não é um fato recente, pois há muito vem sendo utilizada por empresas corporativas, bibliotecas e órgãos da administração pública, como os serviços secretos (CORUJO; SILVA, 2019).

Para Choo (1998), uma organização inteligente utiliza os recursos informacionais para melhorar seu desempenho, usando o conhecimento que dispõe sobre o meio para nortear seu comportamento. A gestão da informação é vista como ferramenta para contribuir com o aprendizado organizacional e consequentemente melhorar seus resultados. Em que pese não haver um consenso quanto ao conceito de Gestão da Informação, vale atentar para a definição apresentada por tal autor, segundo o qual a GI consiste em

> *a cycle of processes that support the organization's learning activities: identifying information needs, acquiring information, organizing and storing information, developing information products and services, distributing information, and using information* (CHOO, 1998, [s.p.]).

O processo de Gestão da Informação é utilizado como caminho para a organização e sistematização da informação, a fim de tirar dela o melhor proveito para atender as suas necessidades. De acordo com Beuren (1998, p.68), o processo da gestão da informação se dá pela:

> identificação de necessidades e requisitos de informação coleta/entrada de informação, classificação e armazenamento da informação, tratamento e apresentação da informação, desenvolvimento de produtos e serviços de informação, distribuição e disseminação de informação, análise e uso da informação.

Freitas e Vianna (2019) lembram que, no sentido etimológico, o conceito de gestão ou administração – *management* – está ligado ao significado de controlar ou ter o controle e a condução de algo. Ressaltam que "no latim (*gestĭo, ōnis*), o termo gestão refere-se à ação e ao efeito de gerir ou de administrar, que, por sua vez, consiste em governar, dirigir, ordenar ou organizar".

Uma das dificuldades enfrentadas pelas organizações modernas é lidar com os excessos informacionais. Assim, a gestão da informação se faz necessária para orientar as

instituições a lidar com o volume de informações disponíveis, selecionando aquelas que forem mais relevantes para realização de seus objetivos.

Cabe observar que as demandas informacionais não foram sempre as mesmas, evoluindo com o passar do tempo. O Quadro 4 aborda as mudanças nas características da GI.

Quadro 4 – Comparativo de fases e características inerentes à Gestão da Informação

Primeira fase	**Segunda fase**	**Terceira fase**
Período: da segunda metade da década de 1960 até ao início da década de 1970	**Período**: entre o final dos anos 1970 e a década de 1980	**Período**: a partir do início da década de 1990
Prioridade: utilização de dados como meta	**Prioridade**: processamento eficiente de informação pelos Sistemas de Informação (SI), com o consequente uso de métodos e de abordagens predominantemente situados na área da Informática	**Prioridade**: utilização dos SI e das Tecnologias de Informação (TI), vistos como soluções inovadoras nas tarefas de gestão e, consequentemente, no cumprimento efetivo da missão e dos objetivos da organização
Ênfase: no uso de métodos e de abordagens eficientes na solução de tarefas de processamento de dados	**Ênfase**: nas abordagens e nas técnicas de gestão eficiente dos recursos de informação (e.g., organização, documentação tecnológica, bibliotecas, etc.); na implementação e no uso dos SI, todavia sem enfatizar o papel dos utilizadores finais; na integração dos processos de informação nas abordagens de gestão, todavia sem enfatizar a importância dos SI e das TI para a inovação ou sem aprofundar o debate teórico acerca da aplicação dos métodos tradicionais de gestão	**Ênfase**: na eficácia no processamento da informação, ou seja, no "fazer as coisas certas" *("doing the right things")*, mas em associação com a eficiência, que implica "fazer as coisas direito" *("doing things right")*. na aplicação de processos padronizados de gestão, no planejamento e no controle, aliados à garantia dos fluxos cotidianos de informação voltados para as tomadas de decisão; no principal efeito do uso dos SI e das TI, ou seja, na "matriz de valor" do trabalho de gestão
Conceito de IM/GI derivado dessa lógica: confunde-se com o conceito de gestão e de processamento de dados	**Conceito de IM/GI derivado dessa lógica:** conjunto de métodos e de abordagens de gestão que atendem às necessidades tecnológicas e à busca da eficiência - na acepção de "fazer as coisas direito" *("doing things right")*; abordagem que compreende o planejamento, a organização e o controle dos recursos de informação, com a consequente contratação, para compor os quadros organizacionais, de gestores e de diretores de informação	**Conceito de IM/GI derivado dessa lógica:** produção, de modo eficaz, armazenamento, recuperação e disseminação de informação em qualquer formato e suporte, para apoiar os objetivos de "negócio" e cumprir as metas da organização

Fonte: Freitas e Vianna (2019).

No que tange à investigação de crimes cibernéticos, observa-se que a Gestão da Informação se adequa às perspectivas abordadas pela terceira fase, apontada no quadro acima.

Nesse contexto, os Sistemas de Informação (SI) e as Tecnologias da Informação (TI) são vistos como soluções para as tarefas de gestão e obtenção de melhores resultados, auxiliando a instituição na realização de seus objetivos. Existe atualmente uma ênfase na eficácia do processamento da informação, na aplicação de processos padronizados de gestão, no planejamento e no controle informação, a fim de proporcionar maior eficiência na tomada de decisões pelo gestor.

3.4.2 Contribuições da GI para a Polícia Federal

Segundo Choo (1995), a Gestão da Informação seria um conjunto de processos que têm como finalidade utilizar os recursos e as capacidades de informação para o desenvolvimento da organização de modo que ela se mantenha atualizada dentro de um ambiente social em constante mutação e esteja apta a atingir seus objetivos.

Ainda segundo o autor, a GI abrangeria seis processos distintos, porém relacionados:

a) identificação de necessidades de informação;

b) aquisição de informação;

c) organização e armazenamento de informação;

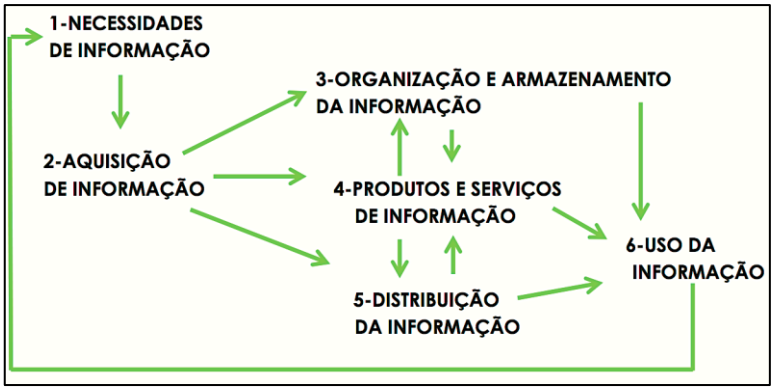
d) desenvolvimento de produtos e serviços de informação;

e) distribuição de informação; e

f) utilização de informação.

Os conceitos acima apresentados relacionam-se à consecução dos objetivos institucionais de uma organização. Eles contribuem para a sobrevivência desta em um ambiente corporativo dinâmico e competitivo (CHOO, 1995).

Figura 3 – Modelo de Choo para Gestão da Informação



Fonte: Choo (1995).

Choo adota uma perspectiva sistêmica sobre Gestão da Informação, como podemos observar pelo texto abaixo:

> *An organization behaves as an open system that takes in information, material and energy from the external environment, transforms these resources into knowledge, processes, and structures that produce goods or services which are then consumed in the environment. The relationship between organizations and environment is thus both circular and critical: organizations depend on the environment for resources and for the justification of their continued existence. Because the environment is growing in complexity and volatility, continuing to be viable requires organizations to learn enough about the current and likely future conditions of the environment, and to to use this knowledge to change their own behavior in a timely (CHOO, 1998, [s.p.]).*

A complexidade e volatilidade apontadas por Choo também podem ser percebidas em relação ao contexto dos crimes cibernéticos, demandando uma constante necessidade de adaptação por parte das organizações de segurança pública a fim de possuir recursos tecnológicos e conhecimentos necessários para obter resultados eficientes na prevenção e combate ao cibercrime.

Thomas Davenport também levou em consideração diversos fatores ao propor um modelo de processo de gerenciamento de informações. Para o autor, o modelo de gerenciamento deve "identificar todos os passos de um processo informacional – todas as fontes envolvidas, todas as pessoas que afetam cada passo, todos os problemas que surgem". Assim, por meio de um processo de gerenciamento, seria possível propiciar que uma informação identificada como precisa alcance seu usuário em tempo hábil para solucionar problemas organizacionais de forma adequada e eficiente (DAVENPORT, 2002, p. 173).

Figura 4 – Modelo de Davenport para Gestão da Informação

Fonte: Davenport (1998, p. 175).

Davenport (1998) compreende a GI como um processo, um conjunto estruturado de atividades, representado pela captura, distribuição e utilização da informação. Tal processo seria composto por quatro etapas: definição dos requisitos ou necessidades informacionais, a

coleta, a distribuição e o uso da informação. O autor propôs uma abordagem de gerenciamento da informação conhecida como “Ecologia da Informação”, que traz um paralelo entre sistemas organizacionais e sistemas biológicos, tidos como como sistemas abertos, interagentes e interdependentes.

> Considero a ecologia, a ciência de compreender e administrar todos os ambientes, apenas uma metáfora. Em vez de modelar um ambiente informacional em máquinas e edifícios, proponho uma abordagem mais harmoniosa com as coisas vivas. Quando começamos a pensar nas muitas relações entrecruzadas de pessoas, processos, estruturas de apoio e outros elementos do ambiente informacional de uma empresa, obtemos um padrão melhor para administrar a complexidade e a variedade do uso atual da informação. Também poderíamos descrever a ecologia da informação com administração holística da informação ou administração informacional centrada no ser humano. O ponto essencial é que essa abordagem devolve o homem ao centro do mundo da informação, banindo a tecnologia para seu devido lugar, na periferia (DAVENPORT, 1998, p. 21).

Segundo Davenport (1998, p. 44), a abordagem ecológica representa uma visão holística da informação ou da administração informacional, sempre levando em consideração sua interação com o ser humano. Para o autor, o ambiente informacional deve apresentar quatro atributos:

- integração dos diversos tipos de informação;
- reconhecimento de mudanças evolutivas;
- ênfase na observação e na descrição; e
- ênfase no comportamento pessoal e informacional.

Tal perspectiva holística pode ser pensada à luz dos agentes envolvidos nas transformações vivenciadas na Sociedade da Informação, não sendo pertinente focar apenas em recursos tecnológicos, mas também nas pessoas envolvidas e nos contextos sociais. Observa-se que, no caso do discurso discriminatório na Internet, para se definir que uma informação caracteriza um determinado tipo penal, faz-se necessário realizar uma análise do contexto dos fatos e da intenção do agente. Uma expressão como “neguinho”, por exemplo, pode caracterizar um xingamento ou uma expressão afetuosa, a depender da situação, da intenção do autor e até mesmo dos costumes regionais que influenciam a linguagem.

Nas investigações criminais, também se deve atentar para a qualidade da informação, posto que, se esta for incorreta ou inidônea, poderá comprometer todo o conhecimento construído acerca do fato investigado. Cabe lembrar que, no caso de órgãos públicos, há uma obrigação constitucional em relação à lisura dos atos administrativos. O art. 37 da Constituição

Federal prevê expressamente que "a administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência" (BRASIL, 1988). Tais requisitos devem ser comtemplados também sob a ótica da qualidade da informação utilizada em investigações policiais.

Corujo e Silva (2019) esclarecem que, seguindo uma abordagem empresarial, a GI seria um processo consciente de utilização da informação para subsidiar a tomada de decisões de forma estratégica, visando atingir um objetivo institucional. Nesse caso, a GI é vista como um ativo, como um recurso estratégico para a organização, similar à gestão de recursos financeiros, de recursos humanos ou de outro ativo qualquer.

> Deste modo, não estamos perante uma função ou um conjunto de procedimentos específicos, mas perante um conceito abrangente, que integra funções relacionadas, mas específicas: planeamento estratégico de informação; engenharia de informação; planeamento de tecnologia de informação; administração de dados; gestão documental; desenvolvimento aplicacional e desenvolvimento de sistemas. A finalidade da gestão de recursos de informação é o planeamento e outras atividades orientadas de uma organização que resultem em informação utilizável, acessível, atempada, segura, integral, económica e precisa para essa organização (CORUJO; SILVA, 2019, p. 151).

Nas investigações policiais, a informação não é encarada sob a perspectiva empresarial, pois a necessidade informacional visa atender a um dever de enfrentamento à criminalidade. É uma demanda fundamentada em obrigações legais atribuídas às instituições policiais, sendo relevante investir em recursos tecnológicos e capacitação do material humano, a fim de viabilizar a aquisição, organização e processamento da informação para chegar à descoberta da autoria e materialidade de crimes.

3.4.3 Relevância do esclarecimento da sociedade sobre práticas discriminatórias na Internet

Diante da constatação acerca da dificuldade de realizar um monitoramento constante da Internet em busca de situações de racismo, chegou-se à hipótese de que uma relevante ferramenta de combate a tal crime em ambiente virtual seria o estímulo à colaboração de usuários da Rede Mundial de Computadores. Assim, pessoas que visualizassem páginas com conteúdo de cunho discriminatório poderiam fazer denúncias aos órgãos policiais responsáveis

pela sua investigação, possibilitando a criação de uma rede de vigilância da informação sem maiores custos para o Estado, fundamentada na conscientização e na cooperação da população.

Um dos fatores que dificultam a tomada de conhecimento acerca dos casos de racismo na Internet pelas instituições policiais e pelo Ministério Público é a falta de esclarecimento sobre quando conteúdos ofensivos propagados pela Rede Mundial de Computadores configuram crimes, quais seriam as espécies de crimes relacionados ao conteúdo de ódio na Internet e que instituições as vítimas devem procurar. Nesse contexto, a informação oriunda da sociedade seria uma das principais ferramentas de combate aos crimes de racismo na Internet.

Uma das questões que demandam esclarecimento é a distinção entre os crimes de injúria racial e racismo, pois é comum que haja confusão entre ambos. A injúria está prevista no art. 140 do CP e faz parte dos chamados crimes contra honra, tipificados nos artigos 138, 139 e 140 do Código Penal, sendo sua prática bastante frequente no ambiente da Internet. Nas palavras de Crespo (2019, S.I.),

> Honra são as qualidades físicas, morais e intelectuais de uma pessoa, fazendo-a respeitada no meio social e que diz respeito, ainda, à sua autoestima. A honra representa verdadeiro patrimônio moral, merecedor de proteção, porque revela o valor social da pessoa, importando sua aceitação ou rejeição social. [...] É o crime de injúria que viola a honra subjetiva. Aqui não há atribuição de fato a alguém, mas de características negativas sobre as qualidades físicas, morais ou intelectuais de cada um de nós. Injuriar é ofender, falar mal, insultar, sem necessidade de atribuir a alguém um fato determinado. Assim, porque a ofensa é dirigida à honra subjetiva, o crime só ocorre caso a vítima tome conhecimento da ofensa, ainda que por terceiro.

O crime de injúria é previsto no art. 140 do Código Penal como “Injuriar alguém, ofendendo-lhe a dignidade ou o decoro”, com previsão de pena de detenção, de três meses a um ano, e multa. A injúria racial está tipificada no parágrafo 3º do mesmo artigo, a saber: “Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência”, com pena de um a três anos de reclusão e multa (BRASIL, 1940).

O crime de racismo é previsto na Lei n. 7.716/1989 e refere-se à prática, indução ou incitação de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional. As condutas tipificadas na Lei do Racismo visam combater atos de discriminação e segregação racial, tais como: impedir acesso a lugares públicos, empregos, meios de transporte, clubes, bares, restaurantes, sempre por conta de preconceito de raça, cor, etnia, religião ou procedência nacional (CRESPO, 2019). O Quadro 5 estabelece as principais diferenças entre a injúria racial e racismo.

Quadro 5 – Diferenças entre injúria racial e racismo

	INJÚRIA RACIAL	RACISMO
BEM JURÍDICO	honra subjetiva	dignidade humana
PRECONCEITO	raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência	raça, cor, etnia, religião ou procedência nacional
PREVISÃO LEGAL	art. 140, § 3.º, CP	Lei 7.716/89
AÇÃO PENAL	pública condicionada à representação	pública incondicionada
FIANÇA	cabe fiança	inafiançável
PRESCRIÇÃO	prescreve (art. 109, CP)	imprescritível
VÍTIMAS	número determinado de vítimas	número indeterminado de vítimas

Fonte: Araújo (2019).

Entre as diferenças apontadas no Quadro 5, importa atentar para o fato de que a injúria racial é um crime de ação pública condicionada à representação do ofendido, ou seja, a ação penal deve ser movida por um membro do Ministério Público mediante representação da vítima. No caso do racismo, a ação penal é pública incondicionada, o Estado não precisa de representação de alguém que se sinta ofendido para investigar ou processar o suposto autor do fato.

Também é possível que o racismo na Internet seja confundido com situações de ofensas caracterizadas como *cyberbullying*, um fenômeno mais recente, que decorre do surgimento da Internet e da popularização das redes sociais. Trata-se da realização no mundo virtual de condutas qualificadas como *bullying*, o qual consiste na prática de atos de violência física e/ou psicológica, de caráter intencional e repetitivo, por um ou mais indivíduos, contra uma ou mais vítimas, que se encontram impossibilitadas de se defender (BRASIL, 2016).

No ciberespaço, a violência causada pelo *bullying* costuma ocorrer por meio de intimidações, chacotas, humilhações e ameaças, via mensagens ou fotografias, causando um dano moral de difícil reparação. Importa observar que não existe um tipo penal específico para o *bullying* nem para o *cyberbullying*. As condutas que caracterizam esses comportamentos podem encontrar descrição nos delitos contra a honra e na ameaça (BRASIL, 2016).

A Lei nº 13.185, de 6 de novembro de 2015, instituiu o Programa de Combate à Intimidação Sistemática (*Bullying*) em todo o território nacional (BRASIL, 2015c). Conforme essa norma, o Programa instituído poderá fundamentar as ações do Ministério da Educação e das Secretarias Estaduais e Municipais de Educação, bem como de outros órgãos aos quais a matéria diz respeito. Trata-se de uma lei que traz conceitos e condutas que caracterizam o *bullying*. Em que pese ser esclarecedora e ter o intuito de combater tal prática, não se trata de uma norma penal, pois não criminaliza nem imputa sanções penais para as condutas tipificadas como *bullying*.

Diante do cenário atual, em que a Internet virou palco para diversos tipos de agressões morais com um número infindável de espectadores, entende-se ser necessário prestar esclarecimentos à sociedade sobre quando os comentários agressivos na seara virtual caracterizam crimes, quais são os delitos correspondentes e qual seria a entidade estatal responsável por sua apuração. A ideia é que o tema seja tratado de forma sucinta e em linguagem acessível, a fim de esclarecer e informar a população.

Inicialmente, pensou-se em elaborar um guia, um documento voltado para instruir a sociedade a respeito de situações que caracterizam crimes de ódio, bem como sobre as medidas a serem tomadas quando se é vítima ou se constata situações dessa espécie na Internet. Assim, a princípio, a pesquisa tinha como um dos seus objetivos a elaboração de um documento dessa natureza, que poderia ser apresentado pela PF à sociedade, com intuito informativo e educacional, podendo ser disponibilizado na própria página da Polícia Federal na Internet.

Contudo, foi possível verificar que algumas instituições já oferecem material com tais características. A ONG SaferNet, que conta com um "Termo de Cooperação Técnica, Científica e Operacional" firmado com a Polícia Federal, disponibiliza em seu site material educativo voltado para o esclarecimento de internautas sobre crimes cibernéticos (entre eles o racismo), contando inclusive com um canal para denúncias. Logo, em vez de elaborar seu próprio material educativo, entende-se que, como medida alternativa de Gestão da Informação, a PF pode proporcionar a divulgação de conteúdo educativo elaborado por seus parceiros, a exemplo da SaferNet, no seu próprio site ou criar de *links* conectando sua página às páginas de seus colaboradores.

Conforme mencionado, SaferNet, disponibiliza em seu site um vasto material sobre diversos crimes cibernéticos. Tal situação pode ser vista como uma oportunidade de utilização da informação proveniente de outras instituições para auxiliar no esclarecimento da sociedade. Entre os conteúdos disponibilizados pela ONG, pode-se destacar o material didático

denominado “Diálogo Virtual”[10], que traz informações sobre situações de risco ocorridas na Rede Mundial de Computadores.

Já como exemplo de ente público que apostou na elaboração de seu próprio material com intuito pedagógico e informativo sobre crime cibernético tem-se o Tribunal de Justiça do Estado de Minas Gerais (TJMG). A Assessoria da Polícia Civil do TJMG (ASPC 2ª Instância) elaborou uma cartilha intitulada “Prevenção contra invasões e crimes informáticos”[11], que tem como escopo o esclarecimento de magistrados e servidores do TJ/MG sobre fraudes eletrônicas na Internet.

A parceria com outras instituições pode ser uma medida de Gestão da Informação relevante para otimizar o combate à criminalidade cibernética, ampliando o acesso da população a conteúdo informacional sobre delitos na Internet a um custo reduzido. No contexto do combate ao crime virtual, o esclarecimento da população é uma estratégia importante, uma vez que muitos fatos criminosos não chegam ao conhecimento da polícia devido ao desconhecimento dos usuários da Internet quanto a sua ilicitude.

3.5 COMPARAÇÃO DE TÉCNICAS INVESTIGATIVAS UTILIZADAS EM OUTRAS ESPÉCIES DE CRIMES

3.5.1 Análise ferramenta já aplicada na investigação de outras espécies de crimes

O objetivo principal da presente pesquisa é aumentar a eficiência da Polícia Federal na investigação de crimes de ódio na Internet, utilizando a Gestão da Informação para auxiliar na identificação de conteúdo ilícito e, consequentemente, melhorar o combate à criminalidade. Um dos caminhos para esse aprimoramento seria a vigilância de conteúdos racistas publicados na Rede Mundial de Computadores. Para verificar a viabilidade da realização dessa vigilância, optou-se por analisar ferramentas já aplicadas na investigação de outras espécies de crimes cibernéticos. Assim, por meio de perguntas formuladas a especialistas, buscou-se comparar a aplicabilidade de uma ferramenta usada na investigação de pornografia infantil na Internet à apuração de crimes de ódio.

---

[10] Disponível em: https://new.safernet.org.br/sites/default/files/content_files/Di%C3%A1logo_Virtual_Low_Web_SN_Unicef_PFDC_CGI.pdf. Acesso em: 15 dez. 2019.

[11] Disponível em https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2020/01/prevencao-contra-invasoes-e-crimes-informaticos.pdf. Acesso em: 18 out. 2019.

Os crimes de produção, reprodução, posse ou compartilhamento de arquivos contendo pornografia infanto-juvenil (PI) estão previstos nos artigos 240 e 241 do Estatuto da Criança e do Adolescente – Lei nº 8.069/1990, alterados pela Lei nº 11.829/2008. Frequentemente a divulgação desse tipo de conteúdo se dá por meio de mensagens eletrônicas e em conexões que usam compartilhamento ponto-a-ponto (P2P), tais como eMule, Gnutella e Ares Galaxy. Nas conexões P2P, não há necessidade da utilização de servidor, pois a comunicação ocorre por meio de nós interconectados, nos quais a ligação entre duas máquinas se dá de forma direta e os nós da rede possuem responsabilidades equivalentes (CAIADO; CAIADO, 2018).

A investigação de crimes ligados à propagação de pornografia infantil na Internet conta com recursos tecnológicos específicos. Em termos de ferramentas disponíveis para o uso dos policiais, a investigação dessa modalidade de crime encontra-se mais evoluída em relação à apuração de crimes de ódio praticados na Internet. A escolha das técnicas de investigação de pornografia infantil pela Internet como parâmetro para comparação se deu justamente em função dos recursos e ferramentas tecnológicas aplicados a este tipo de crime. Tal comparação visa extrair contribuições relevantes para o aprimoramento dos recursos e estratégias de investigação aplicados aos crimes de ódio no ciberespaço.

O compartilhamento de arquivos consiste na disponibilização de arquivos para download entre pessoas que navegam na rede, utilizando a Internet como meio de transmissão. Em regra, compartilham-se músicas, vídeos, jogos, aplicativos, livros, entre outros. Por meio do P2P, o usuário disponibiliza arquivos armazenados no seu próprio computador para outros usuários da rede, ao mesmo tempo em que lhe é possível acessar os arquivos de seus pares. Em regra, não há qualquer tipo de autenticação, contrato ou termos de uso (BRASIL, 2016).

A utilização do programa P2P, em si, não é ilegal. Seu uso pode ser legítimo, por exemplo, para distribuição de *software* livre. Contudo, também é possível o emprego desse tipo de aplicativo para fins ilícitos, como o compartilhamento de materiais que violem normas de direitos autorais ou até mesmo a distribuição de material envolvendo a exploração sexual de crianças e adolescentes (LANGE; RALHA, 2011; BRASIL, 2016).

A fim de rastrear o compartilhamento de arquivos contendo pornografia infantil via P2P, foram desenvolvidas algumas ferramentas, entre as quais destaca-se o programa CPS *(Child Protection System)*. Ao tratar sobre o CPS, Caiado e Caiado (2018, S.I.) fazem as seguintes observações:

> Ademais, com a utilização de conexões P2P em que o servidor não é mais necessário, novas ferramentas de investigação foram desenvolvidas, como o programa CPS

> (Child Protection System), o qual realiza uma identificação automática e é utilizado em 77 países. Contudo, ainda faltam soluções mais avançadas de buscas em redes P2P, especialmente ao buscar arquivos que não sejam somente aqueles já categorizados. Essa atualização é bastante relevante, tendo em vista que os predadores podem alterar os arquivos de forma que não possuam uma correspondência com bibliotecas de hash.

A utilização do CPS como ferramenta para investigação do compartilhamento de pornografia infantil também é esclarecida por Peersman *et al.* (2014, p. 124):

> *The severity of the problem has resulted in a number of solutions that can monitor such activity. Tools such as the Child Protection System (CPS) [6] and RoundUp [7], [8] are able to capture data about paedophile activity on P2P networks and identify child abuse media across different P2P protocols. However, these systems rely on matching the files shared on a network against a hash-value database of known CSA (child sex abuse) media. As a result, they are not able to identify new child abuse media that may be released on to the network. Nor are they able to detect CSA media that is not on record. Identifying such new/previously unknown media is, however, critical, because they can be indicators of recent or even ongoing child abuse. Furthermore, originators of such media can be hands-on abusers and their early detection and apprehension can safeguard their victims from further abuse.*

No combate à propagação de PI na Internet, não basta qualificar o arquivo como pornografia infanto-juvenil é preciso também encontrar os lugares onde esses arquivos estão potencialmente gravados. Contudo, a localização e categorização de arquivos dessa natureza encontra alguns obstáculos. Segundo Caiado e Caiado (2018, p. 19),

> Um estudo de 2013, que analisava tráfego de PI em conexões P2P (HURLEY *et al.*, 2013) identificou 1,8 milhões de nós de eMule (nesse caso instâncias do programa) que continham PI, sendo vários desses arquivos com as mesmas imagens de PI que já haviam sido identificadas e tiveram o seu hash categorizado por agências de forças da lei. Nesse método, encontrar arquivos de PI pelo hash e pelo nome do arquivo tem uma alta relevância, mas estes só funcionam em material já identificado. Se um arquivo for modificado, mesmo que um mínimo bit, o que é uma mudança imperceptível para um humano, este não será mais identificado pela biblioteca de hashes. Da mesma forma, não se pode assumir que todos arquivos de PI já foram categorizados em um mundo onde só há um aumento no tráfego ilegal desse material. Então, torna-se crítico analisar automaticamente todos os arquivos como possíveis arquivos de PI, e não apenas os que foram previamente categorizados.

Com o intuito de analisar a possibilidade de criação de *software* capaz de realizar varreduras na Internet em busca de conteúdo de ódio, mais especificamente aqueles voltados à propagação do racismo na Internet, foi feito um levantamento técnico com dois grupos de especialistas compostos por policiais federais com experiência nas temáticas abordadas. As características das amostras, bem como as questões utilizadas nos respectivos levantamentos, já foram descritas no item 2.3 deste trabalho.

Após a análise das respostas, procedeu-se um estudo comparativo dos resultados no âmbito dos respectivos tópicos. Inicialmente, foi feita uma síntese das respostas obtidas para cada grupo de questões. Cabe destacar que, por se tratarem de temas técnicos, as questões, ainda que respondidas de forma dissertativa, resultaram em respostas semelhantes, fato que facilitou a síntese do conteúdo. Os resultados da comparação entre as respostas são apresentados nos Quadros de 6 a 12, elencados a seguir.

Quadro 6 – Comparativo de respostas: Conexão via servidor

Especialistas em crimes de ódio na Internet	Especialistas no uso da ferramenta CPS	Resultados
Os crimes costumam chegar ao conhecimento da PF por notícia-crime de pessoa que se sinta prejudicada ou de entidades governamentais (como o MP) ou não governamentais. A atuação se dá por demanda, não havendo atuação proativa. Contudo, um especialista informa que, depois do atentado de Suzano, a PF passou a acompanhar a ação de alguns grupos na *deep web* que atuam propagando ideias racistas. Nas situações de conteúdos de ódio relacionados ao terrorismo, esse tipo de acompanhamento na *deep web* também costuma ser feito. Nesses casos, ocorre troca de informações com entidades internacionais e outras forças policiais. O compartilhamento de conteúdo racistas costuma ocorrer na Internet aberta, por conexões via servidores. Não são conhecidos *softwares* específicos para a investigação de racismo na Internet. É unânime a ideia de que softwares específicos facilitariam o acompanhamento da rede, uma vez que um analista policial sozinho não consegue monitorar toda Internet, no máximo alguns alvos. Contudo, especialistas alertam para as dificuldades em distinguir os resultados falso-positivos das situações que efetivamente caracterizam crimes de racismo na Internet. Tal dificuldade também ocorreria para separar as entidades responsáveis pela investigação, pois apenas em casos específicos o crime de ódio é investigado pela PF.	Os crimes costumam chegar ao conhecimento da PF por informações prestadas pelos familiares das vítimas, por organizações nacionais ou internacionais, por outras forças policiais, bem como pela ação proativa da PF, com o uso da ferramenta CPS no monitoramento de conteúdos compartilhados por meio de conexão P2P. O conteúdo criminoso relacionado à pornografia infantil também pode ser compartilhado via servidores. No que tange à ferramenta CPS, ela se aplica para monitorar conexões P2P, nas quais não se utiliza provedor.	Ambos relatam que o fato criminoso costuma chegar ao conhecimento da Polícia Federal por meio de informações oriundas de pessoas que se sintam ofendidas, de órgãos públicos ou instituições particulares. A principal distinção constatada é que, no caso do uso da ferramenta CPS, há uma ação proativa da PF e de outras instituições para investigação do crime de compartilhamento de mídias relacionadas à pornografia infantil. O sistema possibilita que a investigação ocorra sem necessidade de provocação. Cabe esclarecer que, em relação ao CPS, nas hipóteses em que os especialistas relataram o conhecimento do fato criminoso mediante informações oriundas de terceiros, estavam se referindo ao tipo de crime investigado pelo CPS (propagação de pornografia infanto-juvenil) e não à ferramenta em si, pois ficou evidenciado que esta age exclusivamente realizando varreduras em redes de comunicação P2P. Nos casos de crimes de ódio, não há uma ferramenta específica para varredura da rede. Contudo, esses crimes têm um âmbito de atuação muito amplo, não sendo eficiente um monitoramento apenas em redes P2P. Outra distinção é que neles a propagação por textos tem uma incidência bem maior que a por imagens.

Fonte: Elaborado pela autora (2019).

Quadro 7 - Comparativo de respostas: Redes sociais

Especialistas em crimes de ódio na Internet	Especialistas no uso da ferramenta CPS	Resultados
É comum o uso de redes sociais. A mais usada é o Facebook, seguida pelo Twitter e Instagram. As mídias sociais como Whatsapp e Telegram também são muitos utilizadas. Especialistas relatam baixo comprometimento das empresas detentoras das redes sociais em colaborar com as investigações. Esclarecem ainda que, como a maioria delas é sediada nos EUA, e lá a legislação defende o discurso livre, os detentores das redes não costumam cooperar. Em algumas ocasiões, um ofício encaminhado na qualidade de autoridade policial não é suficiente para obter informações sobre um perfil que faz incitação ao crime de ódio; muitas vezes é preciso ordem judicial. No caso dos crimes de ódio, esses detentores são menos colaborativos, por exemplo, que nos casos de pornografia infantil. Entre as principais dificuldades encontradas para a identificação dos autores dos crimes, estão: na *surface web*, costumam recorrer a *proxy*, VPN, perfil falso ou recursos para ocultar o IP e dificultar sua identificação. Nos casos da *deep web* e *dark web,* há anonimização do IP. Ocorrem ainda dificuldades na colaboração por parte das empresas por onde os conteúdos de ódio são propagados (Twitter, Telegram, etc.).	No CPS, não há monitoramento de redes sociais. Conforme um dos especialistas descreve, "A ferramenta CPS não tem recursos para produzir investigações em redes sociais. Seu objetivo é monitorar redes P2P, cuja característica peculiar é viabilizar o compartilhamento direto de arquivos (textos, imagens, áudios e vídeos) entre os computadores dos usuários desse tipo de software, sem a existência de um servidor central".	No caso da propagação de conteúdo racista na Internet, é comum a utilização de redes e mídias sociais. No CPS, as redes sociais não são acompanhadas, pois a ferramenta possibilita apenas o monitoramento em conexões P2P. Em relação ao racismo, apesar de ser frequente a sua prática em redes sociais, as empresas responsáveis não costumam colaborar em virtude de especificidades nas legislações dos países onde suas sedes estão situadas.

Fonte: Elaborado pela autora (2019).

Quadro 8 – Comparativo de respostas: Identificação de IPs

Especialistas em crimes de ódio na Internet	Especialistas no uso da ferramenta CPS	Resultados
Mediante pedido ao provedor pela via judicial. Na *deep web*, há uso de técnicas especiais de investigação, como infiltração e técnicas de engenharia social. Contudo, a descoberta do IP é bem mais difícil. Não são usados IPs previamente catalogados na investigação. Entre os óbices para tal uso está o fato de, no Brasil, o IP ser dinâmico – a cada acesso é atribuído ao usuário um IP diferente. No Brasil, a quantidade de IPs é insuficiente em comparação com o número de usuários. Assim, usa-se o IP, a data, a hora e fuso para identificar o usuário. Segundo um especialista, devido ao aumento da demanda e a escassez de IPs, tem se usado o mesmo IP, com data, hora e fuso idênticos, identificando o usuário pela atribuição de código denominado "porta de origem".	A própria ferramenta captura a conexão da pessoa que está compartilhando arquivo. Junto com arquivo compartilhado vão todos os dados cadastrais do usuário (nome da máquina, o IP com o qual o usuário está conectado naquele momento e outras informações) anexas ao pedaço do arquivo que está sendo encaminhado – ou seja, vai um bloco de arquivos, no qual a primeira parte é a identificação do usuário que está encaminhando. Ao baixar e instalar um software P2P, o usuário do computador ou smartphone concorda em compartilhar (abrir) uma pasta com os outros usuários do programa, assim todos os arquivos contidos nessa pasta (ainda que parciais) podem ser copiados (ou baixados) livremente pelos outros usuários do aplicativo.	No caso dos dados fornecidos pela ferramenta CPS, ao selecionar um arquivo suspeito o IP do usuário é identificado junto com o arquivo. Nos casos dos crimes de ódio propagados pela Internet, que frequentemente se dão por postagens em redes sociais, é necessário solicitar o IP do usuário à rede onde se deu a publicação. Os especialistas relatam como dificuldades enfrentadas nas investigações do racismo na Internet: morosidade das empresas onde as postagens ocorrem em prestar informações, óbices burocráticos, como a falta de representação de algumas empresas no Brasil, diferenças entre a legislação brasileira e a do país onde estão sediadas e questões técnicas, como IPs dinâmicos ou programas para ocultá-los.

Fonte: Elaborado pela autora (2019).

Quadro 9 – Comparativo de respostas: Compartilhamento P2P

Especialistas em crimes de ódio na Internet	Especialistas no uso da ferramenta CPS	Resultados
É possível, porém não se tem conhecimento da casuística nesse sentido e não se faz um monitoramento P2P para crimes de ódio.	O objetivo do CPS é justamente a varredura em conexões ponto-a-ponto (P2P) de conteúdo previamente identificado como pornografia infantil.	No CPS, o compartilhamento do conteúdo criminoso ocorre por conexões P2P. Nos crimes de ódio, essa prática não é comum. Os especialistas relatam que seria tecnicamente possível a propagação de conteúdos racistas pelo compartilhamento de imagens via conexões P2P, mas não há conhecimento de casuística neste sentido.

Fonte: Elaborado pela autora (2019).

Quadro 10 – Comparativo de respostas: *Stop words*

Especialistas em crimes de ódio na Internet	Especialistas no uso da ferramenta CPS	Resultados
No caso dos crimes de ódio, a maioria do conteúdo é propagada por texto, mas pode ocorrer também por imagens (ex. charges racistas). Para um monitoramento preventivo, haveria grande dificuldade em virtude de resultados "falso-positivos", decorrentes de fatores como expressões do vocabulário cotidiano, piadas e situações ambíguas, na qual a mesma palavra pode possuir ou não o dolo de propagar ódio. Alguns especialistas relatam que outros tipos penais (ex.: injúria racial) se dão pelo uso de expressões racistas, o que pode gerar confusão em uma eventual busca por palavras-chave.	Em regra, os crimes relacionados ao compartilhamento de material contendo pornografia infantil se dá pelo compartilhamento de mídias, ou seja, imagens e vídeos. Contudo, pode ser que, juntamente com esse conteúdo, seja compartilhado algum texto referente às práticas ilícitas, como por exemplo um manual ensinando como abusar de crianças. O CPS disponibiliza opção de busca por palavras-chave. Ex.: termos como boy, girl ou ainda referências a idade da vítima como 3yo (3 years old = 3 anos de idade).	Tanto no crime de racismo quanto nas investigações que utilizam o sistema CPS, há possibilidade de busca por palavras-chave, pois a conduta criminosa também pode se dar por meio de textos. O CPS apresenta uma funcionalidade de busca por palavras-chave. No racismo, não se costuma fazer um monitoramento preventivo da rede. Especialistas apontam a imprecisão dos termos que configuram o racismo na Internet e a semelhança com outros tipos penais como óbices que podem resultar em resultados falso-positivos.

Fonte: Elaborado pela autora (2019).

Quadro 11 – Comparativo de respostas: Compartilhamento de imagens e vídeos

Especialistas em crimes de ódio na Internet	Especialistas no uso da ferramenta CPS	Resultados
É possível que o conteúdo de ódio seja compartilhado por imagens, sendo possível a busca inclusive por palavras chave, pois pode haver textos sobrepostos às imagens. Atualmente não existe um monitoramento preventivo via varreduras na Internet em busca de conteúdos racistas. Assim, apesar de possível, não se costuma aplicar palavras-chave na investigação de racismo na Internet.	A função central do CPS é a análise de mídias (imagens e vídeos) compartilhados via conexões P2P. A ferramenta CPS possui opção de busca por palavras-chave. Ela utiliza os nomes dos arquivos para apontar eventuais imagens e vídeos com conteúdo suspeito de pornografia infanto-juvenil, para que possam ser selecionadas e melhor analisadas pelos policiais durante a investigação.	As imagens podem ser utilizadas para cometer crimes de racismo na Internet, bem como os crimes investigados com a ajuda do CPS, relacionados à pornografia infanto-juvenil. As imagens podem ser buscadas pelo respectivo *hash* ou por palavras-chave que lhes podem ser sobrepostas.

Fonte: Elaborado pela autora (2019).

Quadro 12 – Comparativo de respostas: Uso de bibliotecas de *hash* como comparativos

Especialistas em crimes de ódio na Internet	Especialistas no uso da ferramenta CPS	Resultados
No caso do racismo na Internet, não são utilizados códigos *hash* previamente identificados e catalogados como parâmetros de busca na investigação, por que ainda não há um banco de dados de *hashes* já rastreados e catalogados para tal finalidade. Também não há *software* para uma varredura na Internet com essa funcionalidade aplicada especificamente a crimes de ódio.	No CPS é comum a utilização do *hash* como parâmetro de busca. A partir de um catálogo desses códigos de identificação única *(hash)* de arquivos, conhecidos pela polícia, graças a investigações anteriores, podem ser identificados nas pastas compartilhadas pelos usuários dos aplicativos P2P.	A busca por *hash* exige conhecimento prévio da mídia e de sua identificação. O CPS possui um banco de dados de mídias e respectivos códigos *hash* catalogados. Esta funcionalidade não seria possível para os casos de crimes de ódio pela inexistência de uma base de dados específica.

Fonte: Elaborado pela autora (2019).

Ao analisar o CPS, foi possível observar que o uso de um software pode contribuir de forma muito positiva para as investigações policiais. Entretanto, verificou-se que a ferramenta tem características e funcionalidades específicas que garantem a eficiência em um campo restrito de atuação – como, por exemplo, nas redes P2P, onde predomina o compartilhamento de imagens e vídeos.

Tanto em relação ao racismo quanto aos casos de propagação de pornografia infantil na Internet, os especialistas relatam que o fato criminoso costuma chegar ao conhecimento da Polícia Federal por meio de informações oriundas de pessoas que se sintam prejudicadas, de órgãos públicos ou instituições particulares. A atuação policial mediante demanda externa é comum, pois é por meio de notícias-crime que as polícias costumam tomar conhecimento de atos ilícitos.

O CPS destaca-se por permitir uma atuação proativa do investigador, que não precisa esperar que alguém lhe informe sobre determinado fato. Assim, ele utiliza a ferramenta para vasculhar as redes P2P em busca de material pornográfico criminoso.

Nas hipóteses de crime de ódio na Internet, não há uma ferramenta específica para varredura em redes P2P. Nessa modalidade de crime, o âmbito de incidência é muito amplo, predominando sua ocorrência na Internet aberta, em conexões via servidores. Diante de tal contexto, os especialistas são unânimes em afirmar que a existência de *softwares* específicos facilitaria a mineração de conteúdos racistas na Internet, pois um analista policial sozinho não consegue monitorar toda a rede.

No que tange ao racismo na Internet, especialistas alertam que frequentemente a busca por palavras-chave resultaria em resultados falso-positivos para racismo, uma vez que as expressões discriminatórias são usadas em outros tipos de ilícitos, como a injúria qualificada. Em tais situações, seria necessário verificar as entidades responsáveis pela investigação, pois o discurso de ódio deve ser investigado pela PF apenas nos casos em que se configure racismo.

Observa-se ainda que o ambiente virtual onde ocorrem os crimes de racismo na Internet não corresponde aos casos onde se aplica o CPS. Embora todos os especialistas afirmem que existe a possibilidade de divulgação de conteúdos racistas via conexão P2P, eles também são unânimes ao dizer que desconhecem casuísticas quanto a tal modo de atuação. No caso do racismo, os especialistas apontam para uma maior propagação de conteúdo dessa natureza via redes sociais, entendendo que normalmente há um dolo de ofender alguém ou propagar uma ideia discriminatória para o maior número possível de pessoas.

Especialistas apontam ainda para o uso da *deep web* e *dark web* para propagação de conteúdo de ódio. Tais situações, contudo, seriam menos comuns e praticadas por indivíduos com maior conhecimento de tecnologia e preocupação em evitar investigações policiais. Alguns especialistas alertam para o fato de que conteúdos de ódio propagados na *deep web* podem não apenas configurar crime de racismo na Internet, mas estarem também ligados à propagação de ideologias partilhadas por grupos terroristas.

No que tange à *deep web*, um dos especialistas ressaltou que o fato conhecido como "Massacre de Suzano" utilizou informações de um site hospedado na *deep web* denominado *Dogolachan*. O massacre a que o especialista se referiu ocorreu no dia 13 de março de 2019, ocasião em que dois ex-alunos invadiram a escola Professor Raul Brasil e mataram 5 alunos e 2 funcionárias[12].

Cabe destacar que a criação do *Dogolachan* é atribuída a Marcelo Valle Silveira Mello, investigado pela Polícia Federal nas Operações Bravata e Intolerância e acusado de diversos crimes, entre os quais o crime de racismo na Internet (20, § 2º da Lei nº 7.716/1989). Conforme pesquisa realizada no site do STJ, Marcelo Valle teve seu pedido de *habeas corpus* negado em 09 de agosto de 2019 e ainda estaria preso.

> HABEAS CORPUS Nº 525.712 - PR (2019/0232203-4)
> DECISÃO
> Trata-se de habeas corpus substitutivo de recurso ordinário, com pedido liminar, impetrado em favor de MARCELO VALLE SILVEIRA MELLO, em que se aponta como autoridade coatora o Tribunal Regional Federal da 4ª Região.
> Na origem, constata-se que o paciente encontra-se preso desde 10/5/2018, em execução provisória no complexo Médico-Penal do Paraná/PR, cumprindo penas de 5 meses e 10 dias de detenção e 41 anos, 1 mês e 10 dias de reclusão, no regime inicial fechado, e pena de multa de 678 dias-multa, pela prática dos crimes previstos nos arts. 286, 288, 344, todos do Código Penal, 241-A e 241-E da Lei n. 8.069/1990, 20, § 2º, da Lei n. 7.716/1989 e 2º, § 1º, I, da Lei n. 13.260/2016, todos em concurso material. (BRASIL, 2016)

Acerca da investigação do racismo na Internet, a varredura na *surface web* encontra obstáculos ainda em questões burocráticas relacionadas à morosidade no fornecimento dos IPs pelos provedores e sites onde ocorrem as publicações. Outras dificuldades apontadas por especialistas são o uso de programas e recursos para ocultar o IP e o fato de, no Brasil, os IPs

[12] O fato foi amplamente divulgado pela imprensa, podendo-se citar as seguintes matérias: Disponível em: https://g1.globo.com/pr/parana/noticia/2018/12/19/homem-e-condenado-a-41-anos-de-prisao-por-crimes-como-racismo-terrorismo-e-divulgacao-de-pedofilia-na-Internet.ghtml. Acesso em: 23 nov. 2019. Disponível em: https://www.buzzfeed.com/br/tatianafarah/dogolachan-forum-dark-web-massacre-suzano. Acesso em: 23 nov. 2019.

serem dinâmicos, sendo atribuídos IPs aleatórios a cada acesso. Um dos especialistas ressalta que, devido à escassez de IPs, é comum que ocorra o seu compartilhamento por mais de um usuário simultaneamente.

Há ainda os casos de compartilhamento de conteúdo e publicações feitas via *deep* e *dark weeb*, ambientes nos quais os IPs não são rastreáveis. Em tais situações, resta recorrer ao o uso de estratégias especiais de investigação, como infiltração policial e técnicas de engenharia social. Contudo, a descoberta do IP é bem mais difícil nesses casos.

Observa-se que, no caso do CPS, o âmbito de ação da ferramenta é mais restrito, posto que atua fazendo varreduras exclusivamente em conteúdos compartilhados via conexões P2P. Em relação ao racismo, os especialistas relatam o desconhecimento de casos em que o conteúdo racista seja compartilhado por esse tipo de conexão. Ressaltam ainda que, neste crime, ocorre predominância de propagação de conteúdo via texto e que o uso de imagens seria exceção. Desse modo, entendem que o universo de conteúdos racistas passíveis de serem descobertos com auxílio de uma ferramenta idêntica ao CPS provavelmente seria muito pequeno.

Conforme apurado nos levantamentos técnicos, é muito comum o uso de redes sociais na propagação de conteúdo racista na Rede Mundial de Computadores. Segundo os especialistas, a rede social mais usada é o Facebook, mas também são utilizados o Twitter e o Instagram, bem como mídias sociais como Whatsapp e Telegram. Em relação a essa forma de propagação, os especialistas relatam que as maiores dificuldades encontradas para identificação dos responsáveis pelas postagens é o baixo comprometimento das empresas detentoras das redes sociais em colaborar com as investigações.

Em relação à cooperação das empresas detentoras das redes sociais, um dos especialistas ressalta que a maioria delas tem sede nos EUA, onde a legislação defende o discurso livre, sendo essa a razão pela qual não costumam cooperar espontaneamente. Esclarece ainda que, com frequência, um ofício encaminhado na qualidade de autoridade policial não é suficiente para obter informações sobre um perfil que faça incitação ao crime de ódio, sendo necessária ordem judicial. Para outros crimes, como pornografia infantil e terrorismo, a legislação internacional é mais favorável à cooperação com a investigação, que se dá de forma mais ágil e menos burocrática.

Nesse cenário, destaca-se que as principais dificuldades constatadas na identificação dos autores dos crimes na Internet são: na *surface web*, o fato de que os criminosos costumam recorrer a *proxy*, VPN, perfil falso ou recursos para ocultar o IP e dificultar sua identificação e, no caso da *deep* e *dark web*, a anonimização do IP. Há ainda as dificuldades de colaboração por

parte das empresas onde os conteúdos de ódio são propagados, como Twitter ou Telegram, em fornecerem o IP dos responsáveis pelas postagens.

No caso dos crimes de ódio, seria mais eficiente efetuar busca, nas redes sociais, Internet aberta, *deep* e *dark web*, por expressões e termos racistas. Contudo, tal varredura demandaria funcionalidades distintas das utilizadas no CPS e enfrentaria algumas dificuldades para ser implementada. Um dos obstáculos seria o fato de que a busca por palavras-chave e expressões de ódio não resultaria apenas em casos de racismo, mas também outros tipos penais que se concretizam pelo uso de expressões semelhantes. Mesmo obras literárias, textos jornalísticos, históricos, artísticos, enfim, qualquer situação que abordasse o tema do racismo ou da discriminação seria passível de ser confundida pelo *software* com a propagação de conteúdo racista, dificultando a identificação dos crimes reais.

A partir dos levantamentos técnicos, constatou-se que a elaboração de uma ferramenta para rastreamento de conteúdo de ódio na Internet passa por obstáculos diversos. A mesma ferramenta dificilmente poderia ser aplicada para monitorar diversos tipos de ambientes como *surface web*, *deep web*, *dark web*, conexões via P2P e mídias sociais. Seria necessário atentar para a especificidade de cada situação a fim de se pensar em soluções compatíveis.

Com o intuito de se analisar a aplicabilidade de uma ferramenta de varredura para busca de conteúdos racistas em função do local da publicação, foi elaborado o Quadro 13.

Quadro 13 – Comparativo: Ambiente versus ferramenta de varredura

	SURFACE WEB	***DEEP WEB / DARK WEB***	**CONEXÕES VIA P2P**	**MÍDIAS SOCIAIS (WhatsApp e Telegran)**
ADEQUADA			X	
INADEQUADA				X
ADAPTÁVEL	X	X		

Fonte: Elaborado pela autora (2019).

Os especialistas ressaltam a utilidade do uso de ferramentas de busca. Contudo, também destacam que a eficiência destas variam em função do ambiente no qual a varredura é feita. Em relação às mídias sociais, a varredura se mostra inadequada devido ao uso de criptografia ponta-a-ponta em relação às mensagens que nela circulam. Assim, somente os usuários envolvidos na conversa têm acesso às mensagens. Já no caso das conexões P2P, o uso

de ferramentas de varredura se mostra adequado; contudo, conforme apurado nos levantamentos técnicos, tal ambiente não costuma ser utilizado na prática de racismo.

Em relação à *surface web*, *deep web* e *dark web*, o uso de softwares para varredura é possível, porém seriam necessárias adaptações quanto às estratégias usadas na mineração. Na *surface web*, seria relevante delimitar o local de busca com uso de ferramentas para restringi-la a bases específicas, como, por exemplo, uma busca no Facebook. Na *deep* e *dark web*, o mais indicado seria o acompanhamento de sites já conhecidos por propagar o discurso de ódio, como o *Dogolachan*, ou mesmo os relacionados a grupos ligados a práticas de terrorismo.

Tanto na *surface web* como na *deep web* e *dark web,* seria relevante o uso de técnicas de mineração de texto para separar, entre as diversas palavras e expressões relacionadas ao discurso de ódio, aquelas situações com maior probabilidade de caracterização do crime de racismo. Tal necessidade decorre de existirem outras situações relacionadas a expressões de ódio, mas que não configuram crime de racismo.

Pela análise dos levantamentos técnicos, observa-se que as características peculiares que diferenciam o racismo na Internet de outras modalidades de crimes cibernéticos são elementos passíveis de dificultar sua investigação. Assim, ainda que exista a possibilidade de monitorar a Rede Mundial de Computadores por meio de palavras ou argumentos de texto pré-definidos, este procedimento encontraria óbices em relação aos diversos tipos penais que podem ser confundidos com situações de racismo, a exemplo das injúrias raciais e dos casos de *bullying* com argumentos racistas.

Textos jornalísticos, artigos científicos e obras literárias sobre racismo e situações de ódio poderiam conter expressões e palavras passíveis de serem rastreadas, resultando em um resultado falso-positivo. Tais fatores dificultam a utilização da busca por palavras-chave como ferramenta de investigação de crimes por meio de varreduras, seja na *deep web* ou na *surface web*. Mesmo que ferramentas de mineração sejam desenvolvidas e utilizadas, elas serão relevantes para reduzir o universo de análise a ser investigado; todavia, nenhuma ferramenta ainda é capaz de dispensar o olhar do policial acerca das características e as circunstâncias em que se deu a ofensa, a fim de avaliar se caracteriza ato ilícito e em qual tipo penal este se enquadraria.

4 RESULTADOS

4.1 DADOS SOBRE A ATUAÇÃO DA POLÍCIA FEDERAL NO COMBATE AOS CRIMES DE ÓDIO

Em 30 de novembro de 2012, a Lei nº 12.735 determinou que os órgãos da polícia judiciária deveriam estruturar setores e equipes especializadas no combate aos crimes cibernéticos. Contudo, a Polícia Federal já conta com um setor especializado desde 2003, quando da criação do Serviço de Repressão a Crimes Cibernéticos (SRCC) – inicialmente como Unidade de Repressão a Crimes Cibernéticos (URCC). Tal serviço é subordinado à Coordenação-Geral de Polícia Fazendária (CGPFAZ) que, por sua vez, é subordinada à Diretoria de Investigação e Combate ao Crime Organizado (DICOR). O SRCC já coordenou diversas operações policiais, notadamente nas áreas de fraude bancária eletrônica, pornografia infantil, venda de medicamentos pela Internet e pirataria.

Quando da transformação da URCC foi em Serviço (SRCC), os grupos regionais passaram a se chamar a Grupos de Repressão a Crimes Cibernéticos (GRCC). Houve ainda a criação de novos grupos desta espécie, os quais estão presentes em mais da metade dos estados da federação. Além dos trabalhos de investigação, o SRCC também desenvolve projetos, com o objetivo de aparelhar os setores e capacitar seus servidores.

A Polícia Federal conta ainda com a Unidade de Repressão aos Crimes de Ódio e Pornografia Infantil na Internet (URCOP), que é vinculada ao SRCC. A URCOP é responsável pela orientação, coordenação, fomento e acompanhamento de operações policiais relativas a crimes de disseminação e difusão de materiais de pornografia infanto-juvenil e crimes de ódio na Internet.

Em consultas realizadas nas bases de dados da Polícia Federal (acesso em 10 de janeiro de 2020), constatou-se que existem 230 inquéritos em andamento pela instituição para apuração do crime de racismo na Internet, tendo como parâmetro de pesquisa a Lei nº 7.716, art. 20, na base *bi.pf.gov.br*. Constatou-se ainda que, para o mesmo parâmetro de pesquisa e com mesma data de acesso, constam 1.145 inquéritos já relatados (concluídos) pela PF com base no citado dispositivo legal.

Com o intuito de obter uma visão panorâmica sobre os trabalhos já realizados pela Polícia Federal no combate aos crimes de ódio, precedeu-se a uma busca na agência de

notícias[13] mantida no *site* da PF pelos termos "ódio" e "racismo". A agência de notícias é um canal voltado a informar o público em geral sobre os trabalhos realizados pela Polícia Federal. Constatou-se que, em busca pelo termo "ódio", foram encontrados 17 resultados e pelo termo "racismo" foram localizados 6 resultados.

Com base em pesquisas complementares, foram encontrados ainda registros sobre a "Operação Intolerância", ocorrida em 2012. A operação não estava indexada pelos termos *ódio* ou *racismo* no *site* da PF, sendo identificada por meio de buscas em fontes abertas (Google) pelos termos "Polícia Federal" e "crimes de ódio", seguida de pesquisa posterior no endereço *http://www.pf.gov.br/agencia/noticias* pelo termo "intolerância", na aba de buscas, sendo localizados 4 resultados.

Após a leitura de todos os resultados encontrados, foram relacionadas as notícias abaixo, referentes a ações da Polícia Federal no combate aos crimes de ódio.

[13] Disponível em: http://www.pf.gov.br/agencia/noticias. Acesso em: 13 out. 2019.

Quadro 14 – Notícias sobre ações da PF relacionadas ao combate a crimes de ódio na Internet

Data da notícia	Conteúdo	Link
26/04/2016	**PF combate produção e divulgação de pornografia infantil e crimes de ódio** Porto Alegre/RS – A Polícia Federal deflagrou nesta manhã (26/04) a Operação Jizô, para reprimir crimes de divulgação de pornografia infantil e crimes de ódio praticados através da Internet, no Rio Grande do Sul. Policiais federais cumprem três mandados de busca e apreensão: um em Porto Alegre; um em Novo Hamburgo; e um em São Leopoldo. A ação da PF tem por base quatro investigações. O caso de crime de ódio foi identificado na Bahia e apontou para publicações feitas por um jovem de Porto Alegre. De acordo com o que foi descoberto, ele publicou textos de cunho ofensivo e discriminatório, principalmente contra nordestinos. Já a segunda investigação é relacionada a um caso que envolve produção de material de conteúdo pornográfico infantil. Ele chegou à PF por denúncia de uma adolescente chantageada por um funcionário de uma empresa de eventos. A menina gravou e enviou um vídeo com conteúdo erótico para ganhar ingressos para uma festa promovida pela empresa. Os outros dois casos tiveram início por denúncias da Guarda Civil da Espanha, em que um endereço IP de Novo Hamburgo teria divulgado grande quantidade de material de pornografia infantil; e por informações recebidas de uma organização americana – National Center for Missing & Exploited Children (NCMEC), que identificou grande quantidade de conteúdo pornográfico infantil armazenado a partir de um endereço IP de São Leopoldo. O nome da Operação: Jizô ou Jizou é uma divindade budista referida como guardiã das crianças.	http://www.pf.gov.br/agencia/noticias/2016/04/pf-combate-producao-e-divulgacao-de-pornografia-infantil-e-crimes-de-odio. Acesso em: 21 out. 2019.
05/02/2013	**Dia Internacional da Internet Segura: PF realiza campanha** São Luís/MA - A Polícia Federal desencadeou na manhã de hoje, 5, uma ação policial em referência ao Dia Internacional da Internet Segura. O objetivo do trabalho é promover o uso responsável e seguro da Rede Mundial de Computadores e, principalmente, a divulgar as ações de proteção de crianças e adolescentes usuários da Internet. Policiais Federais lotados em São Luís fizeram levantamentos dos locais de existência de lan houses e em alguns estabelecimentos previamente selecionados estão distribuindo cartazes e orientando os responsáveis a cadastrarem os usuários dos serviços de Internet disponibilizados no local. A equipe policial, além de distribuir o material de campanha, também tratou de conscientizar os usuários quanto ao uso seguro da Internet e da necessária colaboração da sociedade civil nas ações de combate aos crimes de ódio e de pornografia infantil na Internet.	http://www.pf.gov.br/agencia/noticias/2013/02/dia-internacional-da-internet-segura-pf-realiza-campanha. Acesso em: 15 set. 2019.

	Este dia vem sendo comemorado anualmente desde 2007 e neste ano tem como tema os Direitos e Deveres online. A participação da Polícia Federal na campanha está prevista nas medidas preventivas, estando diretamente relacionada às suas atribuições no combate aos crimes de ódio e exploração sexual de crianças e adolescentes na Internet, delitos que importam em grave violação à dignidade da pessoa humana. A Campanha foi desencadeada uniformemente e possui escala nacional.	
17/09/2013	**PF realiza Operação Rede Limpa II para combater crimes cibernéticos** Recife/PE – A Polícia Federal deflagrou ontem (16/9) a Operação Rede Limpa II, com o objetivo de combater crimes de ódios, disseminados por meio de imagens que fazem referência ao nazismo, bem como vídeos e imagens de pornografia infantil, compartilhados na Rede Mundial de Computadores. A PF deu cumprimento a quatro mandados de busca e apreensão, expedidos pela 4ª e 13ª Vara Criminal da Justiça Federal em Pernambuco no intuito de combater os crimes de Pornografia Infantil e Neonazismo na Internet. A ação de ontem é resultado de investigações produzidas através três inquéritos policiais. Nos locais de busca, foram apreendidos nove discos rígidos, três notebooks e um aparelho de compartilhamento de sinal de Internet. Todo o material arrecadado passará por perícia técnica para averiguar o conteúdo de suas informações e, caso seja detectado algum vídeo, foto ou material pornográfico envolvendo criança e adolescente e apologia ao neonazismo, os responsáveis poderão ser indiciados e responsabilizados pela prática de tais crimes	http://www.pf.gov.br/agencia/noticias/2013/09/pf-realiza-operacao-rede-limpa-ii-para-combater-crimes-ciberneticos. Acesso em: 18 out. 2019.
29/01/2013	**PF no RS realiza ações no Dia Internacional da Internet Segura** Porto Alegre/RS - A Polícia Federal realizou terça-feira (05/02), ação preventiva em prol do Dia Internacional da Internet Segura. O tema deste ano é "Direitos e deveres on-line". Na ação, foram visitadas lan houses e distribuídos materiais promocionais da campanha, cartilhas para navegação segura e afixação de cartazes. Os proprietários dos estabelecimentos foram orientados acerca da necessidade de cadastramento dos usuários dos serviços de Internet disponibilizados no local, além de conscientização da necessidade de colaboração da sociedade civil em ações de combate aos crimes de ódio e de pornografia infantil na web. O material foi elaborado pela equipe da SaferNet Brasil com o propósito de contribuir para a promoção da utilização da Internet de forma mais segura e ética. Dentre os principais cuidados que os usuários devem tomar ao navegar na Rede Mundial de Computadores, estão medidas como: sempre fazer logoff e evitar gravar senhas em computadores compartilhados, excluir definitivamente	http://www.pf.gov.br/agencia/noticias/2013/02/pf-no-rs-realiza-acoes-no-dia-internacional-da-internet-segura. Acesso em: 19 out. 2019.

	da lixeira ao baixar fotos quando em lan houses, e orientar as crianças e adolescentes sobre os perigos das redes de relacionamento. Atualmente, existem redes sociais específicas para esse público. No ano passado, somente na Superintendência da Polícia Federal em Porto Alegre, foram instaurados 30 inquéritos para apurar a divulgação de arquivos contendo imagens de pornografia infantil na internet.	
14/08/2013	**PF e Safernet realizarão oficina de prevenção para uso seguro da internet** A SaferNet Brasil e a Polícia Federal, por meio do Grupo Especial de Combate aos Crimes de Ódio e à Pornografia Infantil na Internet (GECOP), promoverão oficina sobre o uso seguro da Internet, dia 15 deste mês, no Colégio Olimpo, em Brasília. O evento tem como objetivo orientar crianças e adolescentes sobre como utilizar a Rede Mundial de Computadores com segurança e responsabilidade. A oficina integra um conjunto de ações realizadas entre a SaferNet e a PF para prevenção à prática dos crimes e violações a Direitos Humanos através da web. Em sete anos de trabalho, foram recebidas pela Central Nacional de Denúncias de Crimes Cibernéticos (CND) 3.173.061 denúncias anônimas envolvendo conteúdos na web suspostamente relacionados a pornografia infanto-juvenil, racismo, neonazismo, homofobia e tráfico de pessoas. São frutos ainda da parceria entre as duas instituições ações preventivas e educativas em lan houses. Na abordagem, os proprietários dos estabelecimentos são orientados acerca das formas de prevenir os crimes cibernéticos, além de conscientização da necessidade de colaboração na educação dos usuários sobre o uso ético e responsável da Internet. Em todas as atividades de cooperação são distribuídos gratuitamente cartilhas, cartazes e kits pedagógicos para que as escolas e lans possam multiplicar as dicas de segurança no cotidiano. Somente nos anos de 2012 e 2013, foram instaurados pela Polícia Federal mais de 1500 inquéritos para apuração de disseminação de pornografia infantil na internet. As ações repressivas do órgão resultaram, também nos anos de 2012 e 2013, na prisão em flagrante de 100 pessoas (41 somente em 2013) pela disseminação de pornografia infantil na internet.	http://www.pf.gov.br/agencia/noticias/2013/08/pf-e-safernet-realizarao-oficina-de-prevencao-para-uso-seguro-da-internet. Acesso em: 22 set. 2019.
30/01/2014	**PF deflagra Operação Net Control contra pornografia infantil e racismo** Recife/PE - A Polícia Federal deflagrou, hoje (31/1), em Pernambuco, a Operação Net Control. O objetivo é cumprir quatro mandados de busca e apreensão para combater crimes de pornografia infantil e atos de racismo veiculados e compartilhados na Rede Mundial de Computadores. Os responsáveis pela divulgação de pornografia infantil usaram programas de compartilhamento de arquivos para trocarem fotos e vídeos com o conteúdo ilegal. O indivíduo investigado por racismo fez comentários ofensivos aos negros no site de uma revista de circulação nacional.	http://www.pf.gov.br/agencia/noticias/2014/01/pf-deflagra-operacao-net-control-contra-pornografia-infantil-e-racismo. Acesso em: 29 set. 2019.

	Nos locais de busca foram arrecadados discos rígidos, notebooks, pen drives, e mídias de cds. Os peritos criminais federais, utilizando de tecnologia e sistemas avançados de busca por imagens e vídeos suspeitos, não conseguiram detectar tais reproduções nas máquinas analisadas no local da ocorrência. Entretanto, todo o material passará por perícia técnica profunda para averiguar o conteúdo de suas informações. Caso seja detectado algum conteúdo pornográfico infantil ou racista, os responsáveis poderão ser indiciados pelos crimes contidos nos artigos 241-A e 241-B da Lei 8.069/90-ECA-Estatuto da Criança e do Adolescente e do Artigo 20 § 2º da Lei 7.716/89.	
10/05/2018	**Polícia Federal combate crimes praticados via internet** Curitiba/PR – A Polícia Federal deflagrou nesta manhã (10/5) a *Operação Bravata, que tem por objetivo combater os crimes de racismo, ameaça e incitação ao crime, praticados via Internet. Cerca de 60 policiais federais participam da deflagração da operação e cumprem um mandado de prisão preventiva e oito mandados de busca e apreensão, nas cidades de Curitiba/PR, Rio de Janeiro/RJ, São Paulo/SP, Recife/PE, Santa Maria/RS e Vila Velha/ES. A investigação teve início com base em fatos que ocorreram após a deflagração da Operação Intolerância, no ano de 2012. Foi verificado que outros indivíduos, aparentemente associados àqueles que haviam sido presos na operação, continuaram a praticar crimes por meio dos mesmos sites e fóruns na Internet que costumavam utilizar, tendo inclusive criado novos ambientes virtuais para a prática desses delitos. Os indivíduos investigados vão responder pelos crimes de associação criminosa, ameaça, racismo e incitação ao crime, tendo em vista que nos sites e fóruns mantidos na Internet incentivam a prática de diversos crimes, como o estupro e o assassinato de mulheres e negros. Há evidências de que os investigados também foram responsáveis por ameaças de bomba encaminhadas a diversas universidades do país. A soma das penas dos crimes investigados pode chegar a 39 anos de prisão. O preso será conduzido à Superintendência da Polícia Federal em Curitiba/PR onde permanecerá à disposição da Justiça. Será concedida entrevista coletiva, hoje, às 10h, no auditório da sede da Polícia Federal em Curitiba/PR.	http://www.pf.gov.br/agencia/noticias/2018/05/policia-federal-combate-crimes-praticados-via-internet. Acesso em: 18 ago. 2019.
22/03/2012	**Operação Intolerância prende responsáveis pelo blog Silvio Koerich** Curitiba/PR - A Polícia Federal em Curitiba deflagrou hoje, 22 de março, a "OPERAÇÃO INTOLERÂNCIA" que identificou os responsáveis pelas postagens criminosas encontradas no site silviokoerich.org. Foram cumpridos dois mandados de prisão preventiva contra E.E.R. e M.V.S.M., moradores de Curitiba e Brasília, respectivamente.	http://www.pf.gov.br/agencia/noticias/2012/marco/operacao-intolerancia-prende-responsaveis-pelo-blog-silvio-koerich201d. Acesso em: 18 ago. 2019.

	As investigações iniciaram-se a partir de inúmeras denúncias relacionadas ao conteúdo discriminatório do referido site. Até o dia 14 de março deste ano foram registradas 69.729 denúncias a respeito do conteúdo criminoso do site investigado. As mensagens faziam apologia à violência, sobretudo contra mulheres, negros, homossexuais, nordestinos e judeus, além da incitação do abuso sexual de menores. Os criminosos também apoiaram o massacre de crianças praticado por um atirador em uma escola na cidade do Rio de Janeiro em 2011. O nome "Sílvio Koerich" foi apropriado indevidamente por E.E.R. em represália a uma terceira pessoa que rejeitou as declarações preconceituosas, homofóbicas e intolerantes postadas em um fórum de debates feminista. Além dos mandados de prisão preventiva, a Justiça Federal autorizou o cumprimento de mandados de busca e apreensão nas residências e locais de trabalho dos criminosos. Os presos responderão pelos crimes de incitação/indução à discriminação ou preconceito de raça, por meio de recursos de comunicação social (Lei 7.716/89); incitação à prática de crime (art. 286 do Código Penal) e publicação de fotografia com cena pornográfica envolvendo criança ou adolescente (Lei 8069/90-ECA). O nome Intolerância, mais do que indicar a atuação criminosa dos presos, significa a intolerância da sociedade brasileira para com tais condutas, sempre pronta e vigorosamente reprimidas pela PF [...].	

Fonte: Agência de notícias PF[14] (2019).

[14] Disponível em: http://www.pf.gov.br/agencia/noticias. Acesso em: 13 out. 2019

Da análise das publicações, foi possível apurar notícias sobre a realização de campanhas educativas promovidas pela PF em parceria com a ONG SaferNet, como, por exemplo: "PF no RS realiza ações no Dia Internacional da Internet Segura"[15] e "PF e SaferNet realizarão oficina de prevenção para uso seguro da Internet"[16]. Tais campanhas refletem a relevância da união de esforços com outras entidades para o combate aos crimes de ódio.

De acordo com o *site* da instituição, a SaferNet Brasil é "uma associação civil de direito privado, com atuação nacional, sem fins lucrativos ou econômicos, sem vinculação político partidária, religiosa ou racial. Fundada em 20 de dezembro de 2005, com foco na promoção e defesa dos Direitos Humanos na Internet no Brasil"[17].

A SaferNet Brasil atua no enfrentamento aos crimes e violações aos Direitos Humanos na Internet, travando acordos de cooperação com instituições como a Polícia Federal e o Ministério Público Federal. Segundo informações retiradas da página da própria ONG[18], seu objetivo é combater os crimes cibernéticos ligados à violação de direitos humanos por meio de um canal para recebimento de denúncias, estimulando uma participação colaborativa da sociedade.

A SafetNet age ainda por meio de campanhas visando mobilizar, sensibilizar e educar a sociedade sobre as condutas adequadas no uso da Internet, bem como cuidados em situações de perigo. Conforme a ONG, sua atuação se dá da seguinte forma:

> Criamos e mantemos a Central Nacional de Denúncias de Crimes Cibernéticos operada em parceria com os Ministérios Públicos e a Secretaria de Direitos Humanos da Presidência da República (SDH) para fortalecer as ações de combate aos cibercrimes contra os Direitos Humanos. A SaferNet possui uma diversidade de ações de mobilização, sensibilização e educação para promover um uso ético e cidadão da Internet, especialmente entre as crianças e adolescentes. Além das ações de formação de educadores, pais, alunos, operadores do direito e atores do Sistema de garantia dos Direitos da Criança e do adolescentes, a SaferNet Brasil disponibiliza um serviço online gratuito único e inédito no Brasil para orientar crianças, adolescentes, pais e educadores que estejam enfrentando dificuldades e situações de violência em ambientes digitais, a exemplo dos casos de intimidações, chantagem, tentativa de violência sexual ou exposição forçada em fotos ou filmes sensuais. O canal HelpLine Brasil está disponível on-line, permitindo aos internautas brasileiros obter informações e ajuda em tempo real com a equipe especializada da SaferNet Brasil. (SAFERNET, 2019).

---

[15] Disponível em: http://www.pf.gov.br/agencia/noticias/2013/02/pf-no-rs-realiza-acoes-no-dia-internacional-da-internet-segura. Acesso em: 7 out. 2019.
[16] Disponível em: http://www.pf.gov.br/agencia/noticias/2013/08/pf-e-safernet-realizarao-oficina-de-prevencao-para-uso-seguro-da-internet. Acesso em: 17 out. 2019.
[17] Disponível em: https://new.safernet.org.br/content/institucional#. Acesso em: 27 out. 2019.
[18] Disponível em: https://new.safernet.org.br/content/o-que-fazemos#. Acesso em: 7 out. 2019.

A ONG também disponibiliza em seu site materiais educativos que, segundo a organização, também podem ser elaborados de forma personalizada. Realiza ainda cursos e palestras e atua em colaboração órgãos públicos ligados à área de segurança, desenvolvendo projetos conjuntos que tenham como objetivo a promoção de segurança na *Web*.

Em sua página[19], a SafetNet apresenta os seguintes indicadores como resultados de sua atuação:

> Em 13 anos, a SaferNet recebeu e processou 4.059.137 denúncias anônimas, envolvendo 750.526 páginas (URLs) distintas escritas em 9 idiomas e hospedadas em 67.224 domínios diferentes, de 250 diferentes TLDs e conectados à Internet através de 63.791 números IPs distintos, atribuídos para 104 países em 6 continentes. Ajudou 24.201 pessoas em 27 unidades da federação e foram atendidos 2.315 crianças e adolescentes, 1.947 pais e educadores e 19.939 outros adultos em seu canal de ajuda e orientação. Além disso, foram realizadas 715 atividades de sensibilização e formação de multiplicadores de 297 cidades diferentes, 27 estados, contemplando diretamente 66.861 crianças, adolescentes e jovens, 69.713 pais e educadores e 3.647 autoridades, com foco na conscientização para boas escolhas online e uso responsável da Internet. Em 2018, o novo curso de formação à distância formou mais 7 mil educadores da rede pública de ensino. Estas atividades beneficiaram mais de 2 milhões de pessoas indiretamente nas ações derivadas. (SAFERNET, 2019).

Já em relação ao racismo na Internet, constam as no site da ONG as seguintes informações:

> Em 13 anos, a Polícia Federal recebeu e processou 331.267 denúncias anônimas de Racismo envolvendo 50.499 páginas (URLs) distintas (das quais 18.506 foram removidas) escritas em 7 idiomas e hospedadas em 4.820 domínios diferentes, de 85 diferentes TLDs e conectados à Internet através de 5.132 números IPs distintos, atribuídos para 59 países em 5 continentes. (SAFERNET, 2019).

Ações conjuntas mediante a formação de parcerias podem representar uma estratégia relevante no combate e na prevenção da criminalidade pela Internet. A formação de redes de informação das quais o Estado faça parte representa uma estratégia interessante para o empoderamento estatal na Sociedade da Informação. Segundo Pinheiro (2012),

> as redes e as tecnologias da informação permitiram o desenvolvimento de repositórios, servidores, bancos de dados, advindos de múltiplos centros de informação, coexistindo sem princípios diretores. A colocação do Estado informacional exige o desenvolvimento de sinergias entre esses instrumentos e tal processo precisa integrar as ações informacionais dos diferentes ministérios, ligando um conjunto de informações que componha à identidade nacional. Trata-se, portanto, de unir elos isolados entre as diferentes redes de informação já existentes.

[19] Disponível em: http://indicadores.safernet.org.br/indicadores.html. Acesso em: 5 nov. 2019.

Na Sociedade da Informação, os riscos relacionados ao uso inadequado das tecnologias adquirem relevante dimensão social e não se limitam a indivíduos. Tais riscos atingem, portanto, bens jurídicos difusos, pertencentes a um número indeterminado de titulares ligados por circunstâncias de fato. Assim, a evolução tecnológica informática deve ser percebida no contexto dos novos riscos, por propiciar o progressivo contato de pessoas pelo mundo, reduzindo o planeta e potencializando o intercâmbio de toda espécie de informações. Com um número enorme de usuários e um universo incalculável de dados, os internautas podem se tornar potenciais vítimas ou autores de crimes (CRESPO, 2011).

A cooperação com outras instituições é uma medida que pode ser implementada com o objetivo de aprimorar a coleta de informações. No caso dos crimes de ódio na Internet, o monitoramento constante da Rede Mundial de Computadores é dificultado em virtude do grande volume de dados que nela circula. A prospecção de informações sobre propagação de conteúdos discriminatórios na Internet muitas vezes se dá por meio de dados encaminhados por outras instituições.

As parcerias com outros órgãos podem contribuir com a captação de informações sobre fatos criminosos. Trata-se de um exemplo de estratégia de Gestão da Informação aplicada com intuito de fomentar a fase de coleta. Cabe considerar que é objetivo da GI proporcionar métodos e técnicas para o aprimoramento das diversas atividades relacionas ao uso da informação, prospecção, monitoramento, filtragem, agregação de valor e disseminação da informação (VALENTIM; GELINSKI, 2005).

Firmar parcerias com outras instituições tem se apresentado como alternativa relevante para o combate à criminalidade na Internet. A complexidade e velocidade dos novos riscos causados pelo desenvolvimento tecnológico exige o desenvolvimento de novas estratégias para atuar no combate aos crimes cibernéticos. A união de esforços é cada vez mais necessária diante da dificuldade em se combater de forma isolada fatos criminosos que ocorrem por meio do compartilhamento de dados acessíveis em escala mundial.

4.2 A GESTÃO DA INFORMAÇÃO PLICADA À INVESTIGAÇÃO DE RACISMO NA INTERNET PELA POLÍCIA FEDERAL

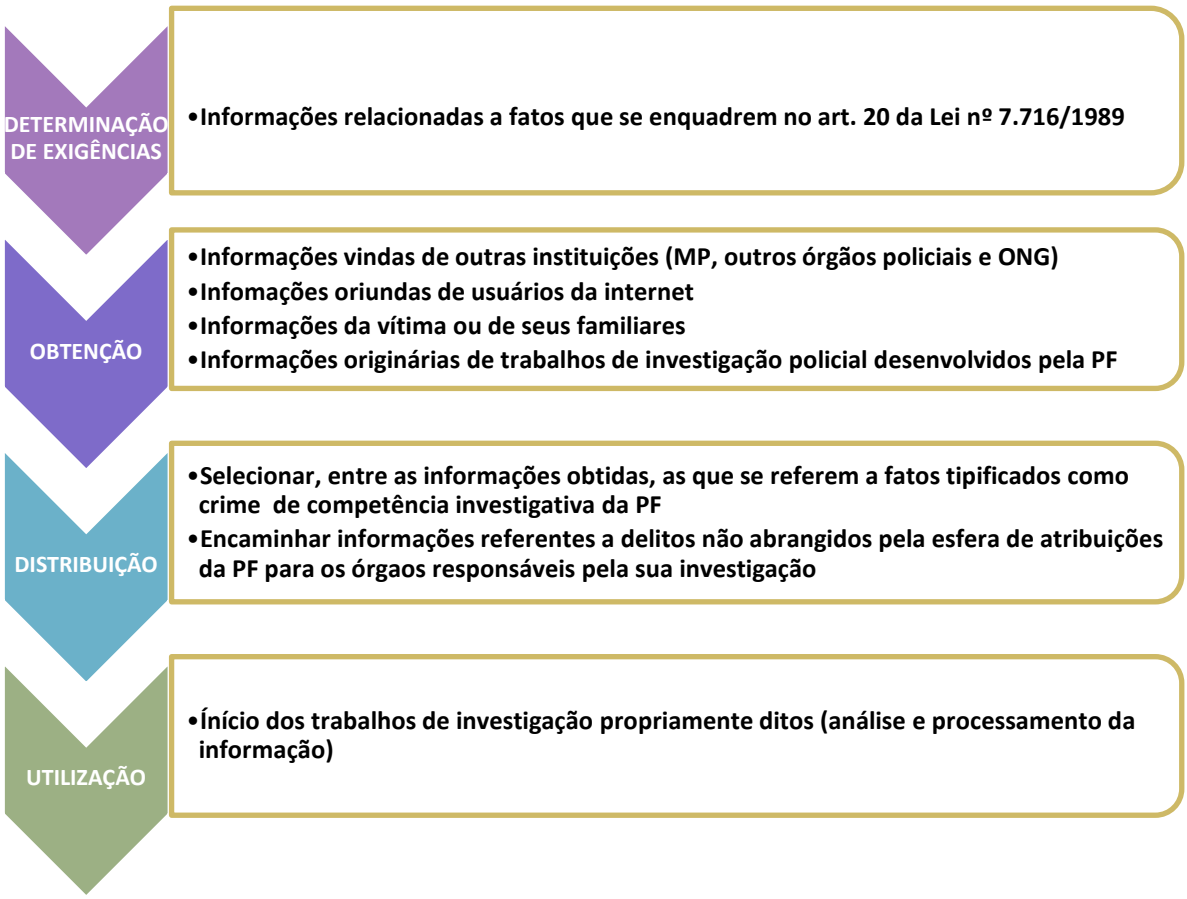
Quanto às atividades de gestão, importa distinguir a Gestão de Informação e Gestão de Recursos de Informação. A GI representa "a tarefa de gerir a relação entre objetivos organizacionais, processos de gestão e necessidades de informação no desenvolvimento de uma estratégia de informação, inferindo dessa estratégia uma estratégia de TI e uma estratégia de sistemas de informação". Já a gestão dos recursos de informação é definida como "a aplicação de princípios gerais de gestão de recursos para identificar recursos de informação distintos, estabelecer a posse e a responsabilidade, determinar o custo e o valor, e promover o desenvolvimento e a exploração quando apropriado" (CORUJO; SILVA, 2019).

No caso da investigação de discursos de ódio relacionados ao crime de racismo na Internet, a fase mais complexa à luz da Gestão da Informação e das etapas elencadas por Davenport seria a da obtenção da informação. A maior dificuldade é que o fato criminoso costuma chegar ao conhecimento da Polícia Federal de diversas formas, com destaque para as informações oriundas de fontes externas, como outros órgãos públicos, ONGs, usuários da internet e de pessoas que se sintam ofendidas. Assim, é preciso lidar com múltiplos fatores externos para a obtenção da informação.

Cabe ressaltar ainda que existem muitos conteúdos de caráter racista e discriminatório na Internet, porém nem todos se encaixam no tipo penal que a PF tem a atribuição legal de investigar. Há situações, por exemplo, de xingamentos que configuram injúria racial, e não racismo. As mesmas expressões de preconceito e ódio podem ser utilizadas para cometer crimes diferentes, dificultando a coleta do que seria uma informação relevante para a Polícia Federal.

Nesse contexto, em analogia ao modelo proposto por Davenport (1998), buscou-se traçar uma representação gráfica das etapas da Gestão da Informação aplicadas à investigação de casos de racismo na Internet. Tal analogia encontra-se representada pela figura abaixo.

Figura 5 – Modelo para Gestão da Informação na Investigação de Racismo na Internet



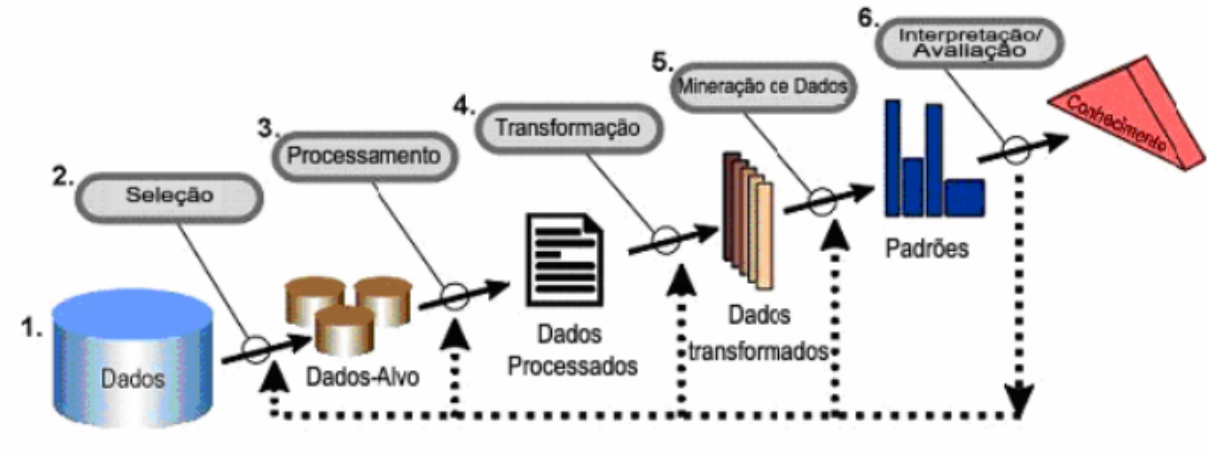
Fonte: Elaborado pela autora (2019).

No que tange à investigação de conteúdo de ódio na Internet, a presente pesquisa deteve maior atenção na fase da aquisição da informação, ou seja, na forma como o conteúdo informacional supostamente criminoso chega ao conhecimento da Polícia Federal para ser investigado. Deve-se ressaltar que o volume informacional encontrado na Internet para ser analisado nessa espécie de investigação é imensurável. Faz-se necessário utilizar a GI para traçar estratégias a fim de acessar e selecionar as informações referentes a tais fatos ilícitos. Uma das estratégias que podem contribuir para a investigação seria o uso de ferramentas de mineração de texto na busca de conteúdo de ódio na Internet.

A mineração de texto, também conhecida como descoberta de conhecimento em texto *(Knowledge Discovered in Texts – KDT)*, consiste no processo de extração de informações úteis em documentos de texto não estruturados. Para tal fim, a mineração de texto utiliza técnicas da recuperação da informação, processamento de linguagem natural e descoberta de conhecimentos em bancos de dados. Difere da mineração de dados *(Knowledge Discovered*

Databases – KDD), uma vez que nesta os dados encontram-se estruturados (BARION; LAGO, 2008). A figura abaixo demonstra as etapas do processo do processo de mineração aplicado a dados.

Figura 6 – Etapas da mineração de dados



Fonte: Corrêa (2003 *apud* BARION; LAGO, 2008).

De acordo com Barion e Lago (2008), as etapas do processo de mineração podem ser sintetizadas da seguinte forma:

1. Dados não estruturados.
2. Seleção de dados: inicialmente define-se o domínio onde será realizada a mineração e em seguida realiza a seleção e coleta dos dados e variáveis.
3. Visa eliminar dados inadequados por meio de algoritmos.
4. Transformação: realiza a armazenagem adequada de dados para facilitar a aplicação de técnicas de mineração.
5. Mineração de dados: realiza a descoberta do conhecimento pelo uso de algoritmos de aprendizagem de máquinas e descoberta de padrões. Também utiliza conhecimentos de estatística, classificação, clusterização e modelos gráficos.
6. Interpretação / Avaliação: apresenta os resultados do processo de descoberta do conhecimento de forma compreensível para o usuário.

Segundo Ambrósio e Morais (2007), a mineração de dados é vista como uma ferramenta de gestão. Seu principal objetivo está na descoberta de correlacionamentos e dados implícitos em registros de bancos de dados, visando extrair conhecimento para ser utilizado em algum processo decisório. Os autores destacam a importância de que o resultado do processo

de KDD seja compreensível a humanos, posto que visa subsidiar os usuários finais do processo, que geralmente são tomadores de decisão.

Quanto à relevância da mineração de dados, Camilo e Silva (2009, p. 22) ressaltam:

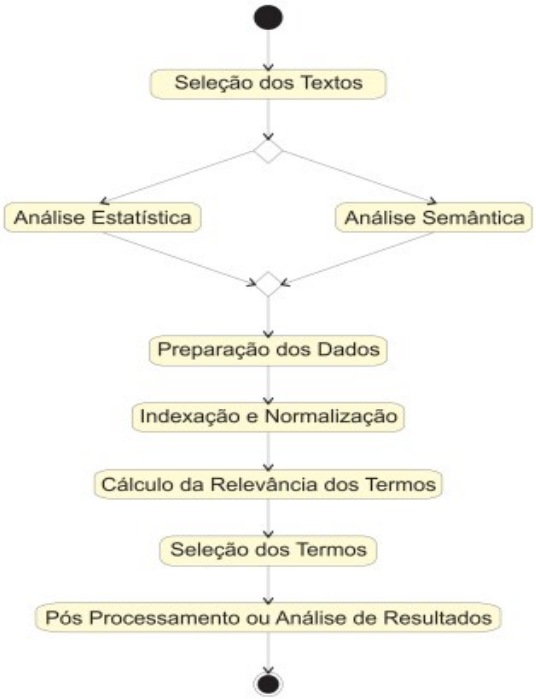
> A Mineração de Dados tornou-se uma ferramenta de apoio com papel fundamental na gestão da informação dentro das organizações. A manipulação dos dados e a análise das informações de maneira tradicional tornou-se inviável devido ao grande volume de dados (coletados diariamente e armazenados em bases históricas). Descobrir padrões implícitos e relacionamentos em repositórios que contém um grande volume de dados de forma manual, deixou de ser uma opção. As técnicas de mineração passaram a estar presentes no dia a dia.

No que tange aos discursos de ódio na Internet, uma das dificuldades encontradas é que tais discursos são constituídos por dados não estruturados, o que dificulta a aplicação das técnicas tradicionais de mineração de dados e enseja a necessidade de aplicação de estratégias de mineração de texto. Para Barion e Lago (2008), "mineração de texto é um conjunto de métodos usados para navegar, organizar, achar e descobrir informações em bases de textos. Pode ser vista como uma extensão da área de *Data Mining*, focada na análise de textos".

Segundo Ambrósio e Morais (2007), a mineração de texto é utilizada para analisar documentos, não correspondendo, portanto, a uma simples busca. A mineração analisa um documento em texto, o resultado da análise precisa ser contextualizado, para só então haver a descoberta de conhecimento. Ela representa um processo que visa auxiliar na descoberta de um conhecimento a partir de documentos textuais.

Ao definir o processo de mineração, os autores estabelecem as seguintes etapas: seleção de documentos, definição do tipo de abordagem dos dados (análise semântica ou estatística), preparação dos dados, indexação e normalização, cálculo da relevância dos termos, seleção dos termos e pós-processamento (análise de resultados). Essas etapas são representadas na figura abaixo.

Figura 7 – Etapas do processo de mineração de texto



Fonte: Ambrósio e Morais (2007).

O processo de mineração de texto compreende dois tipos de abordagens: uma semântica, baseada na funcionalidade dos termos encontrados nos textos, e uma estatística, baseada na frequência dos termos encontrados nos textos. Tais abordagens podem ser utilizadas separadamente ou em conjunto. A análise semântica emprega técnicas que avaliam a sequência dos termos no contexto dos textos, no sentido de identificar qual a sua função, sendo fundamentada em técnicas de Processamento de Linguagem Natural (PNL), especialmente se for incrementado por Processamento Linguístico. Para processamento de linguagem natural é preciso ter, pelo menos, conhecimento morfológico, sintático, semântico, pragmático, do discurso e do mundo. Na análise estatística, a relevância de um termo está na quantidade de vezes que ele aparece no texto. Seu processo envolve o estatístico a partir de dados, o qual costuma incluir as etapas de codificação dos dados, estimativa dos dados e modelos de representação de documentos (AMBRÓSIO; MORAIS, 2007).

O uso da mineração de texto é uma ferramenta relevante para a produção de conhecimento, uma vez que a maioria dos dados disponibilizados, tanto na Internet como nas empresas em geral, é armazenado sob essa forma. A descoberta de conhecimento em texto representa uma técnica com um grande campo de aplicação; contudo, a principal dificuldade

para implementá-la é a falta de técnicas efetivas de análise semântica de textos (AMBROSIO; MORAIS, 2007).

As técnicas utilizadas no processo de mineração de texto são complexas e demandam um estudo específico. No que tange à presente pesquisa, observa-se que a utilização das técnicas de mineração de texto seria uma alternativa viável para buscar termos discriminatórios e racistas na Internet, uma vez que essa é uma reconhecida ferramenta para a descoberta de conhecimento em bases de dados não estruturadas.

5 CONSIDERAÇÕES FINAIS

As tecnologias de informação e comunicação interferem em todos os contextos sociais. A criminalidade e, consequentemente, a investigação policial, também estão sendo impactadas pela necessidade de adaptação à Sociedade da Informação, caracterizada pelo dinamismo e pela inovação contínua dos meios eletrônicos. Gouveia (2004) chama a atenção para o uso da tecnologia pelas pessoas em seus contextos sociais, econômicos e políticos, sendo esse uso em diversos campos que fez surgir a Sociedade da Informação.

> A Sociedade da Informação está baseada nas tecnologias de informação e comunicação que envolvem a aquisição, o armazenamento, o processamento e a distribuição da informação por meios electrónicos, como a rádio, a televisão, telefone e computadores, entre outros. Estas tecnologias não transformam a sociedade por si só, mas são utilizadas pelas pessoas em seus contextos sociais, económicos e políticos, criando uma nova comunidade local e global: a Sociedade da Informação (GOUVEIA, 2004, p. S.I.).

Em virtude dos impactos globais gerados pelas inovações nos meios eletrônicos de comunicação e informação, surgiu uma forte necessidade de se buscar alternativas para adaptação da investigação policial aos contextos da Sociedade da Informação. Desse modo, para lidar com o volume de dados disponíveis e transformá-los em conhecimento relevante a uma investigação, é necessário recorrer a medidas de Gestão da Informação.

No caso dos discursos de ódio em ambientes virtuais, e mais especificamente do crime de racismo na Internet, observou-se que as maiores dificuldades estão na fase de coleta da informação. Contatou-se que nesses crimes a Polícia Federal costuma agir após ter conhecimento de possível fato criminoso por meio de informação de terceiros, pois, em regra, não existe uma constante na varredura na Rede Mundial de Computadores em busca de possíveis discursos de ódio. A ação policial quanto a tais ilícitos, portanto, costuma ser reativa, e não proativa.

Assim, verificou-se que as informações sobre um fato criminoso relacionado à propagação de discurso discriminatório na Internet costumam chegar ao conhecimento da Polícia Federal por meio de informações e denúncias encaminhadas por terceiros (indivíduos, órgãos públicos, instituições particulares e ONGs). Diante desse contexto, uma estratégia de Gestão da Informação aplicada à fase de coleta seria o incentivo à formação de redes de informação, as quais poderiam ser estruturadas por meio de acordos e convênios com outras instituições.

Diante de uma crescente demanda por informação e atualização do conhecimento, e em um momento em que o mundo está cada vez mais conectado e a tecnologia é intensamente utilizada para ligar pessoas e instituições, e, nesse contexto, as organizações policiais não podem agir isoladamente. Assim, no que tange ao posicionamento da PF perante outros entes para o combate aos crimes cibernéticos, a Gestão da Informação pode ser utilizada como uma ferramenta para incentivar e orientar a formação de parcerias.

A colaboração com outras instituições costuma ser formalizada mediante convênios e termos de cooperação institucional. A união entre entidades distintas em prol de objetivos comuns incentiva a construção de redes de informação para intercâmbio de dados, informações e conhecimentos. Deste modo, a colaboração com parceiros como ONGs e órgãos públicos interessados no combate a crimes cibernéticos apresenta-se como um recurso apropriado para o enfrentamento da criminalidade no contexto da Sociedade da Informação.

Em um mundo globalizado e extremamente conectado, não seria uma solução viável combater crimes cibernéticos de forma solitária. Felipe e Marcelo Caiado, ao abordarem a problemática do combate ao compartilhamento de material de pornografia infanto-juvenil, modalidade de crime cibernético, ressaltam a importância de se buscar firmar parcerias com entes de diversas áreas:

> Finalmente, é importante que os governos, as universidades e as indústrias entendam as mudanças no modus operandi dessas atividades criminais, trabalhando continuamente em conjunto para desenvolver novas tecnologias e soluções de investigação, que melhorarão a performance da tecnologia disponível para encontrar material de pornografia infanto-juvenil de uma maneira forense e com um correto estabelecimento da cadeia de custódia. Somente assim poderemos vislumbrar um futuro mais seguro para as crianças, em que todas as ocorrências de abuso sexual e seus danos resultantes (CAIADO; CAIADO, 2018, p. 22).

O crime é um fenômeno social, e seu combate requer subsídios de diversas áreas do conhecimento, corroborando a necessidade de adoção de uma perspectiva sistêmica das demandas informacionais. Assim, faz-se necessário que haja uma adaptação constante das técnicas e recursos de investigação e a colaboração de diversos agentes de várias áreas do saber, como Direito, Ciência da Informação, Tecnologia da Informação, Gestão da Informação e áreas correlatas, para combater as novas formas de criminalidade cibernéticas.

Nos crimes de ódio na Internet, observou-se que o monitoramento de conteúdos racistas é complexo devido à grande quantidade de arquivos digitais que necessitam ser analisados, bem como ao fato de tais arquivos circularem em diversos ambientes, como *surface*

web, *deep web*, *dark web*, conexões P2P e mídias sociais. Logo, entende-se que, se o crime pode ser perpetrado de formas distintas, não é possível combatê-lo de maneira única.

Além das parcerias para obtenção de informação de terceiros, seria possível desenvolver *softwares* para varredura na Internet em busca de conteúdos ilícitos. O desenvolvimento de *softwares* de monitoramento como o CPS representa uma medida de Gestão da Informação relevante para o combate à criminalidade. A aplicação de tal medida corresponde à etapa definida por Davenport (1998) como coleta da informação.

É possível observar, porém, que cada espécie de delito apresenta características específicas, demandando soluções próprias que atentem para suas peculiaridades. Assim, medidas de gestão como capacitação de servidores, investimentos em TI, desenvolvimentos de softwares e intercâmbio de informações devem levar em conta as características do crime que se pretende combater. As melhorias almejadas na busca por uma investigação mais eficiente não são encontradas em uma solução única, mas em conjuntos de medidas que, juntas, podem proporcionar melhores resultados.

Nos crimes relacionados à propagação de conteúdo de ódio e ao racismo na Internet, os especialistas foram unânimes em informar que a PF costuma agir por demanda. Entende-se que a cooperação com instituições que já realizam pesquisas na Rede Mundial de Computadores e que ofereçam canais de denúncia pode otimizar o conhecimento da polícia sobre fatos criminosos. A atuação por demanda acaba por ser menos abrangente, visto que parte de um fato específico, já retratado, para buscar sua autoria e materialidade.

Entre as medidas de Gestão da Informação identificadas como adequadas para aumentar a eficiência na investigação de crimes de ódio, destacam-se:

1. Formação de parcerias com outros entes, públicos ou privados, e com canais informação que liguem a polícia à sociedade. Tal medida é relativamente simples e de fácil implementação, podendo trazer bons resultados a baixo custo, sem que isso signifique, contudo, parar de investir no desenvolvimento de tecnologias e/ou na aquisição de novas soluções tecnológicas.
2. Promoção ou participação de campanhas para informar os usuários acerca dos crimes de ódio na Internet, esclarecendo sobre quando um comentário preconceituoso ou discriminatório configura um crime, que tipos de crime relacionados a esses conteúdos costumam ser cometidos e quais instituições podem ser procuradas para se efetuar uma denúncia. A informação dos usuários é

relevante, pois, conforme relatado pelos especialistas, as denúncias de terceiros e pessoas ofendidas representa uma fonte importante de informação para a polícia.

3. Desenvolvimento ou aquisição de *software* para varredura na Rede Mundial de Computadores por meio de busca por palavras-chave, utilizando técnicas de mineração de texto.

Considerando o volume de conteúdos de ódio que circulam na Internet, seria impossível transformar dados em informações e estas em conhecimentos apenas por meio da análise manual feita por especialistas. Em regra, nos casos em que o volume informacional é muito extenso, o processamento unicamente manual dos dados e informações é inviável, sendo necessário o auxílio de ferramentas de TI.

O KDT (*Knowledge Discovery in Texts* ou Descoberta de Conhecimento Textos) é um caminho para busca de conhecimento em documentos de texto não-estruturados. Desse modo, considerando que especialistas apontam que a grande maioria dos crimes relacionados à propagação de conteúdo de ódio na Internet estão em formato de texto e que existe um volume muito extenso de dados a serem analisados, seria relevante o desenvolvimento de ferramenta que automatizasse essa busca.

A tecnologia aplicada para o desenvolvimento de uma ferramenta com tais funcionalidades seria a mineração de texto. Ela pode ser desenvolvida para buscar conhecimento por palavras-chave relacionadas ao discurso discriminatório em bases de dados delimitadas pelos investigadores.

Vários são os caminhos para a investigação de crimes cibernéticos e, conforme mencionado, não seria possível adotar uma solução única para equacionar demandas diversificadas e dotadas de especificidades. Contudo, resta a certeza de que a tecnologia não vai parar de evoluir e que a criminalidade tende, cada vez mais, a migrar também para o campo cibernético. Assim, serão necessários novos investimentos em TI, novas parcerias, novas estratégias e, sobretudo, um novo olhar para a necessidade de se adotar medidas de gestão compatíveis com as demandas impostas pela Sociedade da Informação.

Ressalta-se que cabe ao Estado brasileiro aprimorar seu aparato repressivo-punitivo, evitando que o ciberespaço se torne um terreno fértil para a discriminação, a agressão moral e o preconceito. A criação de softwares que auxiliem na investigação será extremamente relevante para dar suporte à repressão de crimes que utilizam o discurso de ódio na sua execução.

Destaca-se que o campo de estudo das ferramentas de Gestão da Informação relacionadas ao aprimoramento da investigação de crimes de ódio na Internet é muito amplo. Nesse contexto, propõe-se o desenvolvimento de futuros estudos sobre a criação de ferramentas de mineração de texto aplicadas ao monitoramento de discursos discriminatórios e racistas na Internet.

O uso da tecnologia para mineração de texto no ciberespaço é um campo de estudo que precisa ser explorado, visto que pode contribuir para produção de conhecimentos relevantes acerca do conteúdo que circula na Internet. Tais conhecimentos são estratégicos, pois os Estados necessitam adotar medidas relacionadas às informações propagadas no ciberespaço. Assim, a contribuição de futuros estudos é essencial, posto que as pesquisas científicas representam um caminho para a solução de problemas que afligem a sociedade.

REFERÊNCIAS

AMBRÓSIO, Ana Paula L., MORAIS, Edilson Andrade M. Mineração de Textos. **Relatório técnico**, 2007.

ARAÚJO, Adriano Alves de**. Injúria x racismo:** qual a diferença entre os dois? JusBrasil, 2019. Disponível em: https://alvesaraujoadv.jusbrasil.com.br/artigos/434878258/injuria-x-racismo-qual-a-diferenca-entre-os-dois. Acesso em: 10 jan. 2020.

BARION, Eliana Cristina Nogueira; LAGO, Décio. Mineração de Textos**. Revista de Ciências Exatas e Tecnologia**. v. III, n. 3, 2008.

BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de investigação cibernética** [*Kindle Android version]*. *Retrieved from Amazon.com*, 2016.

BARSOTI, Luciane. As provas digitais e a relevância nas ciências jurídicas da pós-modernidade. *In*: CAMARGO, C. A. (Ed.). **Direito digital**: novas teses jurídicas. Rio de Janeiro: Lumen Juris, 2018. cap. 17. [*Kindle Android version. Retrieved from Amazon.com*].

BEUREN, I. M. **Gerenciamento estratégico da informação**: um recurso estratégico no processo de gestão empresarial. São Paulo: Atlas, 1998.

BITTENCOURT, C. R. **Tratado de direito penal**: parte geral. 24. ed. São Paulo: Saraiva, 2018.

BOCCATO, V. R. C. Metodologia da pesquisa bibliográfica na área odontológica e o artigo científico como forma de comunicação. **Rev. Odontol. Univ. Cidade São Paulo**, São Paulo, v. 18, n. 3, p. 265-274, 2006.

BORKO, H. *Information science: what is it?* ***American Documentation***, Washington, v. 19, n. 1, p. 3 – 5, Jan. 1968.

BRAMAN, Sandra. ***Change of state****: information, policy, and power*. 1. ed. Mit Press, 2006.

BRASIL. **Decreto n.º 65.810, de 8 de dezembro de 1969.** Promulga a convenção internacional sobre a eliminação de todas as formas de discriminação racial. Brasília, 1969. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1950-1969/D65810.html. Acesso em: 17 out. 2019.

BRASIL. **Lei n.º 10.446, de 8 de maio de 2002**. Brasília, 2002. Disponível em: http://www.planalto.gov.br/CCIVIL_03/LEIS/2002/L10446.htm. Acesso em: 17 out. 2019.

BRASIL. **Lei n.º 11.340, de 7 de agosto de 2006.** Brasília, 2006. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11340.htm. Acesso em: 17 out. 2019.

BRASIL. **Lei n.º 12.735, de 30 de novembro de 2012.** Brasília, 2012a. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm. Acesso em: 17 out. 2019.

BRASIL. **Lei n.º 12.737, de 30 de novembro de 2012.** Brasília, 2012b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 07 jan. 2020.

BRASIL. **Lei n.º 13.105, de 16 de março de 2015.** Brasília, 2015b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 07 jan. 2020.

BRASIL. **Lei n.º 13.185, de 6 de novembro de 2015.** Brasília, 2015c. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13185.htm. Acesso em: 07 jan. 2020.

BRASIL. **Lei n.º 13.642, de 3 de abril de 2018.** Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13642.htm. Acesso em: 07 jan. 2020.

BRASIL **Lei n.º 5.172, de 25 de outubro de 1966** (Código Tributário Nacional). Brasília, 1966. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l5172.htm. Acesso em: 07 jan. 2020.

BRASIL. **Projeto de Lei n.º 2496/2019.** Brasília, 2019. Disponível em: https:// www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2199159. Acesso em: 15 nov. 2019.

BRASIL. Supremo Tribunal Federal. **Ação direta de inconstitucionalidade por omissão n.º 26.** Relator: Min. Celso de Mello. Brasília, 13/06/2019. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=4515053. Acesso em: 02 dez. 2019.

BRASIL. Supremo Tribunal Federal. **Embargos de declaração em *Habeas Corpus* n.º 121.283 – DF.** Relator: Min. Roberto Barroso. Brasil, 2014. Disponível em:https://portal.stf.jus.br/processos/downloadPeca.asp?id=223640513&ext=.pdf. Acesso em: 15 nov. 2019.

BRASIL. Supremo Tribunal Federal. **Mandado de Injunção n.º 4733** – DF. Relator: Min. Edson Fachin. Brasil, 2019. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4239576. Acesso em: 15 nov. 2019.

BRASIL. Superior Tribunal de Justiça. **Conflito de competência n.º 146.983** – RJ (2016/0147383-6). Relator: Min. Felix Fischer. Brasil, 2014. Disponível em: https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1564067&num_registro=201601473836&data=20170629&formato=PDF. Acesso em: 15 nov. 2019.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 15 nov. 2019.

BRASIL. **Decreto-Lei n.º 2.848, de 7 de dezembro de 1940.** Código penal. Brasília, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 15 nov. 2019.

BRASIL. **Lei n.º 13.104, de 9 de março de 2015.** Brasília, 2015a. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/lei/L13104.htm. Acesso em: 19 mai. 2017.

BRASIL. **Lei n.º 7.716, de 5 de janeiro de 1989.** Brasília, 1989. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7716.htm. Acesso em: 5 nov. 2019.

BRASIL. Ministério Público Federal. **Roteiro de atuação:** crimes cibernéticos. 3. ed. rev. e ampl. Brasília: Ministério Público Federal / 2ª Câmara de Coordenação e Revisão, 2016. Disponível em: http://www.mpsp.mp.br/portal/page/portal/Escola_Superior/Biblioteca/Biblioteca_Virtual/Livros_Digitais/MPF%203186_Crimes_Ciberneticos_2016.pdf. Acesso em: 12 jan. 2020.

BRESSER-PEREIRA, Luiz Carlos. Estado, estado-nação e formas de intermediação política. **Lua Nova,** São Paulo, n.º 100, p. 155-185, jan. 2017. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-64452017000100155. Acesso em: 10 jan. 2020.

BUCKLAND, M. K. *Information as thing.* ***Journal of the American Society for Information Science***, v. 45, n. 5, p. 351 – 360, 1991.

CAIADO, Felipe B.; CAIADO Marcelo. Combate à pornografia infanto-juvenil com aperfeiçoamentos na identificação de suspeitos e na detecção de arquivos de interesse. *In*. **Crimes Cibernéticos.** Coletânea de artigos, v. 3, Brasília: Ministério Público Federal / 2ª Câmara de Coordenação e Revisão, 2018. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos. Acesso em: 20 out. 2019.

CAMILO, Cássio Oliveira; SILVA, João Carlos da. **Mineração de dados:** conceito, tarefas, metas e ferramentas. Relatório Técnico, 2009.

CASTELLS, M. **A sociedade em rede**. 17. ed. São Paulo: Paz e Terra, 2016. v. 1. (A era da economia sociedade e cultura, v. 1).

CHAER, Galdino; DINIZ, Rafael R. P.; RIBEIRO, Elisa A. A técnica do questionário na pesquisa educacional. **Evidência**, Araxá, v. 7, n. 7, p. 251-266, 2011.

CHOO, C. W. *Information Management for the inteligente organization: roles and implications for the information professions. In:* ***Digital Libraries Conference****, 1995, Singapore. Proceedings. Singapore: National Computer Board of Singapore*, 1995.

CHOO, C. W. ***The knowing organization:*** *how organizations use information for construct meaning, create knowledge and make decisions.* Nova York: Oxford Press, 1998.

CONSELHO DA EUROPA. **Convenção sobre o cibercrime** (Convenção de Budapeste). Budapeste, 23 nov. 2001. [*Kindle Android version]. Retrieved from Amazon.com***.** Disponível em: https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese.pdf. Acesso em: 16 out. 2019.

CORDEIRO, Alexander Magno *et al.* Revisão sistemática: uma revisão narrativa. **Rev. Col. Bras. Cir**, v. 34, n. 6, p. 428-431, 2007.

CORUJO, Luis Miguel Nunes; SILVA, Carlos Guardado. Uma abordagem diacrónica da gestão da informação: conceito, enquadramento disciplinar, etapas e modelos. **Ciência da Informação,** Brasília, DF, v.48 n.2, p.144-164, maio/ago. 2019.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011. [*Kindle Android version. Retrieved from Amazon.com*].

CRESWELL, J. W. **Investigação qualitativa e projeto de pesquisa**. Porto Alegre: Penso, 2014.

DALLARI, D. de A. **Elementos de teoria geral do estado**. 24. ed. São Paulo: Saraiva, 2003.

DARÓS MALAQUIAS, Roberto Antônio. **Crime cibernético e prova:** a investigação criminal em busca da verdade. 2. ed. Curitiba: Juruá, 2015.

DAVENPORT, Thomas. H. **Ecologia da informação:** por que só a tecnologia não basta para o sucesso na era da informação. São Paulo: Futura, 1998.

DAVENPORT, Thomas. H. **Ecologia da informação**. São Paulo: Futura, 2002.

DE SORDI, José Osvaldo de. **Administração da informação.** 2. ed. São Paulo: Saraiva, 2008.

DUMONT, Danilo M.; RIBEIRO, J. Araujo e RODRIGUES, Luiz Alberto. **Inteligência pública na era do conhecimento**. Rio de Janeiro: Revan, 2006.

FREITAS, Maria Cristina V.; VIANNA, William Barbosa. Gestão da informação e ciência da informação: elementos para um debate necessário. **Ciência da Informação,** Brasília, DF, v. 48, n.º 2, p. 191-208, maio/ago. 2019.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social.** 5. ed. São Paulo: Atlas, 1999.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Atlas, 2010.

GOUVEIA, L. M. B. Sociedade da informação: notas de contribuição para uma definição operacional. *In*: **Homepage LMBG**, 2004. Disponível em: http://homepage.ufp.pt/lmbg/reserva/lbg_socinformacao04.pdf. Acesso em: 23 out. 2019.

HARARI, Y. N. **Homo Deus**: uma breve história do amanhã. 13. ed. São Paulo: Companhia das Letras, 2015.

KUMMER, Fabiano Ratton. **Direito penal na sociedade da informação**. 1. ed. Paraná: [s.n.], 2017. [*Kindle Android version. Retrieved from Amazon.com*].

LAKATOS, E. M.; MARCONI, M. de A. **Fundamentos de metodologia cientifica**. 7. ed. São Paulo: Atlas, 2010.

LANGE, Rodrigo; RALHA, Célia Ghedini. Identificação de artefatos periciais do eMule. ***The sixth international conference on forensic computer science*.** 2011. Disponível em: http://icofcs.org/2011/icofcs2011-pp04.pdf. Acesso em: 23 set. 2019.

LEMOS, André. **Cibercultura**: tecnologia e vida social na cultura contemporânea. 7. ed. Porto Alegre: Sulina, 2015. 295 p.

LENZA, Pedro. **Direito constitucional esquematizado**. 22. ed. São Paulo: Saraiva, 2017.

LÉVY, Pierre. **A inteligência coletiva**. 2. ed. São Paulo: Editora Loyola, 1999.

LIMA, Telma Cristiane Sasso de; MIOTO, Regina Célia Tamaso. Procedimentos metodológicos na construção do conhecimento científico: a pesquisa bibliográfica. **Revista Katalysis**, v. 10, p. 35-45, 2007.

MASON, G. *Hate crime and the image of the stranger.* ***The British Journal of Criminology***, v. 45, n. 6, p. 837 – 859, nov. 2005.

MEIRELLES, H. L. **Direito administrativo brasileiro**. 27. ed. São Paulo: Malheiros Editores Ltda., 2002.

MEYER-PFLUG, Samantha Ribeiro. **Liberdade de expressão e discurso do ódio**. São Paulo: Editora Revista dos Tribunais, 2009. 271 p.

ONU. **Declaração Universal dos Direitos do Homem.** Organização das Nações Unidas, 1948. Disponível em https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por. Acesso em: 23 dez. 2019.

ONU. **Convenção Internacional sobre a Eliminação de todas as Formas de Discriminação Racial**. Organização das Nações Unidas, 1965. Disponível em https://unesdoc.unesco.org/ark:/48223/pf0000139390. Acesso em: 23 dez. 2019.

PEERSMAN, Claudia, *et al. iCOP: Automatically Identifying New Child Abuse Media in P2P Networks.* ***IEEE Security and Privacy Workshops*.** 2014. Disponível em: https://www.researchgate.net/publication/286668164_icop_automatically_identifying_new_child_abuse_media_in_p2p_networks. Acesso em: 10 jan. 2020.

PINHEIRO, Marta M. K. Estado informacional implicações para as políticas de informação e de inteligência no limiar do século XXI. **Varia História**, Belo Horizonte, v. 28, n. 47, p. 61 – 77, jan/jun 2012.

PRODANOV, Cléber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do trabalho científico** [recurso eletrônico]: métodos e técnicas da pesquisa e do trabalho acadêmico. 2. ed. São Paulo: Novo Hamburgo: Feevale, 2013.

ROTHER, Edna Terezinha. Revisão sistemática x revisão narrativa. **Acta Paul**. **Enferm**. v. 20, n.º 2, São Paulo, Apr./June June, 2007.

SAFERNET. **Indicadores**. Disponível em: http://indicadores.safernet.org.br/. Brasil, 2019. Acesso em: 15 nov. 2019.

SANTOS Christiano Jorge. **Crimes de preconceito e de discriminação**. 2. ed. São Paulo: Saraiva, 2010.

SANTOS, Cleórbete. Crimes digitais: atualidades e tendências. *In*: CAMARGO, C. A. (Ed.). **Direito digital**: novas teses jurídicas. Rio de Janeiro: Lumen Juris, 2018. cap. 7. [*Kindle Android version. Retrieved from Amazon.com*].

SARACEVIC, Tefko. A natureza interdisciplinar da ciência da informação. **Ciência da Informação**, v. 24, n.º 1, 1995. Disponível em: http://revista.ibict.br/ciinf/article/view/608/610. Acesso em: 15 maio 2019.

SAVIC, Dobrica. *Evolution of information resource management.* ***Journal of Librarianship and Information Science***, v. 24, nº 3, p. 127-138, sep. 1992.

TARAPANOFF, Kira. **Inteligência, informação e conhecimento em corporações.** Brasília: IBICT/UNESCO, 2006. 456 p.

UNESCO. **Declaração sobre a raça e os preconceitos raciais.** Organização das Nações Unidas para a Educação, a Ciência e a Cultura, Paris, 27 nov. 1978. Disponível em https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cdhm/comite-brasileiro-de-direitos-humanos-e-politica-externa/DecRacPrecRac.html. Acesso em: 16 jun. 2019.

VALENTIM, M. L. P.; GELINSKI, J. V. V. Gestão do conhecimento como parte do processo de inteligência competitiva organizacional. **Informação & Sociedade:** Estudos, João Pessoa, v. 15, n.º 2, p. 41-59, jul./dez. 2005.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos**: ameaças e procedimentos de investigação. 2. ed. São Paulo: Brasport, 2013. [*Kindle Android version. Retrieved from Amazon.com*].

WERTHEIN, Jorge. A sociedade da informação e seus desafios. **Ciência da Informação,** Brasília, v. 29, n.º 2, p. 71-77, maio/ago. 2000. Disponível em: http://www.scielo.br/pdf/ci/v29n2/a09v29n2.pdf. Acesso em: 15 nov. 2019.