DOI: 10.5433/1981-8920.2018v23n3p625

DESVELANDO ARCANOS TECNOLÓGICOS: ÉTICA ALGORÍTMICA NO ESTADO INFORMACIONAL

UNVEILING TECHNOLOGICAL ARCANES: ALGORITHMIC ETHICS IN THE INFORMACIONAL STATE

Arthur Coelho Bezerra[a]
Bianca da Costa Maia Lopes[b]

RESUMO

Introdução: as práticas difusas de vigilância informacional por instituições estatais e grandes corporações do século XXI esbarram em questões e dilemas relativos à informação em rede, como as várias formas de opacidade, a privacidade dos indivíduos e os sistemas de governança. **Objetivo**: propomos a ideia de "arcanos tecnológicos" para compreender os segredos enrascados na sociedade em rede, a fim de promover um debate que contemple temas contemporâneos relacionados à ética da informação. **Metodologia**: por meio de revisão bibliográfica, são explorados o contexto de vigilância do Estado informacional e o modelo "*panspectron*"; a noção de segredo pela perspectiva social e pelo viés do ciberativismo; e a dimensão ética que permeia a presença de algoritmos nas redes digitais. **Resultados**: verificamos que a sofisticação e complexidade tecnológicas envolvidas no processo de governança global do ciberespaço configuram uma nova e desconhecida esfera sociopolítica. Nesse sentido, irrompem-se formas de resistência efetivas como estratégias de contravigilância, vazamentos de documentos oficiais por ciberativistas, atuações da mídia em casos específicos e medidas para a prestação de contas pela sociedade. **Conclusões**: uma ética pragmática dos algoritmos deve enfatizar a prestação de contas à sociedade tanto por agentes estatais quanto pelos não-estatais. Reinos digitais formados por oligopólios da internet precisam aceitar a mesma carga de imputabilidade e responsabilização social que exigem de indivíduos, tornando-se imprescindível o aumento da conscientização de todos sobre as estruturas de poder que transpassam os "arcanos tecnológicos".

Descritores: Ética da informação. Estado informacional. Privacidade e Vigilância.

[a] Doutor em Sociologia pela Universidade Federal do Rio de Janeiro (UFRJ). Professor do Programa de Pós-Graduação em Ciência da Informação (PPGCI/IBICT-UFRJ). E-mail: arthurbezerra@ibict.br

[b] Doutoranda em Ciência da Informação pela Universidade Federal do Rio de Janeiro (IBICT-UFRJ). E-mail: bianca.lopes@gmail.com

1 INTRODUÇÃO

s m a i s m r m i l m e p o e t a l e u m i b u n e n u g t t a u i r a s
Galileu Galilei

A epígrafe que abre este artigo[1] reproduz a mensagem de uma carta do astrônomo italiano Galileu Galilei, enviada para o (também astrônomo) alemão Johannes Kepler no início do século XVII. Tratava-se de um anagrama com as descobertas e observações de Galilei a respeito do então desconhecido planeta Saturno. Kepler, infelizmente, não compreendeu a mensagem de seu colega italiano.

Dois séculos depois, o telégrafo elétrico inventado por Samuel Morse proporcionou a representação da escrita mediante pontos e traços. Afora o chamado "Alfabeto Telegráfico Morse", concebeu-se um meta-alfabeto capaz de ressignificar, pela troca de signos por novos signos, o simbolismo da codificação (GLEICK, 2013, p. 160).

Contemporaneamente, no âmbito das tecnologias digitais, percebe-se na rede mundial de computadores o uso expressivo de algoritmos criptográficos, derivados de estudos da criptologia. Por meio deles e para múltiplas finalidades, gigantescos oligopólios da internet erguem verdadeiros reinos digitais, ordenados por sistemas próprios de governança e soberanias privadas no ciberespaço (MacKINNON, 2012).

Os três recortes temporais supracitados, interligados pelo contínuo progresso da revolução científica e tecnológica, remetem a uma sorte de técnicas de camuflagem de informações, interditadas por meio do uso de códigos alfabéticos ou matemáticos. Partimos do pressuposto de que o processo de codificação de mensagens pode servir a um amplo conjunto de propósitos: Galilei, por exemplo, buscava preservar menos sua privacidade do que reivindicar a prioridade da informação de sua descoberta; o invento de Morse, por sua vez, enfocava o sigilo e a brevidade das comunicações; já os

[1] Observações de Saturno no sítio eletrônico "The Galileo Project", da Rice University. Disponível em: <http://galileo.rice.edu/sci/observations/saturn.html>. Acesso em: 23 maio 2017.

algoritmos utilizados pelas corporações Google, Facebook, Microsoft, Netflix e Amazon, dentre outras, evidenciam a adoção de práticas de amplo monitoramento informacional sobre os indivíduos conectados à internet, ensejando condições propícias a regimes de vigilância e controle de dados pessoais.

Admitindo a evolução da tecnologia no decurso do tempo, propomos a ideia de "arcanos tecnológicos" para compreender e abarcar os segredos enrascados na sociedade em rede do século XXI. Em latim, "arcanos" (*arcanus*) referem-se a coisas misteriosas e enigmáticas; no mundo greco-romano (*αρκάν*), remetem-se às religiões de mistérios, sendo também estudados pela filosofia do simbolismo, dentre outros domínios do conhecimento. No tarot, representam tanto as cartas quanto aquilo que está nelas oculto; na alquimia, nomeiam poções mágicas às quais apenas os alquimistas têm acesso.

Para os fins deste artigo, a apropriação que fazemos do termo traça uma ponte conceitual com os "arcanos de Estado" (*arcana imperii*), descritos em 1605 por Arnold Clapmarius para ressaltar que, por trás das diferentes formas de governo, se ocultam os verdadeiros objetivos e meios da dominação política. Para Catanzariti (2012), o termo "arcano" mostra-se mais fértil do que "segredo" ao se aproximar mais da política, permitindo explorar a gradativa falta de visibilidade do poder como estratégia de controle.

Resta claro que os "arcanos" refletem contextos sociais, econômicos e políticos específicos, ancorados em determinado espaço e tempo. Os "arcanos tecnológicos" que iremos abordar são aqueles que acobertam as práticas difusas de vigilância que permeiam os fluxos informacionais deste ainda jovem século XXI, convergindo para a proposta conceitual de "*panspectron*" apresentada por Manuel DeLanda no livro *War in the age of intelligent machines* (1991) e posteriormente atualizada por Sandra Braman (2006a; 2006b). Convém sobrelevar que, além de instituições estatais, grandes corporações globais esbarram em questões e dilemas relativos à informação em rede, como as várias formas de opacidade, a privacidade dos indivíduos e os sistemas de governança.

Para caminharmos em direção a um debate que contemple temas contemporâneos relacionados à ética em informação, primeiramente iremos expor o contexto de vigilância do Estado informacional e o modelo "*panspectron*", detendo especial atenção aos efeitos da promulgação do Ato Patriota (*Patriot Act*) em 2001, medida legislativa norte-americana que autoriza práticas de monitoramento de dados em massa sob o pretexto de detectar e prevenir ações terroristas. Em seguida, a noção de segredo será abordada por uma perspectiva social e pelo viés do ciberativismo, abordando a questão dos vazamentos intencionais de informações governamentais sigilosas. Finalmente, examinaremos a dimensão ética que permeia a presença dos algoritmos nas redes digitais, explorando as principais barreiras ao desafio de desvelar a metafórica "sociedade da caixa preta" (*black box society*) de Pasquale (2015).

2 VIGILÂNCIA NO ESTADO INFORMACIONAL

Nas últimas décadas, o alvorecer do paradigma tecnológico digital realçou significativas mudanças na cadeia de circulação de informação, alterando padrões e comportamentos, permitindo novas abordagens e relações fragmentadas através do advento da rede mundial de computadores. A composição de densas e extensas teias de informação que emaranham saberes e poderes encontra nas tecnologias de informação e comunicação seu epicentro.

Nesse contexto, as relações informação-poder decorrentes da reconfiguração das dinâmicas de produção, processamento, fluxo e disseminação da informação se manifestam imbricadas às tecnologias digitais e ubíquas, pertinentes ao atual regime global de informação:

> Com ênfases nas dinâmicas antes que nas estruturas, o regime de informação permitiria associar a ancoragem espaço-temporal e cultural das ações de informação aos contextos regulatórios e tecnológicos que intervém e perpassam diferentes domínios de atividade, agências e organizações (GONZÁLEZ DE GÓMEZ, 2012, p. 56).

Para Sandra Braman (2006a), o estudo dessa nova configuração é marcado pela transversalidade da infraestrutura de informação. Ao associar o

conceito de “regime de informação” (conforme proposto por Bernd Frohmann e posteriormente discutido por González de Gómez e outros autores da Ciência da Informação) à emergência de um regime global de informação (BRAMAN, 2004), a autora reforça os elementos discursivos, normativos e culturais que se manifestam nas relações entre os agentes que compõem esse regime.

As noções de governo, governança e governabilidade perante a permeabilidade das fronteiras geopolíticas ensejam uma nova conjuntura de papeis desempenhados por agentes estatais e não-estatais, conformando-se aos espaços e termos estabelecidos para a elaboração e implementação de políticas de informação do Estado informacional. Em tal cenário, as tecnologias digitais compreendem uma questão crucial do regime global de informação, na medida em que afetam a autonomia de seus agentes ao alterar os graus de liberdade disponíveis.

A rede mundial de computadores evidencia um espaço politicamente contestado, apresentando novas e instáveis relações de poder entre governos, cidadãos e corporações. Se por um lado as redes digitais dão voz aos indivíduos e permitem que os cidadãos desafiem o poder constituído, por outro lado também autoriza diferentes regimes de governo a dedicar recursos técnicos e humanos para apurar estratégias de potencializar o uso das tecnologias digitais em seu favor, transformando a internet em uma plataforma de extensão de suas práticas de poder. A emergência de um regime global de informação reforça o papel da criação, processamento, fluxo e uso da informação como ferramentas de poder nas relações globais. Por esse ângulo, destacam-se as práticas de vigilância adotadas por governos, na medida em que a política de informação enseja também outros tipos de objetivos políticos.

No que tange aos estudos sobre vigilância, recorrentemente se invoca o conceito modelo do *panopticon,* arquitetado pelo jurista inglês Jeremy Bentham no fim do século XVIII. Popularizado em 1979 por Michel Foucault (2012) para exemplificar a vigilância exercida no que chamou de “sociedade disciplinar”, o *panopticon* benthamiano é reexaminado dois séculos depois sob o viés social das instituições e do poder, considerando a emergência das tecnologias disciplinares. Para Foucault, um elemento central do panoptismo residiria no

fato de que a periferia nunca teria a completa certeza se e quando estaria sendo observada. Nessa configuração, a vigilância seria exercida de forma centralizada – na figura do vigilante ou de uma torre central de comando e controle – e limitava-se a determinados indivíduos, circunscritos a espaços de instituições totais (nos termos de Goffman) como presídios, escolas e manicômios.

A concepção do *panspectron*, apresentada por DeLanda para referir-se às práticas difusas de vigilância de Estado desde a segunda guerra e posteriormente atualizada por Braman para o universo informacional do século XXI, se diferencia do *panopticon* principalmente por compreender um espaço onde a vigilância opera ininterruptamente e sem o seu conhecimento pelo sujeito. Trata-se de uma situação na qual não é possível se esconder fisicamente em razão de câmeras, sensores térmicos, de movimento e reconhecimento facial, além de outros dispositivos de rastreamento, como explica o autor:

> Em vez de posicionar alguns corpos humanos em torno de um sensor central, uma multiplicidade de sensores é implantada em torno de todos os corpos: suas antenas, satélites espiões e interceptações de tráfego de cabo alimentam em seus computadores toda a informação que pode ser recolhida. Isso é então processado através de uma série de "filtros" ou listas de palavras-chave. O Panspectron não apenas seleciona certos corpos e certos dados (visuais) sobre eles. Em vez disso, ele compila informações sobre todos ao mesmo tempo, usando computadores para selecionar os segmentos de dados relevantes para suas tarefas de vigilância (DELANDA, 1991, p. 206, tradução nossa).

A vigilância sobre os indivíduos no atual Estado informacional sofre influência decisiva das tecnologias digitais de informação e comunicação. Se antes havia uma seleção dos indivíduos que se queria interceptar, a estratégia hoje é a de interceptação e armazenamento geral de dados, ou o que Müller-Maguhn chama de “armazenamento em massa – o armazenamento de todas as telecomunicações, todas as chamadas de voz, todo o tráfego de dados, todas as maneiras pelas quais se consomem serviços de mensagem de texto (SMS), bem como conexões à internet” (*apud* ASSANGE *et al.*, 2013, p. 56). Assim, grandes volumes de dados e metadados são coletados e acumulados

sem um propósito previamente definido, até que surja alguma demanda específica que suscite a mineração desses dados em informações já reunidas, a fim de obter as respostas necessárias.

Ainda que ambos os termos aludam aos mecanismos de controle engendrados por Bentham, no *panspectron* a vigilância é inevitável e realizada por algoritmos. Se no espaço arquitetado do *panopticon* o sujeito sabe que pode estar sendo observado, no ambiente do *panspectron* as práticas de monitoramento e controle revelam-se bem mais difusas: transportes urbanos, ruas, escolas, templos religiosos, estabelecimentos comerciais e, principalmente, o ambiente online. Insiste-se, orwellianamente: é praticamente impossível se esconder.

Outra questão consiste em que, para além do conhecimento sobre a situação de vigilância, não há o consentimento do sujeito quanto às suas informações reunidas:

> Os mecanismos de privacidade que parecem naturais para nós como criaturas biológicas – desligar as luzes e fechar as janelas, mover-se à noite, sussurrar, esconder-se – são irrelevantes, embora como organismos ainda nos empenhamos nessas práticas. No ambiente digital, privacidade, como invasões de privacidade, é em vez disso uma questão matemática. Aqueles que estão assistindo usam algoritmos para discernir padrões e relacionamentos que, por sua vez, identificam alvos de observação específicos, e os algoritmos são usados novamente para rastrear todas as atividades, transações e comunicações de indivíduos identificados como de interesse (BRAMAN, 2006b, não paginado, tradução nossa).

Ainda que seja reconhecida a inexistência de uma relação simétrica entre governo e cidadãos quanto à transparência de informações, a opacidade da coleta de dados pelo Estado informacional enfatiza a sua capacidade de reunir e processar informações sobre os indivíduos, de modo a conhecer cada vez mais sobre os mesmos, ao passo que estes são cada vez mais alijados das informações acerca do Estado (BRAMAN, 2006a, p. 314). Desse modo, a lógica do acesso aberto à informação governamental como um imperativo à cidadania, teoricamente facilitada pelos recursos tecnológicos digitais, é invertida em razão da expansão da definição dos tipos de uso da informação que podem ameaçar a segurança nacional (ibidem, p. 321).

Nessa inversão lógica, considerando-se o caráter intersubjetivo das práticas de informação, importa situar a vigilância abordada por Braman no âmbito das mudanças legislativas nos Estados Unidos após os ataques terroristas de 11 de setembro de 2001; em especial, a promulgação do Ato Patriota, assinado por George W. Bush. Com esmagadora aprovação do Congresso estadunidense, o discurso de aplicação da lei através de novas ferramentas para detectar e prevenir o terrorismo operou, em verdade, uma lógica reversa a que lhe deu origem, classificando cidadãos americanos comuns como potenciais suspeitos de terrorismo. Sobretudo, entende-se que essa medida legitimou a espionagem desses cidadãos pelo governo (BEZERRA, 2016), posto que são ampliadas as autorizações para o monitoramento de comunicações telefônicas ou por e-mail, históricos de pesquisas pessoais realizadas por motores de busca na internet e, ainda, o acesso a geolocalização.

O governo norte-americano tenta manter em sigilo os detalhes de diversas medidas antiterrorismo. Agora permitidas, as prisões secretas possuem critérios secretos em si mesmos. O que é definido como padrão para os níveis de ameaças terroristas nos Estados Unidos é secreto. Informações sobre a infraestrutura de plantas de edifícios do governo são secretas. Isto é, todos os esforços para manter potenciais terroristas desinformados também se refletem sobre os cidadãos, impedidos de avaliar a eficácia da atuação governamental. Práticas como as citadas inviabilizam a prestação de contas (*accountability*) de ações governamentais para a sociedade civil, prescindindo o governo da esfera ética que diz respeito à sua responsabilização. Nesse sentido, busca-se, a seguir, captar a essência da noção de segredo em certo *zeitgeist* a fim de compreender políticas de informação baseadas no sigilo, traçando-se uma ponte conceitual com a renovação da ideia tradicional de "arcanos" [2].

[2] Cabe, aqui, esclarecer que a opacidade dessas ações de informação não é exclusividade de governos. É clara a relação incongruente entre leis agressivas para a proteção do sigilo no mercado, porém, silenciosas quando abordam a privacidade dos indivíduos, o que expressa a assimetria de poder assoladora entre ambos os polos envolvidos. Segundo Pasquale, "as empresas buscam detalhes íntimos da vida de potenciais clientes e empregados, mas

3 DOS SEGREDOS AOS "ARCANOS"

A escrita secreta pode ser considerada tão antiga quanto a própria escrita em si. Sob uma perspectiva histórica, o início desta não implicou necessariamente a sua inteligibilidade. Em outras palavras, seria afirmar que o seu estabelecimento como tecnologia, descolado da efetivação de seu acesso e da competência necessária para compreendê-la, não garantiu aos indivíduos, naturalmente, a chave para o indecifrável.

Ao longo dos séculos, o acesso à informação mostra-se cada vez mais atrelado à dimensão do poder e às formas pelas quais é emanado nas sociedades. De tal modo, a tensão existente entre transparência e opacidade na disponibilização e difusão da informação soa anacrônica:

> Dificilmente podemos imaginar uma época em que não tenha existido a necessidade ou, pelo menos, o desejo de transmitir informações de um indivíduo a outro de modo a iludir a compreensão do público. Podemos muito bem, então, supor que a prática de escrever em cifras seja de grande antiguidade (POE, 1841, p. 33, tradução nossa).

As palavras, ora rearranjadas em anagramas, foram convertidas em cifras. Mais de um século após a suposição do escritor Edgar Allan Poe, o filósofo francês Gilles Deleuze (1992) reitera o uso da linguagem codificada por cifras no contexto de transição das sociedades disciplinares – influenciadas pela combinação entre vigilância hierárquica, sanções normalizadoras e o exame – para as sociedades de controle. Segundo o autor, "a linguagem numérica do controle é feita de cifras, que marcam o acesso à informação, ou a rejeição" (DELEUZE, 1992, p. 222).

Quase contemporâneo de Poe, o sociólogo alemão Georg Simmel (1999) também publica, em 1908, reflexões sobre as formas de interação social produzidas pelo segredo, levando-se em conta o embate entre a ocultação e a revelação de algo na vida do indivíduo em relação a outrem. Em especial, dois pontos são destacados por este autor. Primeiro, o fascínio do segredo, na medida em que a aura soturna que o encapsula gera a falácia de que tudo o

fornecem aos reguladores o mínimo de informação possível sobre suas próprias estatísticas e procedimentos" (PASQUALE, 2015, p. 4, tradução nossa).

que há de misterioso adquire importância e essencialidade. Deste modo, opera-se um sentimento de posse sobre quem os detém em relação aos demais que o ignoram:

> O segredo situa a pessoa numa posição de exceção; opera como uma atração pura e socialmente determinada. É basicamente independente do conteúdo que guarda, mas naturalmente torna-se cada vez mais efetivo na medida em que a sua posse exclusiva ganha em amplitude e em significado (SIMMEL, 1999, não paginado).

Outro tópico seria o fascínio da traição, uma vez que a posse do segredo comportaria uma tensão entremeada pela sensação de poder. A tentação de dissipá-lo, aliada aos perigos de ser descoberto, enfatizam o uso do segredo como técnica sociológica. Nesse sentido, para Simmel (1999), a existência do segredo, a tentativa de rompê-lo e o desejo de fazer parte dele estabeleceriam a interação humana.

Segredos são segredos justamente porque escapam ao que está instalado e estabilizado. De certo modo, enunciam uma expressão de potência e pressupõem um pacto; descrevem uma relação diferenciada e oferecem um risco.

Do fascínio ao risco, políticas de informação obtusas se intensificaram após a criação do *WikiLeaks*, organização que se propõe a divulgar, em sua plataforma online, polêmicos documentos secretos de governos, empresas e instituições, comprovando casos de má conduta e falta de responsabilidade ética e social. Criada em 2006 por Julian Assange, a plataforma para o vazamento de informações resulta da influência do movimento “cypherpunk” – com origem no início da década de 1990 –, cujo lema defende privacidade para os fracos e transparência para os poderosos (ASSANGE *et al.,* 2013).

Ciberativista australiano, Assange atenta para a força do que chamamos aqui de “arcanos tecnológicos”, reconhecendo o sigilo e a complexidade que os envolvem. Acima de tudo, destaca que a potencialidade emancipatória que a internet carrega em si pode ser ameaçada por usos escusos do governo e corporações, principalmente, do que chama de Estado de vigilância. Seu discurso é uma chamada à luta através da criptografia e da divulgação a público do testemunho documental de ações ilegais (ou, no mínimo,

questionáveis) de atores estatais e não-estatais, visando ao combate de forças repressoras no espaço da internet:

> Enquanto Estados munidos de armas nucleares podem impor uma violência sem limites a milhões de indivíduos, uma criptografia robusta significa que um Estado, mesmo exercendo tal violência ilimitada, não tem como violar a determinação de indivíduos de manter segredos inacessíveis a ele. Uma criptografia robusta é capaz de resistir a uma aplicação ilimitada de violência. *Nenhuma força repressora poderá resolver uma equação matemática.* [...] Lembre-se de que os Estados são os sistemas que decidem onde e como as forças repressoras são sistematicamente aplicadas. A questão de até que ponto as forças repressoras vindas do mundo físico podem se infiltrar no reino platônico da internet é respondida pela criptografia e pelos ideais dos cypherpunks (ASSANGE *et al.,* 2013, não paginado, grifo nosso).

Sete anos após a fundação do WikiLeaks, revelações sobre programas de vigilância em solo norte-americano atraíram os holofotes do mundo, gerando instabilidade global. Durante uma audiência do Comitê de Inteligência do Senado dos EUA, em março de 2013, James Clapper, ex-diretor de Inteligência Nacional dos Estados Unidos negou ao senador democrata Ron Wyden a prática de coleta de quaisquer tipos de dados pela Agência de Segurança Nacional (NSA) sobre os cidadãos americanos. Menos de três meses depois do episódio, Edward Snowden, antigo agente contratado pela NSA, vazou no WikiLeaks documentos que, além de refutar a afirmação de Clapper, expunham a estrutura rizomática dos programas de vigilância em massa sobre as comunicações dos cidadãos, utilizados por aquela agência: históricos de busca em navegadores da internet, logs de chats, conteúdo de e-mails, áudios pessoais e geolocalização.

O embate entre a exposição da privacidade dos indivíduos sem seu consentimento por meio do acesso aos dados e metadados individuais pelo governo fora transparecido por Snowden, porém a um elevado custo pessoal, como relata:

> Estou disposto a sacrificar tudo isso porque não posso, em boa consciência, permitir que o governo dos EUA destrua a privacidade, a liberdade na internet e as liberdades básicas para as pessoas ao redor do mundo com esta massiva máquina de vigilância que estão construindo *secretamente*

> (GREENWALD; MacASKILL; POITRAS, 2013, tradução e grifo nossos).

Nessa perspectiva, o vazamento de documentos da NSA pela mídia através de Snowden amplia o debate sobre os "arcanos" tecnológicos de Estado, aprofundando as noções tradicionais de segredo pelo viés da tensão entre privacidade básica e vigilância na internet. Um dos pontos mais nevrálgicos para a compreensão de tais "arcanos" consiste no desvelamento do processamento das informações algorítmicas em diversas plataformas da rede mundial de computadores.

4 A ÉTICA DOS ARCANOS TECNOLÓGICOS

Nos contornos do *panspectron* que se realiza no ambiente *online*, reverberam-se a capacidade e os propósitos de governos e corporações de coletarem dados pessoais dos usuários da rede. Quando compiladas, tais informações retratam comportamentos e hábitos individuais com tamanho requinte de detalhes que extrapolam as perspectivas de garantias de direitos a privacidade no uso da internet.

Contudo, para que esse robusto volume de dados pessoais seja processado e categorizado, a fim de servir a um fim qualquer, seu processamento e categorização deve ser realizado via complexas operações algorítmicas sistematizadas por "caixas pretas". Tal recurso metafórico remete tanto à modelagem do sistema de caixa preta, abordado pela ciência da computação, como também à utilização de regras, procedimentos e decisões desconhecidas para o processamento de tais dados, estruturando-se, portanto, de maneira opaca.

De acordo com a ciência da computação, algoritmos são "uma descrição do método pelo qual uma tarefa deve ser realizada" (GOFFEY *apud* ANANNY, 2016, p. 97, tradução nossa), também podendo ser resumidos como conjuntos de instruções automatizadas conforme uma dada sequência lógica para executar uma determinada tarefa. Algoritmos de encriptação, recomendação ou preditivos, por exemplo, integram sistemas bancários, de crédito, controle de

tráfego de veículos, seguradoras, comércios eletrônicos, dentre outros estabelecimentos, a fim de mitigar as dificuldades de ambientes urbanos. Apesar de não estarem presentes apenas na internet, é nesse ambiente em que os algoritmos mais causam impacto sobre o cotidiano dos indivíduos. Facebook, Google, Netflix, Spotify, Amazon, Yahoo!, Uber e Waze são algumas das plataformas da internet que utilizam algoritmos, embora outros usos diversos também sejam possíveis, a exemplo da detecção de fraudes bancárias e do controle do nível de glicose para transplantes de pâncreas.

A criação de perfis a partir de grandes massas de dados disponíveis nas plataformas supracitadas permite a geração de fluxos de entrada de estímulos para, então, propor-se saídas de respostas a eles, customizando-se a experiência *online* de cada indivíduo. Todavia, não é claro para os indivíduos o mecanismo decisional operado por estas caixas pretas, muitas vezes, verdadeiros mistérios para os próprios desenvolvedores dos códigos algorítmicos. Quem promove esse fluxo de entrada e saída de dados coletados? Como são coletados? Para quê são coletados? Indagações dessa natureza suscitam mais questionamentos do que respostas esclarecedoras.

Considerando que os algoritmos tomam decisões que podem influenciar a vida dos indivíduos, se uma decisão é tomada por motivos que não são claros a quem vai se submeter a ela, assume-se que esse indivíduo terá menos poder sobre os aspectos que irão gerar a decisão.

A falta de consciência plena dos indivíduos sobre como o *Big Data*[3] afeta as suas vidas, de opções quanto à gestão de consentimentos e da regulamentação dos conteúdos dos termos de uso e política de privacidade de aplicações na internet – quem efetivamente os lê? – desenha um cenário de caos ordenado por governos e corporações.

Na arena de disputas da internet, a proteção de códigos matemáticos por sigilos, abrigados em segredos e complexidades, promove a ampliação da noção greco-romana de “arcanos” para “arcanos” tecnológicos digitais, uma vez que as decisões processadas pelas caixas pretas são assumidas como

[3] *Big Data* é um termo que se refere a um volume massivo de dados estruturados e não estruturados que é tão grande que se torna difícil de processar usando técnicas tradicionais de banco de dados e *software*.

neutras e meramente técnicas para a manutenção dos interesses dos agentes envolvidos na governança algorítmica. Quem controla, utiliza e implementa os algoritmos os faz em razão de algum interesse, motivo pelo qual tais “arcanos” alteram a dinâmica das relações de poder.

Frank Pasquale (2015) enfatiza a importância da complexidade dessas caixas pretas, cuja legibilidade se restringe a um público especializado, para a manutenção da barreira do acesso aos conteúdos que ocultam: “desconstruir as caixas pretas do Big Data não é fácil. Ainda que elas desejassem expor seus métodos ao público, a internet moderna e os setores bancários colocam desafios difíceis para o nosso entendimento de seus métodos” (PASQUALE, 2015, p. 6, tradução nossa).

Desse modo, a transparência em si não é um elixir milagroso, na medida em que depende de artefatos cognitivos, como a linguagem, para se tornar inteligível aos cidadãos. Eis a imprescindibilidade de agentes reguladores na mediação desse processo:

> O governo frequentemente intervém para exigir divulgação e formatos de "linguagem simples" para consumidores, mas os financeiros esquivaram-se das regras de transparência com transações mais complexas. Quando isso acontece, sem ganhos substanciais em eficiência, os reguladores devem intervir e limitar a complexidade. *A transparência não é apenas um fim em si mesma, mas um passo provisório no caminho da inteligibilidade* (PASQUALE, 2015, p. 8, tradução e grifos nossos).

Convergindo com o pensamento de Pasquale, o irlandês John Danaher (2016) problematiza a relação entre os algoritmos e a opacidade no interior das caixas pretas. Este autor alega que, em geral, se presume como os dados que alimentam o algoritmo são produzidos: os próprios indivíduos os produzem através de suas atividades. Também se conhece normalmente as saídas do algoritmo: os indivíduos são informados ou podem inferir como este categorizou os dados. O que persiste velado nesse processo é o que ocorre no interior da caixa preta: não se sabe quais bits de dados são selecionados pelo algoritmo e como ele usa esses dados para gerar classificações.

John Danaher, professor afiliado ao Institute for Ethics and Emerging Technologies, sugere o termo “algocracia” para abarcar a emersão de uma

governança algorítmica que acarreta problemas diretamente sobre a legitimidade moral ou política dos processos públicos de tomada de decisões:

> Eu uso o termo “algocracia” para descrever um tipo particular de sistema de governança, organizado e estruturado com base em algoritmos programados por computador. Para ser mais preciso, eu o uso para descrever um sistema no qual os algoritmos são usados para coletar, agrupar e organizar os dados sobre os quais as decisões são tipicamente feitas, e ajudar na forma como esses dados são processados e comunicados através do sistema de governança relevante. Ao fazê-lo, os algoritmos estruturam e restringem as maneiras pelas quais os seres humanos dentro desses sistemas interagem uns com os outros, os dados relevantes e a comunidade mais ampla afetada por esses sistemas (DANAHER, 2016, p. 3, tradução nossa).

O autor argumenta que a tomada de decisões baseada em algoritmos, ao ignorar questões como proteção de dados e privacidade, representa uma ameaça significativa à legitimidade de tais processos. No contexto de crescimento de sistemas algocráticos, o autor aponta duas preocupações centrais, que devem ser entendidas de forma balanceada. A primeira relaciona-se com as formas pelas quais os dados pessoais são coletados e utilizados por esses sistemas, observando que o ocultamento de tais formas implicaria também a ausência de consentimento por parte dos indivíduos. Já a segunda volta-se para a base intelectual e racional desses sistemas algocráticos, considerando o interesse de seus desenvolvedores de que tais sistemas permaneçam inacessíveis ou ininteligíveis à compreensão humana (DANAHER, 2016, p. 6).

Outra abordagem relevante sobre o tema é a da professora da Escola de Informação da Universidade da Califórnia, Jenna Burrell (2016), que, ao destacar as variadas implicações da classificação algorítmica, especialmente a desigualdade econômica e a mobilidade social, distingue a opacidade em três formas: como segredo corporativo ou de Estado; como analfabetismo técnico; e resultante das características dos algoritmos de *machine learning* e a escala necessária para aplicá-los de forma útil.

Retornando a Pasquale (2015, p. 213), vemos que a prestação de contas requer o julgamento humano, uma vez que apenas humanos podem exercer a função crítica de garantir que, com a crescente automatização da

comunicação (e, consequentemente, das relações sociais), a dominação e a discriminação não sejam construídas e embutidas de modo invisível nos códigos algorítmicos.

Importa atentar para o fato de que os algoritmos não são um mal em si, mas alguns passos precisam ser dados pela sociedade na direção da regulação de direitos e tecnologias para torná-los mais próximos e confiáveis. Algoritmos são construídos a partir do comportamento e preferências dos indivíduos, o que significa que características indesejáveis ou defeitos humanos podem ser replicados, estimulando condutas tendenciosas, falseadas e negativas.

Para tanto, alguns princípios para tornar a tomada de decisão algorítmica mais suscetível à prestação de contas mencionada consistem na responsabilidade, explicabilidade, acurácia, auditabilidade e senso de justiça, por exemplo. Ademais, ainda que se avente a possibilidade de um algoritmo auditar outro, não se deve olvidar o óbvio: os critérios e parâmetros dos algoritmos seguem sendo definidos por seres humanos.

Assim, entendemos que os princípios éticos que envolvem a sociedade de alguma maneira devem estar refletidos nos algoritmos. Nesse sentido, é pertinente a perspectiva de Mike Ananny (2016) sobre a ética pragmática dos algoritmos, ao afirmar que parte da compreensão do significado e do poder dos algoritmos consiste em indagar quais novas demandas podem ser feitas às estruturas éticas e, ainda, como podem ser responsabilizados por padrões éticos.

Para o autor, a definição tradicional de algoritmo apresentada pela ciência da computação ignora alguns de seus elementos sociológicos e normativos. Por essa razão, Ananny (2016, p. 97) utiliza o termo “algoritmos de informação em rede” (*networked information algorhythm)* para se distanciar do objeto de estudo da ciência da computação, com enfoque puramente matemático e mecanicista, aproximando-se de uma abordagem ética das relações sociotécnicas de produção, interpretação e confiança na formação processada por algoritmos computacionais:

> [...] os algoritmos estão embutidos nas estruturas sociotécnicas; eles são moldados por comunidades de prática,

> incorporadas em padrões e mais visíveis quando falham. Contudo, diferente da infraestrutura, a relevância, qualidade e estabilidade dos algoritmos dependem dos usuários finais. [...] Pouco importa se as "caixas pretas" do código de algoritmo (Pinch e Bijker, 1984) forem abertas ou compreensíveis, uma vez que só se tornam eticamente significativas em relação a outras (ANANNY, 2016, p. 98, tradução nossa).

Pensando nessas interrelações, Ananny define os “algoritmos de informação em rede” como uma reunião de código computacional institucionalmente estabelecido, práticas humanas e lógicas normativas que criam, sustentam e significam relações entre pessoas e dados através de uma ação quase autônoma, minimamente observável.

Recuperando as abordagens de Danaher (2016) e Burell (2016), Ananny (2016) argumenta a favor de uma ampliação do modelo de ética algorítmica para além de um debate acerca da transparência dos códigos algorítmicos. Deste modo, ainda que alguns indivíduos vislumbrem a prestação de contas como transparência de código, outros busquem a regulação estatal de empresas com monopólios algorítmicos e outros, ainda, objetivem construir a alfabetização algorítmica entre os usuários finais, é essencial que não se perca de vista a presença da questão da “imputabilidade moral de agentes e ações de informação” (GONZÁLEZ DE GÓMEZ, 2009, não paginado) entremeada entre zonas de sombra e luz, opacidade e transparência.

Diante da aproximação proposta aos “arcanos tecnológicos”, situar a ética dos algoritmos no contexto do Estado informacional permite-nos transpassar sinuosamente a discussão dos pontos de vista apresentados pelos três autores. Sobretudo, por meio de tais arcanos comunica-se sobre o poder que, na forma dessa comunicação, oculta-se, revelando-se, nesse ocultamento, como poder.

5 CONSIDERAÇÕES FINAIS

No Estado informacional, sob a influência do modelo *panspectron*, as tecnologias digitais tornam a vigilância cada vez mais onipresente e invisível, de modo que a privacidade de dados individuais coletados na internet

dificilmente é garantida por governos ou instituições privadas. Como formas de resistência efetivas a essa configuração sociopolítica, para além de puramente tecnológica, irrompem-se estratégias de contravigilância, vazamentos de documentos oficiais por ciberativistas, atuações da mídia em casos específicos e medidas para a prestação de contas pela sociedade.

O processo de governança global do ciberespaço é novo e desconhecido, dada a sofisticação e complexidade tecnológica envolvida. A legalidade tradicional presente em todo ordenamento jurídico urge pela definição de novos parâmetros para o seu reconhecimento no ambiente digital. É necessário que os algoritmos sejam minimamente regulados, de um ponto de vista técnico, sujeitos a cumprir com certas legislações.

Numa espécie de caos ordenado, às escuras, processos algorítmicos se espraiam pela rede mundial de computadores para operacionalizar a tomada de decisões, sendo estas baseadas em comportamentos e condutas humanas esquadrinhadas a partir de nossas “pegadas digitais”. Uma ética pragmática dos algoritmos deve permear diversas abordagens relacionadas à transparência *versus* opacidade informacional, iluminando a prestação de contas à sociedade tanto por agentes estatais quanto pelos não-estatais. Reinos digitais formados por oligopólios da internet precisam aceitar a mesma carga de imputabilidade e responsabilização social que exigem de indivíduos; para tanto, é imprescindível o aumento da conscientização de todos sobre as estruturas de poder que transpassam os arcanos tecnológicos, a fim de que possam ser minimamente desvelados e, assim, conhecidos pela sociedade.

REFERÊNCIAS

ANANNY, M. Toward an Ethics of Algorithms Convening, Observation, Probability, and Timeliness. **Science, Technology & Human Values**, v. 41, n. 1, p. 93-117, 2016.

ASSANGE, J. *et al*. **Cypherpunks:** liberdade e o futuro da internet. São Paulo: Boitempo, 2013.

BEZERRA, A. C. Privacidade como ameaça à segurança pública: uma história de empreendedorismo moral. **Liinc em Revista**, v. 12, n. 2, p. 231-242, 2016.

BURRELL, J. How the machine 'thinks': Understanding opacity in machine learning algorithms. **Big Data & Society**, v. 3, n. 1, p. 1-12, 2016. Disponível em: <http://bds.sagepub.com/content/3/1/2053951715622512>. Acesso em: 26 nov. 2016.

BRAMAN, S. **The Emergent Global Information Policy Regime**. New York: Palgrave Macmillan, 2004.

_____. Information, policy, and power in the informational state. In: **Change of state:** Information, policy, and power. Cambridge: MIT Press, 2006a, p. 01-08. Disponível em: <https://pantherfile.uwm.edu/braman/www/bramanpdfs/028_Braman_Chapt9.pdf>. Acesso em: 14 nov. 2016.

_____. Tactical memory: The politics of openness in the construction of memory. **First Monday**, v. 11, n. 7, jun. 2006b.

CATANZARITI, M. *et al.* New arcana imperii. **Journal on European History of Law**, n. 2, p. 59-67, 2012. Disponível em: <http://escholarship.org/uc/item/81g0030z>. Acesso em: 14 nov. 2016.

DANAHER, J. The threat of algocracy: Reality, resistance and acommodation. **Philosophy & Technology**, p. 01-24, 2016. Disponível em: <http://philpapers.org/rec/DANTTO-13>. Acesso em: 26 nov. 2016.

DELANDA, M. **War in the age of intelligent machines.** New York: Zone Books, 1991.

DELEUZE, G. Post-scriptum sobre as sociedades de controle. In:_____. **Conversações**: 1972-1990. Rio de Janeiro: Editora 34, 1992. p. 219-226.

FOUCAULT, M. **Vigiar e punir:** nascimento da prisão. Petrópolis: Vozes, 2012.

GLEICK, J. Um sistema nervoso para a Terra. In: _____. **A informação:** uma história, uma teoria, uma enxurrada. São Paulo: Companhia das Letras, 2013. p.134-175.

GONZÁLEZ DE GÓMEZ, M. N. Desafios contemporâneos da ciência da informação: as questões éticas da informação. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO (ENANCIB), 10, 2009, João Pessoa. **Anais....** João Pessoa: UFPB, 2009.

_____. Regime de informação: construção de um conceito. **Informação e Sociedade**, v. 22, n. 3, p. 43-60, 2012.

GREENWALD, G.; MacASKILL, E.; POITRAS, L. Snowden: the whistleblower behind the NSA surveillance revelations. **The Guardian**, v. 9, n. 6, 2013. Disponível em: <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>. Acesso em: 14 nov. 2016.

MacKINNON, R. **Consent of the networked:** The Worldwide Struggle for Internet Freedom. New York: Basic Books, 2012.

PASQUALE, F. **The black box society:** The secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

POE, E. A. A few words on secret writing. **Graham's Magazine**, v. 19, p. 33-38, 1841. Disponível em: <http://www.eapoe.org/works/essays/fwsw0741.htm>. Acesso em: 13 nov. 2016.

RICE UNIVERSITY. **The Galileo Project.** Disponível em: <http://galileo.rice.edu/>. Acesso em: 13 nov. 2016.

SIMMEL, G. O segredo. **Revista de Ciências Sociais Política & Trabalho**, v. 15, p. 221-226, set. 1999.

UNVEILING TECHNOLOGICAL ARCANES: ALGORITHMIC ETHICS IN THE INFORMACIONAL STATE

ABSTRACT

Introduction: the information surveillance diffuse practices by state institutions and large corporations of the 21st century run into issues and dilemmas related to the networked information such as the various forms of opacity, individuals' privacy, and governance systems. **Objective**: we propose the idea of "technological arcanes" to understand the secrets tangled in the networked society, in order to promote a debate that includes contemporary themes related to information ethics. **Methodology**: through a bibliographic review, we explore the context of informational state surveillance and the "*panspectron*" model; the notion of secrecy by the social perspective and by the approach of cyberactivism; and the ethical dimension that permeates the presence of algorithms in digital networks. **Results**: we see that the technological sophistication and complexity involved in the global governance process of cyberspace constitute a new and unknown sociopolitical sphere. In this sense, effective forms of resistance such as counter-vigilance strategies, leaks of official documents by cyberactivists, media actions in specific cases, and measures for accountability by society emerge. **Conclusions**: a pragmatic ethics of algorithms should highlight accountability to society by both state and non-state actors. Digital realms made up of internet oligopolies need to accept the same burden of liability they require of individuals, making it imperative to raise everyone's awareness of the power structures that pass through the "technological arcanes".

Descriptors: Information ethics. Informacional state. Governance systems. Privacy. Surveillance.

DESVELANDO ARCANOS TECNOLÓGICOS: ÉTICA ALGORÍTMICA EN EL ESTADO INFORMACIONAL

RESUMEN

Introducción: las prácticas difusas de vigilancia informacional por instituciones estatales y grandes corporaciones del siglo XXI chocan en cuestiones y dilemas relativos a la información en red, como las diversas formas de opacidad, la privacidad de los individuos y los sistemas de gobernanza. **Objetivo**: proponemos la idea de "arcanos tecnológicos" para comprender los secretos que se han entramado en la sociedad en red, a fin de promover un debate que contemple temas contemporáneos relacionados con la ética de la información. **Metodología**: por medio de revisión bibliográfica, se exploran el contexto de vigilancia del Estado informacional y el modelo "*panspectron*"; la noción de secreto por la perspectiva social y por el enfoque del ciberativismo; y la dimensión ética que permea la presencia de algoritmos en las redes digitales. **Resultados**: verificamos que la sofisticación y complejidad tecnológica involucradas en el proceso de gobernanza global del ciberespacio configuran una nueva y desconocida esfera sociopolítica. En ese sentido, irrumpen formas de resistencia efectivas como estrategias de contravigilancia, filtración de documentos oficiales por ciberativistas, actuaciones de los medios en casos específicos y medidas para la rendición de cuentas por la sociedad. **Conclusiones**: una ética pragmática de los algoritmos debe enfatizar la rendición de cuentas a la sociedad tanto por agentes estatales como por los no estatales. Los reinos digitales formados por oligopolios de internet deben aceptar la misma carga de imputabilidad y responsabilización social que exigen de individuos, haciendo imprescindible el aumento de la concientización de todos sobre las estructuras de poder que traspasan los "arcanos tecnológicos".

Descriptores: Ética de la información. Estado informacional. Sistemas de gobernanza. Privacidad. Vigilancia.