SOCIEDADE DE VIGILÂNCIA: MANIFESTAÇÕES ARTÍSTICAS EM MEIO AO DESCARTE DA PRIVACIDADE

ANTENOR FERREIRA CORRÊA
LORENA FERREIRA ALVES

SURVEILLANCE SOCIETY: ARTISTIC MANIFESTATIONS AMIDST THE DISCARD OF PRIVACY

SOCIEDAD DE VIGILANCIA: MANIFESTACIONES ARTÍSTICAS EN MEDIO DEL DESCARTE DE LA PRIVACIDAD

RESUMO O objetivo deste texto é apresentar o modelo de sociedade de vigilância e refletir sobre os modos propostos por artistas para interrogá-lo e resistir a ele. Observa-se que os cidadãos têm abdicado do direito à privacidade em troca da conveniência trazida com os sistemas complexos de vigilância. Assim, a disponibilização de dados pessoais tornou-se moeda de troca para se viver em um mundo conectado. Neste contexto, analisamos algumas obras do campo da *artveillance*, baseadas na proposta da estética da vigilância, com o intuito de compreender como os artistas têm se posicionado frente a essa situação. Consideramos os conceitos de privacidade, *dataveillance* e a impossibilidade de os cidadãos do século XXI desautorizarem-na. As reflexões baseiam-se nos textos de Jan Holvast (2007) e David Lyon (2009).

PALAVRAS-CHAVE Sociedade de vigilância; Arte e vigilância; Privacidade; Estética da vigilância

Artigo inédito

Antenor Ferreira Corrêa*
Lorena Ferreira Alves**

*Universidade de Brasília (UnB), Brasil
https://orcid.org/0000-0003-0257-3059

**Universidade de Brasília (UnB), Brasil
https://orcid.org/0000-0002-2890-201X

O presente artigo foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001. Os autores, também, agradecem ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) pelo apoio concedido.

DOI: 10.11606/issn.2178-0447.ars2022.167047

ABSTRACT

The purpose of this text is to present the model of surveillance society and to reflect on the ways proposed by artists to interrogate and resist this model. More and more citizens have abdicated the right to privacy in exchange for the convenience brought with complex surveillance systems. Hence, giving away personal data has become the currency for living in a connected world. In this context, we consider some works in the field of artveillance, grounded on the idea of aesthetics of surveillance, in order to understand how the artists have positioned themselves in this situation. We consider the concepts of privacy, dataveillance and the impossibility for 21st century citizens to prevent it. These reflections are based on texts by Jan Holvast (2007) and David Lyon (2009).

KEYWORDS Surveillance Society; Surveillance Art; Privacy; Aesthetic of Surveillance

RESUMEN

El propósito de este texto es presentar el modelo de sociedad de la vigilancia y reflexionar sobre las formas propuestas por los artistas para interrogar y resistir este modelo. Cada vez más ciudadanos han abdicado del derecho a la privacidad a cambio de la comodidad que brindan los complejos sistemas de vigilancia. Por lo tanto, regalar datos personales se ha convertido en la moneda para vivir en un mundo conectado. En este contexto, consideramos algunos trabajos en el campo de la *artveillance*, fundamentados en la idea de estética de la vigilancia, para comprender cómo los artistas se han posicionado en esta situación. Consideramos los conceptos de privacidad, vigilancia de datos y la imposibilidad para los ciudadanos del siglo XXI de prevenirla. Estas reflexiones se basan en los textos de Jan Holvast (2007) y David Lyon (2009).

PALABRAS CLAVE Sociedad de vigilancia; Arte y vigilancia; Privacidad; Estética de vigilancia

INTRODUÇÃO

Uma situação comum no cotidiano dos usuários da internet é ter que clicar em caixas de texto autorizando o uso de *cookies* pelo site que está sendo acessado. O que alguns não sabem, entretanto, é o que esses *cookies* podem trazer riscos à privacidade do usuário. *Cookies* são códigos de texto armazenados no navegador (*browser*) utilizado para acessar as páginas da *web*. Esses códigos existem para a retenção de dados de navegação. Existem os *cookies* de sessão (temporários) e os *cookies* persistentes. *Cookies* de sessão guardam dados somente durante a navegação e, portanto, esses dados não permanecem armazenados na memória do navegador depois que a sessão é encerrada. Ao utilizar sítios de serviços bancários, por exemplo, é esse tipo de *cookies* que está em operação, pois, justamente como medida de segurança, não é desejado que os dados oferecidos ao banco permaneçam na memória do navegador. De modo contrário, os *cookies* persistentes conservam os dados fornecidos até que o usuário os apague da memória do navegador.

Ambos os tipos de *cookies*, quando criados pelo próprio sítio da internet que está sendo visitado, são chamados de *cookies* de primeira parte. Entretanto, a privacidade passa a ser ameaçada pelos *cookies* de terceira parte, que são os *cookies* colocados em páginas da *web* por terceiros, em geral corporações especializadas em *marketing* digital, com o objetivo de constituírem uma espécie de banco de dados dos usuários. Esse banco de dados, posteriormente, poderá ser utilizado para o envio de anúncios de produtos e serviços, mas também ser empregado com intuito de se cometer algum tipo de fraude, como roubo de senha ou de número de cartão de crédito, por exemplo. Ocorre que, devido à pressa, vontade ou mesmo necessidade de acessar alguma página ou sítio da *web*, acabamos por autorizar o uso desses *cookies*, muitas vezes sem pensar nas consequências que essa permissão pode trazer.

A Figura 1 mostra uma janela disparada automaticamente pelo sítio da Yahoo solicitando a autorização do usuário para, justamente, coletar dados com intuito de compreender seus interesses e enviar anúncios personalizados. Vale notar que nessa solicitação há o aviso de que esses dados serão utilizados pela Verizon Media e pelos seus grupos parceiros, apontando, assim, a ampliação do âmbito imediato do *site* que está sendo acessado, uma vez que os dados

coletados pelo dono desse sítio serão compartilhados com outras corporações. Procedimentos tais como o uso de *cookies* mostram que o monitoramento de dados de navegação em rede é a principal base de informações utilizadas por empresas comerciais e por órgãos governamentais para compreender, através de cálculos e estatísticas, o comportamento de tudo o que está conectado à rede mundial de computadores.

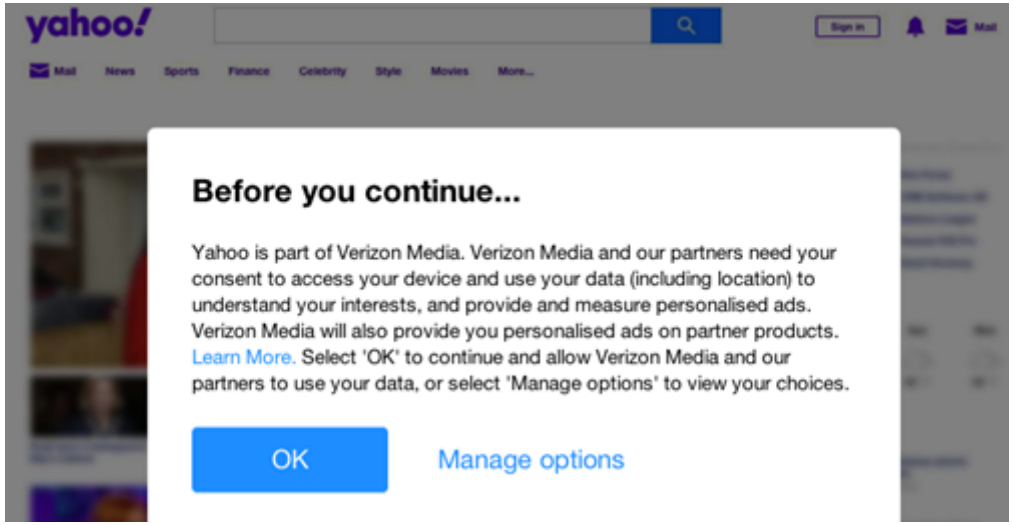

Figura 1.
Solicitação de autorização para coleta de dados do usuário no sítio da Yahoo.

Vale esclarecer que, embora muitos autores usem os substantivos "informação" e "dado" como sinônimos (observe as citações ao longo deste texto), existe uma diferença entre ambos. Dados são a matéria prima, por assim dizer, que, após reunida

e analisada, pode gerar informação. Nesse sentido, os dados são a base para inferir informações. "Dados são uma coleção de detalhes ou fatos que, como tais, não têm sentido; no entanto, quando esses detalhes ou fatos são colocados em um contexto que torna os dados utilizáveis, informações sérias podem ser extraídas" (HOLVAST, 2007, p. 765, tradução nossa). Como exemplo, imagine-se um programa de computador que coleta e envia a uma companhia X os dados de compras *online* feitas por um usuário Y. Digamos que, ao longo de um mês, Y tenha comprado grande quantidade de fertilizante. Esse dado, em si mesmo, permite alguma dedução, como por exemplo pode levar a pensar que se trata de um agricultor. Porém, digamos que seu endereço IP aponte uma área urbana. Isso pode levar a outro tipo de inferência, indicando a possível fabricação de explosivo, pois fertilizantes contêm amônia anidra (fórmula química NH_3), um gás usado para a produção de nitrato de amônio (NH_4NO_3) que pode também ser utilizado na fabricação de explosivos e bombas (usadas nos atentados em Oklahoma City, em 1995, e no ataque em Oslo, em 2011). Percebe-se, assim, que o mesmo dado levaria a informações diferentes, dependendo, portanto, da análise contextual dos dados coletados. Um agente que tivesse rastreado

essa comunicação como proveniente de uma área rural não ficaria preocupado (trata-se de um fazendeiro); todavia, a mesma compra em uma área metropolitana já "levantaria a bandeira vermelha", pois informaria sobre um perigo eminente.

A coleta de dados pessoais e dos rastros de navegação de cada usuário da *web* tornou-se moeda de troca para se viver em um mundo conectado. Esse ambiente no qual a maioria das pessoas está imersa pode ser pensado fazendo uso do conceito sociedade de vigilância, assunto tratado adiante. Desse modo, ao longo deste texto, objetivamos refletir sobre a sociedade de vigilância sob a perspectiva artística. Para tanto, interrogamos como os artistas têm se posicionado frente a essa situação. Será interessante, no entanto, antes de adentrarmos o assunto da vigilância e da quase impossibilidade de os cidadãos do século XXI desautorizarem-na, definir alguns termos essenciais para embasar a reflexão política e artística. Iniciamos, então, apresentando de modo sumarizado o conceito de privacidade e de termos afins, tais como intimidade, isolamento, esquecimento, esferas pública e privada.

DO CONCEITO DE PRIVACIDADE

Uma definição abrangente de privacidade está para ser criada. As áreas da biologia, direito e sociologia, por exemplo, trabalham com distintas definições do substantivo "privacidade" e do adjetivo "privado". No capítulo intitulado "What is Privacy?", Alexandra Rengel (2013) cita diversos autores que intentaram uma definição objetiva de privacidade, porém o assunto está longe de ser resolvido. Citando Robert Post, catedrático de direito da Yale Law School, Rengel destaca que "a privacidade é um valor tão complexo, tão enredado em dimensões concorrentes e contraditórias, tão inchado de significados diversos e distintos, que às vezes me desespero se esta pode ser utilmente abordada" (RENGEL, 2013, p. 31, tradução nossa). Jan Holvast realizou um dos mais abrangentes relatos históricos sobre privacidade, tendo identificado as várias vertentes pelas quais o tema tem sido abordado. Em sua análise, as discussões sobre a privacidade envolvem pontos de partida e bases diversas, tais como a necessidade de privacidade, o direito à privacidade, a invasão da privacidade, as funções da privacidade ou mesmo a proteção jurídica da privacidade. Em vista dessas distintas abordagens e focos, é difícil encontrar um denominador comum para uma definição de privacidade.

Apesar das tentativas de definição não encontrarem consenso, de modo simplista pode-se sugerir que o privado é aquilo que não é ou que foi retirado do domínio público. A etimologia latina confirma essa acepção do termo, uma vez que *privatus* significava aquele "retirado da vida pública" (WILLIAMS, 1988, p. 242, tradução nossa). Paralelamente, a partir dessa definição, nascem os conceitos de esfera pública e esfera privada. Mais especificamente, o professor de direito Wanderlei de Paula Barreto (2010, p. 136) esclarece que essa divisão de âmbitos surgiu no direito alemão com "a chamada teoria das esferas (*Sphärentheorie*) – esfera íntima intangível, esfera sigilosa e privada e esfera social". A teoria das esferas foi sistematizada a partir do livro de Heinrich Hubmann *Das Persönlichkeitsrecht* (1953), obra na qual o autor propôs a existência de três círculos no interior dos quais se desdobraria a personalidade humana: *Intimsphäre* (esfera íntima), *Geheimnisphäre* (esfera secreta) e *Privatsphäre* (esfera privada) (cf. BARRETO; SANTOS, 2006, p. 478-479). Implícito a esse conceito está o fato de que a privacidade passa a ser considerada como um direito do ser humano. Na França, a primeira jurisprudência relatada a reconhecer o direito à privacidade ocorreu em 1856 em um caso envolvendo a atriz Elisa Rachel Felix (cf. VIEIRA, 2016, p. 21). Vários autores concordam,

no entanto, que a publicação de *The Right to Privacy*, de Samuel Dennis Warren e Louis Demitz Brandeis em 1890, na *Harvard Law Review*, tornou-se um marco na história do direito nos Estados Unidos e, consequentemente, influenciou outros países[1]. Este texto fundamentou os princípios constitucionais[2] estadunidenses e gerou a definição de privacidade até hoje adotada: "the right to be let alone", que ao pé da letra seria "o direito de ser deixado a sós". A forma adotada no judiciário brasileiro, todavia, é "o direito de ser deixado em paz".

A privacidade, tratada legalmente como um direito dos cidadãos, acaba por gerar uma série de questionamentos: onde termina a esfera privada e começa o direito à informação pública? Quais são os limites da privacidade de uma personalidade pública? Governantes têm direito à privacidade quando do exercício de funções com mandato público? Um sujeito agente de um ato público atroz tem direito ao esquecimento? O Estado tem o direito de valer-se de todos os meios para obter informação privada dos cidadãos?

São corriqueiros os casos relatados na imprensa de invasão ou de garantia da privacidade de celebridades. No entanto, a mesma garantia da inviolabilidade da privacidade pode levar a situações e entendimentos completamente diferentes. Rengel relata uma ação

movida contra funcionários do serviço de proteção à infância que haviam sido informados sobre abusos cometidos cotidianamente contra uma criança. Todavia, os funcionários não tomaram qualquer atitude para coibir ou impedir esses abusos, uma vez que não tinham o direito de adentrar ao domicílio onde vivia aquela criança sem violar o direito à privacidade do lar. No julgamento da ação, "a Suprema Corte considerou que as autoridades estaduais de proteção à criança não eram, na ausência de discriminação, legalmente responsáveis por uma criança que foi permanentemente ferida por abuso em casa, de que os funcionários estavam cientes" (RENGEL, 2013, p. 37, tradução nossa). Esse fato levaria a questionar que tipo de "proteção" está realmente sendo oferecida à infância, uma vez que os responsáveis por essa suposta proteção se sentem impedidos de agir pelo receio de ferirem o direito à privacidade.

Não obstante, o direito à privacidade foi radicalmente transformado após atentados terroristas que ocorreram em diversos países. Um dos momentos que mais impactou a garantia desse direito e levou o mundo a uma nova condição jurídica foi o ataque contra as Torres Gêmeas do conjunto World Trade Center em Nova York, no dia 11 de setembro de 2001. Esse atentado, que se crê ter sido levado a cabo pelo grupo extremista islâmico Al Qaeda, fez com que

os cidadãos reconsiderassem seu direito à privacidade em troca da segurança que uma vigilância ubíqua e invasiva pudesse fornecer. Segundo Rengel, "a aprovação da legislação antiterrorista afetando as liberdades civis após o 11 de setembro não se limitou aos Estados Unidos" (RENGEL, 2013, p. 174). Algumas semanas após os ataques de 11 de setembro, o então presidente George Bush assinou o que ficou conhecido como Ato Patriótico (Patriot Act), um documento de mais de 300 páginas promulgando uma legislação cujo intuito era, principalmente, "melhorar as habilidades de aplicação de lei dos Estados Unidos para detectar e deter o terrorismo. O nome oficial do Ato Patriótico é: União e fortalecimento da América pelo fornecimento de ferramentas apropriadas para interceptar e obstruir o terrorismo"[3]. O fato é que a promulgação deste e de outros documentos afins levou o mundo a uma nova condição de medo e de restrição de liberdades e direitos, isto é, à chamada sociedade de vigilância.

Obviamente, muitos pensadores, ativistas dos direitos humanos e artistas questionam e contestam os supostos benefícios trazidos com a limitação de liberdades e de direitos dos cidadãos impostos por legislações que visam a combater o terrorismo. Dentre várias, uma das exposições que questionou o direito de

os governos e corporações coletarem e armazenarem informações oriundas da vigilância dos diversos meios de comunicação foi "Watching You, Watching Me: A Photographic Response to Surveillance"[4]. O texto da apresentação dessa exposição deixava claro:

> À medida que governos e empresas de todo o mundo expandem seus esforços para rastrear as comunicações e atividades de milhões de pessoas, isso não apenas ameaça nosso direito à privacidade, mas também abre a porta para que informações sejam coletadas e usadas de maneiras repressivas, discriminatórias e congelem a liberdade de discussão e de expressão. (STAATLICHE Museen zu Berlin, 2017)

Dentre as várias obras exibidas, a série *Blue Sky Day* do premiado fotógrafo belga Tomas van Houtryve convida a pensar sobre os atuais mecanismos e tecnologias de vigilância com as quais convivemos sem ao menos nos darmos conta. A série é um conjunto de fotografias aéreas realizadas por um drone (veículo aéreo não tripulado e controlado remotamente). Houtryve utilizou-o para registrar imagens de localidades dos Estados Unidos similares àquelas que foram alvos de ataques no exterior. Desse modo, Houtryve força a refletir não somente sobre vigilância ou guerra, mas também sobre os efeitos trazidos com essas ações, uma vez que a narrativa das fotos instiga a pensar que os alvos bombardeados no exterior

por drones americanos também existem nos Estados Unidos e estão sob vigilância e sujeitos ao mesmo tipo de ação militar. A Figura 2 mostra uma das imagens da série *Blue Sky Day*, foto da fronteira dos Estados Unidos com o México intitulada *Homeland Secutity* (2013). A série de Houtryve recebeu diversos prêmios, como o ICP Infinity Award for Photojournalism, e foi escolhida dentre as dez fotos mais importantes de 2014 pela revista *Time Magazine*.

Figura 2.
Tomas Van Houtryve, *Homeland Security,* 2013, da série *Blue Sky Days*.
Fonte: https://tomasvh.com/works/blue-sky-days/. Acesso em: 30 nov. 2022

SOCIEDADE DE VIGILÂNCIA

A sociedade de vigilância (*surveillance society*) inicialmente dizia respeito, segundo David Lyon (2009), à vigilância relacionada a áreas de segurança e administração de cidadãos por parte do Estado, como o controle de imigração, passaportes e cartões de identidade pessoais. Lyon informa que esse termo foi utilizado pela primeira vez pelo sociólogo Gary T. Marx em 1985 e passou a representar a vigilância sob as novas tecnologias presentes no cotidiano dos cidadãos, as quais, justamente, procedem coletando dados sobre os hábitos de compra e outras atividades ordinárias. Esses dados são, então, verificados, rastreados e monitorados para diversos fins, e os consumidores são classificados por perfis pelas corporações que são, em grande parte, responsáveis pela coleta de dados.

A sociedade de vigilância, "uma sociedade onde a tecnologia de vigilância é amplamente usada para monitorar as atividades cotidianas das pessoas" (COLLINS English Dictionary, tradução nossa), refere-se, assim, a uma ramificação do monitoramento de ações humanas que percorre todos os âmbitos da vida de um indivíduo, âmbitos estes que vão para além do propósito inicialmente aplicado a essas tecnologias introduzidas no cotidiano social, ou seja, a segurança dos cidadãos. Tecnologias de vigilância, como câmeras

de circuito fechado de televisão, captação e gravação sonora e monitoramento de localização, foram convertidas e incorporadas em dispositivos de comunicação e serviços de assistência pessoal, como os *smartphones* e os assistentes virtuais inteligentes (Alexa, Siri, Google Assistant). Interagimos atualmente com as interfaces de monitoramento desses dispositivos, trazendo-as para dentro de nossas casas e vestindo-as em nossos corpos como instrumentos para experienciar os mundos personalizados que elas nos oferecem.

Como passamos a aceitar e incorporar essas tecnologias de vigilância capazes de influenciar nossos comportamentos e escolhas? É possível pontuar fatos que se tornaram responsáveis, em grande medida, pela inserção da vigilância de dados pessoais e da invasão de privacidade dos usuários da internet. Um dos principais, como já mencionado, foi a introdução da vigilância massiva dos meios de comunicação em escala mundial após os atentados de 11 de setembro de 2001 nos Estados Unidos. O discurso em prol da segurança global elaborado por setores do governo estadunidense definiu formas de aplicação de tecnologias de vigilância de dados na internet, inicialmente com o aval dos cidadãos que aceitavam o argumento de líderes do governo e abriam mão da privacidade em troca da suposta segurança oferecida pelas tecnologias de vigilância.

Laura M. Lacaze (2016), considerando a propaganda veiculada pelas autoridades dos Estados Unidos durante a implementação da vigilância massiva dos meios de comunicação, entende que esse objetivo foi atingido, em grande parte, devido ao estabelecimento de um ambiente de medo e da urgência em prevenir e combater outros atentados terroristas e cyberataques. Desse modo, o país se posicionou como autoridade contraterrorista, propagandeando a vigilância massiva, potencializada com a coleta de dados na internet, como única maneira efetiva para estabelecer a proteção dos cidadãos. Com isso, a regulamentação da vigilância ampla e geral foi implementada no Ato Patriótico, que legitimou a prática da interceptação de telefones e de e-mails por parte das agências e órgãos de segurança dos Estados Unidos, como NSA, CIA e FBI.

A utilização dos dados de navegação dos usuários e de suas informações pessoais, tais como nome, idade e localização, não tardou a ser aplicada como procedimento para prever possíveis públicos-alvo por parte de empresas que estariam hábeis a traçar perfis baseados nas preferências dos usuários e, assim, direcionar conteúdos publicitários, oferecendo produtos. É justamente por conta disso que a parte majoritária de serviços disponíveis na internet, como *chats*, redes sociais e *sites* de busca, opera de

acordo com a administração algorítmica de dados interceptados, tornando a internet a tecnologia de vigilância mais poderosa em termos de eficiência de monitoramento de dados pessoais.

O consentimento à vigilância de dados pessoais, quer esta ocorra no computador pessoal ou em dispositivos portáteis de comunicação, dá-se pela conveniência que essas tecnologias podem oferecer. Robert M. Pallitto (2018) discute como barganhamos facilmente nossa privacidade pela facilidade de acesso a bens e serviços. Desse modo, torna-se cada vez mais difícil optar por não fazer parte de uma sociedade de vigilância ou mesmo de tentar reverter a trajetória do desenvolvimento tecnológico, que tende a uma vigilância cada vez mais incisiva. Considere-se, por exemplo, que muitos serviços (como a compra de passagens) têm o acesso disponibilizado através de sítios ou de aplicativos *online*, aplicativos estes que, além de exigirem dados do usuário, podem ser facilmente rastreados. Em vista desse estado de coisas, Pallitto comenta sobre a vindoura intensificação da vigilância que ocorrerá com a implantação definitiva da Internet das Coisas (IoT) e de sua incorporação às cidades inteligentes, nas quais é praticamente inexistente a opção de não estar online. De modo similar, Jeffrey Jonas (2015, p. 93, tradução nossa) comenta sobre a irresistibilidade da sociedade de vigilância:

> Uma sociedade de vigilância é inevitável e irreversível. O mais interessante é que acredito que uma sociedade de vigilância também se mostrará irresistível. Este movimento não está sendo conduzido apenas pelos governos; ele está sendo conduzido principalmente pelos consumidores – você e eu – à medida que adotamos avidamente números cada vez maiores de bens e serviços irresistíveis, muitas vezes sem saber quais informações pessoais estão sendo coletadas ou como podem acabar sendo usadas.

A barganha de dados foi investigada por Fernando H. Stahl em sua pesquisa sobre a percepção dos cidadãos acerca da vigilância de informações, que teve por objetivo compreender a aceitação e/ou a resistência à vigilância por parte dos usuários. Stahl entrevistou estudantes universitários de faculdades de tecnologia a fim de avaliar suas percepções sobre a exposição à vigilância de seus dados pessoais. O autor identificou, por meio da análise dos questionários aplicados, que a barganha de dados pessoais ocorre quando esses dados são aproveitados para ações mercadológicas direcionadas à promoção de produtos anteriormente buscados pelos usuários. Assim, "se a promoção valer a pena, a troca foi bem realizada" (STAHL, 2019, p. 69). Sobre a percepção da vigilância em rede e a invasão de privacidade, Stahl conclui que o grupo social entrevistado ainda não absorveu o conceito de pegada digital, ou seja, o registro digital de uma gama de comportamentos produzidos

pelo usuário enquanto realiza atividades na internet. Ele alerta, assim, para uma falta de sensibilidade ao fato de que as informações inseridas nas páginas da internet são armazenadas e processadas e, posteriormente, poderão ser acessadas por várias pessoas ao longo dos anos. Essa falta de sensibilidade faz do usuário um alvo ainda mais vulnerável a ações decorrentes da vigilância.

Essa vulnerabilidade também pode ser pensada a partir da compreensão daquilo que é ou não considerado como perda ou invasão de privacidade, e das consequências da vigilância de dados em um nível de controle social. Os resultados da pesquisa de Stahl suportam que, apesar da facilidade em barganhar dados por comodidade, a privacidade ainda é o aspecto da vigilância mais expresso pelos entrevistados. Todavia, a preocupação com a privacidade nesse contexto foi compreendida como a garantia contra intrusões causadas por outros indivíduos, desde empresas até *hackers*. Assim, a privacidade não foi discutida tendo em conta os limites da vigilância da informação e das formas de tratamento e categorização de comportamentos nos meios digitais. Ela foi vista sob uma ótica mais pessoal e menos coletiva, aspecto que também torna o usuário vulnerável ao controle e monitoramento de dados, porque o interesse em torno do problema da privacidade

fica restrito ao nível individual, não extensivo, portanto, a uma discussão no orbe da coletividade. Essa conclusão é significativa, pois aponta o fato de que o indivíduo se coloca à parte, é alienado da comunidade. Esse aspecto parece ser um reflexo da imersão isolada nos ambientes virtuais e da ilusão das chamadas mídias sociais, que levam ao paradoxo de que quanto mais tempo a pessoa vive nas redes sociais, menos tempo ela terá para realizar interações com indivíduos que estão fora de sua bolha de relações *online*.

Ainda que a preocupação com a privacidade seja expressa quando se fala em vigilância, torna-se um desafio localizar no âmbito de uma sociedade de vigilância o que é considerado informação pública ou privada. De acordo com Paula Sibilia (2009), o relato sobre uma intimidade autobiográfica, que ocorria nos séculos XVIII e XIX dentro dos quartos das casas burguesas, onde segredos e fatos referentes a si mesmo eram escritos sem nenhuma intromissão e longe dos ruídos da cidade, tornou-se agora uma intimidade exposta em redes sociais e difundida ao público global. Praticamos, assim, a exposição do íntimo, aquilo outrora considerado um bem privado é agora um bem passível de ser acessado pelo público.

Os dados sobre o comportamento digital e a exposição do íntimo pelo próprio usuário na internet são monitorados por

companhias e, posteriormente, compartilhados como outras empresas. É possível observar, assim, dois níveis de acesso e de compartilhamento de dados pessoais, um que consiste nos dados detalhados dos rastros digitais e das informações de cadastramento que o usuário deixa na rede e são coletados por corporações, e outro, nas informações pessoais geradas pelo próprio usuário para indicar sua presença nas redes sociais. No interior desse ambiente monitorado, a privacidade é praticamente inexistente, pois nem sempre temos ciência dos modos como nossos dados estão sendo coletados e compartilhados entre outros usuários ou por grupos comerciais parceiros.

Em vista da quase impossibilidade de permanecer oculto, quais seriam as estratégias de resistência dos cidadãos preocupados, de modo geral, com direitos e liberdades civis e, em particular, com o direito à privacidade? Alguns estudiosos defendem que a proposta de reversão da vigilância (também chamada de *sousveillance*), ou seja, tornar o observado um observador de si mesmo, gerando assim a "visibilidade total" (ver adiante o caso de Hasan Elahi), é uma das estratégias para lidar com a sociedade de vigilância. Kafer (2016, p. 236, tradução nossa), por exemplo, advoga nesses termos em favor da transparência irrestrita:

> Se a vigilância é inevitável e a privacidade aparentemente inatingível, então nesse contexto a real ênfase deve ser colocada sobre a transparência, tanto em termos das organizações de vigilância quanto do indivíduo "privado". Por um lado, as instituições federais e corporativas devem ser responsabilizadas pelo uso de dados pessoais para impactar de forma não ética indivíduos ou determinadas populações. Por outro lado, deve-se atribuir uma maior compreensão às maneiras pelas quais o compartilhamento de informações pessoais nos canais de telecomunicações, que hoje se tornou a forma dominante de comunicação, formou novos modos de subjetividade.

A problematização sobre a vida em uma sociedade de vigilância não é nova. Desde, pelo menos 1949, ano da publicação da obra de ficção distópica *1984* de George Orwell (que, além de refletir sobre as consequências de um Estado totalitarista, autoritário, repressivo que por meio da vigilância onipresente controlava pessoas e comportamentos da sociedade, cunhou a expressão *big brother*), alguns artistas têm levantado questões e oferecido formas de resistência ao controle total por parte dos governos. No entanto, com a crescente abrangência dos dispositivos de vigilância, visíveis e invisíveis, uma nova forma de lidar com essa situação e responder a ela veio a ser conhecida como estética da vigilância (BRUNO *et al.*, 2012) ou a *surveillance art*.

SURVEILLANCE ART

O que aconteceria se no lugar de tentar dificultar ou impedir o acesso de agências do governo e de instituições comerciais às nossas informações pessoais nós simplesmente informássemos antecipadamente a essas agências nossos movimentos, destinos e atividades realizadas a cada instante? Dito de outro modo, e se, no lugar de existirmos enquanto secretamente observados, nós passássemos a provedores de dados sobre nós mesmos? Essa é exatamente a base da proposta artística do projeto *Tracking Transience: the Orwell Project* do artista Hasan Elahi. Em vez de exigir a preservação de seu direito à privacidade, Elahi decidiu pelo caminho oposto, ou seja, paradoxalmente, abdicar de sua privacidade para se sentir mais seguro. Desse modo, ele criou um *website* no qual disponibilizava voluntária e constantemente informações sobre todas as suas atividades cotidianas.

Elahi, nascido em Bangladesh e naturalizado estadunidense, é atualmente professor no departamento de artes da Universidade de Maryland (Estados Unidos). Todavia, ainda era um desconhecido quando em 2002 foi detido no aeroporto de Detroit sob a errônea acusação de armazenagem de explosivos. Foi, então, retido e interrogado pelo serviço de imigração e informação (INS)

por seis meses. Os interrogatórios eram centrados, sobretudo, em questionar seu paradeiro nos dias anteriores e subsequentes aos ataques de 11 de setembro. As acusações foram, eventualmente, retiradas. Porém, com esse incidente, Elahi foi fichado no FBI, o que tornava sua vida muito mais difícil (pois era frequentemente abordado por seguranças em aeroportos e estações de trem) e insegura (por conta do preconceito gerado contra os grupos étnicos após os atentados terroristas).

Foi então que Elahi decidiu abrir mão de sua privacidade e fornecer, preventivamente, não somente ao FBI, mas a todos os usuários da internet, as informações de seu paradeiro e de suas atividades. A Figura 3 mostra uma das obras desse projeto, uma instalação de diversos registros em vídeos das atividades de Elahi expostas na seção Sundance New Frontier, do Sundance Film Festival, realizado em Utah, Estados Unidos, em 2008. Essa e outras obras resultantes do projeto foram exibidas em diversos festivais e exposições artísticas ao redor do mundo. Elahi recebeu prêmios e distinções, além de uma bolsa da Fundação Guggenheim. Sua apresentação no TED TALKS "FBI, Eu Estou Aqui" é frequentemente citada devido ao impacto e à relevância de seu manifesto artístico, desafiando a vigilância na sociedade atual.

Figura 3.
Hasan Elahi, *Tracking Transience*, 2008.
Instalação na Sundance New Frontier.
Fonte: https://elahi.gmu.edu/.
Acesso em: 30 nov. 2022

Inúmeras propostas, como as de Elahi, para se pensar, questionar e combater a sociedade de vigilância imposta aos cidadãos do mundo têm surgido em diversos segmentos artísticos. Historicamente, a interrogação artística sobre privacidade e vigilância advindas do uso da tecnologia pode remontar, no mínimo, ao início da videoarte, no final da década de 1960. Obras como *Sleep* (1964) e *Outer and Inner Space* (1966) de Andy Warhol, *Claim* (1971) e *Seedbed* (1972) de Vito Acconci, entre outras, foram consideradas transgressivas por apresentaram ao público aspectos e questões sobre a privacidade. Muitos desses artistas fizeram explícito uso de registros em vídeos adquiridos nos chamados CCTV (circuito fechado de TV), tais como Jill Magid (*Evidence Locker*, 2004). Arlindo Machado (1991), em um profético texto de 1991, mencionou a obra *Der Rise* (1983) de Michel Klier como "um poema videográfico (...) realizado com circuitos de vigilância e outros dispositivos de coerção policial (...) expondo a visão perturbadora do Estado policial moderno". Mais recentemente, com o desenvolvimento das tecnologias de vigilância, a invasão de privacidade é muito mais contundente e ubíqua do que poderiam suspeitar mesmo os analistas mais pessimistas.

A escalada do contexto de vigilância em que estamos imersos levou à criação de obras artísticas que justamente objetivam discutir tecnologias, mecanismos, ideologias e a impossibilidade de privacidade. Essa motivação formou e forma parte do manifesto estético de vários artistas e veio a constituir um tipo de criação denominada de *surveillance art*, cujo aspecto distintivo é a utilização explícita, com intenção artística, das próprias tecnologias projetadas para vigiar e registrar a conduta cotidiana dos cidadãos, seja nas ruas ou nos ambientes digitas virtuais. O objetivo principal da *surveillance art* (também chamada de *artveillance*) é refletir sobre o processo de vigilância em si e problematizá-lo, assim como com as tecnologias criadas para sua consecução. Diversos artistas fazem coro a esse manifesto, como os já citados Hasan Elahi e Tomas Van Houtryve, ao lado dos quais poderíamos mencionar Trevor Paglen, Benjamin Males, Christian Moeller e Robert Spence (conhecido como *eyeborg*), por exemplo. Fernanda Bruno e colaboradores (2012; 2018) oferecem um importante levantamento sobre algumas obras de artistas latino-americanos, bem como de exposições significativas no campo da "estética da vigilância".

Uma das artistas mais contundentes no questionamento das tecnologias de vigilância é Heather Dewey-Hagborg, sobretudo com

sua obra na intersecção entre arte e ciência. Um de seus projetos mais incisivos é *Stranger Visions*, no qual a artista ia a locais públicos de Nova Iorque, tais como banheiros, salas de espera, estações e vagões de metrô, para coletar fios de cabelo, pedaços de unha, goma de mascar e bitucas de cigarro descartados pelas pessoas. Dewey-Hagborg valia-se dessas amostras para extrair o DNA e a partir do código genético resultante gerar uma espécie de máscara impressa em uma impressora 3D criada com as prováveis características daquela pessoa que descartou o material (Figura 4). Segundo Dewey-Hagborg, "o projeto intentou chamar atenção para o desenvolvimento da tecnologia forense baseada na fenotipagem do DNA, o potencial para a cultura da vigilância biológica e o impulso ao determinismo genético" (DEWEY-HAGBORG, n.d., tradução nossa).

Figura 4.
Heather Dewey-Hagborg , *Stranger Visions*, 2012.
Fonte: www.deweyhagborg.com/projects/stranger-visions. Acesso em: 30 nov. 2022

Figura 5.
David Rokeby, *Sorting Daemon*, 2003.
Fonte: http://www.davidrokeby.com/sorting.html.
Acesso em: 30 nov. 2022

O artista canadense David Rokeby instiga o questionamento sobre o uso de equipamentos de vigilância com o intuito de categorizar pessoas em grupos pré-determinados. A instalação *Sorting Daemon* (2003, Figura 5), comissionada e instalada no Instituto Goethe de Toronto, é composta por uma câmera instalada dentro da galeria do Goethe, mas apontada para a rua, de onde captura imagens dos transeuntes. Um computador conectado à câmera identifica e isola do pano de fundo a imagem das pessoas que passam. A seguir, essa pessoa é separada e agrupada seguindo um critério de cor e de tamanho. As diversas imagens extraídas, separadas e agrupadas são projetadas em uma parede no interior da galeria. Rokeby esclarece que "*Sorting Daemon* é uma instalação *site specific* desencadeada por minhas preocupações sobre o crescente uso de sistemas automatizados para definir perfis de pessoas como parte da 'guerra ao terrorismo' e é uma tentativa de ajudar a fazer perguntas sobre os usos apropriados da tecnologia" (ROKEBY, n.d., tradução nossa).

Há obras no campo da arte e vigilância que são elaboradas como forma de discutir a ausência de privacidade no ambiente do ciberespaço. Por exemplo, a obra *@xaieneofficial* (2019) de Lorena Ferreira discute o desprendimento da privacidade por parte

do usuário em um ambiente digital onde a exposição de informações e comportamentos consiste na maneira pela qual o usuário se mantém vivo para os outros usuários da web. *@xaieneofficial*[5] (Figura 6) é uma instalação que contém um autômato, uma máquina que possui aparência humana e exerce ações semelhantes à dos seres humanos. Estas, por sua vez, são ações dos próprios indivíduos imersos na sociedade de vigilância que compartilham suas imagens e dados pessoais ao público que acessa sua página do Instagram.[6]

@xaieneofficial possui, como órgão interno responsável pelo seu funcionamento, uma tecnologia de vigilância. Um *smartphone* transmite seus *stories* (vídeos de curta duração), que são refletidos pelos espelhos de seu suporte, onde o espectador, ao mesmo tempo que observa o conteúdo autobiográfico produzido pelo perfil, visualiza seu rosto e se depara com a câmera do dispositivo de vigilância apontada para si. Assim, a obra convida o espectador a se enquadrar no mesmo espelho/universo de *@xaieneofficial*[7] como sujeito que pratica as mesmas ações que o perfil e que está inserido na mesma circunstância de vigilância, aquela produzida pelo próprio usuário, que oferece suas informações íntimas para a visualização do outro. Assim, podemos pensar nossas ações dentro de uma sociedade de vigilância através da obra enquanto autômatos,

máquinas produtoras de informações. Além do *smartphone* observado como órgão de funcionamento, *@xaieneofficial* possui um coração mecânico que opera através de um motor, ao mesmo tempo que sua boca ressoa sons de respiração semelhantes à respiração humana. Os sons produzidos pela instalação se referem ao conceito de escuta íntima, que, segundo Denise Garcia (1998), consiste no espaço de intimidade criado pelo compositor com o ouvinte por meio da manipulação de sons que remetem ao corpo humano, como a voz, o sussurro e a respiração.

Figura 6.
Lorena Ferreira, *@xaieneofficial*, 2019.
Fonte: https://lorenaferreira.gitlab.io/xaiene.html.
Acesso em: 30 nov. 2022.

CONSIDERAÇÕES

A história da privacidade deixa clara a relação inversa entre privacidade e tecnologia. Quanto mais a tecnologia evolui, mais sofisticados tornam-se os meios de vigilância e menos privacidade se tem. Desde o uso de grampos telefônicos já detectados em 1918,[8] passando pelas câmeras de circuito fechado até técnicas complexas de *dataveillance*, o direito à privacidade vem esvanecendo. A política implantada após atentados terroristas como os de Nova Iorque (2001), Madrid (2004) e Londres (2005) mostra que o direito à privacidade é dependente de vontade e determinação políticas. Todavia, como enfatiza Holvast (2007, p. 738), "o desejo político global é mais orientado para o efetivo e eficaz uso da tecnologia na batalha contra a criminalidade e o terrorismo do que para a proteção da privacidade". Os avanços tecnológicos na área da informática haviam engendrado um novo contexto denominado de sociedade da informação (*information society*), que era tido como o resultado do progresso subsequente ao modelo social industrial – que, por sua vez, sucedeu o modelo agrícola. Todavia, a aceitação dessas tecnologias, seja qual for a justificativa para esse consentimento, teve como consequência o surgimento de um novo modelo social denominado sociedade de vigilância (*surveillance society*).

Nas palavras fatídicas de Holvast (2007, p. 766), "a onipresença da tecnologia e a aceitação das políticas e leis para coletar, armazenar e utilizar praticamente todos os dados pessoais está fazendo da sociedade da informação uma sociedade da vigilância".

Uma sociedade de vigilância produz um comportamento social fundamentado nos modos como indivíduos e comunidades lidam com a vigilância. Esses modos são impostos por governos e, também, criados pelos cidadãos. A sociedade da informação, por seu turno, é entendida como um modelo de comportamentos, condutas e atitudes fundamentados econômica, cultural e politicamente na manipulação e integração da informação. Os motores dessa estrutura social são as tecnologias de informação e comunicação que multiplicam rapidamente a informação e provocam transformações em todos os aspectos da organização social, como educação, economia, saúde, beligerância, ideologia, entre outros (cf. BENIGER, 1986).

O modelo de sociedade de vigilância acaba por engendrar certos binarismos, como, por exemplo, a vigilância perceptível e a imperceptível. Este antagonismo entre o que enxergamos e o que nos é ocultado aponta duas modalidades de vigilâncias: visíveis (câmeras de circuito fechado, monitores, detectores de metais etc.) e invisíveis (grampos telefônicos, dispositivos de

aferição de audiência instalados nas TVs, espionagem via satélite, drones, *dataveillance* etc.). A pergunta que precisa ser feita, e que em maior ou menor grau tem sido amplamente levantada pelos artistas atuantes na *artveillance*, é: como as pessoas das diferentes culturas e contextos sociais respondem à vigilância constante? Uma das principais preocupações "é que as pessoas se tornem mais conformistas à medida que suprimem sua individualidade" (HOLVAST, 2007, p. 742, tradução nossa). E essa supressão da individualidade diluída em um coletivo engendrado a partir de dados coletados é de fato notada em razão da abdicação do direito à privacidade.

Após a mobilização mundial elaborada pelos Estados Unidos a favor da utilização de tecnologias de vigilância por parte de seus órgãos de segurança, a perda de privacidade foi sacrificada em favor de um suposto bem maior: a segurança mundial. Logo, com a implementação da vigilância massiva e ubíqua, as tecnologias de vigilância de dados passaram a ser utilizadas para outros fins, como a promessa de aperfeiçoamento dos resultados de buscas de conteúdo na internet. Empresas desenvolvedoras de produtos destinados à navegação na *web*, como o Google, por exemplo, aprimoraram tecnologias de monitoramento na rede mundial

de computadores como maneira de administrar dados pessoais, localização e pegadas de navegação para traçar perfis dos usuários com objetivo de distribuir resultados de busca de maneira personalizada. Desde dezembro de 2009, segundo Pariser (2012), a realização de buscas no site do Google passou, também, a produzir resultados personalizados para cada usuário, por meio de algoritmos que calculam os produtos que mais se aproximam da preferência e das possíveis necessidades desses usuários. Isto significa que a mesma busca realizada por dois usuários de perfis distintos poderá revelar resultados diferentes.

Se a nova regulamentação sobre privacidade teve o intuito de proteger e prever ações criminosas, então por que essa proteção só vale contra os supostos atos terroristas? Como relatado no caso da criança que sofria constantes abusos, embora havendo ciência do delito, as autoridades não agiram em benefício da pessoa lesada (no caso, a criança) e, mesmo tendo cometido essa omissão, foram isentas de responsabilidade pelo tribunal. Com situações similares, percebemos que a privacidade acaba sujeita a escolhas de indivíduos ou de grupos, ou seja, é objeto a ser interpretado. No entanto, não se pode perder de vista que vivemos em sociedade, e a vida social implica restrições, mesmo em relação aos limites

da privacidade. Nesse sentido, Holvast comenta que "viver em comunidade significa, por definição, estar envolvido com os outros" (HOLVAST, 2007, p. 741, tradução nossa). Desse modo, ainda vale, ou deveria valer, o velho entendimento do estado de direitos e deveres. Porém, o que várias pesquisas demonstram é justamente o esvanecimento do direito à privacidade em ambas as suas dimensões, territorial e corporal (*territorial and bodily privacy*), e da privacidade informacional, isto é, relativa à coleta, armazenagem e processamento de dados pessoais.

Em vista desse estado de coisas, governos e empresários iniciaram um procedimento que veio a ser conhecido como contravigilância. Nessa forma, empresas investem altas somas para tentar evitar a espionagem digital e a vigilância de dados (*dataveillance*) por meio de medidas e tecnologias de segurança, denominadas *Privacy-Enhancing Technologies* (PETs) (HOLVAST, 2007, p. 738). Os artistas, por sua vez, têm se posicionado politicamente e intentado com suas obras promover um discurso crítico a respeito da vigilância ostensiva. Duas estratégias para resistir e combater a sociedade de vigilância podem ser verificadas. A primeira é chamar a atenção para o problema (que nem sempre é notado pelo usuário comum) e instigar o público a exigir a preservação de seu direito à privacidade.

A segunda "tática" é a comentada no projeto de Hasan Elahi, ou seja, fornecer e exigir visibilidade, transparência total, para tudo e todos, inclusive, e principalmente, para governos e corporações.

No entanto, de modo geral, podemos observar, após a análise de obras no âmbito da proposta estética da *surveillance art*, que a maioria dos artistas age expondo as tecnologias de vigilância. Assim, os procedimentos de vigilância visíveis (mas que para muitos passam despercebidos) e invisíveis são tornados transparentes para o público. *Grosso modo*, poderíamos dizer que os artistas se valem das tecnologias de vigilância de maneira ativa e passiva. A maneira passiva seria simplesmente mostrar que a vigilância existe, embora nem sempre seja notada. A Figura 7, do grafiteiro britânico Banksy, justamente expõe a existência de uma câmera de vigilância na parede exterior de um banco em Londres. Interessantemente, a imagem por ele pintada provoca os passantes a refletir sobre o que propositadamente se oculta (avestruz que enterra a cabeça no solo) e aquilo que está à vista (câmera), mas que passa sem ser notado, pois já se tornou parte habitual da paisagem urbana. A oposição se dá então entre o que não vemos e o que não queremos ver.

A maneira ativa seria justamente o uso das tecnologias na obra de arte com intuito não somente de fazê-las visíveis,

mas como forma de promover um diálogo crítico e sensível entre artista e público. Algumas vezes essa visibilidade é mais explícita, como na Figura 8, na qual um *hacktivist* faz uma crítica aberta ao presidente Barack Obama parodiando seu famoso slogan de campanha ("Yes, we can!") na imagem modificado para "yes we scan" e, com isso, expondo os procedimentos de vigilância ainda em vigência. Essa imagem (Figura 8) foi usada para substituir a figura original do telefone Galaxy Android que fornecia aos compradores um aplicativo para baixar as músicas do álbum *Magna Carta Holy Grail*, lançado em 2013 pelo rapper Jay-Z. O aplicativo foi clonado pelo *hacker* e funcionava bem, até que em uma data estratégica (4 de julho, Dia da Independência dos Estados Unidos) mudou a imagem para a imagem do presidente Obama. A crítica implícita nesse procedimento, que fez uso da própria tecnologia de espionagem do governo norte-americano, é que os cidadãos deveriam ser libertados (tornados independentes) da vigilância ubíqua imposta pelo governo.

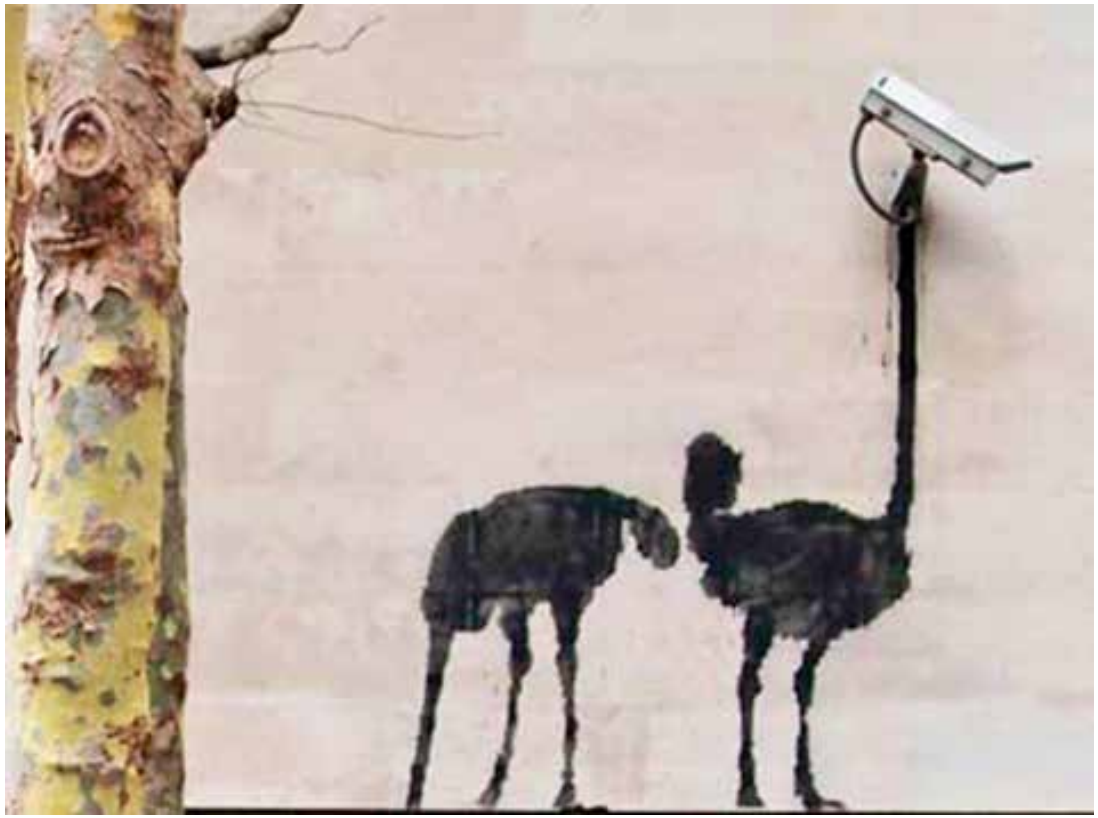

Figura 7.
Banksy, sem título.
Fonte: https://www.banksy.co.uk/out.html

Já outras obras são mais sutis, mas sem deixar de incomodar, como relatado nas propostas de Dewey-Hagborg (Figura 4) e de David Rokeby (Figura 5). Ambos os artistas, a seu modo, criticam de maneira ativa a invasão da privacidade imposta na sociedade de vigilância. Dewey-Hagborg chama a atenção para o problema da vigilância forense agindo como a pessoa que invade o direito à privacidade. Ao coletar (sem permissão) amostras de "resíduos" deixados pelas pessoas, ela força o público a se indignar com esse procedimento, uma vez que as máscaras criadas a partir do DNA resultante das amostras coletadas poderiam mostrar o rosto de qualquer um. Isso levaria o espectador a protestar: eu não autorizei isso! Desse modo, a problemática da invasão da privacidade fica estabelecida. Rokeby, similarmente, grava imagens dos passantes sem sua permissão. Isso também poderia levar a questionar sobre a necessidade da respectiva autorização dos filmados para serem usados em uma obra de arte, o que, por sua vez, promoveria o debate sobre os distintos níveis e ou camadas da invasão. Se agências do governo podem gravar imagens sem autorização, por que o artista também não poderia fazê-lo?

A análise das obras criadas por artistas no âmbito da *surveillance art* mostra uma atitude de combate e de resistência ao perigo imposto

pela sociedade de vigilância, o perigo de a vigilância tornar-se tão assimilada à paisagem cotidiana a ponto de não mais ser percebida. Esse aspecto levaria justamente à perda da individualidade causada pelo conformismo dos cidadãos com a sociedade de vigilância. Os artistas da *surveillance art* têm o mérito de agir criticamente, problematizar e forçar o público a desenterrar a cabeça do solo e exercer o direito à cidadania.

Figura 8.
Imagem adicionada ao aplicativo Android hackeado que funcionava para *download* das músicas do álbum *Magna Carta Holy Grail* (2013), do rapper Jay-Z.
Fonte: https://www.bbc.com/news/technology-23194413. Acesso em: 30 nov. 2022

NOTAS

1. Ver, por exemplo, Vieira (2016), Oliva e Cruz (2014), Barreto e Santos (2006).

2. Vale ressalvar que "embora a constituição dos Estados Unidos não proteja explicitamente a privacidade, esse direito é comumente considerado como criado por certos dispositivos legais, particularmente a Primeira, Quinta e Décima Quarta emendas" (BRITANNICA, 2020).

3. No original: "To improve the abilities of U.S. law enforcement to detect and deter terrorism. The act's official title is, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism". Texto disponível em: https://www.history.com/topics/21st-century/patriot-act. Acesso em: 30 nov. 2022. Tradução nossa.

4. Exposição ocorrida de fevereiro a agosto de 2017 no Museu de Fotografia de Berlim, com a curadoria de Stuart Alexander, Susan Meiselas e Yukiko Yamagata. Organizada por Open Society Foundations (New York) em cooperação com a Kunstbibliothek – Staatliche Museen de Berlin.

5. Registros da obra disponíveis em: https://lorenaferreira.gitlab.io/xaiene.html. Acesso em: 30 nov. 2022.

6. Perfil no Instagram: https://www.instagram.com/xaieneofficial/?hl=pt-br.

7. *Link* de acesso ao vídeo da obra: https://vimeo.com/351907787. Acesso em: 30 nov. 2022.

8. De acordo com David Owen (2002), em 1918, militares norte-americanos perceberam que suas conversas telefônicas estavam sendo ouvidas. Tentando impedir que os espiões entendessem o que era dito, colocaram índios para falar em seu idioma nativo e, assim, transmitirem os conteúdos mais importantes e secretos.

REFERÊNCIAS

BARRETO, Wanderlei de Paula. Os direitos da personalidade na jurisprudência alemã contemporânea. **Revista Trimestral de Direito Civil**, vol. 41, 2010, p.135-159.

BARRETO, Wanderlei de Paula; SANTOS, Luciany Michelli Pereira dos. O conceito aberto da personalidade e os seus elementos constitutivos nas situações de mobbing ou assédio moral. **Revista Jurídica Cesumar**, vol. 6, n. 1, 2006, p. 473-487.

BENIGER, James R. **The Control Revolution**: Technological and Economic Origins of the Information Society. Cambridge, Massachusetts: Harvard University Press, 1986.

BRITANNIA, The Editors of Encyclopaedia. Rights of privacy. **Encyclopedia Britannica**, 26 fev. 2020. Disponível em: https://www.britannica.com/topic/rights-of-privacy. Acesso em: 30 nov. 2022.

BRUNO, Fernanda; BARRETO, Paola; SZAFIR, Milena. Surveillance Aesthetics in Latin America: Work in Progress. **Surveillance and Society**, vol. 10, n. 1, 2012, p.83-89.

BRUNO, Fernanda *et al*. **Tecnopolíticas da vigilância**: Perspectivas da margem. São Paulo: Boitempo, 2018.

COLLINS English Dictionary. Surveillance Society. Disponível em: https://www.collinsdictionary.com/dictionary/english/surveillance-society. Acesso em: 8 nov. 2019.

DEWEY-HAGBORG, Heather. Sci-Fi Crime Drama With a Strong Black Lead. **The New Inquiry,** 6 jul. 2015. Disponível em: https://thenewinquiry.com/sci-fi-crime-drama-with-a-strong-black-lead/. Acesso em: 27 jan. 2020.

GARCIA, Denise Hortência Lopes. **Modelos perceptivos na música eletroacústica**. Tese apresentada ao Programa de Pós-graduação em Comunicação e Semiótica, Pontifícia Universidade Católica de São Paulo, São Paulo, 1998.

HOLVAST, Jan. History of Privacy. In LEEUW, Karl de; BERGSTRA, Jan (eds.). **The History of Information Secutity:** A Comprehensive Handbook. Amsterdam: Elsevier, 2007, p.13-42.

JONAS, Jeffrey. The surveillance society and the transparent you. In ROTENBERG, Marc; HORWITZ, Julia; SCOTT, Jeramie (eds.). **Privacy in the Modern Age:** The Search for Solutions. New York: New Press, 2015, p.93-103.

KAFER, Gary. Reimagining Resistance: performing transparency and anonymity in surveillance art. **Surveillance and Society**. Vol. 14, n. 2, 2016, p.236.

LACAZE, Laura Mabel. Vigilancia masiva de comunicaciones: una (ciber)inquisición. ANAIS IV Simpósio Internacional LAVITS – Rede Latino-americana de estudos sobre vigilância, tecnologia e sociedade. Buenos Aires, 2016.

LYON, David. Surveillance, Power and Everyday Life. In MANSELL, Robin; AVGEROU, Chrisanthi; QUAH, Danny; SILVERSTONE, Roger. **The Oxford Handbook of Information and Communication Technologies.** Oxford: Oxford University Press, 2009, pp.449-468-. Disponível em: https://panoptykon.org/sites/default/files/FeedsEnclosure-oxford_handbook_3.pdf Acesso em: 8 dez. 2019.

MACHADO, Arlindo. A Cultura da Vigilância. **Artepensamento IMS,** 1991. Disponível em: https://artepensamento.com.br/item/a-cultura-da-vigilancia. Acesso em: 30 nov. 2022.

OLIVA, Afonso Carvalho de; CRUZ, Marco A. R. Cunha e. Um estudo do caso Xuxa vs. Google Search (REsp 1.316.921): o direito ao esquecimento na internet e o superior tribunal de Justiça. **Anais do I Congresso Internacional de Direitos da Personalidade**., Maringá, UniCesumar, 2014. Disponível em: http://www.cesumar.br/prppge/pesquisa/mostras/pri_mestrado/pdf/03_GT1_Afonso_Carvalho_Oliva.pdf. Acesso em: 30 nov. 2022.

OWEN, David. **Hidden Secrets:** The Complete History of Espionage and the Technology Used to Support it. Ontario: Firefly Books, 2002.

PALLITTO, Robert M. Irresistible Bargains: Navigating the Surveillance Society. **First Monday**, v. 23, n. 2, 2018, p. 1-19.

PARISER, Eli. **O filtro invisível:** o que a internet está escondendo de você. São Paulo: Zahar, 2012.

RENGEL, Alexandra. **Privacy in the 21st Century**. Leiden: Martinus Nijhoff Publishers, 2013.

ROKEBY, David. Interactive Installations: Sorting Daemon, 2003. Disponível em: http://www.davidrokeby.com/sorting.html. Acesso em: 30 nov. 2022.

SIBILIA, Paula. **O show do eu:** a intimidade como espetáculo. Rio de Janeiro: Nova Fronteira, 2008.

STAATLICHE Museen zu Berlin, 2017. Disponível em: https://www.smb.museum/en/museums-institutions/museum-fuer-fotografie/exhibitions/detail/watching-you-watching-me-a-photographic-response-to-surveillance.html. Acesso em: 30 nov. 2022.

STAHL, Fernando Henrique. **Informações vigiadas?** Percepções dos usuários de wi-fi livre. Dissertação de mestrado. Fundação Getúlio Vargas - Escola de Administração de Empresas de São Paulo, 2019.

VIEIRA, Waleska Duque Estrada. **A privacidade no ambiente cibernético:** direito fundamental do usuário. Monografia apresentada à Universidade Estadual do Ceará, 2016.

WILLIAMS, Raymond. **Keywords:** A Vocabular of Culture and Society. London: Fontana Press, 1988.

SOBRE OS AUTORES

Antenor Ferreira Corrêa é compositor, percussionista e Professor Associado da Universidade de Brasília. Possui pós-doutorado pela Universidade de Granada (Espanha) e pela Universidade da Califórnia, Riverside (Estados Unidos). É coordenador do MidiaLab-UnB – Laboratório de Pesquisas em Arte Computacional. Publicou seis livros e diversos artigos em periódicos científicos, além de CDs e DVD. Possui bolsa produtividade nível PQ2 do Conselho Nacional de Desenvolvimento Científico e Tecnológico – CNPq.

Lorena Ferreira Alves é doutora em Artes (linha de pesquisa Arte e Tecnologia) pelo Programa de Pós-Graduação em Artes Visuais da Universidade de Brasília (UnB) em cotutela com o Programa de Doutorado em História e Artes da Universidade de Granada (UGR - Espanha). É artista multimídia, trabalhando no campo da Arte Sonora na criação de instalações sonoras relacionadas à temática da Arte e Vigilância. Em 2021 foi indicada ao Prêmio PIPA de Arte Contemporânea Brasileira.

Artigo recebido em 25 de fevereiro de 2020 e aceito em 30 de março de 2022.