DIO: um jogo em dispositivos móveis para mapear câmeras de vigilância

DIO: a mobile game to map surveillance cameras

Rafael de Almeida Evangelista*

Tiago C. Soares**

Sarah Costa Schmidt***

Felipe Lavignatti****

RESUMO

Na sociedade contemporânea, as câmeras de vigilância são tecnologias de uso rápido e crescente. As razões dadas para essa proliferação estão principalmente relacionadas a preocupações com segurança. Nos países pobres, a ênfase está no controle da criminalidade urbana. Nos países ricos, elas são justificadas também pela ameaça do terrorismo. DIO é um jogo para celulares, ainda em desenvolvimento, que tematiza a proliferação das câmeras em áreas urbanas, promovendo um mapeamento colaborativo de sua localização geográfica. Os jogadores escolhem uma de duas equipes a quem se associam e desenvolvem as seguintes tarefas: 1) geolocalizar e fotografar câmeras de vigilância distribuídas pelas

ABSTRACT

Surveillance cameras are technologies with fast, growing use in today's society. Their use is usually for security reasons. In poorer countries, the emphasis is on curbing urban crime; in richer nations, it is the threat posed by terrorism. DIO is a game for mobile phones, still in development, which thematizes the rampant proliferation of cameras in urban areas, promoting a collaborative mapping of their geographic location. Players choose which group they will join and have the following tasks: 1) geolocate and photograph surveillance cameras scattered around the city; 2) compete with the other team for control of the cameras. Registered cameras will then be transformed into geolocated points with which the player interacts, with cameras

* Doutor em Antropologia pela Unicamp, pesquisador do Laboratório de Estudos Avançados em Jornalismo da Universidade Estadual de Campinas e professor do Mestrado em Divulgação Científica e Cultural (Labjor/IEL/Unicamp). Endereço: Rua Seis de Agosto, 50, 3º piso, Cidade Universitária Zeferino Vaz, CEP 13083-873, Campinas, SP. Telefone: (19) 3521-2594. E-mail: rae@unicamp.br.

**Mestre em Divulgação Científica e Cultural pela Unicamp, doutorando em História Econômica na Universidade de São Paulo (USP). É associado à Cátedra Unesco em Educação Aberta (Unicamp), e aos grupos de estudo Prometheu (USP), Informação, Ciência, Tecnologia e Sociedade (ICTS/Unicamp) e Antropi (UFRGS). Também colabora com a Rede Latino-Americana de Estudos sobre Vigilância, Tecnologia e Sociedade (Lavits) Endereço: Rua Seis de Agosto, 50, 3º piso, Cidade Universitária Zeferino Vaz, CEP 13083-873, Campinas, SP. Telefone: (19) 3521-2594. E-mail: ticsoares@usp.br

*** Mestre em Divulgação Científica e Cultural pelo Labjor/Unicamp. Pesquisadora do grupo Informação, Comunicação, Tecnologia e Sociedade ICTS/Unicamp. Endereço: Rua Seis de Agosto, 50, 3º piso, Cidade Universitária Zeferino Vaz, CEP 13083-873, Campinas, SP. E-mail: arahcs.jor@gmail.com

**** Mestre em Divulgação Científica e Cultural pelo Labjor/Unicamp. Pesquisador do grupo Informação, Comunicação, Tecnologia e Sociedade ICTS/Unicamp. Endereço: Rua Seis de Agosto, 50, 3º piso, Cidade Universitária Zeferino Vaz, CEP 13083-873, Campinas, SP. Telefone: (19) 3521-2594.E-mail: avignatti@gmail.com.

ruas; 2) competem com o outro time pelo controle das câmeras. As câmeras cadastradas então se transformam em pontos geolocalizados com os quais os jogadores interagem, com as câmeras sendo "capturadas" quando o jogador está fisicamente próximo a elas. Este artigo apresenta o enredo básico do jogo, suas regras e sua dinâmica. Também discute o uso econômico de dados pessoais, sua importância prevista no mercado mundial no futuro próximo e como tematizar essa questão fazendo uso de gameficação.

Palavras-chave: Vigilância; Privacidade; Gameficação; Dados Pessoais; Economia Digital.

being "taken" when the player is physically close to them. This article presents the basic plot of the game, its rules and dynamics. It also discusses the economic uses of personal data, its growing role in the market in the near future and how to thematize this issue through gamification.

Keywords: Surveillance; Privacy; Gamification; Personal Data; Digital Economy.

INTRODUÇÃO

As câmeras de vigilância são tecnologias de rápido e crescente uso na sociedade contemporânea. Somente na Grã-Bretanha, um dos países pioneiros na instalação de sistemas de vigilância públicos dependentes de imagens remotas, as estimativas apontam para até 5, 9 milhões de câmeras no território, somando-se as de uso pelo poder público e por entes privados (BARRETT, 2013).

As justificativas dadas para sua utilização passam, principalmente, por preocupações de segurança. Nos lugares mais pobres, com maior ênfase no controle da criminalidade urbana; nos mais ricos, pelo combate ao terrorismo. É o caso das câmeras instaladas em Manhattan, pela polícia de Nova York. São 4 mil fontes de imagens, públicas e privadas, instaladas em uma região específica da cidade. Um sistema semelhante, porém menor, teria sido usado para identificar os perpetradores dos ataques terroristas de 2013 em Boston, também nos Estados Unidos (KELLY, 2013).

As preocupações com o vigilantismo e dúvidas sobre a real efetividade desses sistemas no combate à violência tornam seu uso polêmico. Nos países democráticos, organizações sociais que zelam pela observância dos direitos civis têm criticado a multiplicação de seu uso como violadora de direitos de privacidade. A Aclu (American Civil Liberties Union), por exemplo, aponta que: 1) elas seriam suscetíveis a abusos; 2) não teriam efetividade comprovada; 3) haveria falta de limites e controle sobre o uso das câmeras; e 4) teriam um efeito paralisante na vida pública (ACLU, 2016).

Na América Latina, a ausência de regulação específica e a fragilidade do sistema legal se combinam com a escassez de um debate público sobre o tema (FIRMINO et al., 2013). Em países como o Brasil, sede de recentes eventos internacionais como a Copa do Mundo de 2014 e as Olimpíadas de 2016, a intensificação no uso de sistemas de monitoramento por câmeras partindo do poder público está, no discurso, associada à prevenção de ataques terroristas. Matéria da revista de tecnologia *Motherboard* mostra esse sistema, instalado no Rio de Janeiro, cidade-sede das Olimpíadas.

> As transmissões das centenas de câmeras de vigilância do Rio de Janeiro podem ser acompanhadas em uma tela panóptica de 85 metros quadrados no Centro Integrado de Comando e Controle

> (CICC) ou na telona igualmente enorme do Centro de Operações Rio (COR), na capital fluminense. São verdadeiros cinemas da vigilância.
> Basta dar uma olhadela nessas transmissões na hora certa para ver passar um ou dois jipes lotados de oficiais armados até o pescoço. Capaz que você até veja a polícia prender os manifestantes que estão execrando aquilo que muitos chamam de golpe contra a presidente Dilma Rousseff. Ou, quem sabe, você não flagra um militar ou policial matando um jovem negro em uma favela ou invadindo uma das dezenas de escolas ocupadas por estudantes ativistas que visam melhorar o sistema educacional brasileiro, subfinanciado. [...]
> O CICC é um centro de inteligência administrado em conjunto por várias agências brasileiras, incluindo a polícia e o exército, e tem acesso à transmissão de pelo menos 3.200 câmeras de vigilância fixas e móveis. O COR, um centro municipal, fornece dados de 560 câmeras à polícia. Apesar desses olhos onipresentes e dos milhões investidos em segurança pelo Estado e governo federal, as preocupações com segurança persistem (KAYYALI, 2016).

A matéria contém ainda a informação de que o processo se iniciou pouco antes da Copa do Mundo de 2014, que trouxe "*drones*, óculos de reconhecimento facial capazes de ler 400 rostos por segundo e compará-los a uma base de dados de até 13 milhões de imagens, e 122 helicópteros de vigilância, muitos deles equipados com câmeras HD e infravermelho". Toda essa tecnologia tem sido usada também na repressão de manifestações políticas.

Historicamente, porém, a maior parte das câmeras que se espalham pelo Brasil cumpre funções mais corriqueiras, nem sempre somente nas mãos do Estado, ligadas, no discurso, à prevenção de crimes e à coleta de provas para investigação e processos legais. No dia a dia, a prevenção da violência se mistura a práticas de segregação e higienização social. O barateamento da tecnologia e a consequente popularização do uso desses equipamentos tornaram quase impossível a circulação por espaços urbanos sem ser alvo das câmeras em algum momento. As novas tecnologias digitais de processamento de imagem potencializam práticas de identificação. O uso disseminado e descontrolado interfere na administração de espaços públicos pela intensificação do policiamento preventivo, permitindo abusos ligados ao chamado *racial profiling* e à gentrificação. Praças públicas, por exemplo, cuja seleção dos circulantes interessa ao setor imobiliário, são monitoradas para darem base à expulsão de populações indesejadas (KANASHIRO, 2006).

Em se tratando de câmeras que alvejam espaços públicos como praças, ruas e calçadas, podemos dizer que a maioria se divide no cumprimento de dois propósitos: o combate à violência e à criminalidade, sendo instaladas e controladas por particulares ou por órgãos públicos; e a administração e disciplinamento do trânsito de veículos, estando sob a responsabilidade das autoridades de trânsito, mas podendo ser administradas e instaladas por empresas privadas terceirizadas. Há situações específicas em que uma acaba fazendo a função da outra, como quando câmeras de controle de tráfego capturam "por acidente" algum evento significativo acontecendo.

Uma das modalidades de moradia que mais tem crescido no Brasil, os condomínios fechados – já representam quase 2% do total de domicílios (UCHINAKA, 2011) – tem na segurança, tipificada pelo monitoramento por câmeras, como um de seus principais atrativos. Em países subdesenvolvidos, o medo da violência urbana está

entre os principais atrativos dessa modalidade de moradia, e o uso de algum tipo de "*technical fix*" (Firmino et al., 2013) complementar ao cercamento físico da área é frequente.

Quando voltadas para as áreas de frequentação comum do empreendimento – como elevadores, salas de convívio comum e espaços abertos de lazer –, as câmeras podem dar margem a abusos, tanto contra os próprios moradores como contra o corpo de funcionários do condomínio. No entanto, além disso, elas também costumam estar voltadas a espaços públicos, como ruas e calçadas, servindo para mapear e prevenir a aproximação de pessoas indesejadas.

Nos shoppings centers, em bares e em estabelecimentos comerciais, as câmeras vigiam, para diversos fins, trabalhadores e clientes frequentadores desses espaços, que nada podem fazer para evitar sua identificação e monitoramento. Os benefícios econômicos da vigilância por câmeras sobre clientes e funcionários fazem parte dos argumentos das empresas vendedoras dessas tecnologias. Uma delas, por exemplo,argumenta como "gerentes podem estudar os hábitos de compras dos consumidores analisando os vídeos gravados por sistemas de vigilância" (LI, 2016).

VISIBILIZAR A VIGILÂNCIA

A tensão articulada nas relações entre poder, vigilância e liberdade é presente em momentos diversos da conformação do que, em termos amplos, é costumeiramente entendido como "cibercultura". Uma profunda preocupação com liberdade de expressão e autonomia individual, em contraposição às dinâmicas tecnocráticas de controle e censura, eram, já na década de 1960, presentes nas movimentações que, nos Estados Unidos, galvanizariam as comunidades que nas décadas seguintes promoveriam os experimentos sociais, artísticos e tecnológicos que culminariam na revolução do microcomputador e nos arranjos culturais mediados pelas novas tecnologias digitais (TURNER, 2010). Do Movimento pela Liberdade de Expressão, na Universidade de Berkeley, nos anos 1960, passando pelos clubes hobbistas e pelas comunidades experimentais autônomas espalhados pela Califórnia, nos 1970-1980, o hegemônico modelo de gestão do conhecimento que emergiu do Vale do Silício no último quarto do século passado colocou no centro do *grid* tecnocientífico a noção de apropriação tecnológica em nível individual. Tornado dispositivo entrelaçado às preferências cognitivas de cada usuário/a, a noção de "computador" no imaginário público se descolou, assim, da ideia dos gigantescos *mainframes* que, em meados do século XX, eram, para os operadores da contracultura californiana, sinônimo de controle, automatização e grandes burocracias. Dos computadores de mesa aos *laptops* e, finalmente, aos *smartphones*, o computador se conformou como artefato de aumento tecnológico, como um dispositivo a se integrar de modo único a cada usuário, libertando suas potencialidades latentes.

Esse movimento, com seus acenos às proposições experimentais e anti-hegemônicas de grupos de tecnólogos do Vale do Silício, influenciados por teóricos radicais como Ivan Illich (1990) nos anos 1970, desenha, porém, uma potente tensão interna. Ao mesmo tempo em que o cada vez mais sofisticado controle individual de dispositivos tecnológicos oferece, com os novos espaços de organização da internet e da *web*, possibilidades de invenção e de ruptura diante de estruturas de poder assimétricas, o colossal volume de dados gerado por esses mesmos dispositivos abre caminho a novas ferramentas de monitoramento e controle. Na esfera do Estado ou de grupos independentes, a articulação em rede de ferramentas como *IMSI-Catchers* (interceptadores de baixo custo utilizados em redes de celular), redes *mesh*, e *toolkits*

de *hardware/software* para monitoramento remoto conformam um horizonte no qual não apenas se intensifica o controle por parte de governos, mas, também, são colocadas em movimento ações de disputa e resistência agenciando grupos diversos da sociedade civil, num jogo perpétuo a contrapor poder e contrapoder.

Bruno (2014) nos lembra sobre a intersecção entre a cultura da vigilância (da videovigilância e das redes sociais na internet) e a sociedade do espetáculo, com vínculos entre vigilância, flagrante e prazer. Certamente, as câmeras de vigilância basicamente repetem as tecnologias de captura de imagens (e às vezes sons) que formam a base dos produtos de entretenimento mais populares do século XX e início do século XXI. Observar por meio delas e ser observado por elas envolve um disciplinamento de corpos e atitudes, mas também práticas associadas à diversão e à expressão.

Nesse jogo e nessa relação entre quem vigia e quem é vigiado, destacam-se, para o exercício do poder, fatores como a visibilidade ou invisibilidade dos dispositivos de vigilância. Ao mesmo tempo que a presença manifesta e evidente disciplina os sujeitos e as ações, o apagamento ou a ausência de debate público sobre seu usos são parceiros da proliferação desregulada dessa tecnologia, que dá margem a casos concretos de abusos. Discutir e mapeá-las é parte de um esforço de resistência a seu poder. Bruno (2014) aponta que o "princípio de dissociação do par ver-ser visto, associado ao princípio de 'inverificabilidade' do poder", são decisivos para que se cumpra um dos efeitos da máquina panóptica apontada por Foucault, o funcionamento automático do poder.

> Se posso discernir o olhar que me espia, domino a vigilância, eu a espio também, aprendo suas intermitências, seus deslizes, estudo suas regularidades,posso despistá-la. Se o olho está escondido, ele me olha, ainda quando não me esteja vendo (MILLER, 2000, p. 78 apud BRUNO, 2014, p. 60).

Então se coloca a questão: dada a penetração dessas tecnologias de videovigilância em nossa sociedade contemporânea, e a ampla, global, utilização de dispositivos portáteis de computação pessoal em rede, o que podemos desenvolver para, por um lado, evidenciar materialmente muitos desses equipamentos de vigilância e processamento informacional, de forma a reconhecê-los, na medida do possível, não somente em sua existência, mas também em suas potencialidades? Por outro, como desnaturalizar sua presença no espaço urbano, de modo a discuti-los para que possamos discipliná-los socialmente? Hoje, é impossível dissociar as redes digitais da dinamização, em seus efeitos, desses dispositivos. As imagens e sons, digitalizadas, circulam pelas redes, formando a matéria-prima de produtos de entretenimento ou jornalísticos. Algoritmos analisam o conteúdo digitalizado e nele reconhecem padrões, que são inter-relacionados com bancos de dados de outra natureza.

Nossa proposta é a de desenvolvimento de um aplicativo para celular[1] que, dialogando com as potencialidades técnicas e contra-hegemônicas a informar a história da computação pessoal e a emergência dos novos arranjos comunitários em rede, integre mapas do espaço urbano públicos e livres e tecnologias de realidade aumentada, em um ambiente jogável, numa plataforma colaborativa de mapeamento

[1] O aplicativo já está em desenvolvimento e possui financiamento da Fundação Ford, dentro de um projeto mais amplo intitulado "Rede Latino-Americana de Estudos sobre Vigilância, Tecnologia e Sociedade (Lavits): interseções entre pesquisa, ação e tecnologia" e que é desenvolvido pela Lavits (Disponível em:<www.lavits.org>).

coletivo de câmeras de vigilância em espaços de circulação pública. Pretendemos que esse jogo seja de uso cotidiano, de modo a que a circulação das pessoas (portando seus aparelhos de celular) por espaços vigiados por câmeras seja contabilizável e acessível pelo jogador. Com isso, pretendemos dar visibilidade e discutir a presença e uso desses equipamentos, dando ênfase em como a circulação no dia a dia é objeto dessa vigilância.

Mais do que se pretender um mapa acurado das câmeras, apontando exatamente quantas e quais são, objetivamos torná-las itens em um ambiente *online* e com as quais nele se pode interagir, mas que existem materialmente e têm efeitos para além desse espaço. Ao mesmo tempo, propomos um resgate de aspectos do debate sobre reapropriação tecnológica que, na crítica às dinâmicas burocráticas e de controle da tecnocracia industrial-militar do século XX, colocavam em questão o uso de novas tecnologias e sua relação com as estruturas de poder. Nessa interconexão entre o ambiente do jogo e o mundo concreto, queremos visibilizar esses dispositivos e discutí-los.

Para articular o debate proposto, oferecemos, como elemento a orientar a ação dos jogadores, uma história de fundo em cujo desenrolar é pretendida a contextualização e experiência de aspectos da inter-relação entre usos e produção da tecnologia na sociedade contemporânea, como a sociedade da vigilância (LYON, 2001), a apropriação tecnológica, e os usos políticos e econômicos dos dados pessoais.

STORYTELLING E DESENVOLVIMENTO

O *software* de georreferenciamento utilizado como plataforma para o jogo é, em sua arquitetura, baseado em soluções comumente aplicadas a ferramentas utilitárias de georreferenciamento para dispositivos móveis. As ações dos usuários no que diz respeito ao *input*, classificação, navegação e processamento da base de dados administrada pela ferramenta são, em sentido estrito, semelhantes às dinâmicas de usabilidade presentes em aplicativos de restaurantes, relacionamentos, táxis ou carona. Partindo da familiaridade com ferramentas de geolocalização por parte de usuários de dispositivos móveis, o uso do *storytelling* busca elaborar uma nova "camada" de uso, acionando, no território lúdico informado pela trama do jogo, um imaginário de reapropriação tecnológica e reflexão crítica ao uso político da tecnologia. Uma narrativa que, articulada ao seu uso prático, como ferramenta, acena não apenas ao debate da vigilância em espaços públicos, mas, também, aos usos e possibilidades de ferramentas tecnológicas cuja presença é "naturalizada" no cotidiano. É interessante recordar, afinal, que as estruturas transnacionais de vigilância apontadas por Edward Snowden (GREENWALD, 2014) neste início de século se apoiam, em parte não desprezível, em ações como o monitoramento de dispositivos pessoais como *laptops* e *smartphone*s.

A elaboração da estrutura narrativa, técnica e funcional do jogo teve, como base, uma série de oficinas conceituais envolvendo a equipe responsável pelo projeto. A essas oficinas, foram agregadas conversas com técnicos e especialistas no debate sobre tecnologia e política, além de investigações sobre o estado da arte dos jogos digitais experimentais realizadas por grupos de pesquisa no país, com o acompanhamento de comunicações em simpósios (CBIE, 2015; LACLO, 2015).

O universo a emergir das discussões realizadas nas oficinas conceituais foi o *ciberpunk*. A escolha parece óbvia à primeira vista – a estética, familiar ao universo

dos *games*, apontaria para um suposto reforço no potencial de engajamento. A decisão, porém, tem também um sentido de contextualização histórica: situar o *ciberpunk* como herdeiro dos movimentos de reinvenção da tecnologia computacional como ferramenta de organização contra-hegemônica, remetendo à tradição do debate crítico sobre política e tecnologia que, nos anos 1960 e 1970, lançaria mão da ficção científica e dos experimentos com tecnologia computacional como ferramentas de questionamento à tecnocracia (FELSENSTEIN, 2013). Ecoando Ballard no manifesto que, nas décadas finais do século XX, sintetizou o que veio a se desenhar na *new wave of science fiction* e sua interface entre contracultura e ficção científica, "Os maiores desenvolvimentos do futuro imediato acontecerão não na Lua ou em Marte, mas na Terra, e é o espaço *interior*, e não sideral, que deve ser explorado. O único planeta realmente alienígena é a Terra" (BALLARD, 1997).

Para a transição da proposição conceitual a uma plataforma jogável, a equipe do projeto passou a pesquisas sobre narrativa e jogabilidade utilizadas em jogos de gerações variadas, além de referências estéticas em documentações e produtos associados aos *video games* e à sua apropriação na cultura popular. Num esforço complementar, foram realizadas, também, investigações sobre temáticas e dinâmicas narrativas no cinema e na literatura de ficção científica. Os dados levantados foram sistematizados em eixos conceituais a serem implementados no desenvolvimento do jogo, a partir de testes de arquitetura de informação e aplicação funcional junto à equipe técnica do projeto.

ARGUMENTO E DINÂMICA

O jogo e seu universo buscam acionar um imaginário que acena ao funcionamento dos *role playing games* tradicionais, aberto e negociado pelos usuários e seus grupos de colaboração. A construção da narrativa e da história pessoal de cada jogador na trama do jogo se dá no simples gerenciamento da plataforma de georreferenciamento e de seus dados, num mundo aberto, sem a utilização de elementos de navegação orientada ou de níveis de jogo "fechados".

O cenário proposto aos jogadores é um futuro próximo. Uma realidade em que a inteligência artificial é empregada pelos governos como ferramenta de controle social. O terrorismo é apresentado como fator central de ameaça à ordem social, uma prática corrente em grupos oposicionistas, chegando aos espectros radicais da luta contra o totalitarismo tecnológico.

Para combater esses grupos, governos e empresas utilizariam tecnologias de vigilância, baseadas em imageamento dos espaços físicos e monitoramento das redes digitais. Para aprimorar esse sistema, é lançado um projeto público-privado de cooperação multinacional para a produção de um padrão tecnológico de integração dos dispositivos públicos de vigilância espalhados pelo planeta. O Digital Information Operative (DIO) é o esforço para a produção de um protocolo técnico inteligente que integre câmeras, formando um sistema em que todas as unidades são acessíveis remotamente. Lançado com pouco alarde, o projeto recebe a colaboração da maioria das empresas e de muitos técnicos, que acreditariam no esforço global, desdenhando alertas sobre violação de direitos. Pouco tempo depois, a iniciativa seria encerrada, também sem alarde, e oficialmente o projeto não entra em operação.

Tudo não passaria, porém, de uma farsa. Assim que iniciados os testes, a inteligência artificial que faria a integração dos dispositivos teria se mostrado incontrolável. Com todas as câmeras integradas, era impossível retirá-las da rede por um período longo

de tempo, uma vez que DIO se incumbia de reestabelecer essa conexão. Publicamente, o projeto foi descontinuado e a existência autônoma de DIO nunca foi admitida, por medo da repercussão negativa de um sistema cujo pertencimento não é opcional. Todas as câmeras do mundo estariam sujeitas ao controle do DIO.

As imagens das câmeras, de todo modo, estariam *online*, disponíveis numa espécie de "*deep web*" acessível a grupos de operação do poder político, econômico e tecnológico. Não seria possível desligá-las: governos e corporações poderiam, enfim, vigiar a todos: seria o fim da privacidade. O DIO seria a transparência total dos mais fracos, enquanto os poderosos se esconderiam. As imagens integradas nessa rede continuariam a ser utilizadas pelos governos. Após uma eficiente campanha de desinformação, a existência do DIO seria vista como um boato.

O que, para a opinião pública, não passaria de teoria da conspiração, seria uma realidade para grupos de resistência. Esta se dividiu em duas, com filosofias diferentes. O grupo Blind acredita que o caminho é cegar todas as câmeras, que a própria tecnologia de captação seria nociva. O grupo Lens acredita que o caminho é restaurar a autonomia dos dispositivos e de seus donos: se as câmeras são desconectadas do DIO, os proprietários originais dos equipamentos poderiam fazer bom uso dele. Os dois grupos aplicam essas percepções diferentes não para lutarem entre si, mas para combaterem o DIO. Porém, o DIO se autorregenera e reativa ou reincorpora as câmeras à rede após um certo tempo. Os grupos seguem lutando enquanto não encontram uma solução definitiva.

As ações dos jogadores e de seu grupo se relacionam ao cenário proposto na história de fundo por uma arquitetura de *input* de dados intrajogo (entre perfis de jogadores cadastrados) e extrajogo (entre jogadores e dispositivos urbanos a serem mapeados e, então, inseridos como elementos jogáveis). Os dispositivos móveis a partir dos quais o jogo é operado ganham, também, nova dimensão no imaginário proposto pelo DIO. Na trama, o aplicativo do DIO se apresenta como um *hack* fictício, que oferece aos jogadores um novo controle sobre seus *smartphones*. "Blindando" os protocolos de vigilância do DIO, e dando a seus donos poderes de ação e resistência sobre esse *grid* tecnológico global, os *smartphones* são, no universo do DIO, dispositivos de reapropriação tecnológica e ação política.

Aos jogadores, de ambas as facções da resistência, a ação se dá: a) na catalogação e geolocalização de câmeras de vigilância espalhadas por espaços públicos; b) na disputa pela "posse" de cada uma das câmeras catalogadas. Para catalogar e geolocalizar a camera, o jogador deve ir até ela, com o GPS de seu celular ligado, e fotografá-la, opcionalmente indicando ainda algumas informações, como para onde a câmera está apontada (lugar público ou privado, por exemplo) ou sua marca/modelo.

Para disputar a posse das cameras, o jogador deve ir até um raio de 50 metros do objeto geolocalizado, com o GPS ligado, para então com ele interagir. Cada interação sua, que pode ser feita em intervalos predefinidos de tempo, aumenta o raio de dôminancia sobre o objeto. Se, por exemplo, a câmera estiver sob o controle do grupo Lens, quando um jogador do grupo Blind passar por essa area, perderá pontos, e vice-versa.

A interação, o *hack*, de uma equipe na câmera anula a interação da rival. As câmeras/objetos possuem um limite preeestabelecido de área de atuação máxima.

A arquitetura de funcionamento do jogo está ainda em fase experimental, e são previstas novas implementações e ajustes no comportamento de ferramentas de jogo.

USO ECONÔMICO DE DADOS PESSOAIS

DIO é um jogo *online* multiusuários. A dinâmica do jogo implica em que cada jogador tenha um nome de usuário e uma quantidade de pontos cumulativa. O acúmulo de pontos permite a aquisição de novos itens jogáveis, que aumentam as potencialidades de cada jogador, a contribuição que pode dar ao seu grupo. Pretendemos, também, que o jogador possa administrar seus dados de vigilância coletados pelo jogo. Por exemplo: que cada usuário possa visualizar os trajetos que fez, em quais dias e horários, e passando por quais câmeras, e perceber e refletir que essas informações podem ser armazenadas também por outros aplicativos.

Essa funcionalidade nos permite abordar a questão do uso econômico dos dados pessoais coletados por meio de vigilância. Do mesmo modo como pensamos a visibilidade dos dispositivos de videovigilância no contexto do jogo, pretendemos dar visibilidade também para a coleta de dados, necessária para o funcionamento do próprio jogo.

O uso econômico de dados pessoais na internet se constitui, assim como as câmeras de vigilância, uma questão social polêmica e que tem sido alvo de novas propostas legislativas. Ela coloca em cena três atores principais: os cidadãos, usuários de serviços na internet; as empresas provedoras desses serviços, que utilizam os dados como matéria-prima de análises de inteligência voltadas para o comércio e fonte de lucros; e os governos, que utilizam os dados coletados para a prestação de serviços públicos e práticas de repressão política e de segurança.

Estima-se que, em 2020, o mercado de "identidades digitais" possa trazer lucros anuais de até 1 trilhão de euros somente no continente europeu (BCG, 2012). As empresas têm feito um esforço significativo em se distanciar da imagem negativa ligada aos governos e à vigilância política. Pretendem se colocar como detentoras de menor poder sobre o cidadão do que os governos. Argumentam que, em razão da livre concorrência, os cidadãos são livres para escolherem serviços alternatives, e que à legislação cabe apenas coibir os maus usos e os eventuais vazamentos de dados pessoais (ASHTON-HART, 2014).

Pode-se argumentar, entretanto, que a troca de serviços como redes sociais não é tão simples. "Se todos os seus amigos são membros de um serviço em especial é difícil que você saia, mesmo se o provedor mude os ajustes de privacidade de uma maneira que você não concorde", lembra Peter Schaar, *chairman* da Academia Europeia pela Liberdade de Informação e Proteção de Dados (SCHAAR, 2014). Os lucros astronômicos projetados pela indústria da informação são outro contra-argumento. O controle e o armazenamento de dados pessoais, que têm sido chamados de o novo petróleo, significam um poder econômico significativo que afetam a economia global e, consequentemente, as relações sociais. Mais do que nunca, informação é poder. Como pontuado por Ceglowski (2016):

> Em nossa tentativa de alimentar o *software* com o mundo, construímos o maior aparato de vigilância que o mundo já viu. Ao contrário de esforços anteriores, este é totalmente mecanizado e, em um grande sentido, autônomo. Seu poder é latente, presente nas vastas quantidades de dados pessoais de populações inteiras permanantemente armazenados.
> Começamos a recolher essa informação por acidente, como parte do nosso projeto para automatizar tudo, mas logo percebemos que ela tinha valor econômico. Poderíamos utilizá-la para tornar esse processo de autofinanciável. E então a vigilância mecanizada se tornou a base econômica da moderna indústria tecnológica.

Argumentar e convencer o público sobre como seus dados pessoais têm valor econômico é uma tarefa difícil. Do ponto de vista do indivíduo, os dados parecem informações muito triviais. A preocupação recai apenas sobre dados sensíveis, como informações bancárias, que podem ser roubadas por criminosos interessados em transferir fundos ilegalmente (FIRMINO et al., 2011). Com o jogo DIO, é possível demonstrar, por meio de itens jogáveis, como os dados agregados, mesmo que anonimizados, podem falar sobre os indivíduos. O que é mais importante, podemos demonstrar como os dados pessoais se tornaram mercadorias comercializáveis. O acúmulo dos dados de outros usuários significa lucros que crescem exponencialmente. Ao mesmo tempo, oferecer essas informações a outrem significa perda de poder.

Em uma fase posterior de desenvolvimento do aplicativo, alguns recursos novos que utilizem essas informações podem ser implementados. É possível criar um sistema em que os jogadores troquem conjuntos de informações, agregadas de acordo com tempo de jogo e anonimizadas, por pontos no jogo. O mercado para essas trocas não seria o "oficial", à administração do jogo caberia apenas regular minimamente a natureza das trocas.

A recompensa em pontos não seguiria uma progressão linear, mas exponencial, enfatizando assim o valor de estar em posse de grandes bases de dados. Da mesma forma, a jogabilidade daqueles que possuem poucos pontos pode ser dificultada, assinalando assim que aqueles que têm mais informação e mais pontos possuem mais poder e mais facilidades.

A criação dessas novas funcionalidades deve se basear, na medida do possível, nas características reais do mercado de dados pessoais. Desse modo, utilizando recursos narrativos da história e funcionalidades do jogo, podemos utilizá-lo como ferramenta de discussão sobre privacidade e dados pessoais.

PROPÓSITOS

Há diversos elementos na história que desenvolvemos para o jogo que dialogam com questões sociais relevantes na atualidade, envolvendo privacidade, vigilância e poder – como a disseminação descontrolada não somente de câmeras, mas de sensores capazes de capturar informações sobre pessoas, grupos sociais, deslocamentos e o espaço urbano; ou a aproximação e troca de dados sem critério entre organismos estatais de repressão e guerra e grandes grupos econômicos de tecnologia da informação. Até mesmo a divisão dos grupos da resistência, entre aqueles que pregam o controle social sobre a tecnologia e outros que pretendem um rompimento mais radical.

A história que desenhamos para o jogo está aberta e novos elementos podem ser agregados junto com novas ferramentas para os jogadores. Os celulares se tornaram, hoje, um poderoso sensor, que produz e transmite dados continuamente, contando com a colaboração do usuário dono do aparelho ou à revelia dele. Esses dados são utilizados economicamente pelas empresas de tecnologia (EVANGELISTA, 2016). Pretendemos desenvolver, no jogo, elementos da história e itens jogáveis que ressaltem esse fato.

Para além da denúncia e do debate público sobre a vigilância, que também são necessários, é preciso desenvolver estratégias e ferramentas que permitam à sociedade perceber sua presença e impactos na vida cotidiana e coletiva.

Artigo recebido em 08/07/2016 e aprovado em 08/11/2016.

REFERÊNCIAS

ACLU [American Civil Liberties Union].*What's wrong with public video surveillance?*. Disponível em:< https://www.aclu.org/whats-wrong-public-video-surveillance>. Acesso em: 28 jun. 2016.

ASHTON-HART, N. The internet is not incompatible with data protection, but the debate we currently have about privacy largely is. In: KLEINWÄCHTER, Wolfgang (Ed.). *Mind 7*: privacy and internet governance. Berlin: Internet & Gesellschaft Collaboratory, 2014. (Collaboratory Discussion Paper Series, 1).

BCG [Boston Consulting Group]. *The value of our digital identity*. Boston: BCG, 2012. (Liberty Global Policy Series). Disponível em:< http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf >. Acesso: 5 jul. 2016.

BALLARD, J. G. Which way to inner space. In: _____. *A user's guide to the millennium*: essays and reviews. Londres: Flamingo, 1997. Texto "Which way to inner space" publicado originalmente em 1962.

BARRET, David. One surveillance camera for every 11 people in Britain, says CCTV survey. *The Telegraph*, 10 jul. 2013. Disponível em:< http://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html >. Acesso em: 28 jun. 2016,

BRUNO, F. *Máquinas de ver, modos de ser*: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2014.

CBIE [CONGRESSO BRASILEIRO DE INFORMÁTICA NA EDUCAÇÃO], 4., 2015, Maceió. *Anais eletrônicos*. Porto Alegre: Sociedade Brasileira de Computação, 2015. Disponível em: <http://www.br-ie.org/pub/index.php/wcbie>.

CEGLOWSKI, Maciej. The moral economy of tech. In: SOCIETY FOR THE ADVANCEMENT OF SOCIO-ECONOMICS ANNUAL CONFERENCE, 28., 2016. Berkeley. Disponível em: <http://idlewords.com/talks/sase_panel.htm>.

EVANGELISTA, R. DE A.; FONSECA, F. Reconhecimento e superação da exploração capitalista em redes criativas de colaboração e produção = Recognizing and overcoming capitalist exploitation in creative networks of collaboration and production. *Liinc em Revista*, v. 12, n. 1, maio 2016.

FELSENSTEIN, Lee. Explorations in the underground 1964-1970. [Registro biográfico]. 2013. Disponível em: <http://www.leefelsenstein.com/?page_id=50>.

FIRMINO, R. J. et al. Fear, security, and the spread of CCTV in Brazilian cities: legislation, debate, and the market. *Journal of Urban Technology*, v. 20, n. 3, p. 65–84, 1 jul. 2013.

FIRMINO, R. J. et al. Social impacts of the use and regulation of personal data in Latin America. Otawa, 2011. Relatório técnico.

GREENWALD, Glenn. *No place to hide*: Edward Snowden, the NSA, and the US surveillance state. Londres: Macmillan, 2014.

ILLICH, I. *Tools for conviviality*. Londres: Calder & Boyars, 1990.

KANASHIRO, M. M.; SANTOS, L. G. DOS. Sorria, você esta sendo filmado: as câmeras de monitoramento para segurança em São Paulo. Campinas, 2006. Dissertação (Mestrado em Sociologia) – Instituto de Filosofia e Ciências Humanas, Unicamp. Disponível em: <http://www.bibliotecadigital.unicamp.br/document/?code=vtls000379198>. Acesso em: 28 jun. 2016.

KAYYALI, Dia. As Olimpíadas estão transformando o Rio em um Estado de vigilância e repressão. *Motherboard*, 13 jun. 2016. Disponível em: <http://motherboard.vice.com/pt_br/read/as-olimpiadas-estao-transformando-o-rio-em-um-estado-de-vigilancia >. Acesso em: 28 jun. 2016.

KELLY, Heather. After Boston: the pros and cons of surveillance cameras. ***CNN***, 26 abr. 2013. Disponível em:< http://edition.cnn.com/2013/04/26/tech/innovation/security-cameras-boston-bombings/>. Acesso em: 28 jun. 2016.

LACLO [Conferência Latino-Americana de Objetos e Tecnologias de Aprendizagem], 10., 2015, Maceió. *Anais eletrônicos...* [S. l.]: Laclo, 2015. Disponível em <http://www.br-ie.org/pub/index.php/teste/issue/view/135>.

LI, Amanda. Why does your business need video surveillance: top 8 reazons. *Reolink*, 20 abr. 2016. Disponível em: <https://reolink.com/why-does-your-business-need-video-surveillance/>. Acesso em: 28 jun. 2016.

LYON, D. *Surveillance society*: monitoring everyday life. Osford: McGraw-Hill Education (UK), 2001.

SCHAAR, P. The internet and big data: incompatible with data protection? In: KLEINWÄCHTER, Wolfgang (Ed.). *Mind 7*: privacy and internet governance. Berlin: Internet & Gesellschaft Collaboratory, 2014. (Collaboratory Discussion Paper Series, 1).

TURNER, Fred. *From counterculture to cyberculture*: Stewart Brand, the whole earth network, and the rise of digital utopianism. Chicago: University Of Chicago Press, 2010.