O ESTADO DA INTERNET 2022

O Estado da Internet 2022

EDIÇÃO
Pedro Fonseca

DESIGN GRÁFICO
Sara Dias
Maria Cristóvão

FOTOGRAFIA DE CAPA
Önder Örtel | Unsplash

PRODUÇÃO
Conclusão das Letras
Versão online em TICtank.pt

DATA DE PUBLICAÇÃO
Outubro 2022

PATROCÍNIO

INTRODUÇÃO

FUTUROS

DADOS

MEDIA

PASSADO

A sociedade da síndrome de Estocolmo na tecnologia

Pedro Fonseca

Há uma relação ingénua com a tecnologia. As pessoas adquirem bens inseguros, vivem despreocupadas sem proteção contra os abusos facilitados e exponenciados pelos dispositivos tecnológicos e, quando tudo corre mal, acusam as empresas a quem foram comprar os equipamentos e os serviços ou responsabilizam quem disponibilizou aplicações gratuitas que usam avidamente.

O investigador Evgeny Mozorov descreveu esta tensão em 2021, considerando que "simpatizar com as tecnológicas é uma forma perversa de síndrome de Estocolmo" (El País, 14 de junho de 2021). Ele acredita que as grandes empresas da tecnologia "estão a fazer o suficiente para preservar os seus modelos de negócio e manter a reputação para não se converterem no mesmo tipo de empresas que foram acusadas de apoiar o apartheid na África do Sul na década de 1970 e 1980".

Para Mozorov, é a "tendência oposta" que o preocupa: "esperamos que as empresas sejam boas" e uma "Microsoft resolva os problemas de cibersegurança que existe em parte porque todos usam os produtos da Microsoft que têm falhas e lacunas que são consequência do modelo de negócios da Microsoft. Ou seja, percebemos os culpados como aqueles que nos podem salvar. É uma forma perversa de síndrome de Estocolmo em que começas a simpatizar com o terrorista que te capturou".

É uma tensão que atravessa a leitura desta recolha de textos. O objetivo é revelar ideias originais na análise de alguns problemas antigos - alguns com mais de um século, como a missiva "Darwin entre as máquinas", escrita por Samuel Butler em 1863: "Dia após dia, porém, as máquinas estão a ganhar-nos terreno; dia após dia estamos a tornar-nos mais subservientes a elas; mais homens são diariamente presos como escravos para cuidar delas, mais homens dedicam diariamente as energias das suas vidas inteiras ao desenvolvimento da vida mecânica", apontava o autor, advogando que "a guerra até a morte deve ser instantaneamente proclamada contra elas. Todas as máquinas de todos os tipos devem ser destruídas pelo simpatizante da sua espécie. Que não haja exceções"...

Mais calma e próxima de nós, a Carta de Copenhaga recusa igualmente uma subserviência à tecnologia, que "não está acima de nós" e "deve servir às nossas necessidades, tanto individuais como coletivas".

O mesmo sentir atravessa as conclusões dos entrevistados que anteciparam um mundo em 2069, em que se procura "criar um futuro digital justo e equitativo", onde as visões otimistas (que repetem desejos do passado como conseguir viver mais e melhor, com menos trabalho e mais lazer) são contrariadas por preocupações como a vivência numa sociedade com riscos exponenciados de opressão agilizada pela Internet - de que a vigilância no jornalismo é precursora, como explicam Dimitri Bettoni e Federico Caruso.

Serão ambientes sem privacidade, em que se estará ligado, mas sozinho, com uma maior divisão entre privilegiados e os que menos têm. Konstantinos Komaitis exemplifica esta divisão com plataformas como o Spotify que "incentiva um ambiente de cidadãos de segunda classe contra os quais as suas políticas de conteúdo são aplicadas com mais rigor. Os criadores de conteúdo não são tratados da mesma forma".

Neste cenário, a indústria dos media continuará a evoluir para "uma aproximação cada vez mais profunda com a indústria do entretenimento", para "levar à consolidação de um modelo de comunicação de características espetaculares", em que os jornalistas são "entertainers" e a informação é um "espetáculo em que só as 'melhores' notícias – as que garantem uma audiência - têm direito à existência", escreveu Rui Trindade. Neste âmbito, o combate à desinformação não passará por "prioritizar conteúdo autêntico e de alta qualidade", como defende Olga Solovyeva.

Também as tecnologias da Internet das Coisas (IoT) serão, segundo Kean Birch, "configuradas como mais uma portagem técnico-económica para extrair mais rendimentos". Será o "fim da propriedade" como a conhecemos quando "carros, smartphones, televisores, grelhadores e outros objetos do quotidiano estão a ser mantidos como reféns através de requisitos de subscrição que desativam a sua funcionalidade se os seus proprietários não pagarem".

Esta assetização (de "assets", ou ativos que podem ser capitalizados para obter receitas), será generalizada: ativos com um potencial de elevado rendimento, como elevadores ou caminhos urbanos, podem ser progressivamente transformados em bens que se podem "possuir, negociar e capitalizar".

A IoT, como outros serviços, vive da agregação de dados - de que outra forma se saberá da viabilidade económica para colocar uma portagem numa rua sem antes saber o número de veículos ou peões que por lá passa?

Isso não será feito por indivíduos, mas pelas empresas habituadas a extrair, gerir e analisar dados. Por enquanto, nota David Moschella, "as alegações de que a Big Tech está a ganhar muito dinheiro com os 'nossos dados' estão erradas" porque os dados da maioria dos indivíduos não valem muito e porque os recolhidos em serviços comerciais já não são deles. Basta olhar para quando «os emissores de cartões de crédito discriminam as nossas compras; as operadoras de TV por cabo registam o que

vemos; as empresas de telecomunicações sabem para que números ligamos; os emissores de cartões de fidelização recompensam os clientes frequentes; os prestadores de serviços de saúde armazenam os nossos registos médicos; as escolas sabem o que estudamos e quais foram as nossas notas; os governos registam que imóveis possuímos, que países visitamos e muito mais. Ninguém duvida que essas organizações têm estes dados. Podemos ser capazes de vê-los, desafiar a sua exatidão ou limitar o seu uso, mas de nenhuma forma são ‹nossos›".

No entanto, diferente do ouro ou do petróleo, os dados são "bens não-rivais, o que significa que o meu uso de um produto não impede outrem de usá-lo também".

A constatação de Moschella é complementada por Deborah Yates, que aponta a necessidade de "considerações éticas na maneira como uma organização recolhe, usa e partilha dados", porque "deixar de cumpri-las pode ser mais prejudicial" para essa entidade.

Em resumo, os "bens não-rivais" podem ser partilhados e re-utilizados em novas dimensões, sem que as organizações que os têm o possam impedir ou, para evitar acusações prejudiciais, os estraguem. Gry Hasselbalch aborda esse "novo movimento verde para a sustentabilidade dos dados", notando que "a verdadeira sustentabilidade dos dados significa ter em conta todo o complexo de um ecossistema inter-relacionado impactado pela datificação das nossas sociedades".

Uma datificação com riscos, reforça Bernardo Beiriz quando fala das "dinâmicas da securitização do ciberespaço" e do "paradoxo do hacker", em que, "dependendo das suas ações, dotadas ou não de intencionalidade (algo que, principalmente no âmbito digital, não pode ser verificado), utilizadores comuns podem ser classificados como ameaças, resultando num estado constante de caracterização como 'ameaças potenciais'".

Uma ameaça que só pode ser atenuada quando o problema é resolvido por quem antes criou a falha técnica, as "empresas boas" de que fala Mozorov. Mas, naturalmente, impõe-se então essa "forma perversa de síndrome de Estocolmo".

Os próximos 50 anos da vida digital

Pew Research Center/Elon University

No 50º aniversário da primeira ligação em rede, a maioria dos especialistas afirmou que a humanidade será mudada para melhor pela vida digital nos próximos 50 anos. Eles alertaram, no entanto, que essa expectativa só será satisfeita se humanos e sistemas humanos evoluírem para melhor abordar a cooperação digital, a segurança, os direitos individuais e as desigualdades económicas.

A 28 de outubro de 2019 – em homenagem ao 50º aniversário dessa primeira ligação "host-to-host" da ARPANET, precursora da Internet –, tecnólogos, académicos, profissionais, pensadores estratégicos e outros foram convidados pela Elon University e pelo Pew Research Internet and Technology Project para imaginar a evolução social e tecnológica nos próximos 50 anos – até 2069. A maioria disse que a vida online continuará a ser uma mistura principalmente positiva de desafios e oportunidades. Eles temperaram as suas descrições otimistas do futuro positivo que consideram possível com preocupações como o aumento da vigilância e o abuso dos dados, a segurança porosa e uma cada vez maior divisão económica.

Entre os principais temas emergentes das respostas dos 530 entrevistados estão:

Criar um futuro digital justo e equitativo

1) Responsabilidade da humanidade: A vida digital continuará a ser o que as pessoas fazem dela. Para um futuro melhor, os humanos devem tomar decisões responsáveis sobre a sua parceria com a tecnologia.

2) Políticas públicas e regulação: A era de uma Internet maioritariamente desregulamentada irá terminar. Responsáveis eleitos e líderes tecnológicos avançarão com estruturas regulatórias destinadas a proteger o bem público. A alternativa sem lei causou perturbações perigosas em toda a sociedade.

3) Internet de Tudo: Em 50 anos, o uso da Internet será quase tão difundido e necessário quanto o oxigénio. Uma conectividade perfeita será a norma, e pode ser impossível desligar-se.

4) Visões do futuro: De avanços surpreendentes a desenvolvimentos distópicos, os especialistas imaginam uma ampla gama de cenários possíveis para o mundo daqui a 50 anos.

Visões otimistas para 2069

1) Viver mais e sentir-se melhor: a tecnologia possibilitada pela Internet ajudará as pessoas a viverem vidas mais longas e saudáveis. Os avanços científicos continuarão a diluir a linha entre o humano e a máquina.

2) Menos trabalho, mais lazer: as ferramentas orientadas por Inteligência Artificial (IA) assumirão o trabalho repetitivo, inseguro e fisicamente desgastante, deixando os humanos com mais tempo para o lazer.

3) Experiências individualizadas: A vida digital será adaptada aos utilizadores.

4) Colaboração e comunidade: Um mundo totalmente ligado em rede aumentará as oportunidades de colaboração global, cooperação e desenvolvimento comunitário, sem impedimentos de distância, idioma ou tempo.

5) Poder do povo: O acesso expandido à Internet pode levar a uma maior ruptura das existentes estruturas de poder social e político, reduzindo potencialmente a desigualdade e capacitando os indivíduos.

Visões Preocupantes de 2069

1) Ampliando as divisões: A divisão entre os que têm e os que não têm vai crescer à medida que alguns privilegiados acumulam os benefícios económicos, de saúde e educativos da expansão digital.

2) Opressão possibilitada pela Internet: Uma elite poderosa controlará a Internet e a usará para monitorizar e manipular, enquanto oferece entretenimento que mantém as massas distraídas e complacentes.

3) Conectado e sozinho: O futuro hiperconectado será povoado por utilizadores isolados incapazes de formar e manter relacionamentos humanos não mediados.

4) O fim da privacidade: A privacidade pessoal será um conceito arcaico e desatualizado, pois os humanos trocam voluntariamente a discrição por melhores cuidados de saúde, oportunidades de entretenimento e promessas de segurança.

5) Confiança mal alocada: A vida digital desnuda os utilizadores. Pode inspirar uma perda de confiança, muitas vezes ganhar demasiada confiança e regularmente exige que se avance, mesmo que não se tenha absolutamente nenhuma confiança.

6) Não há planeta B: O futuro da humanidade está inextricavelmente ligado ao futuro do mundo natural. Sem medidas drásticas para reduzir a degradação ambiental, a própria existência da vida humana em 50 anos pode estar em questão.

Artigo original "The Next 50 Years of Digital Life" publicado pelo Imagining the Internet Center da Elon University (CC).

Fonte: The Most Visited Website in Every Country (That Isn't A Search Engine)

Rêverie – atenção, vigilância, hipnose

Rui Trindade

Ante-câmara

A essência deste trabalho radica num outro: naquele que me ocupou durante as duas últimas décadas e que foi vivido no meio dos "media". Mas não é, fundamentalmente, da minha prática que aqui se trata, mas de uma prática que diz respeito a todos nós enquanto sujeitos e objectos de um universo cada vez mais regido pelas determinações das indústrias mediáticas. Este é, aliás, o ponto de partida desta reflexão: a observação do modo como o dispositivo mediático tem vindo a permear todas as instâncias sociais, não apenas a determinante económica, ou as expressões culturais, mas também a arquitectura dos espaços ou a esfera íntima. Este efeito de contaminação, absolutamente generalizado, faz então com que todos nós sejamos hoje habitantes de um espaço mediático, e isto de uma forma literal: o discurso e a lógica comunicacional regem, actualmente, de uma forma porventura insidiosa, mas sempre presente, o essencial do nosso ambiente relacional. Das arquitecturas urbanas ao negócio político, da sexualidade ao comércio, deambulamos hoje por uma multiplicidade de espaços cuja articulação profunda é dominada pelos imperativos da mediação os quais, tendo nascido em contextos precisos e localizados (e que todos conhecemos bem) foram migrando sucessivamente para outras esferas ocupando agora, por inteiro, a paisagem que nos rodeia.

Uma segunda linha de observações, na sequência do que atrás se disse, prende-se com a natureza que esta mediatização global foi assumindo. A indústria dos "media" pode servir, a este respeito, como um bom exemplo pois o seu movimento interno tem-na feito evoluir no sentido de uma aproximação cada vez mais profunda com a indústria do entretenimento. Com que consequências? Essencialmente a de levar à consolidação de um modelo de comunicação de características espectaculares ou, dito de outro modo, fazendo com que mesmo as instâncias informativas obedeçam hoje a uma lógica distractiva. Os jornalistas tornaram-se "entertainers" e a informação num espectáculo em que só as "melhores" notícias – as que garantem uma audiência - têm direito à existência. Esta prevalência da função distractiva, que já levou Umberto Eco a reflectir sobre o seu significado na perspectiva de um entendimento sobre o que pode acontecer a comunidades como as nossas, que vivem sob o signo de um Carnaval permanente, estende-se, actualmente,

à generalidade das práticas colectivas e impregna, de forma quase absoluta, aquilo que definimos mais acima como o espaço da mediatização global. Como veremos mais à frente, todos os negócios assentam hoje, no limite, num modelo que tem o entretenimento como matriz. E porquê? Porque no universo em que nos movemos hoje a disputa da atenção tornou-se um elemento central. Sobrecarregados por uma pluralidade de estímulos, dispersos por mil e uma solicitações, a nossa atenção ganhou um valor económico decisivo.

Aqui chegados, desembocamos no terceiro domínio de reflexões que compõem este trabalho e que constituem a sua motivação central. Importa, com efeito, averiguar como se desenha esta nova economia da atenção e de que forma ela se exerce. A questão da atenção não é propriamente um tema novo, como Jonathan Crary teve oportunidade de demonstrar, pelo contrário, ela está intimamente ligada ao desenvolvimento da sociedade industrial e à sua necessidade de garantir um indivíduo produtivo, controlável e previsível. Mas a combinação resultante do fenómeno da globalização, da disseminação das tecnologias de informação e dos imperativos comunicacionais das últimas duas décadas produziu um dispositivo de controle cuja capacidade de manipulação está muito para além do que se poderia alguma vez prever. Com efeito, nas sociedades contemporâneas assiste-se a uma conjugação de modalidades muito diversas: o indivíduo tanto é objecto duma atenção vigilante como sujeito de imperativos que procuram fixar, de forma persistente e obstinada, a sua atenção. Desenha-se assim em seu torno uma paisagem fortemente coerciva, mesmo quando as formas de coacção assumem características dissimuladas. A questão que se coloca então é a de saber como, nestas "sociedades de controle", como lhes chamou Gilles Deleuze, se pode insinuar a resistência ou a dissidência. Ou, dito de outro modo, como pode o pensamento sobreviver aos actuais dispositivos de coacção e fixação e garantir as condições de uma permanente deriva.

O mercado da atenção

O reconhecimento da centralidade da atenção no sistema económico actual é verificável em múltiplas frentes e os últimos dois anos têm sido férteis em ensaios abordando o tema.

O que caracteriza, de um modo geral, estas abordagens é a noção de que na fase actual do capitalismo – seja ele o "capitalismo cultural" na descrição de Jeremy Rifkin ou o "capitalismo em rede" de Manuel Castells – do que se trata já não é, essencialmente, de vender produtos mas sim experiências. Entrámos numa fase em que a materialidade dos bens se tornou secundária. O que conta é a informação e o investimento simbólico neles contido. É a este nível que se realiza hoje a apropriação dos bens materiais, tornando-os, a bem dizer e em rigor, completamente imateriais. Um dos livros que melhor descreve esta situação, não de um ponto de vista teórico ou académico, mas numa perspectiva instrumental é "The Experience Economy"

de Joseph Pine e James Gilmore. Para estes dois consultores, as empresas terão de se capacitar que, para serem bem sucedidas, têm de perceber que o seu negócio reside no "fabrico de memórias" e não na produção de bens materiais. Por exemplo, quem fabrica e vende carros tem de perceber que é a "experiência da condução" que está a vender, não os carros. Ora a construção desta experiência, para que ela seja verdadeiramente eficaz e se torne memorável, tem de assentar numa narrativa consistente e, acima de tudo, estimulante. É aqui que entra, então, o "entertainment". Pine e Gilmore desenvolvem no livro um paralelo com o teatro e propõem às empresas que se organizem na perspectiva de uma performance – tal como no teatro. Ou seja, do que se trata, segundo eles, é de estruturar a produção na perspectiva desta se assumir como um elemento determinante da fábrica de sonhos em que o negócio se tornou. Nesta perspectiva, que melhor modelo existe para uma fábrica de sonhos do que Hollywood? É isso que um outro livro propõe exactamente.

Em "The Entertainment Economy", Michael J. Wolf defende que no contexto de uma economia da atenção como é aquela em que vivemos, a única estratégia possível tanto para as empresas como para os indivíduos é a adopção das regras fundamentais do "show business". Segundo ele, o velho dizer "there's no business like show business" já não corresponde à realidade presente pois o que está a acontecer é que "every business is show business". Isto é, estamos todos no negócio do entretenimento. Michael Wolf começa, aliás, por descrever no seu livro como é que o "espectáculo" tomou conta das nossas vidas – como é que aquilo que era uma dimensão específica do viver colectivo contaminou a totalidade do real ao ponto de se tornar na sua força estruturante – para se concentrar depois na explicitação das regras de sobrevivência em sociedades dominadas pelo imperativo da atenção. Que nos diz ele a este propósito? Bem, se se tomar Hollywood como modelo, não há nada mais simples, a receita é conhecida: é precisa uma boa história e uma estrela de primeira grandeza. Tal como para Pine e Gilmore, também para Wolf do que se trata é de fabricar memórias e vender experiências. Mas Wolf introduz a questão da celebridade na equação como uma mais-valia fundamental para garantir um poder de atracção superior. É sabido que a existência de uma celebridade num contexto de grande densidade comunicacional funciona sempre como um elemento importante para fixar as atenções. Mas do que Wolf está a falar é de uma realidade em que todo e qualquer um se pode assumir como estrela.

Foi também isso que compreendeu Robert Kelley no seu livro "How to Be a Star at Work". Colocando-se já numa perspectiva eminentemente prática, num registo do tipo "saiba como fazer", leva às últimas consequências os pressupostos avançados pelos anteriores autores. É que se a lógica que permeia todas as actividades e é o motor determinante dos mercados é a do espectáculo então, mesmo no mais circunscrito dos microcosmos, é aquele que é capaz de se tornar numa celebridade quem define as regras do jogo, fixa as

atenções e faz a economia andar. No limite, não só todos estamos no negócio do entretenimento como todos podemos (e se calhar devemos) tornar-nos celebridades.

Nam June Paik ironizou, em tempos, sobre o facto de vivermos numa época em que "já não há nada para comprar". A referência tinha como implícita a ideia de que, nas sociedades de consumo, se tinha atingido um nível de saturação completo. Paik estava obviamente enganado, mas ele não podia adivinhar que um dia até as "relações humanas" seriam incluídas no dispositivo mercantil e comercializadas sob a forma de "experiências". Como escreve Norman Denzin, da Universidade do Illinois, "as 'vivências' tornaram-se na derradeira mercadoria na circulação do capital".

Esta mercantilização do "vivido" nem sempre surge empacotada comercialmente; antes se situa, muitas vezes, num plano cujas ligações ao mercado são, de algum modo, indirectas. É o caso dos milhares de "webcams" que hoje povoam a Internet e abrem a vida íntima do mais anónimo dos cidadãos à observação planetária. Mas esta exposição global da intimidade individual – aquilo a que o teórico alemão Florian Rotzer denomina "a publicação do íntimo" - o que atesta, no fundo, é mais uma vez um desejo de atenção ou, nas palavras de Rotzer, um desejo de proeminência. Mais do que mera cumplicidade voyeurística, o que transparece nesta publicitação da intimidade é a adopção da lógica da mediatização global. A esfera privada torna-se pública e todo e qualquer condomínio um pequeno palco onde, 24 sobre 24 horas, se joga uma performance: entediante, dramática, excitante ou anódina, pouco importa. Do que se trata é de partilhar a mediaesfera global e esperar que as "regras da atracção" funcionem no mercado mundial da atenção e uma qualquer proeminência seja alcançada. O próximo passo, neste domínio, pode, aliás, ser antecipado: com a evolução dos chamados "wearable computers", isto é, um tipo de computadores que estarão imbuídos no vestuário e em todo o tipo de aplicações portáteis, cada um poderá estar então sempre ligado à Internet e transmitir em directo e em tempo real a sua experiência pessoal e única.

Vigilância e coacção

Gostava de me deter agora um pouco na questão da atenção e da sua contextualização em termos históricos para podermos compreender melhor como chegámos aqui.

Jonathan Crary demonstrou de forma exaustiva em "Suspensions of Perceptions" que a maneira como ouvimos, vemos ou nos concentramos em algo tem um carácter eminentemente histórico. Assim, escreve Crary: "Seja o modo como nos comportamos em frente do ecrã luminoso do computador ou a maneira como vivemos uma performance na ópera, a forma como realizamos certas tarefas sejam elas produtivas, criativas ou pedagógicas ou ainda, de uma forma mais passiva, o modo como desempenhamos tarefas rotineiras como guiar um carro ou assistir à televisão, estamos sempre numa dimensão da

experiência contemporânea que requer que cancelemos ou excluamos do domínio consciente uma grande parte do ambiente que nos rodeia". Nesta perspectiva o que interessou a Crary foi investigar o modo como a modernidade ocidental exigiu dos indivíduos desde o século XIX que se definissem e se redesenhassem a si próprios em termos da capacidade de "prestar atenção", isto é, da capacidade de se desligarem, grosso modo, do que os rodeia para se focarem num número reduzido de estímulos. Esta necessidade de focar a atenção está óbvia e intimamente ligada às necessidades do capitalismo nascente e ao imperativo de estabelecer um regime disciplinar que garantisse uma massa de indivíduos produtivos e socialmente integrados. O que torna a situação mais complexa, no entanto, é a natureza dinâmica do capitalismo cuja lógica incessante de inovação gera, ela própria, mecanismos de desatenção. "A modernidade capitalista gerou um processo de constante recriação das condições da experiência sensorial", escreve Crary. E acrescenta que é mesmo possível entender a modernidade como "uma crise permanente da atenção, na qual as constantes reconfigurações do capitalismo levam continuamente o binómio da atenção/distracção a novos patamares, através de uma interminável sequência de novos produtos, fontes de estímulo e fluxos de informação que, por sua vez suscitam novos métodos de gestão e regulação da percepção".

Do ponto de vista deste trabalho, que é o da observação do desempenho das indústrias da informação e da comunicação, o que importa reter é que desde os finais do século XIX há quem tenha tido a intuição de que "um sujeito atento podia ser produzido e gerido através do conhecimento e do controle de procedimentos externos de estimulação e do uso de uma série de tecnologias de atracção". Estas tecnologias de atracção correspondiam, no final do século XIX, aos primeiros passos da cinematografia. Mas ao longo de todo o século seguinte as noções relativas ao entendimento do que é a percepção ou a atenção vão evoluir e transformar-se em paralelo com a emergência de novas formas tecnológicas ligadas ao espectáculo, seja no domínio da representação, da projecção ou da gravação. Todas estas transformações fazem-se acompanhar, por sua vez, pelo desenvolvimento de novos conhecimentos acerca do comportamento e da subjectividade dos seres humanos.

Esta combinação, por um lado, da convicção que é possível impor uma atenção aos indivíduos a partir de estímulos externos, nomeadamente tecnológicos, e por outro a aquisição de conhecimentos que possibilitam manipular os comportamentos, não tem cessado de se reforçar e funciona hoje a uma escala sem precedentes. Vale a pena sublinhar, de passagem, que este imperativo de controle através da fixação da atenção não passa, em rigor, pelos chamados conteúdos, isto é, pelo que eventualmente possa passar no ecrã do computador ou da televisão. Como refere Raymond Williams em "Television and Cultural Form", seja no domínio do consumo de massas ou dos meios mais individualizados como o computador, do que

se trata, em todos os casos, é de situar os indivíduos num contexto de conformidade ou, para retomar a expressão de Michel Foucault, de gerar um "corpo dócil".

Esta docilidade é hoje obtida através de uma série de técnicas e tecnologias cuja sofisticação as torna, a maior parte das vezes, invisíveis. Um excelente relato, a este respeito, pode encontrar-se em "Coercion: Why We Listen to What They Say", de Douglas Rushkoff. O autor que, em obras anteriores se tinha mostrado um firme defensor do poder libertador das novas tecnologias, procede em "Coercion" a um relato implacável dos diversos instrumentos de persuasão e controle que agem actualmente na mediaesfera.

Do mundo da publicidade aos centros comerciais, da Internet às relações públicas, o que sobressai é o extraordinário poder da aliança entre as tecnologias de informação e as disciplinas do comportamento. Isto é particularmente visível no modo como são configurados os novos espaços urbanos, em especial os centros comerciais, onde das cores escolhidas, à música e às fragrâncias que impregnam os diversos ambientes, nada é deixado ao acaso. Mas talvez o mais impressionante neste domínio do controle comportamental é o papel que desempenha a análise, baseada no vídeo e no computador, dos movimentos dos consumidores nestes grandes espaços.

É com base nestas análises que se definem os itinerários, as rotinas e as modalidades de uma persuasão tão discreta quanto eficaz. E se os domínios fechados como os centros comerciais constituíram uma primeira instância na articulação dialéctica do espectáculo e da manipulação, encontramos essa mesma dinâmica em espaços abertos, quer naqueles que, como os parques temáticos, mantêm dispositivos de controle sobre os movimentos das massas, quer inclusivé naqueles em que, como em Nova Iorque, na confluência da Rua 42 com Times Square, esses controles não existem.

Estas estratégias de controle funcionam também, embora de forma completamente diversa, nos mecanismos de vigilância que hoje se espalham pelos espaços urbanos, tanto públicos como privados. Como é sabido, a proliferação de câmaras intensificou-se extraordinariamente nas últimas duas décadas. Só num país, o Reino Unido, existem hoje mais de 200 mil câmaras de vídeo cobrindo todo o tipo de locais: de supermercados a parques de estacionamento, de elevadores a estações de metropolitano. A estas câmaras vieram, entretanto, juntar-se sensores de movimento, sensores térmicos, sistemas de controle de voz, etc. Esta vigilância contínua que nos torna, por uma vez, em "objectos" de atenção, tende, no entanto, a induzir comportamentos tipificados que procuram garantir uma normalidade e uma insuspeição a toda a prova. Relembre-se, a título de exemplo, que um programa de computador desenvolvido pela Universidade de Leeds, para análise de imagens de vídeo, pretende ser capaz de distinguir entre um comportamento normal e um outro suspeito a partir do tratamento de milhares de horas de

imagens recolhidas em supermercados, parques de estacionamento, etc.

"Talvez um dia – escreve com ironia Florian Rotzer – o acesso a espaços não-monitorizados venha mesmo a constituir um elemento de distinção social, um privilégio destinado a descomprimir dos constrangimentos de uma normalidade identitária imposta". Para já, o que sabemos – e não vamos poder agora entrar em detalhes – é que todos temos hoje uma sombra digital, um rasto deixado por cartões de crédito, telemóveis e usos da Internet.

O factor hipnótico

Para terminar, gostaria de retomar uma citação referida mais acima, extraída do trabalho de Jonathan Crary, a qual notava o modo como a partir do final do século XIX foi ganhando peso em determinados sectores da sociedade a convicção de que seria possível produzir um indivíduo atento através do uso de estímulos externos, nomeadamente de tecnologias de atracção. Tom Gunning demonstra num texto seu, em "The Cinema of Attractions: Early Cinema, Its Spectator, and the Avant-Garde", que o que está em jogo nesses primórdios do cinema – estamos a falar dum período entre 1880 e 1890 – não são tanto questões relativas à representação, à imitação, à narração ou à adequação das formas teatrais, mas acima de tudo a definição de estratégias que fixem a atenção do espectador. Ora este é também um período histórico em que se assiste, curiosamente, à emergência da hipnose como um campo científico novo e cheio de potencialidades. E a hipnose é claramente entendida então como um modelo ou uma variação extrema do fenómeno da atenção pois envolve uma intensificação da concentração. Como nota Jonathan Crary, este interesse pela hipnose só pode ser compreendido num contexto de racionalização de processos. "Tal como as inovações fotográficas e cinematográficas nos anos de 1880 e 1890 definiram os termos em que se processou a automatização da percepção, também a hipnose, apesar dos paradoxos que revelou, era uma tecnologia que trazia consigo a promessa de tornar o comportamento automático e predizível".

Mas a existência da hipnose enquanto campo disciplinar reconhecido e aceite foi de curta duração. Ao longo de quase todo o século XX, sobreviveu apenas de forma marginal e só agora parece retomar o seu lugar de cidadania no discurso científico (vejam-se, por exemplo os mais recentes trabalhos de Isabelle Stenghers, a colaboradora de Prigogine). Para Jonathan Crary, esta situação deve-se ao facto da "hipnose implicar de uma forma poderosa possibilidades tão excessivas de controle cognitivo e perceptual que, independentemente delas estarem ou não empiricamente provadas, a hipnose se tornou incompatível com as concepções dominantes sobre o carácter autónomo e voluntarista da subjectividade humana".

Esta saída de cena é sintomática e sublinha, de algum modo, a dificuldade de pensar situações nas quais a vontade humana é modificada ou controlada por forças exteriores. Apesar disso alguns

autores estão hoje a retomar de uma forma renovada e despreconceituada uma análise da contemporaneidade com base nas referências clássicas dos procedimentos hipnóticos. É o caso, por exemplo, do objecto televisivo em torno do qual Daniel Bougnoux tem trabalhado. Em "L'impensé de la Communication" - um texto incluído na colectânea "La suggestion: Hypnose, influence, transe" - este investigador francês demonstra claramente o papel que a sugestão desempenha em sociedades dominadas pelo paradigma comunicacional incluindo nesta definição de sugestão "os efeitos de moda, mimésis, psicologia de massas, contágio mediático e influências de todos os tipos". Também J.J. Wunenburger num texto incluído no dossier "L'Ére du Divertissment" da revista "Cités" aborda a televisão enquanto indutor hipnótico e Douglas Rushkoff, já aqui citado, trabalha no seu livro "Media Virus" a hipótese da mediaesfera configurar um sistema de propagação viral de ideias e comportamentos cuja filiação poderia, de certa maneira, encontrar-se também na noção de "sugestão". Entre muitos exemplos possíveis gostaria apenas de citar, para finalizar, um que é dado por Marie Winn em "The Plug In Drug: Television, Children and the Family". Nele se relata como os produtores da famosa série "Sesame Street" desenvolveram uma metodologia de teste para analisar o grau de atenção das crianças aos episódios da série. Usando um terminal de vídeo com capacidade de monitorizar os espectadores, os produtores da "Sesame Street" procederam a uma metódica e sistemática análise de cada segmento, de cada episódio, no sentido de maximizar ao limite as possibilidades de cativar a atenção das crianças. Do que se trata aqui é muito mais do que definir personagens e histórias interessantes: é acima de tudo saber gerir a quantidade de movimento no ecrã ou a velocidade de mudança de umas imagens para as outras.

A esta luz, talvez não tenha sido inteiramente acidental a definição que Guy Debord deu na "Sociedade do Espectáculo" ao descrevê-la como tendo um "comportamento hipnótico".

Rêverie

Por cada mudança no regime da atenção há, em paralelo, também uma mudança nas tipologias da desatenção. Há por isso uma história ainda por fazer: a da averiguação de como a atenção foi e é o lugar de uma tensão entre as estratégias de controle e os impulsos de resistência e deriva. Nesta história haveria sobretudo que saber até que ponto aquilo que se designa por "day dreaming" ou "rêverie" constitui hoje a essência de uma resistência interna à coacção. Ou ainda de que modo modalidades criativas de transe e de inatenção podem florescer nos interstícios de um sistema cujas lógicas de apropriação não toleram qualquer exterioridade.

Fonte: The Most Visited Website in Every Country (That Isn't A Search Engine)

A assetização da vida social

Kean Birch

O que vai acontecer no próximo ano? Ou no ano seguinte? Ou mesmo daqui a cinco anos? Se ao menos pudéssemos prever o futuro, poderíamos fazer algo a respeito disso agora. Se nos preocupamos com o mundo, podemos torná-lo melhor promovendo mudanças sociais, políticas ou económicas específicas... ou, se tivermos uma mentalidade menos social, podemos simplesmente lucrar com a nossa previsão. No entanto, nenhum de nós consegue olhar para o futuro. Mas isso não impede que as pessoas ganhem bem como futuristas e visionários, que institutos de pesquisa, "think tanks" e outras organizações atraiam financiamento prevendo e promovendo tendências futuras, ou investidores façam declarações financeiras a prometer lucros futuros acima da média. Em nenhum lugar tais promessas e visões futuras são mais prevalentes do que na economia política da ciência e tecnologia, especialmente numa era dominada por grandes empresas de tecnologia como Apple, Amazon, Microsoft, Alphabet/Google e Meta/Facebook.

As promessas tecno-económicas são poderosas. As esperanças de novas tecnologias digitais e algorítmicas brilham especialmente nas narrativas de instituições como o Fórum Económico Mundial (WEF) quando promove um mundo radicalmente alterado por cidades inteligentes, blockchain, Internet das Coisas e um fluxo interminável de "sistemas ciber-físicos" transformadores. Apresentando essas promessas como a Quarta Revolução Industrial – 4IR se concordar com mais uma "buzzword" da gestão –, o WEF reformulou-se desde meados da década de 2010 como um bastião de visões tecnológicas para um futuro melhor, impulsionado pelas ideias de seu fundador e presidente executivo, Klaus Schwab. Segundo ele, podemos esperar um mundo de "supercomputação móvel, ubíqua. Robôs inteligentes. Carros autónomos. Melhorias neurotecnológicas do cérebro. Edição genética. A evidência de uma dramática mudança está à nossa volta e a acontecer a uma velocidade exponencial". É importante lembrar que WEF e Schwab estão a oferecer mais do que promessas.

O engraçado sobre essas promessas tecnológicas é que elas geralmente não se concretizam. Os carros autónomos – e outras diversas maravilhas – são tão propensos a funcionar e a tornarem-se comuns quanto os carros voadores imaginados há décadas enchendo os céus de hoje. Embora essas visões tecnológicas raramente se materializem, elas cumprem uma função político-

económica. As visões das tecnologias futuras abrem caminho para decisores de políticas, políticos, empresas, instituições internacionais e outras, como o WEF, gerarem expectativas que configuram como pensamos sobre o futuro, especialmente quando se trata de mudanças tecno-económicas. Ao fazerem promessas, entidades como o WEF e o seu fundador podem forçar hoje mudanças nas políticas, regulamentações e instituições para realizarem as suas preferidas visões de futuro. E isso tem implicações significativas em como entendemos a mudança tecno-económica e as suas consequências.

Há um lado sombrio nos futuros tecnológicos que o WEF prevê. A visão que sustenta o 4IR promovido por Schwab e pelo WEF, por exemplo, depende de narrativas de constantes e imparáveis transformações tecnológicas e político-económicas do nosso mundo e vidas. A tecnologia irá, na visão deles, alterar radicalmente a forma como vivemos e, além disso, como devemos viver as nossas vidas. Um exemplo-chave dessa transformação radical é o lançamento da chamada Internet das Coisas (Internet of Things ou IoT), que tem como premissa a extensão total da vigilância digital nas nossas vidas por meio do rastreamento, recolha e exploração de dados digitais sobre tudo o que fazemos. Para quem não sabe o que a IoT envolve, é basicamente a inserção de "tags" digitais, monitores e processadores em todos os objetos do nosso mundo para que possamos ajustar melhor o seu desempenho à medida que os usamos. Quer aumentar a eficiência na compra de alimentos? Então compre uma geladeira "inteligente" para lhe dizer – ou, mais provavelmente, ao seu entregador de comida – quando comprar mais tomates. Quer aumentar a sua eficiência de lavagem? Então coloque um "chip" nas suas roupas para dizer à máquina de lavar a melhor forma de lavá-las. E assim por diante, em todos os aspetos das nossas vidas. As tecnologias de identificação por radiofrequência (RFID) já são omnipresentes – tendo descolado em grande estilo desde 2012, de acordo com o investigador de media Jordan Frith – e geralmente estão integradas em roupas, smartphones, sensores de portas, cartões bancários, passes de viagem e outros artigos semelhantes. Mas as tecnologias RFID atuais são frequentemente passivas e limitadas no seu processador de dados, enquanto a IoT tem como premissa aumentar o papel das tecnologias digitais para que elas possam recolher mais dados e comunicar com mais partes de um ecossistema digital cada vez maior.

Isto pode parecer útil – e pode ser, se formos capazes de pensar e planear cuidadosamente a sua implementação e possíveis impactos sociais. Mas, neste momento, as tecnologias de IoT parecem ser cada vez mais implementadas e configuradas como mais uma portagem técnico-económica para extrair mais rendimentos. A conta do Twitter Internet of Shit aborda alguns dos absurdos dessas tentativas de alargar o arrendamento ["rentiership"] em todos os aspetos das nossas vidas. A frase deles, "coloque-lhe um 'chip'", reflete as inúmeras tentativas das empresas de explorar a gama de tecnologias digitais emergentes para ganhar dinheiro

com as nossas vidas, quaisquer que sejam as consequências. Carros, smartphones, televisores, grelhadores e outros objetos do quotidiano estão a ser mantidos como reféns através de requisitos de subscrição que desativam a sua funcionalidade se os seus proprietários não pagarem. Tudo isso é possibilitado por uma gama de tecnologias digitais e algorítmicas concebidas especificamente com essa tarefa em mente – extrair essas rendas. Como os juristas Aaron Perzanowski e Jason Schultz apontam, é realmente o "fim da propriedade" como a conhecemos.

O que me traz de volta a Klaus Schwab e ao WEF. À medida que o 4IR é implementado como uma solução política para o problema social de jeur, ele acaba apoiando o desenvolvimento omnipresente de tecnologias digitais e algorítmicas que permitirão às empresas "monitorizar e otimizar ativos e atividades a um nível muito granular" – para usar as palavras de Schwab. Isto significa o quê? Na sua essência, significa a transformação de quase tudo em nosso redor num ativo político-económico que pode ser controlado, negociado e capitalizado com base nos seus fluxos de futuros lucros. Há duas dimensões importantes para esta assetização das nossas vidas sociais: como é que as coisas são transformadas em ativos ["assets" ou "qualquer coisa que pode ser controlada, negociada e capitalizada como um fluxo de receita"]? E como é que essa transformação configura e restringe os nossos futuros? Um crescente interesse em diferentes processos de assetização é descrito num livro que recentemente coeditei com o sociólogo Fabian Muniesa intitulado "Assetization: Turning Things into Assets in Technoscientific Capitalism" – também em acesso aberto. O nosso objetivo com o livro é mostrar quantas coisas – quase qualquer coisa, na verdade – podem ser transformadas num ativo com o adequado conhecimento técnico-económico, práticas de cálculo, dispositivos técnicos, organizações e assim por diante. Um ativo, porém, é mais do que uma simples reivindicação de propriedade; é, mais fundamentalmente, uma reivindicação política sobre o futuro, especialmente através do direito a receitas futuras. E isso cria um dilema político e de política quando se trata da IoT e da sua extensão de recolha e exploração de dados.

Existem vários aspetos problemáticos para as novas tecnologias digitais e algorítmicas que sustentam a IoT (assim como blockchain, tokens não fungíveis, cidades inteligentes e outras visões futuras)

Primeiro, eles implicam e dependem da contínua recolha maciça e análise de dados digitais, particularmente dados pessoais – os nossos nomes, histórias pessoais, atividades e comportamentos diários, gostos e desgostos e assim por diante. E por maciço, quero dizer maciço. Tudo o que fazemos torna-se valioso quando é registado numa base de dados digital porque pode ser canalizado para a analítica de dados para fazer previsões e julgamentos inferenciais sobre as nossas ações – "o que vai o Johnny comprar de seguida" – e porque a própria capacidade de registar digitalmente todas as nossas ações abre um leque de possibilidades de valorização da própria vida social, à qual voltarei.

Em segundo lugar, essa massificação da recolha de dados e a sua exploração tem um efeito de autorreforço no qual os maiores recolectores – principalmente empresas de Big Tech – podem criar os seus próprios enclaves de dados incrivelmente úteis socialmente – por exemplo, informações sobre a frequência com que as pessoas usam uma determinada linha de trânsito ou estrada e quais as razões – que são valiosas precisamente por causa das limitações que a Big Tech impõe ao acesso a esses dados. Não é surpreendente, assim, descobrir que essas empresas de Big Tech são agora algumas das maiores e mais poderosas empresas do mundo, como demonstra um relatório recente do SOMO. Por fim, o desenvolvimento de tecnologias algorítmicas – geralmente chamadas de Inteligência Artificial (IA) – é dominado por preocupações e imperativos corporativos, especialmente os das grandes empresas de tecnologia precisamente por causa dos seus enclaves monopolistas de dados. Meredith Whittaker, cofundadora do AI Now Institute, argumenta que os investigadores dependem desses enclaves de dados e do poder de computação dessas grandes empresas de tecnologia para fazerem a sua pesquisa, o que não apenas fortalece o seu poder de mercado (limitando a ascensão de concorrentes) mas dá-lhes a capacidade de moldar o próprio futuro dessas importantes tecnologias.

Isto tem implicações profundas, algo que tenho investigado nos últimos anos com vários colegas. Parece que a inovação e os nossos futuros tecnológicos estão a ser impulsionados pela assetização total da própria vida social; de tudo o que fazemos gratuitamente hoje e de muitas coisas que nem conseguimos pensar ainda no futuro. O que pode isso significar na prática? Não preciso ir muito além das ideias do próprio Klaus Schwab que postulou: "A capacidade de prever o desempenho de um ativo também oferece novas oportunidades para atribuir preços a serviços. Ativos com elevado rendimento, como elevadores ou caminhos, podem ser precificados pelo seu desempenho". As implicações da implantação da IoT, cidades inteligentes, IA e toda uma série de outras tecnologias digitais é que tudo nas nossas vidas pode ser progressivamente transformado num ativo que alguém pode possuir, negociar e capitalizar. Como ilustra a citação de Schwab, com os dispositivos técnicos e político-económicos certos, podemos transformar objetos mundanos em recursos geradores de dinheiro; por exemplo, uma escada pode ser monetizada por meio de sensores digitais que se ligam aos nossos smartphones, recolhem os nossos dados pessoais e cobram-nos de cada vez que subimos ou descemos as escadas. O mesmo pode aplicar-se a elevadores, escadas rolantes, portas, corredores, calçadas, semáforos e muito mais. Todos os aspetos das nossas vidas podem ser monetizados dessa forma.

Outro exemplo emergente dessa assetização da vida social é a maneira como as nossas escolas e instituições de ensino estão a ser transformadas por meio da implantação da chamada tecnologia educacional, ou 'EdTech'. Novamente, o WEF está muito interessado nessa transformação da educação através da introdução de novas tecnologias digitais que

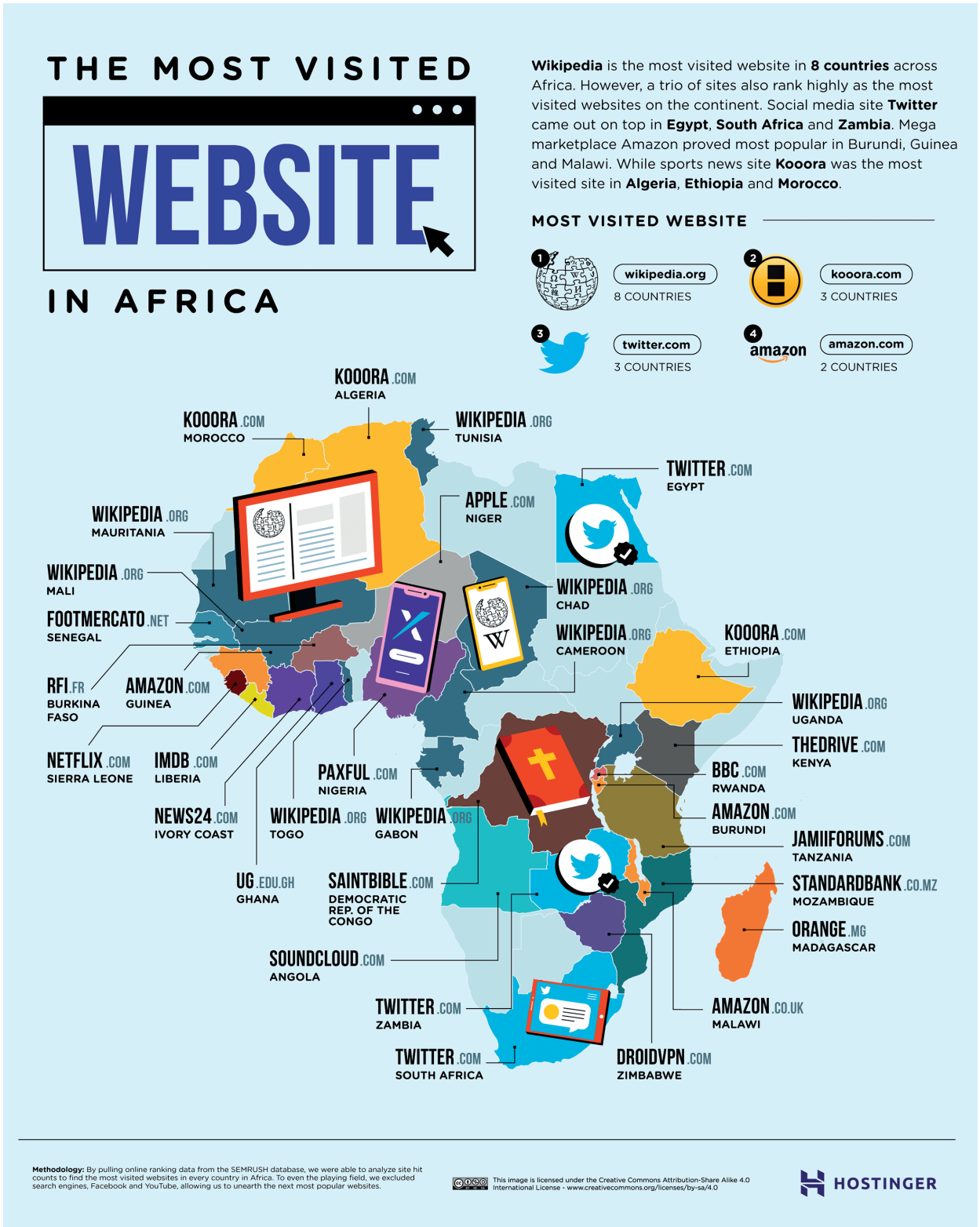
podem "criar melhores sistemas e fluxos de dados". A própria EdTech varia da gestão de programas online para estudantes (por exemplo, Moodle), passando por software organizacional (por exemplo, Teams) e plataformas de ensino (por exemplo, MOOCs), e tudo isso foi acelerado pela pandemia de Covid, pois o ensino online teve de substituir o presencial.

A trabalhar num projeto liderado por Janja Komljenovic na Lancaster University, examinei as maneiras pelas quais a EdTech é minada pela assustadora assetização das nossas universidades. Está a transformar estudantes, educadores e as próprias instituições em mais uma oportunidade de ganhar dinheiro para os negócios. Muita da EdTech – e especialmente a visão que o WEF tem dela – tem como premissa a ideia de que o mercado é o melhor mecanismo para resolver os nossos problemas sociais, mas essa nem é a pior parte desta transformação.

Como Komljenovic aponta no seu trabalho anterior, a EdTech envolve novas plataformas digitais que não apenas cobram taxas de assinatura pelo uso, mas também recolhem dados de alunos, educadores e instituições. As universidades vão ficar presas a um futuro em que não poderão desenvencilhar-se dos fornecedores de EdTech sem perderem o acesso a todos os dados e informações de que precisam para operar. E isso deixando de lado os problemas de consolidação na EdTech e o surgimento de monopólios que podem cobrar o que quiserem. Basicamente, o que isto significa é que os alunos passarão pelos seus anos de escolaridade e de universidade e todos os dados recolhidos sobre eles serão transformados num ativo privado que as empresas de EdTech podem explorar.

Há muitos outros exemplos que se poderiam considerar – e tenho feito isso em investigação – mas o ponto fundamental a transmitir é que tudo isto é uma escolha. Os ativos são feitos. Alguém ou alguma organização tem de transformar a nossa vida social num ativo que pode ser monetizado, capitalizado e explorado. A assetização não é um processo técnico ou neutro, é inerentemente político e contestável, se o desejarmos. Compreender como isso acontece – como as pessoas transformam as vidas em ativos – é extremamente importante porque ajuda-nos a identificar onde se pode intervir no processo para o interromper ou parar, ou para garantir que é feito democraticamente e no suporte a algum tipo de bem social, se tiver de ser feito. A assetização é uma das questões mais importantes dos nossos dias, porque é sobre quem será o dono do futuro e como fará isso.

Artigo original de Kean Birch, publicado no Bot Populi (CC).



Fonte: The Most Visited Website in Every Country (That Isn't A Search Engine)

Os seus dados não são ouro; nem são seus

David Moschella

As alegações de que a Big Tech está a ganhar muito dinheiro com os "nossos dados" estão erradas de duas maneiras fundamentais: os dados sobre a maioria dos indivíduos não valem muito – e quando os consumidores usam um serviço comercial, os dados resultantes não são "deles".

Ouve-se isto com tanta frequência que é fácil supor que deve ser verdade. "Os nossos dados são ouro e devemos ser compensados por isso". Essas duas declarações basicamente dizem aos consumidores que estão a ser aproveitados, até mesmo roubados, pela Big Tech. Não surpreendentemente, isto levou a ressentimentos e apelos à ação. Mas há apenas um problema: ambas as afirmações estão muito mais erradas do que certas. As principais empresas de tecnologia atualmente são extraordinariamente lucrativas, mas isso deve-se muito mais aos recursos exclusivos da economia da informação do que a qualquer propriedade de dados ou abusos no seu uso.

Quanto valem os seus dados?

Nos últimos anos, houve vários esforços para determinar quanto valem os nossos dados individuais. Alguns estudos analisaram a receita por utilizador da Big Tech; outros focaram-se na capitalização de mercado por utilizador. Pensamos que os lucros por utilizador são o melhor ponto de partida, porque qualquer pagamento contínuo aos consumidores individuais sairia diretamente dos resultados da empresa.

Calcular os lucros por consumidor é muito mais fácil de fazer a um nível global porque é onde os dados financeiros divulgados publicamente estão disponíveis de forma mais consistente. Podemos simplificar ainda mais as coisas apenas avaliando a Alphabet (Google) e a Meta (Facebook). Embora a Apple, a Microsoft e a Amazon vendam de alguma forma publicidade baseada em dados, é uma parte muito pequena do seu negócio em geral. Da mesma forma, não é preciso incluir o Twitter porque é relativamente pequeno e perdeu dinheiro em 2021.

Vamos começar com a Alphabet. No ano que terminou a 31 de dezembro de 2021, a empresa teve receitas de 257 mil milhões de dólares e um lucro líquido de 76 mil

milhões. De acordo com a sua declaração fiscal anual, as receitas de publicidade representaram 209 mil milhões de dólares, ou 81% da receita total. Como os anúncios são a vaca leiteira da Alphabet, vamos supor que 90% dos seus lucros também são da publicidade. Isto traduz-se em 68 mil milhões em lucros com a publicidade em 2021. Agora vamos supor que, por qualquer motivo, a Alphabet tem o gesto extraordinário de devolver metade disso (34 mil milhões de dólares) às suas fontes de dados.

Como a Alphabet obtém dados valiosos tanto dos utilizadores dos seus serviços quanto da Internet, YouTube e outros fornecedores de conteúdos, digamos que dá a ambos os grupos metade dos 34 mil milhões, ou 17 mil milhões de dólares a cada. Como devemos dividir esses 17 mil milhões? A Alphabet diz que tem nove empresas com mais de 1.000 milhões de utilizadores – Search, Chrome, Gmail, Android, YouTube, Maps, Google Play, Google Drive e Google Photos. As melhores estimativas são de que cerca de 4.000 milhões de pessoas usam pelo menos um produto da Alphabet. Usando os mesmos 81% acima referidos, digamos que cerca de 3.000 milhões usam os seus serviços com anúncios publicitários. Se dividirmos 17 mil milhões de dólares por 3.000 milhões de utilizadores, teremos 5.60 dólares por consumidor em 2021, mais perto de uma chávena de café do que de um pote de ouro.

Podemos fazer a mesma análise para a Meta. As receitas da empresa em 2021 foram de 118 mil milhões de dólares, com um lucro líquido de 39,4 mil milhões, praticamente todo conseguido na publicidade. Mais uma vez, vamos supor que a Meta fica com metade dos seus lucros e divide a outra metade (19,7 mil milhões) entre os seus consumidores e fornecedores de conteúdos. No entanto, como a Meta depende muito menos de fornecedores de conteúdo externos do que a Alphabet, damos apenas um quarto dessa divisão (4,9 mil milhões) aos fornecedores e três quartos (14,8 mil milhões) aos estimados 2.900 milhões de consumidores da Meta. Dividir 14,8 mil milhões por 2.900 milhões de clientes traduz-se em 5.10 dólares por utilizador, notavelmente semelhante aos 5.60 dólares da Alphabet.

Se os pagamentos da Alphabet e da Meta aos consumidores forem somados, cada cliente receberá 10.70 dólares por ano. Ao incluir metade dos lucros baseados em publicidade da Microsoft, Amazon e Apple, terá pouco mais de 12 dólares. Mas lembre-se: isso é assumir a colossal suposição de que todas essas cinco empresas cedem metade dos seus lucros baseados em publicidade. Se devolverem apenas 10%, o pagamento anual total seria de cerca de dois dólares por utilizador por ano.

Embora qualquer um desses números anuais continue a crescer, eles não aumentarão muito em breve. Além disso, o esforço necessário para calcular e dispersar pequenos pagamentos individuais seria enorme. Talvez mais fundamentalmente, quem acha que os serviços que essas empresas fornecem gratuitamente não valem muito mais do que 12 dólares por ano? Por esta métrica, é uma das grandes pechinchas da história económica, e é por isso que estas empresas são tão bem-sucedidas.

Pode-se argumentar que os dados de algumas pessoas valem muito mais do que os 12 dólares. Isso é certamente verdade. Mas os dados que mais valem tendem a vir dos mais ricos. Será que realmente queremos argumentar que os clientes mais ricos da Alphabet e/ou da Meta devem receber muito mais do que os 12 dólares, sabendo que isso significaria que todos os outros receberiam muito menos? O mesmo acontece geograficamente. Os lucros por utilizador nos Estados Unidos e na Europa para a Alphabet e a Meta são maiores do que no mundo em desenvolvimento, mas queremos realmente que os consumidores de países menos desenvolvidos recebam muito pouco, mesmo que usem os serviços tanto quanto os consumidores em países mais ricos?

Os baixos números dos pagamentos, os altos custos de implementação e a sensibilidade à justiça social explicam por que a Big Tech provavelmente permanecerá relutante em apoiar estes esquemas de qualquer maneira, mesmo que sejam realmente a versão digital de um tradicional programa de fidelização. Esses desafios operacionais também explicam por que o Data Dividend Project e start-ups relacionadas, como a Invisibly e a UBDI, ainda não triunfaram. É inteiramente possível – talvez até provável – que, eventualmente, alguma combinação de blockchain, arquiteturas "peer-to-peer", avatares, agentes virtuais, NFTs, criptomoedas e novas normas de recolha e uso de dados gere uma geração de importantes intermediários de dados, mas atualmente tais esforços são em grande parte inviáveis e de valor duvidoso.

Não são os seus dados, de qualquer maneira

Os princípios da propriedade dos dados do cliente são tão familiares quanto a manutenção dos registos de negócio. Os emissores de cartões de crédito discriminam as nossas compras; as operadoras de TV por cabo registam o que vemos; as empresas de telecomunicações sabem para que números ligamos; os emissores de cartões de fidelização recompensam os clientes frequentes; os prestadores de serviços de saúde armazenam os nossos registos médicos; as escolas sabem o que estudamos e quais foram as nossas notas; os governos registam que imóveis possuímos, que países visitamos e muito mais. Ninguém duvida que essas organizações têm estes dados. Podemos ser capazes de vê-los, desafiar a sua exatidão ou limitar o seu uso, mas de nenhuma forma são "nossos".

As regras que governam o uso deste tipo de dados são baseadas em entendimentos explícitos ou implícitos entre consumidores e fornecedores, com cada sector a ter o seu próprio conjunto de normas, obrigações e limitações. Embora os consumidores possam decidir se devem manter um registo dos produtos e serviços que usam, a maioria de nós não se incomoda a fazê-lo. Os fornecedores, no entanto, não têm essa escolha. A recolha detalhada de dados é normalmente necessária para fins jurídicos, de contabilidade, de cobrança, de atendimento ao cliente e muitos outros. A única questão é como esses dados são ou não são usados. É a mesma pergunta com a Big Tech.

De qualquer forma, os direitos dos fornecedores são ainda mais fortes quando os serviços são suportados por publicidade e, portanto, fornecidos gratuitamente. Como diz o velho ditado, se não paga por um produto, você é o produto, pois os anunciantes estão a pagar pela sua atenção. Além disso, os consumidores de tecnologia geralmente têm mais opções do que em muitos dos sectores antes referidos.

A maioria das pessoas não precisa de usar o Facebook; é fácil mudar da pesquisa da Google para o DuckDuckGo ou usar uma das muitas alternativas ao Gmail. Essas alternativas da Big Tech continuarão provavelmente a ganhar impulso no futuro. Considere-se o crescimento impressionante do TikTok, ou a forma como o Alexa da Amazon usa o Bing da Microsoft como seu motor de busca.

Nada disto pretende argumentar que consumidores e decisores políticos não podem ou não devem tentar melhorar os termos dos acordos de uso de dados.

Atualmente, acordos de licenciamento ao utilizador final, configurações de privacidade, implementações de anonimato, serviços de perfil de clientes, suporte à portabilidade e muitas outras práticas são de natureza bizantina, e até consumidores sofisticados geralmente não se incomodam em entendê-los ou ajustá-los. Mas mesmo os esforços mais valiosos para melhorar a protecção de dados do consumidor não mudarão o facto fundamental de que os fornecedores são os proprietários dos dados, e você não.

Economia triunfa às analogias

Alguns leitores podem argumentar que, embora tudo o que foi dito acima seja verdade, ainda nos deixa com o problema das empresas de Big Tech ganharem "demasiado dinheiro". Os lucros combinados das cinco grandes empresas atingiram uns surpreendentes 350 mil milhões de dólares em 2021, e continuam a aumentar. (Mas recorde-se de que esses mesmos elevados lucros permitiram a estas empresas investirem 136 mil milhões de dólares em investigação e desenvolvimento em 2020 e certamente mais em 2021.)

A razão pela qual os líderes tecnológicos de hoje são tão lucrativos tem muito mais a ver com a economia da informação do que com a propriedade dos dados. Embora a economia da informação seja um termo usado de várias maneiras, usamo-lo para abranger as características únicas da tecnologia digital – economias de escala quase infinitas, poderosos efeitos de rede, zero custos marginais, reprodutibilidade perfeita, aumentos exponenciais em volume e tendências "winner-take-all" em quota de mercado. Por dia, a Google realiza mais de 5.000 milhões de buscas e 300 milhões de fotos são carregadas na Meta. É esta combinação em escala massiva e elevada utilidade – não abusos publicitários ou propriedade desleal de dados – que melhor explica as vastas riquezas dos atuais gigantes da tecnologia.

É por isso que as analogias com ouro ou petróleo – bem como comparações menos frequentes com eletricidade, água, ar e extração – normalmente produzem mais

sombra do que luz. Os dados não são como o ouro, que é uma mercadoria escassa com uma oferta amplamente fixa e um conjunto restrito de potenciais usos. A analogia entre dados e petróleo é melhor, pois ambos podem impulsionar negócios, a inovação e criar grande riqueza. No entanto, como o ouro, o petróleo não possui nenhuma das características da economia da informação listadas acima. Talvez mais fundamentalmente, dados e software sejam bens não-rivais, o que significa que o meu uso de um produto não impede outrem de usá-lo também. Nenhum bem material possui esta propriedade. Essas diferenças explicam por que os esforços para entender o extraordinário sucesso da Big Tech devem basear-se muito mais na economia do que em analogias.

Na maioria dos sectores, margens de lucro excecionalmente altas tendem a ser reduzidas ao longo do tempo pela concorrência, maturação do mercado, novos modelos de negócios, disrupção tecnológica, novos empreendimentos caros e/ou custos exagerados que as empresas normalmente assumem quando ficam ricas. As probabilidades são de que forças económicas semelhantes acabarão por também controlar a Big Tech.

Mas, por enquanto, dados, informação e conhecimento compreendem uma hierarquia única de valor a que as analogias históricas não conseguem acompanhar. Uma das maravilhas da era da informação é como dados que valem muito pouco ao nível individual se tornam extraordinariamente valiosos quando recolhidos em grande escala. É como uma forma moderna de alquimia. Os seus dados não são ouro; nem são seus. Mas quando os dados de todos são recolhidos e aproveitados, o valor para as empresas – e para a sociedade – vale mais do que todo o ouro no planeta Terra.

Artigo original de David Moschella publicado pela Information Technology & Innovation Foundation (CC).

Fonte: The Most Visited Website in Every Country (That Isn't A Search Engine)

Confiança nos dados é mais do que apenas ética

Deborah Yates

A questão da confiança nos dados tornou-se uma questão dominante – enquanto muitos ainda optam pela abordagem "scroll-and-click" para marcas confiáveis, no período pós-Cambridge Analytica, estamos todos um pouco mais cautelosos…

Houve um tempo em que quase todos reagimos a um novo conjunto de termos e condições – sejam eles de um fornecedor de software ou de um fornecedor de serviços – indo até ao seu final e clicando em "concordo". Queríamos chegar às guloseimas e não pensámos muito sobre onde os nossos dados iriam parar ou como as nossas ações seriam rastreadas.

Mas no período pós-Cambridge Analytica, somos um pouco mais circunspectos. Muitos ainda optam pela abordagem "scroll-and-click" para marcas em que confiam, mas mesmo assim é muito mais provável entrarem e editarem as preferências de dados. Quando se trata de aplicações, inquéritos e inscrições em marcas desconhecidas, pode-se estar disposto a renunciar a quaisquer supostos benefícios para reter os nossos dados pessoais.

Por outras palavras, a questão da confiança nos dados tornou-se uma questão dominante, embora muitos daqueles que tomam essas decisões possam não perceber que a confiança nos dados e a confiança nas organizações que recolhem e usam os dados é um problema com o qual estão a interagir. Eles podem citar "confiança na marca" ou "segurança", mas isso são ilustrações da confiança nos dados e porque ela é agora importante para todas as empresas. As organizações devem entender que aqueles que interagem com elas têm o direito de perguntar como e porque são recolhidos os dados, como são usados e quem tem acesso a eles. Afinal, são essas pessoas que vão considerar se a sua empresa é confiável ou não.

Não se pode considerar a confiança como um dado adquirido, é muito parte de um relacionamento que os clientes ou parceiros de negócios dão a uma marca ou empresa após ter sido conquistada – e a definição de "ganhá-la" é diferenciada e dependente do contexto. Isso pode ser por experiência ou pela reputação, mas qualquer uma delas também pode ser uma porta de entrada para a perda de confiança.

Claro que a demonstração de valores éticos desempenha um papel importante na construção da confiança. Isso pode tanto pintar uma imagem de como uma organização funciona e falar aos valores daqueles que interagem com ela. Há uma razão pela qual muitas organizações falam sobre a sua abordagem ao bem-estar da equipa, meio ambiente, testes em animais ou a sua posição sobre salários justos para os fornecedores.

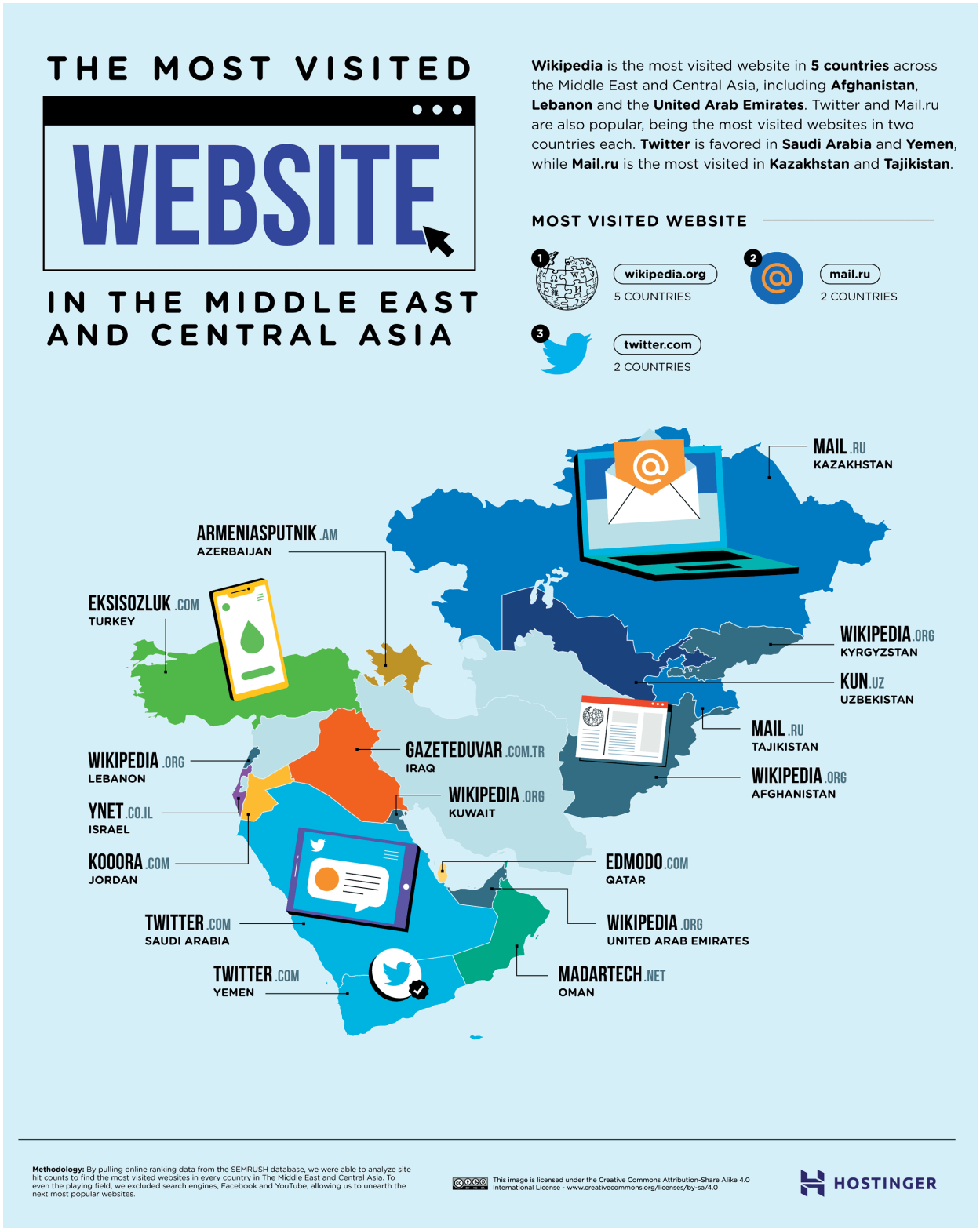
Estas questões podem falar à base dos valores dos clientes, mas mostram algo mais amplo. Estabelecem uma marca como considerada, pensadora e confiável. Revela uma bússola moral e, esperançosamente, reflete valores em muitos aspectos.

Considerações éticas na maneira como uma organização recolhe, usa e partilha dados estão cada vez mais na agenda – tanto do ponto de vista social quanto económico. A ascensão da ética dos dados – definida como uma forma distinta e reconhecida de ética que considera o impacto dos dados e das práticas de dados nas pessoas, sociedade e meio ambiente – como disciplina reconhecida é uma prova disso.

No entanto, demonstrar a recolha e o uso éticos de dados é apenas um elemento de uma administração confiável de dados. Ganhar confiança exige que as organizações vão além das boas práticas da governança de dados. Elas precisam de demonstrar confiabilidade na privacidade e na segurança, ética e transparência, empenho e responsabilidade, bem como equidade e justeza. Abordar cada uma dessas áreas pode ajudar a aumentar a confiança nos dados, bem como nas empresas ou organizações que lidam com eles. Ao fazê-lo, os que abordam cada área mudam do [plano] teórico para o prático.

Afinal, é fácil para as organizações reivindicarem qualquer elemento da sua ética ou práticas com os dados, mas bem diferente é demonstrar visivelmente que essa ética está integrada e incorporada no dia-a-dia dos negócios. Reivindicar práticas éticas certamente atrairá atenção no curto prazo, mas deixar de cumpri-las pode ser mais prejudicial para uma organização do que falhar em estabelecer tais linhas de orientação.

Artigo original de Deborah Yates, publicado no Open Data Institute (CC).



Fonte: The Most Visited Website in Every Country (That Isn't A Search Engine)

Poluição de dados e poder

Gry Hasselbalch

Há uma tendência para reduzir a complexidade da mudança sociotécnica em silos disciplinares e sectoriais e interesses específicos das partes interessadas ["stakeholders"]. No entanto, ambientes inter-relacionados complexos não conhecem fronteiras e, como tal, a falta de coordenação e tradução entre vários campos de especialização, grupos de "stakeholders" e de interesses, pode limitar a mitigação dos impactos ambientais adversos da poluição de dados. Precisamos de terminologia partilhada e de uma plataforma conceptual para colocar as questões mais urgentes sobre poluição de dados a serem abordadas dentro da agenda global de desenvolvimento sustentável.

Como conceito no discurso político e empresarial, a sustentabilidade tem sido articulada nas últimas cinco décadas juntamente com a identificação dos impactos adversos da Era Industrial nos ambientes sociais, económicos e naturais. Desde o início, representou uma abordagem mais holística para a gestão de riscos e impactos ambientais. Inclui o reconhecimento de que os problemas ambientais globais são em grande parte o resultado dos padrões insustentáveis de consumo e produção do Norte Global, juntamente com a pobreza generalizada no Sul Global.

O potencial das tecnologias de inteligência artificial [IA] e Big Data para enfrentar os desafios ambientais tradicionais e alcançar as metas do Green Deal (UE) ou do Desenvolvimento Sustentável (ONU) foi amplamente explorado e é repetidamente destacado nas políticas de IA e dos dados. A sustentabilidade da IA e da Big Data, por outro lado, é predominantemente tratada como um campo de ação separado na política e na investigação científica.

Aqui, queremos, como van Wynsberghe descreve, tratar a sustentabilidade para e dos dados de IA como dois lados da mesma moeda. Ou seja: precisamos de reconhecer que a IA não pode ajudar-nos a alcançar objetivos de desenvolvimento sustentável se ela própria for insustentável.

Exploraremos a poluição de dados no contexto do desenvolvimento de tecnologias de IA e da criação de infraestruturas sociotécnicas de IA ("Artificial Intelligence Socio-Technical Infrastructures" ou AISTIs) em particular. A Big Data é o principal recurso da sociedade dos grandes dados e das "Big Data Socio-Technical

Infrastructures" (BDSTIs), mas é um recurso vazio sem sistemas complexos de processamento de dados para análise. Hoje, no início dos anos 2020, os sistemas de IA dão sentido à Big Data. Eles ganharam cada vez mais força nos sectores público e privado como "criadores de sentido" na era dos fluxos de Big Data. Assim, a IA é usada para dar sentido a grandes quantidades de dados, prever padrões, analisar riscos e agir sobre esse conhecimento na saúde, fabricação, Administração Pública, redes sociais, finanças e na maioria das outras áreas da sociedade.

Um inquérito sobre a adoção da IA na Europa descobriu que quatro em cada dez empresas (42%) adotaram pelo menos um programa de IA, com um quarto delas já tendo pelo menos dois. As empresas de negócios e de tecnologia começaram geralmente a renomear os seus esforços de Big Data como "IA" e, no campo da formulação de políticas, a IA ganhou importância estratégica em todo o mundo.

Nos sectores público e privado, os processos de tomada de decisão são progressivamente informados por e até substituídos por sistemas de IA de Big Data.

Os sistemas de avaliação de risco procuram padrões nos antecedentes dos réus para informar os juízes sobre quem tem maior probabilidade de cometer um crime no futuro.

Os sistemas de personalização e recomendação estão a criar perfis com base nos dados pessoais para decidir o que se vê e lê e com quem nos relacionamos online.

Os sistemas de triagem analisam os registos médicos e as informações demográficas dos pacientes para decidir quem recebe um novo rim.

Na sua forma atual, os sistemas de IA servem para muito pouco sem dados e a maioria deles precisa que os dados estejam disponíveis, acessíveis, recolhidos e armazenados. Como destaca o Data Governance Working Group (WG) da Global Partnership of AI (GPAI) num relatório sobre dados de IA:

> ...a disponibilidade de dados (se os dados existem) e a acessibilidade (se os dados estão acessíveis) são os principais fatores por trás do desenvolvimento de produtos que usam tecnologias de IA.

Negócios, economias e políticas estão a mudar juntamente com a adoção de novas infraestruturas sociotécnicas de IA e Big Data e, com elas, também as decisões e escolhas morais que estão cada vez mais entrelaçadas com o complexo processamento de dados dos sistemas de IA. Assim, os interesses no combustível da IA – dados – como um recurso para adquirir, proteger e partilhar unem-se nos esforços para dirigir o desenvolvimento da IA na sociedade.

A poluição dos dados como um termo fala num novo movimento verde para a sustentabilidade dos dados. O movimento ambiental global surgiu originalmente como uma resposta ao impacto ambiental tangível do desenvolvimento industrial e da urbanização, como a introdução de poluentes nocivos nos nossos ambientes naturais, redução/mudanças no habitat,

extinção de diferentes espécies e danos à terra, água e florestas.

Lidar com este tipo de impacto ambiental tornou-se um impulsionador para novas estruturas e políticas legais e leis ambientais nacionais e internacionais. Transformou sectores inteiros, como a indústria automóvel, e impulsionou o desenvolvimento de novos campos e ciências, como tecnologias ecologicamente corretas (ESTs ou "Environmentally Sound Technologies"), "tecnologia verde". Hoje, estamos a passar por um processo semelhante ao articular a nossa resposta social aquele que o tecnólogo de segurança informática e privacidade Bruce Schneier descreveu em 2006 como o principal problema ambiental da era da Big Data:

> ...este maremoto de dados é o problema da poluição da era da informação. Todos os processos de informação a produzem. Se ignorarmos o problema, ele permanecerá para sempre. E a única maneira de lidar com isso com sucesso é aprovar leis regulando a sua geração, uso e eventual eliminação.

Tivemos debates políticos e públicos sobre a privacidade e as implicações sociais da Big Data desde o início dos anos 2000, e agora estamos a ter conversas mais sérias sobre a pegada de carbono do armazenamento e processamento de dados. Além disso, a sociedade começa a falar sobre os atores mais poderosos neste campo, como regiões, governos, organizações intergovernamentais e gigantes da tecnologia. No entanto, ainda há muito pouca consciencialização sobre a poluição dos dados como um "problema ambiental" e a perturbação de ecossistemas inteiros.

O que é necessário é um novo movimento verde para a poluição de dados e uma melhor compreensão da dinâmica da energia que molda o campo em diferentes problemas da poluição de dados. A esse respeito, muitos dos conceitos do movimento ambiental global e do discurso de "desenvolvimento sustentável" na política e nos negócios podem ser reapropriados para ajudar a mapear e identificar poluição de dados e energia.

Poluição de dados

A poluição de dados é o impacto adverso inter-relacionado que a geração, armazenamento, manuseio e processamento de dados digitais tem no nosso ambiente natural, ambiente social e ambiente pessoal. É o manuseio, distribuição e geração insustentáveis de recursos de dados. Uma diligência justa da poluição de dados significa gerir – na prática organizacional, política e de design – os efeitos adversos e os riscos da exaustão dos dados nos ecossistemas natural, social e pessoal.

Desde meados da década de 1990, assistimos a uma transformação das nossas sociedades possibilitada pelas tecnologias computacionais e dirigida por uma conversão de quase tudo em vários formatos de dados (datificação). Big Data é um movimento impulsionado por uma visão particular sobre o papel dos dados digitalizados na sociedade. Durante muitos anos, indústrias, governos e cientistas perceberam a Big Data como um fim em si mesmo, com a promessa de usos futuros ilimitados; um recurso inesgotável

que nunca desaparecerá e, portanto, é distinto de outros recursos naturais, que se podem esgotar (como o petróleo ou a água). No entanto, a Big Data é cada vez mais entendida como uma força social de mudança que, como a industrialização, não apenas trouxe crescimento, mas também tem consequências negativas, incluindo o impacto que vemos no nosso ambiente natural na forma de mudança climática.

Dois usos tradicionais do termo poluição de dados podem assim ser combinados: em primeiro lugar, a poluição de dados pode ser entendida como o impacto adverso nos ambientes pessoal e social, por exemplo nos direitos individuais, como a proteção de dados ou o direito à vida privada, e nas instituições democráticas e nos equilíbrios de poder. Em segundo lugar, a poluição de dados pode ser entendida como os efeitos adversos materiais no nosso ambiente natural, por exemplo, a pegada de carbono da Big Data.

1. Impacto nos ambientes social e pessoal

Originalmente, o termo poluição de dados foi usado para referir as assimetrias invisíveis de poder de uma crescente economia de Big Data e a datificação de vidas e sociedades individuais. Como tal, a poluição de dados passou a representar as consequências adversas concretas da Big Data para ambientes pessoais e sociais.

Assim, com este termo, Schneier enfatizou os efeitos reais e materiais da recolha e processamento massivo de Big Data por empresas e governos sobre o direito das pessoas à privacidade. Depois disso, a "poluição de dados" foi expandida na definição de uma abordagem de governança mais holística para os efeitos adversos da economia de Big Data, reconhecendo que não apenas ambientes pessoais estão em jogo, mas também ambientes sociais. Como afirmamos em 2016 em "Data Ethics - The New Competitive Advantage", ao definir e modelar um papel para o termo "ética de dados" em políticas e debates públicos sobre Big Data:

> A privacidade individual não é o único valor social sob pressão na atual infraestrutura saturada de dados. Os efeitos das práticas de dados sem ética podem ser múltiplos – tratamento injusto, discriminação e oportunidades desiguais. Mas a privacidade está no seu núcleo. É a agulha no medidor do equilíbrio de poder da sociedade.

Desde então, [Omri] Ben-Shahar introduziu a poluição de dados no campo jurídico como forma de repensar os malefícios da economia de dados para gerir as externalidades negativas da Big Data com uma lei ambiental para proteção de dados reconhecendo que a prejudicial exaustão dos dados não está apenas a atrapalhar os direitos de privacidade e proteção de dados dos indivíduos, mas também tem um impacto adverso em todo um ecossistema digital de instituições sociais e de interesse público:

> O conceito de poluição de dados convida-nos a expandir o foco e a examinar as maneiras pelas quais a recolha de dados pessoais afeta instituições e grupos de pessoas – além daqueles cujos dados são recolhidos e além dos danos à sua privacidade.

2. Impacto no meio ambiente natural

A outra vertente de usos do termo poluição de dados aborda o impacto ambiental mais tradicional de Big Data no nosso ambiente natural. Isto é o que [Federica] Lucivero e [Gabrielle] Samuel, juntamente com um grupo interdisciplinar de estudiosos, chamam de insustentabilidade orientada por dados. O impacto no ambiente natural causado pela poluição de dados das tecnologias digitais deve-se à sua complexidade, que, por mais difícil que seja ter uma visão completa, é inegável.

O "think tank" francês que defende uma mudança para uma economia pós-carbono, o Shift Project, estima que a quota das emissões globais de gases de efeito estufa produzidas por dados aumentou de 2,5% em 2013 para 3,7% em 2019. Nesse sentido, os centros de dados respondem por 1% (e em constante crescimento) da procura global total de eletricidade. A maior parte desse crescimento é atribuída à computação em nuvem pelas maiores empresas de Big Data, como Amazon, Google e Microsoft.

O impacto das tecnologias de uso intensivo de dados, como a IA, também é significativo. Por exemplo, um famoso estudo de Strubell et al. descobriu que o treino (incluindo ajuste e experimentação) de um grande modelo de IA para processamento de linguagem natural, como tradução automática, usa sete vezes mais carbono do que um humano médio num ano. É importante realçar que a poluição ambiental de tecnologias digitais baseadas em dados, como a IA, não é apenas uma questão de dados, mas também de eliminação das TIC e consequências mais difíceis de discernir (como o consumo de energia pelos consumidores ao usarem serviços digitais).

Para os propósitos deste texto, esses dois usos do termo poluição de dados são combinados com o objetivo de identificar a poluição de dados num ecossistema comum de poder e, consequentemente, considerar ações com uma abordagem de governança mais holística para o problema de poluição causado pela era da Big Data.

A Agenda 2030 para o Desenvolvimento Sustentável da ONU, adotada por todos os Estados-Membros das Nações Unidas em 2015, estabeleceu a sustentabilidade como uma questão inter-relacionada a ser abordada em vários campos de ação. Assim, os 17 Objetivos de Desenvolvimento Sustentável (ODS) da agenda abordam o equilíbrio das três dimensões do desenvolvimento sustentável – económica, social e ambiental – com estratégias para lidar com as mudanças climáticas, melhorar a saúde e a educação, reduzir a desigualdade e estimular o crescimento económico. No documento, a poluição de dados é abordada de forma semelhante não apenas como um tipo de impacto ambiental, mas sim como os efeitos adversos inter-relacionados em equilíbrios delicados nos nossos ecossistemas e ambientes natural, social e pessoal.

Conforme descrito, o termo poluição de dados é usado atualmente para enfatizar o impacto ambiental adverso muito real e material da Big Data nesses ambientes. Como tal, o objetivo de um novo "movimento

verde" para Big Data é a "sustentabilidade dos dados", que atravessa os ODS com considerações de sustentabilidade ligadas às várias mudanças ambientais causadas pelo volume e diversidade da Big Data, desde os seus efeitos sobre a paisagem natural às nossas decisões e à democracia.

O pressuposto é que a poluição de dados não assume uma forma facilmente identificável. Ela afeta ecossistemas inteiros de ambientes "materiais" e "não-materiais". Assim, independentemente da definição a que se refere, o impacto da poluição de dados nos nossos ambientes social, pessoal ou natural é tão "real" e "material" quanto os poluentes da Era Industrial e deve ser gerido como tal. Isso também significa que não podemos combater um efeito adverso sem também combater outros. Uma empresa, por exemplo, não pode alegar ter "práticas de dados sustentáveis" apenas reduzindo a sua pegada de carbono e, ao mesmo tempo, deixando por gerir os riscos que o manuseio, armazenamento e processamento de Big Data representam para os nossos ambientes pessoais e sociais. A verdadeira sustentabilidade dos dados significa ter em conta todo o complexo de um ecossistema inter-relacionado impactado pela datificação das nossas sociedades.

Excerto de "Data Pollution & Power - White Paper for a Global Sustainable Development Agenda on AI". Referências no texto original, publicado pelo The Sustainable AI Lab da Bonn University (CC).

Fonte: The Most Visited Website in Every Country (That Isn't A Search Engine)

Informação e desinformação

Olga Solovyeva

A manipulação da informação é um fenómeno e prática comum nos contextos dos países selecionados para o relatório "The Unfreedom Monitor: Information". Geralmente, as campanhas de desinformação nestes países são apoiadas pelo Estado e beneficiam atores políticos dominantes ou concorrentes. A desinformação torna-se uma ferramenta para a luta pelo poder num contexto socialmente polarizado causado por eventos políticos problemáticos (por exemplo, golpes de Estado, eleições, mudanças de governo e mobilização de protestos). Na maioria dos casos, a desinformação visa comprometer adversários políticos, destacar conquistas do regime político ou reprimir a dissidência. O fator que desempenha um papel crucial nessas sociedades é a proliferação comparativamente elevada da Internet e o entusiasmo do público em usar os media sociais, que anda de mãos dadas com alguma falta de liberdade da media tradicional. No entanto, as estratégias de desinformação tornam-se não apenas uma ferramenta de operação da política doméstica, mas também uma maneira de estabelecer influência política fora de fronteiras.

Apesar do facto de que a ideia de estratégias de autoritarismo digital é impulsionada e realizada com ferramentas modernas de TI, na essência elas são semelhantes às técnicas de propaganda. As táticas visam legitimar certas narrativas injetando-as no ecossistema mediático e depois repetindo-as para que se tornem o novo senso comum para a população. Tal abordagem é amplificada pela tecnologia da Internet, que permite a criação de ecossistemas credíveis de media, imitando os reais e preenchendo-os com utilizadores falsos agindo de forma semelhante ao comportamento humano online.

Entretanto, a segmentação publicitária nos media sociais cria oportunidades para executar uma campanha influente que agora se estende para lá do caso Cambridge Analytica. No entanto, é discutível se a comunicação direcionada pode alcançar uma mudança de atitude ou formar uma atitude. Em vez disso, o público deve estar preparado para mudar de atitude em resultado do que Jacques Ellul conceptualizou nos anos 1960 como pré-propaganda: "o condicionamento das mentes com grandes quantidades de informação incoerente, já dispensada para fins ulteriores e posando como 'factos' e como 'educação'".

Este termo é relevante para as atuais estratégias digitalizadas de manipulação

da informação. Como mostra o panorama de casos e práticas de desinformação, as campanhas de desinformação tornam-se mais sofisticadas e dispersas, visando preparar o público para aceitar um determinado ponto de vista. Para Ellul, a pré-propaganda, "sem agressão direta ou percetível, está limitada a criar ambiguidades, reduzir preconceitos e difundir imagens, aparentemente sem propósito". Como na disseminação da desinformação, o efeito primário é psicológico – criar uma imagem alternativa da realidade para o indivíduo.

Para resumir, três fatores definem a manipulação atual da informação nos países observados. Primeiro, há um melhoramento contínuo das capacidades técnicas da desinformação para superar as medidas tomadas pelas plataformas de TI e tornar a desinformação mais confiável, especialmente usando IA. Em segundo, as grandes estratégias e narrativas para a desinformação tornam-se mais complexas, pois as narrativas e táticas são usadas para um efeito psicológico amplificado, como criar desconfiança, levantar dúvidas, etc. Elas são utilizadas de forma semelhante à pré-propaganda e à própria propaganda. O terceiro fator continuam a ser os traços subjacentes da natureza humana, como o pensamento preguiçoso, a tendência para consumir mais conteúdo emocional, etc.

Existem duas correntes principais de discussão que analisam o futuro do combate à desinformação. A primeira sugere que a ferramenta mais promissora para a combater é capacitar as sociedades pela literacia mediática contínua e melhoria geral da qualidade do ambiente mediático. Incentivar o jornalismo de elevada qualidade e apoiar a sociedade civil são algumas das principais ações. Outro debate surge com o trabalhar na crescente qualidade do conteúdo que circula nas plataformas, incluindo os media sociais. Além do investimento contínuo em moderação de conteúdos, recomenda-se prioritizar conteúdo autêntico e de elevada qualidade. Algumas das iniciativas já foram executadas por empresas como a Google.

No entanto, eliminar a desinformação política em países autoritários onde os campos de informação permanecem sob controlo estatal pode ser irrealista. Apesar de muitas das plataformas usarem media sociais globais, que podem ser regulamentadas pelas suas próprias normas, muitos países bloqueiam as plataformas existentes, limitam o acesso com ferramentas legislativas ou desenvolvem plataformas domésticas alternativas. A prática da desinformação torna-se a ferramenta de execução para o desenvolvimento do autoritarismo digital ao usar meios digitais para doutrinar narrativas favorecidas pelo Estado. O discurso sobre desinformação, em simultâneo, torna-se uma ferramenta de contínua repressão à liberdade de expressão, pois os Estados usam legislação sobre notícias falsas para silenciar a dissidência interna. No entanto, o desenvolvimento da tecnologia blockchain pode capacitar os criadores de conteúdo e os ativistas digitais nesses países com oportunidades de validação de factos de forma independente e incentivar a criação de conteúdo autêntico.

Artigo original de Olga Solovyeva, publicado na Global Voices (CC).

Uma conversa sobre vigilância no jornalismo

Dimitri Bettoni e Federico Caruso

Da investigação do spyware Pegasus à vigilância em massa: um diálogo com o investigador Philip Di Salvo, da Università della Svizzera italiana, para entender o impacto das novas tecnologias para todos os envolvidos no jornalismo e não só.

Ouvimos falar da investigação do Pegasus, um software intrusivo que visava muitos jornalistas em todo o mundo. Pode explicar como essas ferramentas podem colocar em risco os jornalistas, as suas fontes e quão difundida é a questão da vigilância no jornalismo?

A resposta é algo que ecoa há anos: a maior parte do que há sobre vigilância no jornalismo ainda está por descobrir, e essa é a principal preocupação. É por isso que foi tão importante ver a publicação da investigação do Pegasus Project no Verão [de 2021]. Foi um daqueles momentos de acerto de contas, onde obtivemos provas sobre o quão perigoso e difundido é o uso da tecnologia de spyware. Isso é uma coisa rara, pois ter acesso a detalhes e evidências sobre como as empresas de vigilância funcionam é muito difícil. Essas empresas são muito secretas e difíceis de abordar, elas tendem a trabalhar muito sem chamar a atenção. Esta investigação foi fundamental para levantar ainda mais questões sobre como os estados e os atores privados estão a usar tecnologias de spyware para atingir dissidentes e jornalistas. Pelo menos 180 jornalistas proeminentes foram alvos do Pegasus em todo o mundo e o meu receio é que isso seja apenas a ponta do iceberg. Por exemplo, ainda não sabemos muito sobre os utilizadores desse spyware. O mais assustador é que, uma vez que alguém se torna um alvo, há muito pouco que essa pessoa possa fazer. Não há como ter qualquer prova de que esse spyware foi instalado num dispositivo sem executar uma análise forense profissional e técnica. Portanto, na constelação da vigilância atual, e da vigilância digital em particular, os spywares são um dos dispositivos mais perigosos. Eles são capazes de fornecer acesso remoto e completo a tudo o que está armazenado num smartphone, incluindo toda a comunicação que passa por aquele dispositivo. Este é um cenário de pesadelo quando se trata da proteção de fontes, de proteger o desenrolar de uma investigação e a segurança dos próprios jornalistas.

Como foi a consciencialização em torno dessa questão nas redacções?

As revelações de Snowden em 2013 foram um ponto de viragem para a segurança da informação no jornalismo. Antes, até mesmo a consciência da existência do problema limitava-se aos jornalistas de investigação mais avançados. Isso traduziu-se na adoção de estratégias e ferramentas anti-vigilância nalgumas redações mas, no geral, temo que a consciencialização ainda seja muito baixa, e a maioria dos jornalistas tenha pouca ou nenhuma ideia sobre o que está a acontecer e quais os riscos envolvidos. No que diz respeito ao Pegasus, devemos sublinhar como a utilização de um spyware tão sofisticado é algo que exige um conhecimento técnico de altíssimo nível. Quer dizer, um spyware é definitivamente o cenário mais assustador, mas pelo menos até agora isso pertence a cenários muito restritos. Por outro lado, a vigilância além do spyware, e a vigilância maciça em particular, são questões de extrema urgência para todos os envolvidos no jornalismo.

O medo é uma condição emocional que afeta a capacidade jornalística de realizar um trabalho com significado. Pode-se dizer que o dano psicológico não está estritamente relacionado à certeza de ter um spyware no telemóvel, mas sim à possibilidade de tal ameaça?

Sim, definitivamente. Os spywares não servem apenas para obter acesso à informação, mas para controlar a vida dos jornalistas, silenciá-los. Instalar o medo não está estritamente relacionado com a instalação de um spyware. Pense em Jamal Khashoggi: devemos estar cientes de que a vigilância contra jornalistas às vezes leva à sua morte. Além disso, a vigilância está-se a tornar cada vez mais comodificada, de modo que o acesso a ferramentas como spyware ou outro software de vigilância é cada vez mais fácil e barato. Claro que não é algo que se compra por 20 euros, mas está a tornar-se mais acessível. Recentemente, a emissora pública sueca publicou uma história sobre como os bancos na Suécia estavam a usar spyware para monitorar jornalistas que investigavam economias offshore. Quando as revelações de Snowden foram publicadas, ouvimos essa visão desdenhosa da vigilância, dizendo que se deve temê-la apenas quando se estiver a cobrir a segurança nacional ou o aparelho da inteligência: isso já não é assim. Essa crescente sensação de medo e paranóia em torno dos jornalistas tem consequências a longo prazo na prática do jornalismo, pode levar à censura e à autocensura e, definitivamente, tem impacto na qualidade da informação com que o público é servido. Precisamos de mais provas, de abrir mais dessas caixas pretas onde a vigilância prospera para produzir mais responsabilidade. Esta é a única maneira de combater esse sentimento de medo que está a impactar o trabalho dos jornalistas em todo o mundo.

Acho que há uma diferença entre freelancers e funcionários que trabalham para grandes empresas de media na forma como se apercebem desse nível de paranóia. A condição de freelancer é parte do problema?

Foto: Etienne Girardet | Unsplash

Em última análise, chega-se a uma avaliação de ameaça: qualquer jornalista deve estar ciente de quem são os potenciais jogadores que tentam colocá-lo sob vigilância e tomar as ações consequentes. Definitivamente, os freelancers são deixados em paz quando se trata de um investimento de tempo e dinheiro para ter as ferramentas e as estratégias necessárias para se sentir seguro. Acho que mais deveria ser feito pelo Estado: deveria haver programas de assistência para freelancers. Por exemplo, a única estratégia para se sentir seguro contra spyware é trocar de smartphone regularmente. Isso é muito caro para os freelancers. Além disso, o que aprendemos com a investigação do Pegasus Project é que às vezes os alvos de spyware não são os próprios jornalistas, mas as pessoas ao seu redor. No caso de Khashoggi, por exemplo, há provas de que pessoas no seu círculo mais próximo de amigos e familiares foram alvos do spyware. Assim, talvez os jornalistas tenham alguma experiência

em segurança da informação e isso possa dificultar serem um alvo direto. Mas as pessoas em seu redor podem assim ficar ainda mais expostas.

Mencionou a necessidade de analisar o sector da vigilância, o que pode ser feito de duas maneiras, através de regulamentação e de supervisão. De que tipo de regulamentação a nível nacional e internacional, e de que tipo de organismos, capazes de fiscalizar efetivamente o mercado e a utilização de tecnologia de vigilância, necessitamos?

A questão da regulamentação é crucial e existem algumas regras em torno, por exemplo, de disciplinar a exportação de tecnologias de vigilância pela UE para evitar que essas tecnologias sejam vendidas para países não-democráticos.

Infelizmente, aprendemos com as investigações que isso é fácil de contornar. Uma grande investigação da Al Jazeera chamada Spy Merchants mostrou como as empresas europeias eram capazes de vender vigilância digital para o Irão, Arábia Saudita e outros países na lista negra usando intermediários, ocultando as suas transações dessa maneira. O problema é que o spyware e outras tecnologias de vigilância são as chamadas tecnologias de uso dual, e essa é a questão, porque é fácil dizer que vamos proibir as armas nucleares, pois não há uso de armas nucleares, exceto para matar milhares de pessoas. Mas é mais complicado quando se trata de spywares, porque as autoridades ainda podem usá-los para investigar crimes.

A minha opinião é que, com a exclusão de casos muito limitados como investigações de terrorismo, crime organizado e outros crimes graves, não deveria haver nenhum uso de spyware, ponto final. O uso e a circulação de spywares são quase impossíveis de monitorizar, pelo que deveria haver regulamentações muito rígidas sobre quem pode usar essas ferramentas, quem pode comprá-las e assim por diante. As limitações devem ser colocadas nas empresas, pois elas não devem vender esses produtos para lá de uma lista de clientes aprovados.

Assim, fazer cumprir isso ainda é problemático, porque as empresas desse sector geralmente estão muito bem ligadas aos estados, a ponto de às vezes ser difícil separar as duas entidades. Para responder brevemente à sua pergunta, acho que deveria haver uma regulamentação internacional, talvez ao nível das Nações Unidas, decidindo quais são os usos aceitáveis de spyware e essa deveria ser a linha vermelha para todos.

Falando em jornalismo, podem as tecnologias de vigilância representar uma oportunidade mais do que uma ameaça?

A confiança é definitivamente a questão central quando se trata do impacto da vigilância e não temos transparência suficiente, especialmente dos atores estatais. Temos pouca ou nenhuma ideia sobre quais são as capacidades de vigilância da maioria das democracias ao redor do mundo, começando pela UE. Infelizmente, na esteira das revelações de

Snowden, alguns países europeus até se deram mais poderes de vigilância quando se trata de vigilância em massa e há uma transparência muito limitada sobre como tudo funciona. Além disso, há o grande ponto de interrogação sobre os atores privados terem acesso às tecnologias de vigilância, que é ainda mais obscuro.

Dito isto, é absolutamente verdade que existem formas de vigilância que são benéficas. Quer dizer, cuidamos das pessoas com vigilância para que elas não se aleijem, esse é o ponto de partida do que é vigilância. Mas a vigilância é fácil de ser abusada, em particular a vigilância relacionada com tempos de crise. Vimos isso há 20 anos com todos os programas de vigilância introduzidos na UE e nos EUA após os ataques do 11 de setembro. Estamos a ver isso com as tecnologias de reconhecimento facial, por exemplo, introduzidas em todo o país explorando os medos. Mesmo quando as técnicas de vigilância são benéficas, elas devem ser submetidas a uma estrita supervisão, porque o abuso está sempre próximo e é muito fácil sair da área benéfica aceitável e entrar noutra coisa.

Como podem investigadores, jornalistas e a sociedade civil em geral contribuir para iluminar o mundo opaco da vigilância?

Precisamos de alianças entre academia, "geeks" e jornalistas. O Pegasus é, nesse sentido, muito interessante pela forma como foi conduzido. Começou com investigações jornalísticas coordenadas entre 16 parceiros de media em todo o mundo. Eles pediram ajuda à Amnistia Internacional, que tem um departamento técnico muito importante que corroborou as conclusões iniciais com análises técnicas nos telefones das vítimas. Eles também trabalharam com o Citizen Lab, um centro de investigação da Universidade de Toronto, que também está a realizar um trabalho de investigação e consciencialização extremamente importante sobre o mundo do spyware. Precisamos desse tipo de aliança porque é uma combinação de conhecimentos e capacidades que só podemos ver plenamente operacionais quando jornalistas, ativistas e investigadores trabalham juntos.

Ainda há poucos trabalhos vindos da academia nessa área. O que temos é ótimo e está a tornar-se ainda mais visível, mas precisamos de mais. O nível de análise aprofundada que a academia pode fornecer é necessário para entender como os jornalistas podem abordar e narrar o problema.

Precisamos que todas essas forças se unam para ter o impulso necessário de todas essas áreas para uma mudança positiva. Caso contrário, sem supervisão nem responsabilidade, temo que esta seja uma batalha que vamos perder.

Entrevista original de Dimitri Bettoni e Federico Caruso, publicada no Osservatorio Balcani Caucaso Transeuropa/ EDJNet (CC).

O que Spotify, Neil Young e Joe Rogan nos dizem sobre a moderação de conteúdos

Konstantinos Komaitis

A moderação de conteúdos é complexa, difícil e, francamente, exaustiva. Um exemplo recente envolve o Spotify e a sua decisão de manter o controverso apresentador de podcast, Joe Rogan, em detrimento de outros criadores. Não há dúvida de que o Spotify tem o direito de determinar quem hospeda, lucra com ou rejeita da sua plataforma; o que preocupa, no entanto, é o Spotify abdicar da sua responsabilidade ética com os seus utilizadores para tomar tais decisões de forma transparente e consistente.

Vamos começar do início.

No que foi um caso amplamente divulgado, Neil Young exigiu a remoção do seu catálogo do Spotify como forma de protesto contra o acordo do Spotify em ser a plataforma exclusiva para o podcast extremamente popular The Joe Rogan Experience, alegando que o podcast dissemina desinformação sobre a vacina do Covid-19. Pouco depois, outros músicos, incluindo Joni Mitchell, India Arie e Nils Lofgren, também pediram que o seu conteúdo fosse removido. A psicóloga social de sucesso Brene Brown recusou-se inicialmente a gravar novos podcasts, mas regressou depois, citando "poucas opções". Até a Casa Branca opinou. Tudo isto após uma carta aberta em dezembro de 2021 ao Spotify de 270 especialistas em saúde dos EUA expressando preocupação com a desinformação médica no The Joe Rogan Experience, denominando-a de "ameaça à saúde pública".

A resposta do Spotify foi em duas frentes. Primeiro, Daniel Ek, o seu CEO, escreveu que se iria comprometer a "fazer mais para fornecer mais equilíbrio e acesso a informações amplamente aceites das comunidades médica e científica". E, em segundo, o Spotify anunciou que os podcasts que discutem o Covid-19 passavam a ter avisos de conteúdo. Este parece ser um esforço do Spotify para garantir que o pequeno movimento iniciado por Neil Young não se estenda a artistas que são mais populares (e mais importantes) para o Spotify, como Taylor Swift, Bad Bunny ou BTS.

Mas, mesmo que essa estratégia consiga interromper um êxodo maior e mais prejudicial para o Spotify, nenhuma dessas ações aborda o problema subjacente do Spotify: um ambiente político confuso e inconsistente que parece privilegiar

alguns criadores em detrimento de outros.

No seu texto, Ek afirmou: "Sabemos que temos um papel crítico a desempenhar no apoio à expressão do criador, equilibrando-a com a segurança dos nossos utilizadores. Nesse papel, é importante para mim que não assumamos a posição de ser censores de conteúdo, enquanto nos certificamos que existem regras e consequências para aqueles que as violam".

O Spotify, como praticamente todas as outras empresas que albergam conteúdo, está sempre a tomar decisões de curadoria como essas. Por exemplo, em 2018, o Spotify impôs o que ficou conhecido como a "regra R. Kelly", instituindo uma política para banir ou "enterrar" músicas ou artistas que considerava odiosos, mas reverteu isso mais tarde. Além disso, durante o verão de 2021, o Spotify eliminou até 750 mil músicas de artistas independentes sem nenhuma

Há duas questões bastante separadas que merecem uma clarificação.

A primeira é que o Spotify, como qualquer outra empresa privada, não é obrigado a fornecer uma plataforma a ninguém; ele tem o direito de decidir que conteúdo hospeda, com que conteúdo lucra e qual o conteúdo que não aceita.

explicação além de terem aparentemente violado a sua política sobre aumentar artificialmente os números de reprodução.

No entanto, de acordo com a revista Rolling Stone, "a remoção abrupta expõe um duplo padrão na política do Spotify", considerando que em janeiro de 2020 Justin Bieber pediu aos seus fãs que

ajudassem a impulsionar artificialmente a sua música "Yummy" ao "colocá-la em 'loop' ou fazendo download de VPNs". No entanto, Justin Bieber não foi banido da plataforma nem a sua música foi removida.

Aí está o cerne do problema. O Spotify e outras plataformas têm padrões duplos para os criadores de conteúdo. Mesmo quando o Spotify respondeu às preocupações de médicos profissionais e de artistas, publicando as suas Regras da Plataforma sobre "informações médicas enganadoras", não deu motivos para acreditar que essas regras não serão impostas e aplicadas de forma discriminatória, dependendo do artista. Se ele é popular como Justin Bieber ou diretamente lucrativo como Joe Rogan, então as regras podem não se aplicar; mas se o artista é alguém que não é tão popular, então as políticas do Spotify serão aplicadas e mais rapidamente do que um piscar de olhos.

Quer estejamos a falar de regras legais impostas por governos ou políticas corporativas, um requisito primordial é que elas sejam previsíveis, consistentes, necessárias e proporcionais, para que reflitam os padrões básicos de transparência e responsabilidade. Este é o mínimo que qualquer cidadão participante da vida social ou, qualquer utilizador participante do ambiente online, deve poder esperar. Na sua ausência, os cidadãos enfrentam uma grande dificuldade em se expressar e partilhar a sua arte de forma eficaz.

Similar a outras plataformas, o Spotify incentiva um ambiente de cidadãos de segunda classe contra os quais as suas políticas de conteúdo são aplicadas com mais rigor. Os criadores de conteúdo não são tratados da mesma forma, como estes casos demonstram claramente. Os artistas não deveriam ter de encenar um protesto para obter o mínimo de transparência e responsabilidade. Cabe ao Spotify manter políticas que permitam aos criadores de conteúdo entender o ambiente em que estão prestes a entrar, as regras que regem a sua participação e a forma como essas regras são aplicadas.

Artigo original de Konstantinos Komaitis e imagem publicados pela Electronic Frontier Foundation (CC).

Neo e o "paradoxo do hacker": uma discussão sobre a securitização do ciberespaço

Bernardo Beiriz

[A caracterização de hackers como "profissionais de TI" ou como "hackers informáticos" pelo Estado influencia as dinâmicas da securitização do ciberespaço.]

No filme Matrix, Neo (nome de código do personagem Thomas A. Anderson) leva uma vida dupla: durante o dia trabalha como programador numa empresa de desenvolvimento de software, mas durante a noite revela-se um cibercriminoso: um hacker.

Nos estudos de cibersegurança, referências a filmes como Matrix (1999) podem soar repetitivas ou até mesmo como a reprodução de estereótipos. A sucinta descrição da dupla identidade de Neo, no entanto, abre espaço para a discussão sobre um dos elementos que fundamentam esse campo de estudo: "o paradoxo do hacker". Abordo essa ideia do ponto de vista da teoria da securitização e dos seus desenvolvimentos no campo das Relações Internacionais, analisando o papel do hacker como identidade e como objeto de referência na securitização do ciberespaço.

Antes de prosseguir com o desenvolvimento deste conceito, é necessário entender o que é cibersegurança; de que maneiras o ciberespaço pode ser securitizado? Myriam Dunn Cavelty e Thierry Balzacq definem cibersegurança como "um conjunto multifacetado de práticas concebidas para proteger redes, computadores, programas e dados de ataques, danos ou acesso não autorizado – em resumo, são práticas padronizadas por muitos atores diferentes para tornar o ciberespaço (mais) seguro".

Em que termos podemos definir a identidade de "hacker" a partir desta definição de cibersegurança? A reação inicial tende a classificar os hackers como aqueles que atentam contra esse conjunto multifacetado de práticas desenvolvidas para proteger as redes; como aqueles que quebram esse conjunto de "leis". Em Matrix, os "agentes" fazem parte de um programa de Inteligência Artificial na Matriz cujo trabalho é mantê-la "segura". Promover a segurança na Matriz envolve combater cibercriminosos como Neo, evitando que hackers alterem o funcionamento

do conjunto de redes, computadores e sistemas que compõem a simulação computacional que é a Matriz.

A apresentação de Neo (ou Thomas A. Anderson) como programador durante o dia, no entanto, chama a atenção para uma questão fundamental de cibersegurança, que denomino de "paradoxo do hacker". Leonie Maria Tanczer argumenta que "a suposta dicotomia e oposição binária entre hacker versus profissionais de TI e cibersegurança" esclareceria quais atores seriam responsáveis por fazer "bem" e quais estariam fazendo mal, definindo o que seria "seguro" e o que seria "inseguro".

O paradoxo está justamente na coexistência dessas duas identidades no mesmo indivíduo. A caracterização de um sujeito como hacker ou como profissional de TI, portanto, tem implicações importantes para a securitização do ciberespaço. Essa classificação de determinados indivíduos como "bons" ou "maus" pode ser exercida pelo Estado delimitando os que estão "dentro da lei" e os que estão "fora da lei", mas também pode ocorrer a partir da aprovação ou reprovação de um público externo.

Grupos hacktivistas como os Anonymous, por exemplo, podem ser classificados pela opinião pública em qualquer extremidade da escala subjetiva do "bom" ou "mau". Essa classificação depende de um reconhecimento das atividades dos "hacktivistas" como "produtivas": devem atender a solicitações coletivas ou mesmo gerar entretenimento e empenho públicos.

Compreender a classificação dos hackers como "bons" ou "maus" pela opinião pública é um exercício filosófico-político-sociológico que foge ao escopo deste artigo. Os resultados da caracterização desses hackers como "profissionais de TI" ou como "hackers informáticos" pelo Estado, no entanto, influenciam as dinâmicas da securitização do ciberespaço e serão aqui analisados.

O hacker e a insegurança ontológica no ciberespaço

A NSA, uma das principais agências de segurança nacional dos Estados Unidos da América, está diretamente associada à contratação de hackers, ou "profissionais de TI" (dependendo da classificação utilizada). O uso do termo hacker aqui é propositado, pois muitos dos indivíduos contratados por agências como a NSA têm um histórico de comportamento criminoso considerando "práticas destinadas a proteger redes"; à luz das "leis" do ciberespaço.

A prática de contratação desses indivíduos ocorre por dois motivos: primeiro, o conhecimento que eles possuem é extremamente necessário para produzir mecanismos de defesa e ataque para o Estado em questão; além disso, estes hackers/profissionais navegam em "águas cinzentas". Nelas, eles não são necessariamente protegidos por leis formalmente reconhecidas, assim como não serão necessariamente condenados por essas mesmas leis. Dependem, em última instância, da classificação do Estado: cabe ao Estado determinar se esses indivíduos são criminosos ou heróis,

com base numa área do Direito marcada por interpretações subjetivas e decisões judiciais ou mesmo pela falta de leis e jurisprudência aplicável.

Mas de que forma essa possibilidade de caracterização do hacker como "bom" ou "mau" pelo Estado é atravessada pela securitização do ciberespaço? A partir daqui, torna-se necessário abordar alguns pontos sobre a teoria da securitização.

A Escola de Copenhaga, segundo Lene Hansen e Helen Nissenbaum, entende a segurança como um "ato de expressão que securitiza, ou seja, que constitui um ou mais objetos de referência, historicamente a nação ou o Estado, como ameaçados à sua sobrevivência física ou ideológica e, portanto, em urgente necessidade de proteção". A securitização, por seu lado, especialmente no campo da cibersegurança, funciona ao ligar diferentes objetos de referência", particularmente fornecendo uma ligação entre aqueles que não invocam explicitamente um humano limitado coletivamente, como "rede" ou "indivíduo", com aqueles que o fazem.

Outra maneira de entender a securitização é a partir das descrições fornecidas por Didier Bigo e por Barry Buzan, Ole Waever e Jaap de Wilde. Para Buzan, Waever e de Wilde, "securitização é o movimento que leva a política além das regras estabelecidas do jogo e enquadra a questão como um tipo especial de política ou como acima da política". Um "movimento de securitização", portanto, deve ser capaz de convencer um público externo, legitimando a "securitização" da questão, legitimando assim a sua transferência para um campo "acima da política", acima das regras praticadas.

Bigo apresenta a segurança como sendo baseada num processo intersubjetivo: "algo" passa a ser apresentado a "alguém" como uma questão de segurança. É a prática do discurso que faz de uma determinada questão uma questão de segurança e não necessariamente a existência "real" de uma ameaça: nomear algo como ameaça pode ser um primeiro "movimento de securitização". Finalmente, para transformar "algo" (ou alguém), um objeto de referência em questão de segurança, para securitizá-lo, o agente securitizador deve possuir credenciais, produzindo uma aceitação da audiência.

O ciberespaço é constantemente atravessado por essas dinâmicas de (in) securitização, seguindo a ideia de Bigo de que segurança e insegurança podem caminhar juntas, ou seja, que o enquadramento de uma questão como segurança gera o papel/posição de insegurança para outras. Entendendo o ciberespaço como um ecossistema constituído pela convivência entre humanos e "não humanos", como uma mescla entre infraestrutura física, código e interação humana, percebe-se a complexidade desse espaço e a pluralidade de relações existentes.

O hacker é um exemplo de desafiar a divisão entre humanos e não humanos. O empenho do humano com a "matéria" no ciberespaço a partir do código, daí a ação de Neo como "hacker informático", muitas vezes confunde ações "humanas" com falhanço: quando um

sistema de informação pára de funcionar, pode-se inicialmente atribuir isso a uma "falha de processamento", inerente à lógica de funcionamento da própria tecnologia, quando na realidade ela está ligada à ação deliberada de um hacker.

Essa característica reforça a noção de ciberespaço como um ambiente perigoso em que não se pode ter certezas. Além disso, algumas ações de utilizadores "comuns" podem facilitar a ação dos cibercriminosos, de modo que os primeiros também são transportados para o "paradoxo do hacker": dependendo das suas ações, dotadas ou não de intencionalidade (algo que, principalmente no âmbito digital, não pode ser verificado), utilizadores comuns podem ser classificados como ameaças, resultando num estado constante de caracterização como "ameaças potenciais" – o que retoma uma ideia de estado de alerta constante desenvolvida pelos Estados Unidos no contexto da guerra contra o terror. Numa interessante passagem do texto de Hansen e Nissembaum, os autores afirmam que "assim como nos discursos sobre epidemias e contágio, as ciberinseguranças são geradas por indivíduos que se comportam de forma irresponsável, dessa forma comprometendo a saúde do todo".

Num passo ousado, afirmo que, em suma, há uma inerente insegurança ontológica nos sistemas de informação. A primeira maneira de ver essa insegurança está no "paradoxo do hacker" descrito anteriormente. Marco A. Vieira argumenta que "no sentido convencional, portanto, a segurança ontológica diz respeito à capacidade psicológica dos indivíduos de sustentar um sentido coerente e contínuo de quem são". Considerando a lógica da (in) securitização descrita por Buzan, Waever, de Wilde e Bigo, a dupla identidade atribuída ao hacker/profissional de TI produz uma ameaça constante, a ser determinada pelo Estado (assim como por outros agentes de securitização, como agências privadas de cibersegurança). Este processo, por isso, leva à erosão justamente dessa capacidade psicológica dos indivíduos de terem um sentido da sua identidade.

A diferenciação entre "nós" e "outros", caracterizando objetos referenciais como "segurança" ou "insegurança", perde-se quando hackers/profissionais de TI fazem parte simultaneamente do "nós" e dos "outros". O "paradoxo do hacker", por isso, reforça a lógica da (in)securitização ao ofuscar a diferenciação das identidades, tornando todos os responsáveis pelo desenvolvimento e promoção da "segurança" nas redes como potenciais ameaças.

Outra forma de compreender a insegurança ontológica dos sistemas informacionais é atentar no funcionamento do ciberespaço e na "quase-agência" da matéria. Sobre o funcionamento dos sistemas digitais, é necessário entendê-lo a partir da mistura descrita anteriormente: existem vários pontos de "falha" na interseção entre interação humana, código e infraestrutura física. "As ameaças surgem de falhas de software e de hardware e não podem ser corrigidas com tecnologia digital e programação melhoradas". O ciberespaço é atravessado por ameaças sistémicas, geradas pela imprevisibilidade da ação de

computadores e de sistemas de informação. Essas falhas, no entanto, ao ocorrerem num sistema que engloba tanto o "real", o analógico, o concreto, e o digital, podem gerar situações potencialmente perigosas para os próprios sistemas de informação ou para os sistemas físicos e humanos nos quais estão inseridos.

vulnerabilidade humana às múltiplas e infinitas falhas possíveis que surgem nos sistemas digitais. Fomentar uma relação de dependência é, de certa forma, aceitar lidar com uma insegurança que não pode ser resolvida, pois não reside apenas na ação dos humanos que compõem essa mistura, mas na interação "autónoma" das próprias máquinas.

Neo é capaz de manipular a Matriz através de uma forma específica de hacking, porém, estando ligado diretamente a esse "cibersistema", ele também sofre as consequências do que acontece na Matriz. Por outras palavras, e usando exemplos mais concretos, ataques como o Stuxnet (que interferiu no funcionamento das centrais nucleares iranianas) ou ataques de ransomware responsáveis pelo mau funcionamento de hospitais, mostram a

Uma oportunidade indispensável surge agora para a discussão da "quase agência" da matéria descrita pelos estudos de ciência e tecnologia. Primeiro, a abordagem mais objetiva é feita por James Breasset e Nick Vaughan-Williams, com base na ideia de resiliência atribuída ao [sistema de detecção de intrusos] "CNI2000 Intruder Detection System (IDS)". Esse sistema, segundo os autores, seria capaz de determinar de forma autónoma se

uma ameaça é real, não dependendo da interpretação humana. Segundo eles, o sistema seria "capaz de realizar os seus próprios movimentos de (in)securitização". O CNI2000 IDS seria assim um exemplo claro de como existe "uma crença e uma dependência na capacidade de agenciamento das tecnologias de proteção para se protegerem: para garantir que as infraestruturas de resiliência permanecem resilientes".

O agenciamento do CNI2000 IDS é explícito e facilmente identificado, pois ocorre a partir da automação, da tomada de decisões por máquinas, substituindo e mimetizando a ação humana. A descrição do funcionamento do ciberespaço feita antes, no entanto, possibilita uma discussão mais interessante. Argumento que no ciberespaço, na mistura que o constitui, cada "unidade de matéria", seja um rato de computador, uma linha de código, um conjunto de servidores ou um clique feito por um "humano", é dotado de agenciamento: todas essas "unidades de matéria" são capazes de causar diferença, sendo esta a definição de agenciamento para autores como Bruno Latour (mas também lembrando a ideia de Anthony Giddens de que agenciamento é a capacidade de interferir na estrutura). O agenciamento dos hackers, assim, é indiscutível, pois eles, direta e indiretamente, possuem a capacidade de interferir nos sistemas digitais de diversas formas.

Pensando nos algoritmos e na sua relação com a ciber(in)segurança, é possível interpretá-los como "arranjos ético-políticos de valores, pressupostos e proposições sobre o mundo". Esses arranjos, no entanto, são ferramentas tecnológicas que "precisam de estar embutidas numa combinação de humano e/ou máquina para serem executadas". A necessidade para essa incorporação é parte fundamental da conexão "ciborgue" estabelecida entre o "digital" e o "humano", portanto, do ciber-ecossistema. Os hackers participam neste movimento de incorporação do ciborgue: os hackers são os sujeitos desse embutimento.

A incorporação e a execução do código, cruzando as fronteiras entre humano e não humano, perpassa a lógica da securitização e também deve ser pensada em termos éticos e filosóficos: a produção deliberada de mecanismos capazes de realizar os seus próprios "movimentos de (in)securitização" constitui a efetiva e indiscutível implementação de agenciamento para estas entidades tecnológicas. Embora tanto "unidades de matéria" quanto "humanos" possam simultaneamente "possuir agenciamento", a produção destes mecanismos autónomos/automatizados leva à questão: isto não faz parte de um processo de substituir o agenciamento humano pelo agenciamento tecnológico?

Por outras palavras, a capacidade de causar diferença descrita por Latour permanece a mesma quando nem mesmo os movimentos de (in)securitização são realizados por "humanos"? Isto altera a "identidade" do hacker ou o "paradoxo do hacker"? São perguntas abertas, para as quais não há respostas simples.

Conclusão

O ciberespaço, visto como um ecossistema que engloba "humanos" e "não humanos", torna-se o ambiente ideal para a proliferação de ameaças, reforçando a multiplicação de movimentos de (in)securitização, sejam produzidos por "humanos" ou por "unidades de matéria" (com base numa interpretação ampla de agenciamento). O hacker, como uma identidade, ameaça e objeto de referência destes movimentos de (in) securitização, está sujeito a uma constante instabilidade, pois ocupa simultaneamente o lado do "nós" e do "eles" na produção de segurança e de insegurança. Acredito que esse movimento ocorre não apenas na perceção e interpretação externa sobre os hackers; que essa instabilidade não está presente apenas na visão dos agentes (des)securitizadores, mas também internamente. Assim como Neo em Matrix, dado um contexto de instabilidade, em que o sujeito não consegue ter a certeza sobre o seu "lado", é possível que surja uma "dúvida interna" para os hackers sobre a sua posição nesta dinâmica. O "paradoxo do hacker" neste contexto assume uma face externa e interna, uma ideia que ainda não foi explorada.

Esta instabilidade e as características de imprevisibilidade e interconectividade do ciberespaço reforçam os movimentos de (in)securitização, pois torna todos os componentes do ciberespaço possíveis ameaças: de um utilizador leigo em questões de cibersegurança que age de forma "perigosa" ou "insegura" ao fazer o download de música de um site "não confiável" a um componente de hardware específico de um sistema de deteção de intrusão que falha imprevisivelmente no momento de uma intrusão, todos são dotados de agenciamento em cibersegurança e portanto retratados como possíveis ameaças.

A segurança no ciberespaço não deve ser ignorada. Garantir o bom funcionamento dos sistemas de informação vai para lá de um exercício retórico, pois a mistura do ciber-ecossistema mostra-nos a dependência da vida humana da infraestrutura digital. Estas discussões, no entanto, devem ser capazes de coordenar com parcimónia as práticas de (des)securitização, uma vez que elas podem ser responsáveis por caracterizar o ciberespaço apenas como uma questão de "segurança", o que não sucede. Deve-se atentar também para a substituição do agenciamento "humano" pelo agenciamento "tecnológico", alcançado através do desenvolvimento de sistemas automatizados, capazes de definirem os seus próprios movimentos de (in)securitização.

Referências disponíveis no texto original, publicado na E-International Relations (CC).

Foto: Dan LeFebvre | Unsplash

Darwin entre as máquinas

Samuel Butler

[Ao Editor do The Press, Christchurch, Nova Zelândia - 13 de junho de 1863.]

Senhor - Há poucas coisas das quais a geração atual se orgulha mais do que as maravilhosas melhorias que estão a ocorrer diariamente em todos os tipos de aparelhos mecânicos. E, de facto, é motivo de grandes felicitações por muitos motivos. É desnecessário mencioná-los aqui, pois são suficientemente óbvios; o nosso negócio actual reside em considerações que podem tender um pouco a humilhar o nosso orgulho e a fazer-nos pensar seriamente nas perspetivas futuras da raça humana. Se voltarmos aos primeiros tipos primordiais de vida mecânica, à alavanca, à cunha, ao plano inclinado, ao parafuso e à polia, ou (por analogia que nos levaria um passo adiante) àquele único tipo primordial do qual todo o reino mecânico foi desenvolvido, queremos dizer a própria alavanca, e se então examinarmos a maquinaria do Grande Oriente, ficamos quase impressionados com o vasto desenvolvimento do mundo mecânico, com os passos gigantescos com que avançou em comparação com o lento progresso do reino animal e vegetal. Acharemos impossível abster-nos de nos perguntar qual será o fim desse poderoso movimento. Em que direção tende? Qual será o seu resultado? Dar algumas sugestões imperfeitas para a solução destas questões é o objetivo da presente carta.

Usamos as palavras "vida mecânica", "reino mecânico", "mundo mecânico" e assim por diante, de forma avisada, pois como o reino vegetal foi lentamente desenvolvido a partir do mineral, e da mesma maneira o animal sobreveio ao vegetal, então agora, nestas últimas eras, surgiu um reino inteiramente novo, do qual ainda vimos apenas o que um dia serão considerados os protótipos antediluvianos da raça.

Lamentamos profundamente que o nosso conhecimento tanto de história natural quanto de maquinaria seja muito pequeno para nos permitir empreender a gigantesca tarefa de classificar as máquinas em géneros e subgéneros, espécies, variedades e subvariedades, e assim por diante, de traçar os elos de ligação entre máquinas de características muito diferentes, de apontar como a subserviência ao uso do homem desempenhou entre as máquinas aquele papel que a seleção natural desempenhou nos reinos animal e vegetal, de apontar órgãos rudimentares

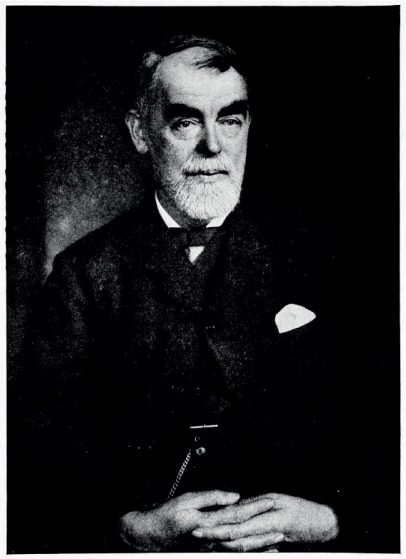
que existem nalgumas poucas máquinas, debilmente desenvolvidos e perfeitamente inúteis, servindo no entanto para marcar a descendência de algum tipo ancestral que pereceu ou foi modificado nalguma nova fase de existência mecânica. Podemos apenas apontar este campo para investigação; deve ser seguido por outros cuja educação e talentos tenham sido de uma ordem muito mais elevada do que qualquer uma que possamos reivindicar.

Nalgumas poucas pistas decidimos aventurar-nos, embora o façamos com a mais profunda modéstia. Em primeiro lugar, gostaríamos de notar que, como alguns dos vertebrados mais baixos atingiram um tamanho muito maior do que desceu até aos seus representantes vivos altamente organizados, uma diminuição no tamanho das máquinas muitas vezes acompanhou o seu desenvolvimento e progresso. Veja-se o relógio, por exemplo. Examine-se a bela estrutura do pequeno animal, observe-se o jogo inteligente dos membros diminutos que o compõem; no entanto, esta pequena criatura é apenas um desenvolvimento dos incómodos relógios do século XIII - não é uma deterioração deles. Pode chegar o dia em que os relógios ["clocks"], que certamente não estão a diminuir em volume nos dias de hoje, sejam inteiramente substituídos pelo uso universal dos relógios ["watches", de bolso ou de pulso], caso em que os "clocks" se extinguirão como os primeiros sáurios, enquanto o "watch" (cuja tendência alguns anos foram mais para diminuir em tamanho do que o contrário) continuará a ser o único tipo existente de uma raça extinta.

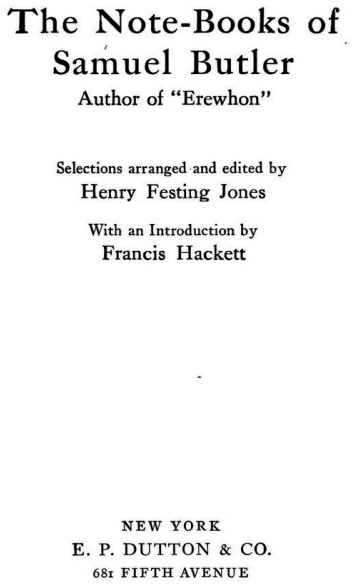
As visões da maquinaria que estamos a debilmente indicar sugerirão a solução de uma das maiores e mais misteriosas questões da época. Referimo-nos à pergunta: que tipo de criatura será o próximo sucessor do homem na supremacia da terra? Muitas vezes ouvimos isso ser debatido; mas parece-nos que nós mesmos estamos a criar os nossos próprios sucessores; estamos diariamente a aumentar a beleza e a delicadeza da sua organização física; estamos diariamente a dar-lhes maior poder e a suprir por todos os tipos de dispositivos engenhosos aquele poder autorregulador e auto-actuante que será para eles o que o intelecto tem sido para a raça humana. No decurso dos tempos, vamos encontrar-nos como a raça inferior. Inferiores em poder, inferiores naquela qualidade moral de autocontrolo, devemos olhar para eles como o ápice de tudo o que o melhor e mais sábio homem pode ousar almejar. Nenhumas paixões diabólicas, nenhum ciúme, nenhuma avareza, nenhuns desejos impuros vão perturbar o poder sereno dessas criaturas gloriosas. Pecado, vergonha e tristeza não terão lugar entre elas. As suas mentes estarão num estado de calma perpétua, o contentamento de um espírito que não conhece desejos, não é perturbado por arrependimentos. A ambição nunca os torturará. A ingratidão nunca lhes causará a inquietação de um momento. A consciência culpada, a esperança adiada, as dores do exílio, a insolência do cargo e os desprezos que o mérito paciente dos indignos recebe - tudo isso lhes será totalmente desconhecido. Se querem "alimentar-se" (de que pelo uso desta palavra traímos o nosso reconhecimento deles como organismos vivos), eles serão atendidos

por escravos pacientes, cujo negócio e interesse será cuidar para que nada lhes falte. Se estiverem desligados, serão prontamente atendidos por médicos que estão completamente familiarizados com as suas constituições; se morrerem, pois mesmo esses gloriosos animais não estarão isentos dessa consumação necessária e universal, entrarão imediatamente numa nova fase de existência, pois qual máquina morre inteiramente em todas as partes num e mesmo instante?

nossos cavalos, cães, gado e ovelhas, em geral, com grande bondade; damos-lhes o que a experiência nos ensina a ser o melhor para eles, e não pode haver dúvida de que o nosso uso de carne aumentou a felicidade dos animais inferiores muito mais do que a diminuiu; da mesma maneira, é razoável supor que as máquinas nos tratarão com bondade, pois a sua existência depende tanto da nossa quanto a nossa depende dos animais inferiores. Eles não podem matar-nos e comer-nos como fazemos



SAMUEL BUTLER IN 1898
FROM A PAINTING BY EMERY WALKER


The Note-Books of
Samuel Butler
Author of "Erewhon"

Selections arranged and edited by
Henry Festing Jones

With an Introduction by
Francis Hackett

NEW YORK
E. P. DUTTON & CO.
681 FIFTH AVENUE

Supomos que, quando chegar o estado das coisas que acima tentámos descrever, o homem se terá tornado para a máquina o que o cavalo e o cachorro são para o homem. Ele continuará a existir, ou mesmo a melhorar, e provavelmente estará melhor no seu estado de domesticação sob o domínio benéfico das máquinas do que no seu atual estado selvagem. Tratamos os

com as ovelhas; não só exigirão os nossos serviços no parto dos seus filhos (cujo ramo da sua economia permanecerá sempre nas nossas mãos), mas também em alimentá-los, arranjá-los quando estiverem doentes, enterrar os seus mortos ou trabalhar os seus cadáveres em novas máquinas. É óbvio que se todos os animais da Grã-Bretanha, exceto o homem, morressem,

e se ao mesmo tempo todas as relações com países estrangeiros fossem tornadas perfeitamente impossíveis por alguma catástrofe repentina, é óbvio que, em tais circunstâncias, a perda da vida humana seria algo temível de se contemplar - da mesma forma, se a humanidade cessasse, as máquinas estariam tão mal quanto ou ainda piores. O facto é que os nossos interesses são inseparáveis dos seus, e os delas dos nossos.

Cada raça depende da outra para inúmeros benefícios e, até que os órgãos reprodutivos das máquinas se tenham desenvolvido de uma maneira que ainda não somos capazes de conceber, elas estão inteiramente dependentes do homem até mesmo para a continuidade das suas espécies. É verdade que esses órgãos podem ser desenvolvidos em última instância, na medida em que o interesse do homem for nessa direção; não há nada que a nossa enfatuada raça desejasse mais do que ver uma união fértil entre duas máquinas a vapor; é verdade que a maquinaria é ainda hoje empregada na geração de maquinaria, tornando-se o parente das máquinas muitas vezes segundo a sua própria espécie, mas os dias de "flirt", namoro e casamento parecem ser muito remotos e, de facto, dificilmente podem ser antecipados pela nossa imaginação débil e imperfeita.

Dia após dia, porém, as máquinas estão a ganhar-nos terreno; dia após dia estamos a tornar-nos mais subservientes a elas; mais homens são diariamente presos como escravos para cuidar delas, mais homens dedicam diariamente as energias das suas vidas inteiras ao desenvolvimento da vida mecânica. O resultado é simplesmente uma questão de tempo, mas que chegará o tempo em que as máquinas terão a real supremacia sobre o mundo e os seus habitantes é o que nenhuma pessoa de mente verdadeiramente filosófica pode questionar nem por um momento.

A nossa opinião é que a guerra até a morte deve ser instantaneamente proclamada contra elas. Todas as máquinas de todos os tipos devem ser destruídas pelo simpatizante da sua espécie. Que não haja exceções, nenhum quartel revelado; voltemos imediatamente à condição primitiva da raça. Se for afirmado que isso é impossível pela condição atual dos assuntos humanos, isso imediatamente prova que o mal já está feito, que a nossa servidão começou a sério, que criámos uma raça de seres que está para lá do nosso poder de a destruir, e que não estamos apenas escravizados, mas absolutamente aquiescentes na nossa escravidão.

Por ora, deixaremos este assunto, que apresentamos gratuitamente aos membros da Philosophical Society. Se eles consentirem em valer-se do vasto campo que indicamos, devemos esforçar-nos para trabalhar nele nalgum período futuro e indefinido.

Carta assinada por Cellarius (pseudónimo de Samuel Butler). Transcrita nas páginas 42 a 46 dos "The Note Books of Samuel Butler", em re-edição (1917) de Henry Festing Jones.

Carta de Copenhaga

A todos os que moldam a tecnologia hoje.

Vivemos num mundo onde a tecnologia está a consumir a sociedade, a ética e o âmago da nossa existência.

Está na altura de assumir a responsabilidade pelo mundo que estamos a criar. Altura de colocar os humanos antes dos negócios. Altura de substituir a retórica vazia de "construir um mundo melhor" por um compromisso para a ação real. É a altura de organizar e de nos responsabilizarmos uns aos outros.

A tecnologia não está acima de nós. Deve ser governada por todos nós, pelas nossas instituições democráticas. Deve seguir as regras das nossas sociedades. Deve servir às nossas necessidades, tanto individuais como coletivas, assim como aos nossos desejos.

Progresso é mais do que inovação. Somos criadores de coração. Vamos criar uma nova Renascença. Vamos abrir e dinamizar conversas públicas honestas sobre o poder da tecnologia. Estamos prontos para servir as nossas sociedades. Aplicaremos os meios à nossa disposição para fazer avançar as nossas sociedades e as suas instituições.

Vamos construir a partir da confiança. Vamos construir para a verdadeira transparência. Precisamos de cidadãos digitais, não de meros consumidores. Todos dependemos da transparência para entender como a tecnologia nos molda, quais os dados partilhamos e quem tem acesso a eles. Tratar-nos uns aos outros como mercadorias das quais extrair o máximo valor económico é mau, não apenas para a sociedade como um todo complexo e interconectado, mas para todos e cada um de nós.

Design aberto ao escrutínio. Devemos incentivar uma reflexão contínua, pública e crítica sobre a nossa definição de sucesso, pois ela define como construímos e projetamos para os outros. Devemos procurar projetar com aqueles para quem estamos a criar. Não toleraremos design para vícios, enganos ou controlo. Devemos conceber ferramentas que gostaríamos que os nossos entes queridos usassem. Devemos questionar a nossa intenção e ouvir os nossos corações.

Vamos passar do design centrado no ser humano para o design centrado na humanidade.

Somos uma comunidade que exerce grande influência. Devemos proteger e nutrir o potencial de fazer o bem com ela. Devemos fazer isso com atenção à desigualdade, com humildade e com amor. No final, a nossa recompensa será saber que fizemos tudo ao nosso alcance para deixar o nosso jardim um pouco mais verde do que o encontrámos.

Nós, que assinamos esta carta, vamos responsabilizar-nos e uns aos outros para colocar essas ideias em prática. Esse é o nosso compromisso.

Publicada originalmente em 2017 (CC). Debatida e redigida no Techfestival.