

Joguemos o Jogo

Ana Isabel Carvalho e Ricardo Lafuente

Em fevereiro de 2009, com mais duas pessoas, fundámos o primeiro *hackerspace* do Porto, o Hacklaviva, um espaço de emancipação tecnológica. O nosso fascínio pela cultura *hacker*, pelas implicações da tecnologia no dia-a-dia e pelo desejo de aprender e partilhar levou-nos a precisar de um espaço físico onde pudemos cruzar estas vontades. Desde workshops de soldagem, desmontagem e reciclagem de computadores, maratonas de tradução de *software*, conversas, design colaborativo de fontes, redes *wireless* comunitárias, produção portuguesa de música com software livre e um sub-coletivo dedicado ao *hacking* de dados abertos, vivemos três anos intensos e precários, cheios de energia e sem apoios financeiros. O Hacklaviva cessou as atividades em março de 2012, deixando por conta própria o coletivo do Transparência Hackday, que segue incansável a viagem por entre os dados abertos, a cidadania consciente e a informação pública.

Apesar da frequência com que falamos de temas como *hacking*, *software* e cultura livre ou dados abertos, raramente parámos para as descrever. A desafio dos Visões, sentámo-nos pela primeira vez para escrever sobre estes mundos, focando sobretudo a desmistificação de temas e termos deste universo.

Há vários anos que colaboramos com os Visões Úteis. Essa colaboração costuma aparecer num momento mais tardio, e restrita sobretudo criação da imagem gráfica do material da peça. Apesar desse carácter mais recuado, temos sempre acesso à pesquisa e apontamentos que o grupo reúne durante a construção das peças. Um arquivo cheio e vasto, com apontamentos de várias viagens coletivas. Nestas colaborações vamos entrando no seu processo criativo, como convidados para jantar na casa de um amigo. Com a peça Ficheiros Secretos convidaram-nos a entrar na cozinha, a seleccionar ingredientes e condimentos enquanto os víamos colocar coisas sobre o lume e mexer a colher de pau.

No final sentamo-nos todos juntos à mesa. Falemos de ficheiros e de segredos.

Não te posso deixar fazer isso

O cinema mostra-nos muitas vezes representações de tecnologia emancipada. Máquinas inteligentes, concebidas por humanos, que inesperadamente ganham vida própria, se revoltam contra o seu criador e se tornam uma ameaça para toda a raça humana. É um retrato comum, que nos sugere um perigo implícito na criação tecnológica: usos e vontades da máquina que não foram previstos pelo seu criador mas que se tornaram reais. Funções e desígnios que passaram despercebidos no processo de conceção. O HAL 9000 de *2001* ou a Skynet de *Terminator* são os melhores exemplos deste arquétipo.

Em *War Games*, um adolescente consegue, através do seu computador de casa, ter acesso ao super computador do exército dos EUA. Inicia aquilo que a princípio lhe parece apenas mais um jogo de

estratégia, uma simulação de guerra, até que descobre estar prestes a começar um conflito real. A mensagem é que é perigoso procurarmos explorar os limites da tecnologia que temos à nossa disposição, visto que em última análise ela poderá facilmente mostrar-nos caminhos imprevistos e perigosos, ou desprender-se das nossas vontades e seguir a sua própria.

Nas últimas décadas, o computador transformou-se num objeto indispensável, central na nossa vida quotidiana, usado para trabalho e para lazer, assumindo novas formas e propósitos nas nossas vivências: os *smartphones* e televisões HD são computadores com propósitos específicos, pouco diferindo do nosso portátil na forma como funcionam. Ao mesmo tempo, as notícias continuam a construir narrativas simplistas à volta do mundo escondido do computador e da internet. Um submundo desconhecido, povoado de figuras anónimas com intenções duvidosas, que navegam pela rede, manipulando os códigos e protocolos que a movem, e subvertendo a tecnologia de forma a dela extrair o pior.

O *hacker* na cultura pop

As histórias de comportamentos rebeldes ou desviantes no meio digital precisam de imagens para vingar completamente. Personagens e aventuras tão emocionantes precisam de imagens que agarrem os olhos. A parte mais complicada desta equação é que na maioria das vezes não se conhece a identidade do delinquente, não há fotos dele, não há impressões digitais na cena do crime, em certos casos não há sequer cena de crime. E por mais que as palavras inflamadas de uma notícia nos tentem prender, não há como uma imagem para nos fazer vibrar, uma imagem que se guarda na memória. É a imagem de alguém a digitar no seu teclado durante horas não se ajusta facilmente ao imaginário tecno-glamoroso a que os habituais narradores costumam recorrer.

O recurso mais simples e óbvio é o universo maravilhoso da *stock art*, ilustração e fotografia pré-fabricada e pronta a acompanhar qualquer texto, seja notícia, artigo ou história ficcional. É aqui, através da caixa de pesquisa, entre imagens de famílias felizes, mulheres a sorrir para taças de salada, homens de negócio e paisagens idílicas que vemos surgir imagens do estereótipo do *hacker*.

Vestido de escuro e com cara tapada por uma balaclava, de luvas e com uma lanterna apontada ao teclado. Empunhando um martelo com o qual ameaça destruir um cadeado físico, que protege um portátil. Com um olho tapado, igual a um pirata dos velhos tempos, este ladrão de informação espalha uma sombra assustadora sobre um computador. A sua mão chega a nossa casa vinda do ecrã enquanto apanha com precisão cirúrgica uma *password* desprotegida. A máscara de Guy Fawkes.

A linha de fundo que permeia todas estas imagens é a de que se trata de personagens perigosas e obscuras, enredadas em operações criminosas. É a única forma de as associar a este universo de crime é colocá-las em cenários comuns, tal como assaltantes empunhando uma arma carregada a um teclado, vandalizando ecrãs LCD com graffitis, escondendo a identidade como os ladrões de bancos.

Virtual e real

Desde os primórdios da Internet que nos referimos aos seus meandros como um mundo virtual. Talvez por influência de narrativas futuristas onde são idealizados mundos paralelos potenciados pela tecnologia, existe uma distinção constante entre o virtual e o real - este último referindo-se à existência física concreta, longe da mediação dos sistemas digitais.

Esta distinção introduz um terrível nevoeiro na nossa tentativa de compreender o que se está a passar neste momento da história: é que as experiências “virtuais” de ação, interação não são menos reais por passarem por uma mediação do digital.

Era frequente - e ainda não desapareceu - a descrição de espaços de conversa online como sendo espaços virtuais, onde fazemos amigos virtuais; mas as conversas, as experiências e as vivências são integralmente reais, tidas com pessoas reais, mesmo que assumam formas que não correspondam diretamente ao seu paralelo no mundo físico. Lentamente fomos suavizando coletivamente a nossa estranheza, graças ao Facebook e à sua insistência no uso de identidades reais (ao contrário de pseudónimos), que veio evidenciar como o uso de plataformas online para a comunicação não vem beliscar o caráter real da sua essência. “Virtual” é um termo que só pode dificultar uma compreensão honesta, séria e crítica do estatuto da tecnologia nas nossas vidas individuais e coletivas.

Podemos encontrar outras expressões que tornam evidente o caráter difuso da nossa relação com os media digitais, como é o caso do prefixo “ciber-”. Falamos de “ciber-crime” como uma categoria autónoma de delinquência. Formas bem mais comuns de ilegalidade não mereceram a mesma urgência de prefixação: a condução sob influência do álcool não é um “auto-crime”; a fraude financeira não é um “econo-crime”. A singularidade terminológica para classificar o que ocorre na Internet é mais um sintoma da estranheza que ainda temos perante o digital e a forma como opera.

Poder na técnica

Neste novo contexto histórico, onde a tecnologia digital vem causar profundas alterações em todas as facetas da humanidade, são os seus operadores quem se encontra, subitamente, com um poder desmesurado. Falamos dos administradores dos sistemas e das redes, as pessoas que criam e mantêm as enormes bases de dados e as estruturas que as sustentam, sem qualquer restrição de acesso. É quem controla a técnica quem tem maior poder sobre ela.

Este ponto pode ser enfatizado voltando ao Estado Novo, onde a censura institucionalizada tornava o acesso à verdade um bem extremamente escasso; aqui, encontramos uma manifestação inusitada de poder na mão de quem controla o processo técnico: os linotipistas e compositores tipográficos tratavam da impressão dos livros e notícias antes de estes passarem pelo lápis azul. Pelas suas mãos passavam os textos originais por filtrar, conferindo aos técnicos um precioso acesso a uma realidade vedada à enorme maioria da população. Podemos constatar um fenómeno semelhante no ofício de telefonista durante a

maior fatia do século XX, com fácil acesso a qualquer conversa a decorrer.

O controlo do artifício como fonte de várias nuances de poder não é, portanto, uma novidade.

Algoritmos e o fim da responsabilidade

Um ponto central deste tema é a desresponsabilização do operador face à máquina. Esta torna-se expressa numa frase-chave que encontramos no Google News, bem no fundo da página após todas as notícias: “A selecção e a publicação das notícias nesta página foram realizadas automaticamente por um programa de computador”. Aqui encontramos ecos da Skynet, o sistema autónomo e consciente de *Terminator*, que toma decisões por si, independentes de qualquer vontade humana e, por isso, inimputáveis aos operadores já que a responsabilidade é da máquina - um fator decisivo nos vários episódios de litígio entre os grupos de média e a Google.

Apesar do seu profundo *savoir-faire* no campo do digital, a Google delega de forma aparentemente ingénua as responsabilidades aos maneirismos do programa, descartando qualquer possibilidade de intervenção humana. O mecanismo é automático, e as decisões são tomadas por um programa de computador. As narrativas a que a cultura popular nos habituou, onde as máquinas são independentes e pensam autonomamente, muitas vezes de forma contrária aos seres humanos, são responsáveis por criar esta cortina de impotência face ao determinismo digital.

Mas por trás de qualquer programa estão as intenções, a vontade, as idiossincrasias e as dúvidas de um operador humano - a pessoa que escreveu o código que faz o programa concretizar-se. Nenhum programa toma decisões automaticamente; o que pode fazer é, sim, seguir caminhos específicos com base nas premissas programáticas estabelecidas pelo autor do programa. Podemos ir mais longe e admitir que nenhum programa e nenhum computador toma decisões por si; eles apenas podem obedecer às prioridades, regras e estipulações dos seus criadores para, com base nelas, seleccionar cegamente o caminho a seguir.

Sob esta perspetiva, só poderemos encarar posturas como a da Google - e de qualquer outra entidade que aponte para qualquer sistema digital o ónus de tomar decisões certas ou erradas - como uma posição profundamente nebulosa e perigosa, por perpetuar a ideia de que a tecnologia poderá ser de alguma forma independente e inquestionável, atribuindo-lhe uma vontade própria que apenas encontramos em ficções distópicas.

O sistema não assume

A desculpabilização do operador e a delegação da responsabilidade ao algoritmo vem encontrar outra consequência notória: a elevação da “falha técnica” ao magno pretexto para qualquer acidente, imprevisto ou problema.

Se antes a responsabilidade desembocava inevitavelmente numa pessoa - supervisor, gerente, funcionário - agora temos a possibilidade de descartar qualquer ónus ao atribuir essa responsabilidade ao programa,

ao sistema, ao algoritmo, e é extremamente difícil conseguirmos denunciar que, por trás de cada programa, sistema e algoritmo, está uma vontade e uma intenção cristalizadas no código - a partitura a partir da qual os sistemas executam as suas delicadas e precisas performances.

A responsabilidade descorporiza-se, e torna-se sujeita aos humores do sistema, essa entidade indefinida, inamovível e intransponível, descrita de forma próxima da que usamos para descrever atualmente os “mercados”, entidades quase-biológicas que se apresentam como turbulentas, com euforias e depressões, apresentando calma ou nervosismo.

O valor dos hábitos

Uma tática comercial contemporânea, levada a cabo principalmente por grandes cadeias de distribuição, consiste na cedência de cartões de desconto em troca da monitorização dos hábitos de compra. A empresa sai, sem dúvida, a ganhar: o lucro perdido neste intercâmbio é largamente compensado pela cedência de um perfil de consumo extremamente valioso, não só para esta empresa mas também muitas outras que pagarão confortavelmente pelo acesso aos perfis individuais e agregados, que descrevem hábitos, preferências, tendências e motivações por vezes íntimas e pessoais, manifestas no critério de compra de cada um de nós.

O aparecimento de cartões de desconto que abarcam mais do que uma empresa, resultado de parcerias e alianças corporativas, resultam no desenho de um mapa de vários hábitos e movimentos cruzados: as horas em que se abasteceu o depósito do automóvel, a hora de compra de cada alimento e cada acessório, as preferências culturais de cada um na forma dos filmes que vê no cinema ou aluga no videoclube online. Lentamente, ganha forma o potencial de criar verdadeiros mapas de comportamento, contendo informação abundante sobre a vida privada de cada pessoa - onde esteve, o que consome, como se comporta -, o sonho último de qualquer Stasi ou KGB.

Escudar-nos-emos facilmente no “quem não deve, não teme”, até um dia descobrirmos que houve fundamento para a privacidade ter sido um direito historicamente defendido, e que existem alturas onde é melhor que o mundo permaneça ignorante dos nossos hábitos, intenções e preferências. Em fevereiro de 2012, um pai indignado dirigiu-se ao supermercado Target, exigindo explicações para a sua filha ter recebido cupões de desconto para berços, roupas e alimentos para bebé; uns dias depois, apresentou um pedido de desculpas ao supermercado, que graças à sua análise de comportamentos de compra, deduziu a gravidez da filha antes do seu próprio pai.

Comportamentos = números

Esta tendência crescente de digitalizar e quantificar comportamentos está presente em imensas facetas da nossa vida contemporânea. O conjunto de opiniões, perspetivas e preferências à volta de um tema específico torna-se quantificável - o número de “likes” -, analisável e, portanto, comerciável. A maior fonte de lucro para a Google e o Facebook, entre muitas outras, é exatamente esta informação

quantificada, com que podemos mapear preferências e tendências em rankings imaculados que poderão ser revendidos ou cedidos a terceiros, num mercado em franca ascensão.

Quando cai o pano, o que acontece a essa informação? Podemos confiar que os computadores são desligados no final das análises, e que os dados serão esquecidos? Irão os operadores dessas bases de dados, bem como os autores dos programas que as gerem ou os seus superiores, assumir responsabilidades no caso de fuga de informação ou quebra de privacidade?

Para que estes mecanismos funcionem, é necessário acostumar a opinião pública e tranquilizá-la, apresentando a vontade de recolher informação cada vez mais pormenorizada como algo benéfico e natural. Introduzem-se palavras sonantes (“big data”, “marketing behavioral”) e ofertas ou descontos aliciantes como forma de suavizar o caráter invasivo e totalizador desta recolha profunda de informação pessoal. Propõe-se o seu uso comercial como mais uma forma de empreendedorismo, e extingue-se qualquer contestação fazendo o público esquecer que houve um dia em que essa concentração dos nossos pormenores não era, de todo, aceitável.

Paninformicon

Na sequência do escândalo da NSA e das revelações da hiper-vigilância global que têm sido levadas a cabo, com recurso a inúmeras bases de dados (incluindo as dos supermercados), é oportuno recordarmos Jeremy Bentham e o seu Panopticon, uma ideia para um sistema de vigilância e controlo total e perfeito. Trata-se de um edifício configurado para conter vários indivíduos em celas; um guarda pode observar, a partir do seu posto, todas as celas e o comportamento de todos os indivíduos. Por outro lado, cada prisioneiro permanece ignorante sobre se está a ser observado num dado momento.

Reencontramos hoje essa assimetria, com enormes bases de dados nas mãos de autoridades e grandes grupos corporativos. No entanto, ela não é tão evidente por a vigilância não ser visual, e por isso mais difícil de enquadrar - mostra disso é a indignação comum em qualquer instância de vídeo-vigilância, em contraste com a adesão significativa a programas de desconto e análise de mercado, com a necessária cedência de informação pessoal: pela carteira morre o cidadão. O atual cenário, em que a nossa informação pessoal já está distribuída por inúmeras bases de dados acessíveis por igualmente inúmeros agentes, afigura-se-nos como um estranho Panopticon incorpóreo que não é ótico, mas numérico e textual - não é disparatado enunciar que nos encontramos confortavelmente instalados num enorme Paninformicon.

O *hacking* como saída

O termo *hacker* surge nos anos 60, no MIT (Massachusetts Institute of Technology), associado ao modelismo de comboios. Identifica o gozo e a determinação em encontrar soluções para a partir de meios ou combinações inesperadas. Aquilo a que poderíamos chamar “pensar fora da caixa”, ou “espírito MacGyver”. Uma pitada de desenrascanço e uma pitada de elegância para resolver qualquer problema que

seja, seja uma maquete de linhas de comboio ou um pedaço de código que cria arco-íris no ecrã do nosso computador.

O *hacker* é a pessoa que consegue esta dose de equilíbrio entre a inteligência e o humor na forma de lidar com determinadas situações. A ideia generalizada de que os *hackers* são génios da programação que resolvem tudo através do computador, à distância, no aconchego do seu quarto, é um retrato limitado..

Cracker é o termo utilizado para descrever os hackers que preferem operar fora dos confins da lei para ganho próprio. Um dos *crackers* mais conhecidos e eficazes, Kevin Mitnick, executou grande parte dos seus feitos através de técnicas daquilo a que chamamos engenharia social: obter acesso sem recurso a artifícios técnicos, dependendo da interação com outras pessoas e contextos para explorar as fraquezas da natureza humana. Atos tão simples como ligar, fingir que somos a operadora telefónica e pedir para confirmar o código que está impresso no telefone; entrar num departamento com fato de técnico de ar condicionado, um sorriso e uma conversa casual com o segurança das instalações, enquanto se liga discretamente uma *pen-drive* ao sistema central. São formas simples de conquistar sistemas e aceder a informação classificada sem passar pelas vias que esperaríamos de um “ciber-criminoso”. São também formas perversas, que nos mostram como a interação humana tem tantas falhas exploráveis como um sistema informático.

O nosso inconsciente coletivo está, assim, semeado com representações algo erróneas do que é o perigo das redes e dos sistemas digitais hoje em dia, de uma forma tão decisiva que ainda continuamos a temer ladrões encapuçados ao volante do seu computador e a imaginar máfias a invadir o nosso reduto digital. Ao mesmo tempo, atribuímos menos valor e indignação a outras ocorrências bem mais gravosas de abuso de confiança nas redes, como é um exemplo claro o recente escândalo da NSA e da vigilância global.

Vários ativismos - ou hacktivismos - surgiram ao longo dos últimos anos, longe da esfera do *cracking* e mais próximo do sentido original e positivamente ingénuo do *hacker*. No Brasil encontramos o Ônibus Hacker, uma camioneta re-convertida em centro de média que percorre a América do Sul para proporcionar workshops e outras atividades destinadas a uma visão crítica sobre a tecnologia e a forma como ela molda a sociedade. Em Berkeley surgiram as HackerMoms, um coletivo que procura chegar a um bom compromisso entre as necessidades da maternidade e a cultura hacker - para que ter um filho não signifique termos de largar o ferro de soldar ou estar longe dos hobbies digitais, procurando tornar o *hacking* numa atividade de família.

Desde coletivos que contestam a intervenção excessiva das autoridades em casos como o Pirate Bay até grupos de cidadãos que, juntos, procuram esmiuçar a informação pública para dela extrair alguma iluminação sobre a forma como a nossa sociedade se move, é nos hacktivismos que poderemos encontrar respostas para lidar com os dilemas que descrevemos. Promover a informação, a educação e a abertura, deixando de parte a demonização do mundo digital e as histórias hiperbólicas dos seus fictícios habitantes. O mundo digital é o mundo em que vivemos.

O poderoso computador de *War Games*, quando confrontado com o jogo do galo e a sua lógica, conclui

laconicamente: *”É um jogo estranho. A melhor jogada é não jogar de todo.”* Neste momento, estamos todos no jogo e não é plausível voltar atrás: estamos irremediavelmente enredados nas consequências que a massificação dos meios digitais em rede nos coloca. O que nos resta, neste momento, é perder os complexos face à tecnologia, procurar cultivar em nós e nos outros um grau de literacia digital e de postura crítica, e com ela tentar nivelar as relações de poder através da informação pública e da recusa determinada em aceitar incursões contra a privacidade individual e coletiva.

Joguemos, portanto, o jogo.