UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
PROGRAMA DE PÓS-GRADUAÇÃO EM PSICOLOGIA SOCIAL E INSTITUCIONAL

BRUNO EDUARDO PROCOPIUK WALTER

HACKING E PRÁTICAS DE LIBERDADE:

CONSPIRANDO COM HACKERS OUTROS MUNDOS

Porto Alegre
2019

BRUNO EDUARDO PROCOPIUK WALTER

HACKING E PRÁTICAS DE LIBERDADE:

CONSPIRANDO COM HACKERS OUTROS MUNDOS

Tese apresentada ao Programa de Pós-Graduação de Psicologia Social e Institucional da Universidade Federal do Rio Grande do Sul, como parte dos requisitos para a obtenção do grau de Doutor em Psicologia.

Orientadora: Profa. Dra. Inês Hennigen

Porto Alegre
2019

CIP - Catalogação na Publicação

Walter, Bruno Eduardo Procopiuk
Hacking e práticas de liberdade: conspirando com hackers outros mundos / Bruno Eduardo Procopiuk Walter. -- 2019.
177 f.
Orientadora: Inês Hennigen.

Tese (Doutorado) -- Universidade Federal do Rio Grande do Sul, Instituto de Psicologia, Programa de Pós-Graduação em Psicologia Social e Institucional, Porto Alegre, BR-RS, 2019.

1. Hacking. 2. Objetos técnicos. 3. Práticas de liberdade. 4. Governamentalidade Algorítmica. 5. Comum. I. Hennigen, Inês, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

BRUNO EDUARDO PROCOPIUK WALTER

HACKING E PRÁTICAS DE LIBERDADE:

CONSPIRANDO COM HACKERS OUTROS MUNDOS

Tese apresentada ao Programa de Pós-Graduação de Psicologia Social e Institucional da Universidade Federal do Rio Grande do Sul, como parte dos requisitos para a obtenção do grau de Doutor em Psicologia.

BANCA EXAMINADORA

_____
Orientadora: Profa. Dra. Inês Hennigen
Universidade Federal do Rio Grande Do Sul – UFRGS

_____
Profa. Dra. Cleci Maraschin
Universidade Federal do Rio Grande Do Sul – UFRGS

_____
Prof. Dr. Alexander Gerner
Universidade de Lisboa - UL

_____
Prof. Dr. Marcos Adegas de Azambuja
Universidade - UFSM

Porto Alegre, 16 de maio de 2019.

Aos meus pais, Celso e Rosa, que sempre me incentivaram a seguir o caminho dos estudos.

AGRADECIMENTOS

À Alice, pelo companheirismo, amizade e parceria que tornaram a jornada de um doutorado mais leve, prazerosa e significativa.

À professora Inês, cuja dedicação às atividades de orientação e de docência é um grande exemplo para mim. Sem deixar de lado o zelo pela produção acadêmica de qualidade e de relevância social, seu cuidado, atenção e forma de ver o mundo contribuíram de modo decisivo para que eu pudesse problematizar e repensar minha própria existência.

Ao Guilherme Paim, ao Edson Dias, ao Cristiano Hamann e aos demais colegas do grupo *Leituras do Contemporâneo e Processos de Subjetivação*, pelos encontros potentes por meio dos quais emergiram novas sensibilidades, desestabilizando verdades tidas como certas.

À professora Cleci Maraschin, ao Carlos Cardoso, ao Carlos Baum (*in memoriam*), ao Póti Gavillon, à Renata Kroeff e aos outros integrantes do *Oficinando em Rede*, por terem me recebido no grupo e pelas boas risadas e fecundas discussões das quais pude participar.

Ao Israel Aquino, secretário do Programa de Pós-Graduação em Psicologia Social e Institucional, pela presteza em sanar dúvidas e esclarecer os caminhos burocráticos.

Aos professores Alexander Gerner e Nuno Nabais, ao Vinicius Jonas de Aguiar e aos demais participantes do grupo de investigação *Philosophy of Human Technology*, pelo acolhimento e pelos ricos ensinamentos recebidos durante o período do doutorado sanduíche que tive a oportunidade de realizar no Centro de Filosofia das Ciências da Universidade de Lisboa.

À Universidade Tecnológica Federal do Paraná, pela concessão do afastamento para cursar o doutorado e, especialmente, aos colegas do Departamento de Educação, do Campus Campo Mourão, por assimilarem minhas funções durante o período em que estive ausente no trabalho.

HACKER: one who hacks, or makes them. A hacker avoids the standard solution. The hack is the basic concept; the hacker is defined in terms of it.

(SAMSON, 2005a, sem paginação)

WALTER, Bruno Eduardo Procopiuk. **Hacking e práticas de liberdade:** conspirando com hackers outros mundos. 2019. 177F. Tese (Doutorado em Psicologia Social e Institucional) – Universidade Federal do Rio Grande do Sul, Porto Alegre, 2019.

RESUMO

Nesta tese buscamos pensar/problematizar/tensionar nosso modo de relação ordinário com os objetos técnicos, conspirando com os hackers modos outros de relação que ampliem o nosso grau de liberdade. Mais do que os hackers em si, interessamo-nos pelos outros mundos possíveis que eles carregam consigo, pelas práticas de liberdade que efetuam e que nos permitem participar de outros modos de relação com os saberes e os poderes instituídos. Para isso, não só descrevemos alguns *hacks*, mas, sobretudo, também operamos no sentido de abrir objetos técnicos que, no geral, nos são como que caixas-pretas. Na primeira das três partes que compõe esta tese, tendo Gilbert Simondon como interlocutor privilegiado, discorremos acerca de algumas posições que podemos ocupar nos encontros com os objetos técnicos (a de inventor, a de produtor, a de consumidor, a de usuário etc.), destacando que o *hacking* aparece enquanto um movimento inventivo por meio do qual o sujeito retoma virtualidades dos objetos para atualizá-las. Não só abordamos nosso modo de relação com os objetos técnicos tangíveis, mas também com um tipo muito especial de objeto que são os softwares, colocando em questão sua abertura/fechamento. Na segunda parte, detemo-nos a pensar e problematizar nossos encontros com redes de objetos técnicos heterogêneos que participam de diferentes estratégias de vigilância e condução de condutas. Sobretudo com Antoinette Rouvroy, discorremos acerca de dois fenômenos aos quais se têm referido por meio dos termos Internet das Coisas e Big Data, ressaltando a ubiquidade dos objetos técnicos, a coleta massiva de dados – não raro em tempo real – e a produção de perfis por meio dos quais opera o que a autora denomina de “governamentalidade algorítmica”. Com as práticas hackers, que vão desde práticas de anonimato até a criação e disponibilização de programas e seus códigos-fonte, buscamos apresentar outros modos de composição que podem contribuir para exercermos práticas liberdade. Por fim, na terceira e última parte, dedicamo-nos a abordar a criação de novos mundos. Para isto, apropriando-nos do pensamento de Michel Hardt e Antonio Negri, discorremos a respeito de lutas em torno do comum (contra sua expropriação, pela sua produção colaborativa e pelas formas de geri-lo). Também, por um viés mais filosófico, retomamos a criação de novos mundos por meio do *hacking*, enquanto ação inventiva, pensando-o a partir de Gilles Deleuze e Pierre Lévy. Assim, por meio de inúmeros encontros – com objetos, com algoritmos, com hackers, com filósofos, com ativistas etc. –, ressaltamos, ao longo desta tese, a urgência de repensarmos o modo pelo qual nos relacionamos com os objetos técnicos.

Palavras-chave: *Hacking*; Objetos técnicos; Práticas de liberdade; Governamentalidade Algorítmica; Comum.

WALTER, Bruno Eduardo Procopiuk. **Hacking and practices of freedom**: conspiring other worlds with hackers. 2019. 177F. Thesis (Doctorate in Social and Institutional Psychology) - Federal University of Rio Grande do Sul, Porto Alegre, 2019.

ABSTRACT

This thesis aims at thinking/discussing/tensioning our ordinary way of relating with the technical objects, conspiring to other types of relations with the hackers in order to broaden our degree of freedom. More than the hackers themselves, there is the interest for other possible worlds they carry around, the practices of freedom they perform, allowing us to participate in other types of relations with knowledge and the ruling power. To achieve this, we didn't only describe some *hacks*; but, above all, we also operated in the sense of opening technical objects which, in general, we see as black boxes. The thesis is composed by three parts; in the first one, having Gilbert Simondon as a privileged interlocutor, we addressed some positions that we can occupy in the encounters with the technical objects (as an inventor, a producer, a consumer, a user, and so on), highlighting that hacking appears as an inventive movement whereby the individual takes back the object virtualities to update them. We do not only approach our way of relating with the tangible technical objects, but also with a very special type of objects, which are the softwares, calling into question their opening/closing. In the second part, we dwelled on thinking and discussing our encounters with the nets of heterogeneous technical objects that participate of different surveillance strategies and conduct of conducts. Especially with Antoinette Rouvroy, we addressed two phenomena which have been referred by the terms Internet of Things and Big Data, highlighting the ubiquity of the technical objects, the massive data collection – not rare in real time – and the profile production through which is operated by what the author calls "algorithmic governmentality". With the hackers' practices, going from anonymity practices to the creation and provision of programs and their source code, we aim at presenting other forms of composition that can contribute, so we can exercise practices of freedom. Lastly, in the third and final part, we dedicated ourselves to address the creation of new worlds. To achieve this, we took as basis the thoughts of Michel Hardt and Antonio Negri, we argued about the fights over the common (against its expropriation, for its collaborative production and for ways of dealing with it). Also, employing a more philosophical background, we resumed the creation of new worlds through hacking as an inventive act, considering it under the views of Gilles Deleuze and Pierre Lévy. Thus, by means of countless encounters – with objects, with algorithms, with hackers, with philosophers, with activists, etc. – we emphasize, throughout this thesis, the urgency of rethinking the way we relate with the technical objects.

Keywords: Hacking. Technical Objects. Practices of Freedom. Algorithmic Governmentality. Common.

WALTER, Bruno Eduardo Procopiuk. **Hacking et pratiques de liberté: en conspirant d'autres mondes avec des hackers**. 2019. 177F. Thèse (doctorat en Psychologie Sociale et Institutionnelle) - Université Fédérale de Rio Grande do Sul, Porto Alegre, 2019.

RÉSUMÉ

À travers cette recherche, nous cherchons à penser/problématiser/tordre notre mode de relation ordinaire avec les objets techniques, en conspirant avec les hackers d'autres modes de relations qui amplifient notre degré de liberté. Plus que les hackers en eux-mêmes, nous nous intéressons aux autres mondes possibles qu'ils portent avec eux, aux pratiques de liberté qu'ils effectuent et qui nous permettent d'accéder à d'autres modes de relations avec les savoirs et les pouvoirs institués. Cependant, nous ne décrivons pas seulement quelques hacks, mais, surtout, nous opérons aussi dans le sens d'ouvrir des objets techniques qui, en général, sont des boîte-noires pour nous. Dans la première des trois parties, qui constituent cette thèse, en ayant Gilbert Simondon comme interlocuteur privilégié, nous parlons de quelques positions que nous pouvons occuper pendant les rencontres avec les objets techniques (comme inventeur, producteur, consommateur, utilisateur, etc.), en soulignant que le hacking apparaît comme étant un mouvement inventif à travers lequel le sujet reprend les virtualités des objets pour les actualiser. On n'aborde pas seulement notre mode de relation avec les objets techniques tangibles, mais aussi avec un type très spécial d'objets qui sont les softwares, en mettant en question leurs ouverture/fermeture. Dans la deuxième partie, nous nous retardons à penser et à problématiser nos rencontres avec les réseaux d'objets techniques hétérogènes qui participent à différentes stratégies de la surveillance et de la conduction des conduites. Principalement, avec Antoinette Rouvroy, nous parlons de deux phénomènes qui sont définis avec les termes Internet de choses et Big Data, en accentuant l'omniprésence des objets techniques, la récolte massive de donnés – qui ne sont pas rares en temps réel – et la production de profils selon lesquels ils opèrent et que l'auteure définie comme "gouvernementalité algorithmique". Avec les pratiques hackers, qui vont au-delà de l'anonymat jusqu'à la création et la disponibilisation des programmes et de leurs codes source, nous cherchons à présenter d'autres modes de composition qui puissent contribuer à exercer des pratiques de liberté. Enfin, dans la troisième et la dernière partie, nous nous consacrons à aborder la création de nouveaux mondes. Pour cela, on prend les idées de Michel Hardt et Antonio Negri, et nous parlons des combats autour du commun (contre sa expropriation, pour sa production collaborative et pour les formes de le gérer). Aussi, en s'appuyant sur une vision plus philosophique, nous reprenons la création de nouveaux mondes par le biais du hacking, en tant qu'action inventive, en se basant sur Gilles Deleuze et Pierre Lévy. Ainsi, à travers d'innombrables rencontres – avec les objets techniques, les algorithmes, les hackers, les philosophes, les activistes, etc. - nous soulignons, tout au long de cette thèse, l'urgence de repenser le mode à travers duquel nous nous relions avec les objets techniques.
.

Mots-clés: Objets techniques. Pratiques de liberté. Gouvernementalité Algorithmique. Commun.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ADR	Applied Data Research
ALGOL	Algorithmic Language
AT&T	American Telephone and Telegraph Company
BBS	bulletin board system
COBOL	Common Business-Oriented Language
DIY	do-it-yourself
DMCA	Digital Millenium Copyright Act
EMACS	The extensible, customizable self-documenting display editor
ENIAC	Eletronic Numerical Integrator and Computer
EUA	Estados Unidos da América
FORTRAN	Formula Translation
FSF	Free Software Foundation
GPL	General Public License
GPS	Global Positioning System
IA	Inteligência Artificial
IBM	International Business Machines
IoT	Internet das Coisas
ISP	Information Search Process
ITS	Incompatible Time-sharing System
LDR	Light-Dependent Resistor
MIT	Massachusetts Institute of Technology
MITS	Micro Instrumentation and Telemetry System
NSA	Agência de Segurança Nacional dos Estados Unidos
PL/1	Programming Language 1
RFID	Radio-Frequency IDentification
TMRC	Tech Model Railroad Club

SUMÁRIO

INTRODUÇÃO

A vida é feita de encontros[1]. E, em cada encontro, ocupamos uma determinada posição e estabelecemos um modo de relação. Não são as mesmas maneiras tecer relações que aparecem quando estamos diante de um amigo ou de um desconhecido, diante de um ser vivo ou de um objeto técnico[2]. No decorrer desses encontros – em que relações são efetuadas – somos constituídos. Dá-se, então, a importância de aprendermos a conduzirmos a nós mesmos ao longo da vida, organizando os encontros, privilegiando aqueles que nos convêm – os bons encontros – e evitando aqueles que não nos convêm – os maus encontros. E, quanto aos encontros que nos são inevitáveis, ainda podemos nos esforçar para tecer relações sob as conexões que mais nos sejam proveitosas.

Para bem nadar, por exemplo, é necessário um aprendizado que tem seu lugar apenas quando se entra no mar, na piscina, no rio etc. De igual modo, para encontros alegres com os objetos técnicos, é necessário uma série de experimentações. Salvo em ocasiões específicas, como em um acidente, podemos escolher o momento em que nos lançamos na água para nadar. Porém, no caso da realidade técnica, estamos como que nela imersos durante toda a vida – a regra é tê-la sempre presente.

Ao longo do século XX e início do século XXI, acostumamo-nos a ter em nossa companhia o rádio, a televisão, o computador, o celular, a internet, os cartões de débito

---

[1] A temática dos encontros atravessa o conjunto das aulas ministradas por Deleuze (2008) entre novembro de 1980 e março de 1981, na Universidade de Vincennes, em Saint-Denis. O termo “encontro” é mais explicitamente enunciado na classe VII – *Tres pertenencias de la esencia: potencia, afeccione y afectos* –, estando subordinado, sobretudo, a uma questão fundamental: de que maneira viver? Trata-se de problematizar a própria existência, indagando-se acerca dos encontros que poderiam e mereceriam ser evitados e aqueles que seriam convenientes de participar – critério de seleção dos encontros. Ainda assim, em cada encontro faz-se importante questionar-se acerca do modo de neles se posicionar e da maneira de compor com o(s) outro(s) corpo(s). Enfim, sem nos atermos estritamente à letra de Espinosa-Deleuze, apropriar-nos-emos de um certo movimento de pensamento expressado por Deleuze (2008), ou seja, seguiremos a noção de que somos continuamente constituídos nos encontros, nas composições que se dão entre as relações de nossos corpos com as relações de outros corpos.

[2] Retomamos a expressão “objeto técnico” de Simondon (2017h, p. 226, tradução nossa) que a define enquanto “um agenciamento finalizado de funções”, ou seja, o objeto técnico é o “resultado da ação do homem sobre a natureza, cristaliza em uma estrutura funcional o dinamismo de um esforço de consciência e de ação” (SIMONDON, 2017f, p. 237, tradução nossa). Enquanto produto do trabalho humano, o objeto técnico é “um feixe coerente de esquemas objetivados por um suporte material” (SIMONDON, 2017f, p. 247, tradução nossa). Para ele, um objeto técnico é um intermediário em duplo aspecto: (1) ele pode atuar como intermediário entre o ser humano e a natureza, ou seja, entre duas ordens de grandeza diferentes; (2) pode atuar enquanto “símbolo inter-humano” (SIMONDON, 2017f, p. 246), pois carrega consigo a ação inventiva que solucionou algum problema. Neste caso, ele só é um intermediário em sentido pleno quando se reconhece no objeto técnico a ação humana depositada, pois caso contrário, o objeto técnico permanece tendo parte de sua existência ignorada. Trata-se ainda de, com a expressão “objeto técnico”, dar-lhe um estatuto para ser pensado e problematizando, tal qual os objetos religiosos e os objetos de arte (SIMONDON, 2017c).

e de crédito, o *Global Positioning System* (GPS), as etiquetas Radio-Frequency IDentification (RFID), as câmeras de videovigilância, entre tantos outros. Tais dispositivos não são neutros, ainda que, por vezes, tenham sua presença naturalizada e nos passem desapercebidos. Como já indicado, é nos encontros que o ser humano devém. Assim, faz-se de grande importância interrogarmo-nos acerca de nossos encontros com esses objetos técnicos que, em grande parte das vezes, não funcionam isolados, mas em redes complexas.

Para muitos, sentar-se em frente a um computador é deparar-se como uma caixa-preta, uma máquina que responde aos cliques no mouse ou às teclas digitadas. Entre a ação realizada e a resposta recebida, permanece um vasto mundo desconhecido que tem sua própria dinâmica e regras de funcionamento. Enquanto apresenta o resultado desejado, o computador é bem-vindo, mas quando falha fica sujeito a tornar-se um inimigo, alvo de sentimentos hostis. Neste caso, trata-se de um modo de relação semelhante àquele do indivíduo que, sem saber nadar, vai ao mar, diverte-se com as ondas, mas quando estas o pegam de surpresa causam-lhe um bom susto, quando não lhe afogam. Sem conhecermos a realidade técnica, corremos o risco de ficarmos à deriva, sujeitados ao que nos acontece – isto é, tanto aos bons encontros quanto aos maus encontros.

Não se trata de afirmar que deveríamos ser enciclopédias ambulantes, capazes de descrever todos os elementos do universo – dos microscópicos aos colossais –, mas de assinalar que no espaço desconhecido do mundo dos objetos técnicos, ao qual por vezes ignoramos, residem aspectos importantes que produzem efeitos em nossas maneiras de sentir, de pensar, de agir, de ser e de viver. Navegar na internet, por exemplo, é interagir com poderosos algoritmos[3] por meio dos quais é possível conduzir nossas condutas, afetando-nos ainda que deles não tenhamos consciência. Por meio deles, somos incitados a clicar, a escrever, a enviar imagens, a falar e nos calar, a participar de grupos, a sorrir, a odiar, a amar, a trabalhar, a comer, a acordar e a dormir etc. Assim, apropriar-se da lógica de funcionamento desses algoritmos – e de outros softwares – não significa tomar consciência de cada linha de código, mas aprender a

[3] De modo simples, pode-se dizer que os algoritmos são como as receitas de cozinha, ou seja, uma série de instruções que, quando performadas, permitem obter um resultado.

maneira pelo qual eles operam criando, desse modo, possibilidades de outras composições. Não é necessário ser um *expert* ou um hacker para se dar conta de que as palavras utilizadas em ferramentas de busca são, por vezes, reutilizadas para apresentar produtos que poderiam nos interessar. Pesquisamos um determinado calçado – um sapato *mocaccino*, por exemplo – e logo aparecem inúmeros anúncios de objetos semelhantes e/ou associados como outras peças de vestuário. De repente, corremos o risco, sem nos apercebermos, de passar a desejar, inclusive, o que nem imaginávamos que existisse.

É preciso algum cuidado para que não se caia em um discurso moralizante categorizando tais algoritmos – ou mesmo outros objetos técnicos – como sendo a encarnação do Mal. É necessário, portanto, precaver-se quanto à tecnofobia. Quantos já não tiveram a grata surpresa de receber a indicação de uma música pelo *Spotify* daquelas capazes de transformar o dia, trazendo o colorido que estava ausente? E quantos já não se depararam com aquele filme selecionado pelo *Netflix* que parecia ter sido escolhido a dedo por alguém que te conhece há tantos anos? Sim, é possível ter bons encontros, ou seja, encontros alegres com os objetos técnicos. Mas confiar cegamente nos encontros selecionados pelos algoritmos também possui seus riscos. Assim, um outro modo de relação, que não seja fundado na recusa radical ou na aceitação cega, poderia pautar-se na construção de uma aprendizagem, por meio da experimentação, com certa prudência, uma espécie de cuidado de si, de zelo que realize esforços no sentido de evitar os encontros tristes sem, contudo, nos privar do acaso – e as boas surpresas que ele pode trazer consigo.

Começamos afirmando a importância de um certo aprendizado[4] quanto à realidade técnica. Mas do que se trata o aprender? Já dissemos que não se reduz à aquisição quantitativa de conhecimento, ou seja, ao seu simples acúmulo. Aprender, como dizia o

[4] Simondon (2017e), neste sentido, discorre acerca da necessidade de uma iniciação técnica que, inclusive, seria anterior ao conhecimento científico e abstrato. Na experiência realizada com seus alunos, de 12 a 14 anos, ele buscava proporcionar “a compreensão intuitiva do ser técnico pela jovem inteligência” (SIMONDON, 2017e, p. 214, tradução nossa), ou seja, tratava-se de criar condições para que tais estudantes pudessem compreender os seres técnicos a partir de sua “enteléquia e não na inatividade, no estado estático” (SIMONDON, 2017d, p. 290, tradução nossa). O que ele propõe aproxima-se do conceito de intuição em Bergson (2010). Para este, enquanto a inteligência coloca-se fora das coisas, recortando o devir artificialmente – tal qual na ciência –, a intuição é capaz de instalar-se no devir interior das coisas. A proposta simondoniana não é a disjunção entre intuição e inteligência, mas sim que a inteligência seja assentada sobre a intuição. Ou seja, que seres humanos e objetos técnicos possam estabelecer um modo de relação no qual o objeto técnico não é capturado apenas enquanto exterioridade a ser utilizada, dominada, comercializada etc., mas, antes, que os objetos técnicos possam ser compreendidos em sua própria ontogênese.

filósofo, é fazer uma espécie de seleção, é “organizar o encontro” (DELEUZE, 2008, p. 307, tradução nossa). Ou seja, é ao longo de inúmeras experimentações que podemos desenvolver uma arte de viver tal qual o do capitão do barco que, considerando a “natureza da tempestade, põe sua embarcação na melhor velocidade e na melhor posição em relação à onda, para que o movimento da onda e o movimento do barco se componham, em vez do movimento da onda decompor o movimento do barco” (DELEUZE, 2008, p. 308, tradução nossa). Tal saber, como estamos propondo, não se reduz ao conhecimento teórico – ainda que possa envolvê-lo –, mas diz respeito a uma compreensão prática por meio da qual escapamos, na medida do possível, dos encontros e enfrentamentos às cegas[5]. Aprender não é apropriar-se de uma capacidade como se estivesse adquirindo um bem, mas é um contínuo *savoir-faire*, sempre relacional, que se atualiza em cada encontro e que só faz sentido no próprio ato existencial.

Dentre aqueles que fazem de suas vidas um contínuo aprendizado na relação com os objetos técnicos – o que inclui também os softwares, como veremos mais detidamente ao longo desta tese – estão os hackers. Ciente de que tal categoria descritiva comporta grande ambiguidade, pedimos ao leitor o benefício da dúvida, deixando, por ora, em suspenso tudo o que já ouviu ou leu acerca dos hackers. Não gostaríamos de ingressar em controvérsias infrutíferas, mas de experimentar uma outra abordagem que se diferencia daquelas que, na maioria das vezes, têm sido realizadas quando tais sujeitos são referenciados ou analisados. Assim, reconhecendo que o próprio termo hacker está inserido em um campo de disputas[6], buscaremos rapidamente situar o leitor acerca das imagens que foram constituídas acerca dos hackers para, na sequência, esclarecermos qual será a nossa abordagem e o porquê pretendemos das outras nos afastar.

Podemos dizer que inicialmente, ao longo dos anos de 1960 e 1970, os hackers eram, no geral, caracterizados como entusiastas da computação, hobbistas adeptos ao

---

[5] Para alguém inexperiente, o acaso se impõe e suas chances de sobrevivência em alto mar estão reduzidas. Poderíamos dizer que, na relação com o mar agitado, pouco lhe resta de liberdade, pois é dominado pelas forças que tendem a tragar e decompor não só seu barco, mas também ele mesmo. Já o capitão experimentado evita o encontro frontal com as ondas que podem despedaçar sua embarcação; ele busca, na própria duração do tempo, um modo de, na relação com o mar, extrair o que lhe será mais proveitoso. Ele não domina o mar e nem é dominado por ele, pois "compõe” com o mar.

[6] Não ignoramos as divergências existentes nas definições do que seria um hacker. A esse respeito, há um rico tópico – “O ser hacker em discussão” – na tese de Evangelista (2010, p. 199) que descreve e analisa os embates, na lista de discussão PSL-Brasil, desencadeados a partir da afirmação do ex-ministro da Cultura, Gilberto Gil, quando ele referiu-se a si como sendo um “ministro hacker”.

do-it-yourself (DIY), e ser considerado um hacker era, entre seus pares, uma honra. Se no início de 1980 tal imagem ainda prevalecia, durante essa década duas outras imagens acerca de quem seriam os hackers foram produzidas: a de cibercriminosos / ciberterroristas e a de libertários (GALLOWAY, 2004; HAFNER; MARKOFF, 1995).

Partindo de um viés moralizante e jurídico, por vezes oscilando mais para um ou mais para o outro, a questão de fundo que passou a se colocar na imprensa era: os hackers são mocinhos ou bandidos? A reportagem da *Newsweek*, de 1983, ainda que privilegie a primeira opção, mantém a tensão entre ambas. Em sua capa, a revista trazia a foto de Neal Patrick, um dos membros do grupo hacker *The 414s*, que teria obtido acesso a dezenas de sistemas computacionais, comerciais e governamentais, nos Estados Unidos da América (EUA) e no Canadá. Apesar de o artigo apontar para insuficiência de leis para crimes informáticos, as práticas dos jovens hackers foram apresentadas mais como travessuras do que como atos de grande potencial destrutivo. Ao final do texto, explicitamente se reconhecia que a mídia não só era complacente com os hackers, mas que também os glorificava como sendo os *Robin Hoods* da era da informação. No mesmo artigo, figurava uma breve referência à fala do vice-secretário de comunicações e inteligência do Pentágono que, em tom de ameaça, teria afirmado: "It's time to put the fear of God into people". Para ele, tratava-se de desestimular as práticas hackers, já consideradas pelo governo dos EUA indesejáveis ou mesmo perigosas (BEWARE..., 1983).

Poucos anos depois, em 1985, a *Time* publicou o artigo *A Threat from Malicious Software.* Nele, partindo do pressuposto de que os hackers eram foras-da-lei, em tom apocalíptico, Murphy (2005) relata que, naquele ano, por pouco um código malicioso não teria interrompido os sistemas que controlavam o fluxo de água e eletricidade de Los Angeles, produzindo um verdadeiro desastre que poderia ter afetado 1,2 milhões de clientes. Ele indicava a existência de perigosos códigos maliciosos – vírus e cavalos de tróia [*Trojan-horse*] – que teriam um imenso potencial destrutivo, advertindo que os crimes informáticos estavam crescendo e que tais sabotagens “poderiam significar a perda de milhões de dólares ou de centenas de vidas” (tradução nossa). Além disso, utilizando-se da expressão “jovem sabotador”, Murphy (2005), em tom de reprovação, fez referência a um dos membros do *The 414s*, ressaltando que o hacker teria conseguido

acesso não autorizado aos registros de um hospital por meio de um tipo de programação subversiva e que, apesar de seus feitos e de ter se declarado culpado, o hacker teria recebido a pena máxima de seis meses de prisão e uma multa de apenas U$ 500.

Assim, ao final da década de 1980, havia se produzido uma imagem segundo a qual os hackers seriam piratas cibernéticos, envolvidos com roubo de informações, propagação de vírus, invasão de sistemas, enfim, verdadeiros foras-da-lei da era da informática. O hacker, portanto, passou a ser visto como um delinquente, ou seja, um sujeito que é percebido como perigoso não só pelo que tem feito, mas, sobretudo, pelo que pode fazer, sendo, portanto, uma ameaça constante. Não devemos esquecer, tal como indicou Foucault (2010), que a delinquência cumpre um papel político-econômico, pois sem ela dificilmente seriam toleráveis as coerções exercidas pelo Estado como, por exemplo, as ações policiais ou o aumento do controle e a redução da privacidade. O medo do delinquente, do sujeito virtualmente perigoso, justifica a multiplicação e a difusão no tecido social de práticas de controle.

Em um dos mais conhecidos glossários hackers denominado *The Jargon File*, esclarece-se que justamente para operar um descolamento dessa imagem negativa que passou a ser produzida pela imprensa, alguns hackers, em 1985, cunharam o termo *cracker*. Com este, buscavam identificar e diferenciar-se daqueles, cujas práticas, marcadas por ilegalidades, eram alvo de condenação na mídia (RAYMOND, 2003a). Ressalta-se que, embora alguns hackers façam distinção entre hackers e *crackers*, outros a questionam (COLEMAN, 2013). De fato, é mais comum que os hackers que não estão envolvidos em práticas transgressoras acusem aqueles que o estão de não serem hackers autênticos ou mesmo de serem *crackers* (COLEMAN, 2012).

A outra imagem dos hackers a que fizemos referência – a de libertários – tem algumas de suas primeiras linhas traçadas, em 1984, pelo jornalista Steve Levy (2012b). De título sugestivo – *Hackers: Heroes of the Computer Revolution* , no original em inglês –, seu livro inicia caracterizando os hackers como heróis, pessoas fascinantes e criativas que transformaram o mundo, “aventureiros, visionários, gente que assume riscos, artistas as pessoas que viram mais claramente porque o computador é uma ferramenta realmente revolucionária” (LEVY, 2012b, p. VII).

E no segundo capítulo – um dos mais revisitados e comentados de seu livro, Levy (2012b) discorre acerca da "Ética hacker"[7] que, segundo ele, era composta por preceitos que, apesar de não terem sido muito debatidos ou publicados em manifestos, teriam, em sua opinião, se tornado consensuais[8]. Não podemos deixar passar desapercebido que, ao final do livro, há um capítulo dedicado à Richard Stallman e que recebe por título "O último dos verdadeiros hackers" (LEVY, 2012b, p.407). Além de ser o fundador da *Free Software Foundation* (FSF), Stallman foi também o criador da *General Public License* (GPL), um *hack* jurídico da lei de propriedade intelectual cujo propósito era, segundo ele, defender os usuários contra toda a forma de dominação. Para isto, partindo do sistema de *copyright*, que restringe e delimita os direitos de cópia e uso, a GPL garantiria os direitos de acesso, cópia, modificação e redistribuição dos programas – as chamadas "4 liberdades" básicas do software livre (FREE SOFTWARE FOUNDATION, 1989; KELTY, 2008).

Em ambas as imagens – a do ciberterrorista e a do libertário –, tem-se em comum o pressuposto de uma identidade hacker. É como se fosse possível descrever seus contornos, elaborando uma espécie de retrato falado por meio do qual o hacker poderia ser identificado. Ao afirmar que os hackers "são" ou "foram" corre-se o risco de obnubilar o que os hackers "fazem" ou "fizeram" e, sobretudo, as estratégias que puseram e põem em ação. Trata-se, nesta tese, de escapar aos modelos idealizantes que conceituam e teorizam acerca dos hackers por meio de abstrações que seriam capazes de explicá-los a partir de uma suposta essência imutável, de uma identidade reconhecível. Interessa-nos, antes, estabelecer com os hackers algo da ordem da conspiração[9] – sim, almejamos

[7] Em síntese, os hackers das mais diversas gerações teriam em comum uma filosofia de compartilhamento, de abertura, de descentralização e, também, marcada pelo prazer de colocar as mãos sobre as máquinas, custando o que custasse. Os princípios elencados por Levy (2012b, p.26-31) são: (1) "O acesso aos computadores – e a tudo que possa ensinar algo sobre o funcionamento do mundo – deve ser ilimitado e total. Siga sempre o imperativo do Mãos à Obra"; (2) "Toda informação deve ser aberta e gratuita"; (3) "Desconfie da autoridade – promova a descentralização"; (4) "Os hackers devem ser avaliados por seus resultados práticos, e não por falsos critérios como formação acadêmica, idade, raça ou posição social"; (5) "Você pode criar arte e beleza em um computador"; (6) "Computadores podem mudar sua vida para melhor".

[8] A antropóloga Enid Gabriella Coleman (2013, p. 18, tradução nossa) afirma que, embora os princípios da ética hacker – composta por imperativos estéticos e pragmáticos – possam ter um núcleo comum, a "investigação etnográfica rapidamente demonstra que semelhante a qualquer esfera cultural, podemos facilmente identificar grande variação, ambiguidade e, até mesmo, pontos sérios de controvérsias. Portanto, uma vez que confrontamos o *hacking* em termos históricos e antropológicos, algumas semelhanças se dissolvem em um mar de diferenças".

[9] Tal qual transmitido na Rádio Alice, "c*onspirar quer dizer respirar junto*" (GUATTARI, 1985, p.59). Tratava-se, no caso da iniciativa Alice de respirar outros ares, de produzir composições cuja prática subversiva fosse coletiva e marcada por bons encontros, ou seja, por afetos alegres.

respirar outros ares com hackers. Se recorremos às suas práticas – ou seja, “o que eles fazem e a maneira pela qual o fazem” (FOUCAULT, 2015, p.366) – é porque buscamos, com isso, articular/criar condições para outras modalidades de relação com os objetos técnicos que não aquelas que, em nossa sociedade, estão naturalizadas e se fazem hegemônicas.

Assim, que fique claro a seguinte ressalva quanto ao uso do termo “hacker”: não buscamos com ele fazer referência a uma suposta essência platônica e nem mesmo, no caso do plural “hackers”, enquanto representativo da totalidade dos hackers. Entendemos, portanto, que hackers são constituídos em diferentes contextos históricos, sociais, políticos, econômicos, tecnológicos, ou seja, engendrados nas mais diferentes linhas de forças. O que nos interessa não é “o” hacker, mas o *hacking*, a própria prática de hackeação, isto é, as formas de compor nos encontros com outros corpos (computadores, softwares, aparatos legais, entre outros).

Compreendemos que a existência hacker é um efeito transitório, um certo modo de estar no mundo e de nele operar. Não se trata, na hackeação, de visar, em última instância, o aumento de rendimento dos objetos técnicos, de fazê-los ainda mais eficientes. Antes, o que está em jogo é a criação de outras possibilidades, a invenção de outros mundos. Neste sentido, diferenciando hackers e engenheiros, o Comitê Invisível (2016, p. 151) nos oferece algumas pistas acerca do que seria a atitude hacker:

> A figura do hacker se opõe, ponto por ponto, à figura do engenheiro, quaisquer que sejam as tentativas artísticas, policiais ou empresariais de a neutralizar. Enquanto o engenheiro captura tudo o que funciona, e isso para que tudo funcione melhor a serviço do sistema, o hacker se pergunta ‘como é que isso funciona? ’ para encontrar as falhas, mas também para inventar outras utilizações, para experimentar. Experimentar significa, então, viver o que implica *eticamente* esta ou aquela técnica. O hacker vem arrancar as técnicas do sistema tecnológico, libertando-as. Se somos escravos da tecnologia, é justamente porque há todo um conjunto de artefatos de nossa existência cotidiana que temos como especificamente ‘técnicos’ e que consideramos sempre como meras caixas-pretas das quais somos inocentes usuários.

Portanto, a questão mais geral que nos norteia nesta discussão – sem ter em momento algum a pretensão de esgotá-la – é: a que modalidades de relação com os objetos técnicos somos geralmente conduzidos e de quais outras podemos participar? Assim, buscaremos mapear algumas dessas práticas, descrevendo-as e criando, desse modo, condições para que possamos nos abrir para outros modos de existência. Nossa

tese parte do pressuposto de que é necessário pensarmos o presente, colocarmos em questão as forças que nos atravessam e nos constituem – esta é considerada, por Foucault (2015), tarefa filosófica e existencial por excelência. Faz parte também das premissas que nos norteiam a valorização de uma espécie de educação quanto aos objetos técnicos, ou seja, de um aprendizado que não se resume ao uso instrumental – o que foi enfatizado por Simondon (2007) –, mas que busca operar as melhores seleções com os objetos técnicos, escolhendo sempre aquilo que melhor nos convém – lição que retomamos de Espinosa, a partir Deleuze (2002; 2008).

Pretendemos, portanto, abordar não os termos de uma relação específica – nem somente o hacker nem apenas o objeto técnico. Antes, interessamo-nos pela própria relação na qual seres humanos e objetos técnicos participam e, por meio da qual, são engendrados e se transformam. É na relação que se produz um complexo jogo de incitações recíprocas, de ação sobre ações, de resistências e de inventividade, é nela que as articulações e composições se produzem. Em dado encontro, ao efetuarmos tal ou qual relação, é a nossa própria liberdade que está questão, ou melhor, o nosso grau de liberdade.

Entendemos por liberdade não algo que possa ser conquistado em definitivo e, nem mesmo, que possamos perder como se fosse um bem. Antes, acompanhando Foucault (1995, p. 244), pensamos que a liberdade é o suporte para as relações de poder e, ao mesmo tempo, aquilo que lhe resiste, “aquilo que só poderá se opor a um exercício de poder que tende, enfim, a determiná-la inteiramente”. Retenhamos esse caráter de jogo – de ações sobre ações – na qual a liberdade pode ser exercida. Se falamos de (graus de) liberdade é sempre fazendo referência a uma situação específica na qual podemos resistir em maior ou menor medida. Para nós, o problema da liberdade não é o de ser livre, antes é o das próprias práticas de liberdade, isto é, de “encontrar uma saída, ou uma entrada, ou bem um lado, um corredor, uma adjacência etc” (DELEUZE; GUATTARI, 2015, p. 17). É sempre no encontro com este ou aquele ente que estaríamos mais ou menos determinados pelo que nos acontece, ou melhor, que saberíamos compor em maior ou menor medida com o outro. Assim, problematizar as nossas relações com os objetos técnicos é, em última instância, um ato ético-político por meio do qual buscamos aberturas para outros modos de existência.

Nosso objetivo, portanto, é pensar/problematizar/tensionar nosso modo de relação ordinário com os objetos técnicos, conspirando com os hackers modos outros de relação que ampliem o nosso grau de liberdade. O que nos interessa não é, em última instância, os próprios hackers, mas os mundos de possíveis que eles carregam consigo. Ao encontrá-los buscamos a abertura para novas sensibilidades e modos de existência.

Após a presente introdução, segue a Primeira Parte, intitulada “Para Além da Posição de Usuário”. Nela abordaremos algumas posições que podem ser ocupadas nos encontros entre seres humanos e objetos técnicos: a de inventor, a de produtor, a de consumidor, a de usuário etc. Para isto, partiremos das noções de arquitetura aberta e fechada – eminentemente classificatórias – para, em seguida, pensá-las a partir da noção de relação. Diante do modo ordinário de compor com os objetos técnicos – desconhecendo sua realidade técnica e fazendo deles simples utilitários –, o *hacking* aparece enquanto um movimento inventivo, por meio do qual mesmo o objeto técnico fechado pode novamente ser aberto, recebendo outros devires. A questão da abertura ou do fechamento dos objetos técnicos passa a ser recolocada em outra dimensão, ou seja, não mais no sentido de categorizar os objetos técnicos por aquilo que são, mas de pensar as condições para tenham sido feitos e mantidos, mais ou menos, abertos ou fechados. E, além disso, quais os efeitos que tais objetos têm em nossos modos de existência. Se um objeto técnico fechado nos conduz, geralmente, a ocuparmos a posição de usuário, mantendo com ele um modo de relação marcado pelo uso instrumental, no *hacking* tal objeto é tornado aberto, sendo a posição ocupada a do inventor, ou seja, daquele que retoma as virtualidades do objeto para atualizá-las. Como veremos, tal discussão não se restringe ao âmbito dos objetos técnicos tangíveis (uma televisão, uma catedral, a rede de metro, um satélite etc.), mas também diz respeito aos softwares que apesar de nos parecerem destituídos de realidade material, não deixam de estar inscritos na realidade física.

Nesta parte, teremos como interlocutor privilegiado Gilbert Simondon, pensador que, na segunda metade do século XX, problematizou profundamente o modo pelo qual nos relacionamos com os objetos técnicos. Sem dúvida, o mundo em que ele vivia era povoado, sobretudo, por objetos técnicos tangíveis. Porém, como se sabe, linhas e linhas de código passaram, cada vez mais, a fazer parte de nossas vidas. Assim como em

relação aos demais objetos técnicos, podemos ocupar a posição estrita de usuários em relação aos softwares. Entretanto, podemos também problematizar e tensionar essa posição. É o que fizeram, por exemplo, hackers do Software Livre, convidando-nos a outras modalidades de relação.

Na Segunda Parte, intitulada “Governamentalidade Algorítmica”, nos propomos a descrever e problematizar a nossa relação tanto com o que tem sido denominado de Internet das Coisas (IoT – *internet of Things*), quanto com o que tem sido designado como Big Data. Ou seja, trata-se de colocar em questão nossos encontros com redes de objetos técnicos heterogêneos que cumprem a finalidade de conduzir condutas utilizando-se, para isto, da coleta massiva de dados e a ação sobre ações, não raro, em tempo real. Que modo de relação estabelecemos com tais redes de objetos técnicos? Muitos hackers, ocupando outras posições que não a de usuário, buscaram organizar tais encontros por meio de estratégias tais como o anonimato e produção do espetáculo (“diante do inevitável da vigilância, façamos um show”). Mesmo quando se tem ciência da existência dessas redes, elas permanecem, na maior parte das vezes, opacas e, portanto, incompreensíveis. Abrindo-as torna-se possível conhecê-las e com elas tecer novas modalidades de relação.

Faz-se necessário, entretanto, reconhecer que o que está em jogo na operação dessas redes já não se reduz à identificação de indivíduos, mas age, sobretudo, tanto no nível infra-individual quanto supra-individual. Neste sentido, buscaremos dialogar com Antoinette Rouvroy que retoma de Michel Foucault a noção de governamentalidade para propor que, nos dias de hoje, estaríamos ingressando em um novo regime de poder a que denomina de governamentalidade algorítmica.

Por fim, na Terceira Parte, denominada o “A criação de novos mundos”, buscaremos abordar a potência criativa das práticas hackers que não se restringem à produção de novos objetos técnicos, mas que podem contribuir para que outros mundos sejam efetuados. Para isto, começaremos com as práticas hackers que contribuem para a produção e gestão do comum. Sem dúvida, nem todas as hackeações cumprem esse papel, entretanto, há aquelas que se destacam, sobretudo, por serem atravessadas por aquilo que denominaremos de espírito enciclopédico. Diferentemente dos enciclopedismos anteriores, quando se disponibilizavam os esquemas, diagramas e

conhecimentos existentes, por meio do *hacking* sujeitos passam a compartilhar também os próprios objetos técnicos concretizados enquanto softwares. Assim, o que é colocado em questão é o regime jurídico-econômico que transforma bens não rivais em propriedade privada. É justamente a natureza do software, que permite multiplicá-lo com um custo bastante baixo, que torna possível este novo enciclopedismo. Trata-se não apenas de fazer da técnica um meio de comunicação para universalizar o acesso aos conhecimentos, mas de compartilhar as próprias máquinas técnicas, de multiplicá-las. Para encaminhar tais análises e discussões, contaremos, dentre outros, com a presença de Antonio Negri e Michael Hardt, autores que têm pensado o comum não apenas por meio do aspecto jurídico ou econômico, mas, sobretudo, ético-político.

Também abordaremos, de um ponto de vista mais filosófico, o *hacking* enquanto invenção. Para isto, recorremos aos seguintes conceitos: virtual, atual, possível e real. Se na Primeira Parte a função do inventor será abordada, sobretudo, a partir do pensamento de Gilbert Simondon, nesta trataremos não exatamente da função, mas do processo de invenção, isto é, da atualização de virtuais. Assim, teremos como interlocutores privilegiados Gilles Deleuze e Pierre Lévy.

PRIMEIRA PARTE - PARA ALÉM DA POSIÇÃO DE USUÁRIO

1 ABRINDO A CAIXA PRETA

Diante de si, Carlos C. tinha uma caixa de plástico cujo conteúdo estava inacessível. Para evitar que outros a abrissem, o fabricante a havia fechado utilizando-se de parafusos especiais e restringindo o uso da chave capaz de retirá-los. Alguém interessado em desparafusá-los, por mais esforçado que fosse, não seria bem-sucedido apenas com uma chave de fenda simples. Nem mesmo uma Allen ou uma Tri-Wing poderiam ajudá-lo.

Para acessar o interior da caixa, conhecer suas entranhas e nelas operar, Carlos C., que não possuía a chave especial, buscou alternativas. Em suas pesquisas, descobriu não só que outros já haviam se deparado com desafios semelhantes, mas que também haviam registrado os procedimentos utilizados para superá-los. Assim, adaptando algumas das “receitas” já existentes, a solução por ele encontrada foi transformar uma caneta de plástico comum na tão desejada chave especial.

Primeiro, as partes da caneta foram separadas, retendo apenas o tubo de plástico. Depois, a ponta do tubo foi levada ao fogo. Após alcançar certa consistência, tornando-se flexível, a ponta do tubo foi pressionada levemente sobre um dos parafusos. Então, ele esperou alguns segundos até o plástico enrijecer-se novamente. A caneta tornou-se uma chave e, assim, foi possível retirar os parafusos. O conteúdo da caixa estava exposto e um novo mundo se descortinava. Sem dúvida, foi um belo *hack*.

A caixa em questão era um antigo videogame Super Nintendo que Carlos C. queria transformar em uma central de mídia e de emulação para jogos antigos de console. Mesmo tendo adquirido legalmente o videogame, tornando-se o proprietário, existiam barreiras físicas para abri-lo, pois, os fabricantes haviam introduzido uma série de empecilhos para que apenas pessoas autorizadas pudessem ter acesso ao seu interior, fazer reparos e modificações. A arquitetura fechada tinha efeitos: evitava, em grande parte das vezes, interações com o aparelho que eram consideradas indesejadas pelos fabricantes. O Super Nintendo havia sido planejado e produzido para ser comercializado e utilizado de uma única maneira: enquanto um videogame. Mas assim como a caneta, ele também foi hackeado transformando-se em algo outro.

Retomando a terminologia consagrada na literatura, poderíamos afirmar que o videogame, sendo um computador, pode ter uma arquitetura aberta ou fechada. Mas o que estes termos significam? No âmbito da informática, Sawaya (1999, p.81) define arquitetura fechada [c*losed architecture*] da seguinte maneira: "(1) Qualquer projeto de computador cujas especificações não foram divulgadas. (2) Sistemas de computador que não possuem *slots* de expansão". A arquitetura aberta [*open architecture*], por sua vez, é por ela definida como: "(1) Qualquer projeto de computador ou periférico cujas especificações tenham sido tornadas públicas"; e "(2) um tipo de projeto que incorpore *slots* de expansão à placa-mãe, permitindo a inclusão de placas" (SAWAYA, 1999, p.330).

Portanto, são dois diferentes aspectos considerados pela autora. O primeiro, diz respeito aos dados técnicos disponíveis acerca do computador, ou seja, se eles são ou não acessíveis ao público em geral. Trata-se não do computador em si, mas daquilo que se pode conhecer acerca dele. Na falta de um termo melhor, denominemos este aspecto de epistêmico. O segundo aspecto, refere-se à própria materialidade do computador, ou seja, ao modo pelo qual ele está constituído, se permite ou não o acréscimo de novos dispositivos, se pode ou não ser ampliado. Denominemos este aspecto de organização estrutural.

Teríamos, assim, uma classificação segundo a qual um computador, seus periféricos e outros objetos técnicos seriam ou de arquitetura aberta ou fechada, devendo-se considerar sempre os dois aspectos que acabamos de mencionar. Ou seja, ele pode ser aberto nos dois aspectos, fechado nos dois aspectos ou aberto quanto a um dos aspectos e fechado quanto ao outro. Evitando um binarismo radical, diríamos ainda, levando em conta cada um dos aspectos, que um objeto técnico se encontra em algum ponto entre dois polos extremos – o da abertura total e o do fechamento total. Assim, quanto mais estiverem disponíveis as especificações do objeto, maior será a abertura, quanto mais protegidas e sigilosas, maior será o fechamento. Quanto mais numerosas forem as possibilidades de acoplamentos, mais aberta será a arquitetura, quanto mais restritas, mais fechada. Enfim, uma arquitetura aberta terá por característica a condição de ser conhecida e complementada, enquanto que em uma arquitetura fechada tais

modificações, quando possíveis, são o privilégio de apenas um indivíduo ou de um grupo muito restrito detentor dos conhecimentos necessários para realizá-las.

Ainda que tais classificações tenham sua utilidade, parece-nos que algo nos escapa. É porque ao tentar enquadrar os objetos, definindo-os enquanto abertos ou fechados, deixamos de lado justamente as relações a partir das quais não só são constituídos, mas também retomados. A que modalidade de relação corresponde o estado atual deste ou daquele objeto técnico? Como ele teria vindo a se tornar o que é no presente? E que modalidade de relação estabelecemos com tal ou qual objeto? Ao discorrer acerca dos objetos técnicos de arquitetura aberta ou fechada, precisamos, antes, pensar nas relações efetuadas nas quais tanto nós quanto os objetos técnicos somos engendrados.

Assim, ao longo deste capítulo buscaremos relocar a questão do aberto/fechado. Entendemos que os objetos técnicos não são algo dado em definitivo, pois mesmo quando se considera que estão concluídos, eles continuam a conter a potência de devir. E de que maneira eles devêm, pergunta-se Santamaría (2015, p.130, tradução nossa). Ao que responde: “não devêm por eles mesmos nem se reproduzem por sua própria conta, senão em sua relação com o ser humano”. Eis aqui o ponto que nos interessa: objetos técnicos e seres humanos efetuam relações e, por meio delas, se transformam[10]. Há, nessas relações, “constituição mútua” (MAURENTE; MARASCHIN; BIAZUS, 2008, p.107). Para pensar tais relações recorreremos, portanto, a Simondon, o filósofo que, buscando conferir outro estatuto para a realidade técnica, afirmava que “o objeto técnico deve ser *salvo*” (SIMONDON, 2017i, p.431, tradução nossa).

1.1 Abertura e Fechamento dos Objetos Técnicos

[10] Não se trata de afirmar que é no ser humano que está localizada, em última instância, a capacidade inventiva. Como Simondon (2007, 2013, 2015) propõe, ao longo de seus trabalhos, se o ser humano age inventivamente é somente porque nele reside algo do pré-individual, o que não ocorre em individuações físicas nas quais o potencial energético teria se atualizado completamente. Lembrando que o pré-individual que o indivíduo carrega consigo permanece em relação com outros pré-individuais. De maneira aproximada, também poderíamos nos remeter a Deleuze (2000, p.247) – leitor de Simondon – quando ele afirma que “o pensamento só pensa coagido e forçado”. Ou seja, o pensamento – a serviço da vida em sua potência criativa – só ocorre quando forças nos atravessam, quando nossa potência está em condições de ser afetada por tal ou qual força a partir da qual o pensamento deriva – nos dois sentidos do termo apontados por Lazzarato (2014): tem sua origem e se desvia. Assim, ao discorrermos acerca da ação inventiva, temos sempre em mente, que ela não está fundada no sujeito, mas que é engendrado em determinadas relações de forças, ou na relação com o pré-individual, que alguma ruptura inventiva pode encontrar lugar.

Além dos dois aspectos já mencionados – o epistêmico e a organização estrutural –, teríamos, portanto, um terceiro aspecto: o relacional[11]. Este já não diz respeito ao grau de abertura ou fechamento do objeto técnico, mas, sobretudo, à posição ocupada pelo sujeito na relação com o objeto técnico. Cada modo de produção – o que não significa necessariamente uma sucessão histórica linear e progressiva entre eles – produz diferentes condições de relação com os objetos técnicos. Ao discorrer acerca dessas condições, Simondon (2017d) descreve a situação de produção artesanal, a de produção industrial em série e a de produção industrial avançada e elaborada, também referenciada por ele como pós-industrial.

Ao retomar a produção artesanal, o filósofo não busca erigi-la como modelo ou ideal, mas sim indicar que nela o objeto técnico está em condição não só de ser produzido enquanto aberto como também de permanecer aberto. O artesão constrói seus objetos por meio de etapas sucessivas, nas quais é necessário o constante ajuste das peças umas às outras por meio de procedimentos reversíveis (o tarugo, a fixação com pernos, o ajuste por meio de cunhas etc.). Assim, uma primeira característica da organização estrutural desses objetos é a reversibilidade, ou seja, após introduzir alguma modificação mantém-se a possibilidade de retornar ao estado anterior. Além disso, o objeto do artesão tem uma constituição ajustável e amplificável: é possível adaptá-lo, acrescentar ou retirar elementos. Uma peça desgastada, por exemplo, pode ser substituída por outra. Quanto ao aspecto epistêmico, o objeto artesanal é, no geral, legível, compreensível. Não porque ele está acompanhado por um manual ou tem suas especificações técnicas publicizadas, mas porque a própria forma pela qual ele está constituído comunica, deixa-se conhecer. Por fim, quanto ao aspecto relacional há uma breve passagem de Simondon (2017g, p.69, tradução nossa) que gostaríamos de fazer menção: “o olhar artesanal captura o objeto como um material reformável, prolongável”.

Poderíamos dizer que o objeto com o qual o artesão trabalha é um “objeto quase”, pois não lhe é possível acrescentar um termo último, pois é considerado inconcluso. Ele – o objeto quase – não conhece o ponto final, apenas vírgulas, travessões ou pontos-e-

[11] No tocante ao par aberto/fechado, enquanto os aspectos epistêmicos e organização estrutural dizem respeito a diferenças de grau – mais ou menos aberto ou fechado –, o aspecto relacional diz respeito a diferenças de natureza, ou seja, há inúmeras posições a serem ocupadas nas relações com os objetos técnicos, todas elas irredutíveis umas às outras.

vírgula[12]. Mesmo quando o artesão entrega o produto de seu trabalho àquele que o encomendou não significa que o destino do objeto seja o progressivo desgaste pelo uso. Isto porque, quando sai do ateliê, passando a estar sob os cuidados de um outro, o objeto não se desliga do ato artesanal, pois quando apresenta desgaste ou defeito, ele permanece aberto ao ato de reparação que "recupera as atitudes e procedimentos do ato de produção" (SIMONDON, 2017g, p.69, tradução nossa). Portanto, trata-se de um modo de relação em que o objeto técnico "é neoténico[13], em certa medida sempre está em estado de construção, à imagem de um organismo em vias de crescimento" (SIMONDON, 2017g, p.67, tradução nossa).

Na produção industrial em série, por sua vez, o objeto técnico é produzido por meio de procedimentos que fazem dele uma "unidade, isto é, um todo completo, porém fechado, indissociável em si mesmo, indivisível, não-reparável" (SIMONDON, 2017g, p.70–71, tradução nossa). O fechamento do objeto se expressa por barreiras físicas como o uso de parafusos especiais cujas chaves correspondentes são inacessíveis (como no caso de Carlos C., acima relatado) e a utilização de solda e/ou rebite ao invés de engates ou parafusos comuns. Sobretudo estes últimos procedimentos, assim como o uso de cola, são operações irreversíveis. Uma vez realizados não se pode retornar ao estado anterior, pois haverá, na melhor das hipóteses, algum prejuízo, e, na pior, a destruição do objeto. Às barreiras físicas acrescentam-se ainda as barreiras legais tais como a perda da garantia quando os lacres ou selos são rompidos, e a proibição de reparo ou manutenção por pessoas não autorizadas. Assim, o objeto técnico fechado, obra da mecânica industrial, torna-se de difícil compreensão – aspecto epistêmico. Por mais que estejam próximos do usuário enquanto objetos de uso no dia-a-dia, eles são distantes porque estão codificados e, portanto, dificilmente decifráveis. Ao encontrar tal objeto técnico, o ser humano não consegue mais reconhecê-lo como resultado de uma operação de construção e como

[12] Aquilo que designamos por objeto quase aproxima-se das expressões que Bruno (2017) emprega ao discorrer acerca das gambiarras, ou seja: objeto em ação, objeto-trajeto, objeto-montagem e, sobretudo, objeto-processo.

[13] De acordo com Barthélémy (2015, p.11, tradução nossa), o termo "neotenia" teria sido cunhado pelo biólogo Julius Kollmann por meio da composição de duas palavras gregas: neo – que significa jovem – e téinein – que significa prolongar, alongar. Assim, inicialmente neotenia faria referência à conservação de características juvenis nos adultos de uma espécie. O autor ainda ressalta que, de maneira singular, Simondon sustenta a hipótese da "neotenia generalizada", ou seja, a de que "o vivente, em geral, será o desenvolvimento lento e prolongado de uma fase inicial [*inchoative*] da individuação física nela mesma, da mesma forma que, no interior do vivente, o animal será o desenvolvimento lento e prolongado de uma fase inicial [*inchoative*] do desenvolvimento do vegetal, etc".

> [...] já não é mais decifrável desencoraja a preocupação com a sua manutenção; o usuário espera que ele seja capaz de funcionar a maior quantidade de tempo possível sem ser retocado, e após este tempo, o objeto será reformado em sua totalidade (SIMONDON, 2017g, p.72, tradução nossa).

Como, a princípio, no objeto industrial fechado não são possíveis reparos, adaptações, aperfeiçoamentos e acréscimos, o momento de sua maior glória, de sua maior perfeição, é quando sai da fábrica e ingressa no mercado para ser comercializado. Neste momento, ele pode ser aceito ou rejeitado, comprado ou ignorado. Ele até pode ter seu valor e novidade reconhecidos, mas com o passar do tempo envelhece, deixa de ser apreciado e se degrada ainda que não tenha sido utilizado. Por estar encoberta por uma espécie de capa, a própria essência técnica[14] do objeto não é reconhecida, os gestos humanos nele depositados são desprezados e, assim, o objeto técnico fechado tem como destino, cedo ou tarde, o descarte (SIMONDON, 2017g; 2017c).

Se na produção artesanal o ato do produtor estava em continuidade com o ato do usuário – mesmo que por meio de atos de reparação, como vimos –, na produção industrial ambos se distanciam, isto quando não se rompe completamente a comunicação entre eles. Entretanto, de acordo com Simondon (2017g; 2017d), a estandardização dos elementos técnicos e a criação de uma rede de fornecedores (que funciona como extensão do produtor) constitui uma nova condição de abertura, ou seja, do estabelecimento do laço entre o produtor e o usuário. Para ele, o objeto aberto, na produção pós-industrial, seria aquele constituído por duas partes, uma tão próxima quanto possível da indestrutibilidade, sendo produzida para ser permanente; e outra concebida para ser transitória, modificável e renovável, permitindo a adaptação a cada uso, a substituição em caso de desgaste ou a ruptura em caso de mal funcionamento. A introdução do fusível, por exemplo, cumpre bem esse papel. Um pequeno e débil dispositivo que, em caso de sobrecarga, é destruído e protege o conjunto. Ao ser substituído ele restitui ao objeto sua condição anterior. O que não era possível na situação artesanal, a substituição das peças defeituosas por outras padronizadas, passa a encontrar agora condição de existência.

[14] Importa esclarecer que a essência do objeto técnico reside, como assinala Barthélemy (2016, p.20, tradução nossa), “no funcionamento particular do objeto e não em seus usos”. Ou seja, está ligada ao seu regime de funcionamento e não aos possíveis empregos que lhe podem ser dados.

Mas a utilização de máquinas[15] abertas pós-industriais exige, como lembra Simondon (2017g, p.74, tradução nossa), “um certo nível de competência técnica, portanto um certo laço entre o produtor e o usuário”, ao que acrescenta uma tese que muito nos interessa: “a abertura pode ser mais completa quanto mais forte for esse laço, e supõe um nível mais elevado de saber, e uma atitude que aceita a vigilância e a manutenção da máquina”.

Caso a relação com um objeto técnico aberto não seja acompanhada desse *savoir-faire*, pouco se diferenciará da relação estabelecida com um objeto fechado. Um aparelho doméstico – um micro-ondas, por exemplo – pode ser descartado por inteiro se após um temporal deixa de funcionar e o usuário o trata como um objeto fechado. Ainda que tenha fusíveis queimados, facilmente substituíveis, a atitude do usuário é que determinará seu destino. Ao que acrescentamos outra situação de igual importância. Um objeto técnico fechado, efeito de inúmeras operações que tenham tornado-o um objeto criptotécnico, pode participar enquanto termo de uma relação na qual é feito aberto. Eis aqui o que nos aproxima do *hacking*. Se consideramos o aspecto relacional, o que está em jogo não é a invasão de computadores e sistemas, mas, sobretudo, uma atitude, um modo de relação no qual o outro termo é feito objeto aberto. Ou seja, trata-se de considerar mesmo os objetos fechados como objetos quase, objetos que podem ser retomados ganhando novos devires.

O simples ato de abrir um objeto fechado – por exemplo, desmontar um rádio decompondo-o em elementos menores – não é, necessariamente, hackeá-lo. A hackeação ocorre quando, ao analisar o objeto, o sujeito é capaz de compreender, em maior ou menor medida, sua essência técnica, seu modo de funcionamento, estando em condições de retomar virtualidades não atualizadas, isto é, ocupando a posição de inventor. A hackeação, enquanto abertura de um objeto técnico, participa de uma relação

[15] De acordo com Raunig (2008, p.40, tradução nossa), tal qual o grego *mechané*, o latin *machina* assume o significado mais geral de “meio”, “criação”, “dispositivo” e não distingue entre meios materiais e imateriais, mas permite que ambos se sobreponham e se fundam. Ele acrescenta ainda que, no grego e no latim antigos, a aplicação do termo teria se expandido fundamentalmente para dois campos: a guerra e o teatro e que, em ambos, manteriam o significado “técnico de aparato, marco, dispositivo, assim como o significado psicossociológico de truque, artifício, engano. Maquinar é tanto inventar um dispositivo como inventar uma história sob a forma de engano, de maquinação”. Ainda que utilizemos, neste capítulo, o termo máquina isoladamente – poderíamos ter feito uso da expressão mais específica “máquina técnica”. Não ignoramos, portanto, que “a máquina tecnológica é apenas um caso de maquinismo. Há máquinas técnicas, estéticas, econômicas, socais, etc.” (LAZZARATO, 2008, p.109, tradução nossa).

de poder, tensionando-a, desestabilizando a condição de fechado que foi imposta ao objeto em sua produção ou *a posteriori*.

1.2 HACKEANDO O SISTEMA TELEFÔNICO

Não teria sido essa a atitude de muitos daqueles que passaram a ser conhecidos como hackers de telefone durante a segunda metade do século XX, isto é, a de abri-los para dar-lhes outros devires? Se para a maioria das pessoas daquela época o telefone era um objeto apreciado, sobretudo, por sua utilidade, os *phone freaks* estabeleciam relações com o sistema telefônico que não poderiam ser reduzidas ao par usuário/utensílio para efetuar chamadas. Como a água que encontra passagem em pequenas frestas e atravessa montanhas, tais hackers habitavam o subterrâneo do sistema telefônico, encontravam passagens que até então eram ignoradas, inclusive pelos próprios técnicos da companhia telefônica. Os *phone freaks* faziam da imensa máquina – que era o sistema telefônico – um objeto quase, acrescentavam alguns elementos e retiravam outros, experimentavam acoplamentos metaestáveis, enfim, inventavam novos modos de relação com esse objeto técnico.

Um desses hackers é Josef Carl Engressia Jr., mais conhecido como Joybubbles, um cego de nascença que ficou famoso por ser capaz de realizar chamadas telefônicas apenas assoviando. No final da década de 1950, por volta dos 7 ou 8 anos de idade, ele já era capaz de emitir com seus lábios um som que, captado pelo aparelho telefônico, encerrava a chamada de longa distância que estivesse em curso (COLEMAN, 2012; LAPSELY, 2010). Aos poucos, à medida em que progredia em seus experimentos, ele desenvolvia novos modos de composição e aprendia a organizar seus encontros com o sistema telefônico. Um telefone fixo era, para ele, um "*laboratório*, um lugar onde uma pequena criança poderia experimentar coisas e onde ela poderia conduzir tantos experimentos quanto ela quisesse. Era um mundo de possibilidades, um mundo no qual estava pressuposta a mais das intoxicantes palavras: *se*" (LAPSELY, 2010, p.119, tradução nossa). O telefone não era tratado por ele como algo dado em definitivo – um objeto fechado –, mas como um outro mundo a ser habitado, a ser conhecido e transformado.

Outro hacker de telefone, chamado John T. Draper, recebeu o apelido de Capitão Crunch porque descobriu como fazer ligações utilizando o apito que os fabricantes de um cereal matinal – o *Cap'n Crunch* – incluíam como brinde. Quando assoprado, o som emitido era exatamente o tom de 2600 Hz, que também era utilizado pelo sistema telefônico para liberar acesso a chamadas de longa distância (o mesmo que tom que *Joybubbles* utilizava por meio do assovio). No decorrer de seus esforços em conhecer melhor como o sistema telefônico funcionava, ele fez inúmeros experimentos descobrindo, por exemplo, como alguns números de teste para os quais duas pessoas, que estivessem em qualquer lugar nos EUA, poderiam ligar e conversar como se um deles tivesse ligado diretamente para o outro (ROSENBAUM, 1971).

Nos encontros com o sistema telefônico, os hackers esforçavam-se por produzir modos outros de composição construindo inclusive dispositivos que pudessem ajudá-los em seus experimentos. O mais famoso deles foi, sem dúvida, a *Blue Box*, que permitia àquele que a possuía agir como se fossem um operador da empresa de telefone, ganhando acesso e condições para realizar inúmeras operações. Com a *Blue Box*, hackers descobriram os caminhos necessários para configurar conferências, também conhecidas como *party lines*, nas quais várias pessoas "se reuniam para conversar, fofocar e compartilhar informações de tecnologia" (COLEMAN, 2012, p.103, tradução nossa).

No início da década de 1970, Rosenbaum (1971) publicou, na revista *Esquire*, o artigo *Secrets of the Little Blue Box*, que foi acolhido com muito entusiasmo. As atividades dos hackers de telefone, desconhecidas pelo público em geral, foram nele descritas com grande colorido e, assim, contribuiu para atiçar a curiosidade de alguns de seus leitores que, por vezes, inspirados pelos personagens das histórias relatadas, colocaram em prática os conhecimentos adquiridos (COLEMAN, 2012). Além disso, é provável que, nesse artigo, pela primeira vez tenha sido utilizado o termo *phreak,* uma mescla de *phone freak* (LAPSELY, 2010).

Um dos leitores do artigo, que havia sido classificado como ficcional pela revista, foi Steve Wozniak. Para ele, os personagens e os detalhes supostamente inventados pareciam verdadeiros demais para serem falsos. Ele estava certo, as histórias apresentadas, como a do Capitão Crunch, eram reais. Desconfiado de que não se tratava

de uma ficção, Wozniak começou a reunir materiais para obter os conhecimentos técnicos necessários para construir uma *Blue Box*. Em suas investigações, ele descobriu um esquema da *Black Box*, um dispositivo que era capaz de impedir que as pessoas que ligassem para o número ao qual ela estivesse acoplada fossem cobradas pela ligação. Com o passar do tempo, ele reuniu conhecimentos e meios suficientes para construir a sua *Blue Box* implantando, de sua parte, alguns aperfeiçoamentos (WOZNIAK; SMITH, 2011). Para ele, não era uma simples questão de fazer ligações gratuitas, mas de "descobrir aspectos do sistema de telefonia que ninguém mais conhecia: coisas como bugs, buracos e fraquezas inerentes ao sistema, e, certamente, maneiras de tirar vantagem de tudo isso" (WOZNIAK; SMITH, 2011, p.76). Ao menos para ele, a verdadeira missão do hacker de telefone "não era bagunçar o sistema, mas encontrar falhas, aspectos curiosos e segredos que a companhia telefônica nunca contou a ninguém" (WOZNIAK; SMITH, 2011, p.93).

Steve Jobs, que esteve envolvido com Wozniak na aventura de produzir uma *Blue Box*, conta que no início o dispositivo por eles construído era utilizado para diversão e travessuras como, por exemplo, quando telefonaram para o Vaticano fingindo ser Henry Kissinger, um diplomata norte-americano, e pedindo para falar com o papa que, no momento, encontrava-se dormindo. Foi Jobs, inclusive, quem propôs que a *Blue Box* poderia ser mais do que meramente um hobby. Sua ideia, que foi levada adiante durante algum tempo, era fabricá-las para vender (ISAACSON, 2011).

O que as inúmeras e heterogêneas práticas dos hackers de telefone tinham em comum era uma identidade de relação – não uma relação de identidade –, ou seja, uma certa maneira de se relacionar com a realidade técnica, mais especificamente com o sistema telefônico. Tratava-se de uma atitude segundo a qual se buscava conhecê-lo, apropriando-se dos seus esquemas de funcionamento[16] e agindo nele e com ele de tal forma a transformá-lo em algo outro.

Nos três casos acima citados – o de Joybubbles, o do Capitão Crunch e o de Wozniak – o essencial não estava na aquisição de conhecimentos abstratos acerca do

[16] O esquema técnico – ou organização estrutural – é, para Simondon (2007, p.128, tradução nossa), uma "relação entre várias estruturas e uma operação complexa que se cumpre através de ditas estruturas". O esquema técnico ou de funcionamento não deve ser confundido com o esquema puro de funcionamento, pois este captura a função ideal a partir de uma perspectiva exterior, podendo ser concretizado por diferentes esquemas de funcionamento (GROSMAN, 2016).

sistema telefônico. Eles não buscavam ocupar a posição de engenheiros ou cientistas – o uso do aparelho fonador ou de um apito para operar o aparelho telefônico é prova disto. Também não eram sujeitos que seguiam estritamente as instruções oferecidas pelos fabricantes por meio dos chamados “Manual do usuário” ou “Manual do proprietário”, documentos estes que prescrevem as formas consideradas “corretas” e “seguras” de utilizar o telefone. Tais hackers resistiram às relações de poder-saber hegemônicas produzindo rupturas. Não é sem razão que uma das definições de *hack* é: “um projeto realizado a partir de um auto-conselho ruim” (SAMSON, 2005a, sem paginação, tradução nossa). Ainda que um tanto confusa, tal definição pode ser melhor compreendida pela explicação que Samson (2005b) sugere décadas depois da publicação do *Tech Model Railroad Club (TMRC) Dictionary*. Para ele, tratava-se de enfatizar uma aplicação não convencional, não ortodoxa da tecnologia que, se fosse julgada por razões técnicas de engenharia, seria preterida.

Nessas práticas de hackeação o aparelho telefônico não foi tomado como um simples intermediário para se conectar a outra pessoa em algum lugar do mundo. Antes, ele é o próprio objeto a ser aberto, a receber acoplamentos, a ser transformado podendo, desse modo, ganhar novas finalidades. Ao hackear não só o aparelho telefônico, mas o próprio sistema telefônico, tratava-se, antes de tudo, de ocupar uma posição, de agir como inventor, recuperando o ato inventivo que esteve presente na concepção do objeto técnico, ampliando-o, deslocando-o, retomando virtualidades e atualizando-as. Enfim, o *hacking* constitui-se, assim, enquanto uma prática de abertura de objetos fechados (o que pode implicar resistências aos poderes hegemônicos ou desvios em relação aos modos naturalizados de se relacionar com os objetos técnicos), transformando-os em objetos quase e dando-lhes novos destinos.

1.3 Nem Senhores, Nem Escravos

A questão que Simondon traz à tona, e na qual nos deteremos neste tópico, é: como tratamos os objetos técnicos? Ou seja, que modo de relação estabelecemos com eles? Que atitude temos diante da realidade técnica? Na introdução de sua tese complementar – *El modo de existencia de los objetos técnicos* – ele traça um paralelo

que é, no mínimo, ousado e desconcertante. Tal qual os escravos de antigamente, os objetos técnicos atualmente, sem receberem o reconhecimento da realidade humana que contêm, estariam excluídos da cultura. Diante do "humanismo fácil" (SIMONDON, 2007, p.31) que opõe cultura e técnica, seres humanos e máquinas – um dos objetos técnicos, por excelência –, ele convida-nos a participar de uma espécie de "humanismo difícil"[17], considerando que a "máquina é o estrangeiro; é o estrangeiro no qual está encerrado o humano, desconhecido, materializado, tornado servil, mas que, entretanto, segue sendo o humano" (SIMONDON, 2007, p.31, tradução nossa). Faz-se necessário, portanto, não somente repensarmos nossas relações com os objetos técnicos, mas também transformá-las.

Sua instigante tese – enunciada em 1958 por ocasião de sua defesa de doutorado, mas nem por isso de todo ultrapassada, pois, no geral, ainda mantemos o mesmo tipo de atitude em relação com os objetos técnicos – é que a maior causa de alienação no mundo contemporâneo não é posta em jogo pela máquina – em última instância, não é ela que nos domina –, mas reside no desconhecimento da essência da máquina e dos demais objetos técnicos. Pode parecer forçado ou mesmo exagerado a analogia entre a máquina e o escravo ou o estrangeiro ignorado e, por isso, vamos acompanhar um pouco mais de perto seu pensamento.

Sem desconsiderar a alienação econômico-social – aquela que ocorreria entre o capital e o trabalho –, Simondon (2007; 2017g) supõe a existência de uma alienação ainda mais fundamental que seria a separação entre o ser humano e a realidade técnica. É considerando este último que ele pôde afirmar que a mudança do regime de propriedade – por meio da coletivização dos meios de produção – não pode acabar com a alienação em si mesma, pois, ainda que com estatutos sociais diferentes, na produção industrial tanto o proprietário quanto os trabalhadores já não estão em relação de continuidade com o indivíduo técnico. Em outras palavras, seja enquanto senhor e proprietário, seja enquanto obreiro e servidor, em ambos os casos a relação com a máquina é de exterioridade. É possível comandar a máquina ou a ela obedecer sem, de fato, conhecê-la na interioridade da própria relação.

[17] A expressão "humanismo difícil" foi primeiramente empregada por Barthélémy (2008).

A ruptura que ocorre na alienação técnica é a “que se produz entre a ontogênese do objeto técnico e a existência deste objeto técnico” (SIMONDON, 2007, p.266, tradução nossa). Ou seja, na ontogênese do objeto técnico o ser humano atua como inventor e construtor. E para que o objeto técnico continue sua jornada, por meio de uma gênese contínua, é necessário que o ser humano não abandone essas funções, mas continue a exercê-las. Só assim a gênese do objeto técnico permanece contemporânea de sua existência. Porém, quando há descontinuidade, fechando-se o objeto técnico, impõe-se a ele a condição de obsolescência. É por isso que tanto o trabalhador que opera diretamente a máquina, mesmo quando a dirige, quanto os proprietários poderiam estar alienados, pois ambos podem relacionar-se com a máquina sem necessariamente prolongar a atividade de invenção – e, por conseguinte, mantendo-a enquanto objeto técnico fechado.

Estabelecer uma relação com a máquina pautada na simples utilização, sem conhecê-la, é deparar-se com aquilo a que Simondon (2007, p.265, tradução nossa) denomina de “zona obscura central”, ou seja, quando “o funcionamento da máquina, a proveniência da máquina, a significação do que faz e a maneira em que está feita” permanecem ocultas àquele que com ela se relaciona e, assim, “o homem conhece o que entra na máquina e o que sai dela, mas não o que faz” (SIMONDON, 2007, p.265, tradução nossa). É o que denominamos de caixa-preta, pois nela o processo está oculto mantendo visíveis e apreciáveis apenas os *inputs* e *outputs*. Indo um passo adiante, não se trata tanto da maneira pela qual objeto está constituído quanto do modo com o qual nos relacionamos com ele, isto é, quando nos interessam apenas as entradas e saídas e não o que realmente acontece lá dentro.

Sem conhecer sua gênese, o modo pelo qual está constituída e a maneira pela qual opera, a máquina ingressa na relação como um objeto utilitário substituto do escravo, pois “como ele, deve obedecer sem falhas, ser fiel, não manifestar espontaneidade inventiva, não entrar em rebelião. Não deve manifestar sua vida interior, seu mecanismo, suas dificuldades” (SIMONDON, 2017f, p. 246, tradução nossa). Estão dadas, dessa maneira, as condições para que a máquina seja avaliada, sobretudo, pelo seu rendimento, por seus resultados, por aquilo que produz.

Ao submeter a máquina a um imperativo de rendimento, impõe-se, por consequência, determinado ritmo àqueles que nela operam – ainda que sejam dela proprietários. Bontems (2015, p.200, tradução nossa), estudioso de Simondon, é luminoso quanto a esse aspecto quando afirma: "não somente o operador deve compreender a máquina para poder fazê-la funcionar de acordo com sua vontade e seu ritmo, mas também que é impossível passar do trabalho para a atividade técnica livre enquanto *a própria máquina está submetida*". Não se trata, assim, de lutar contra as máquinas, mas de transformar o modo de relação que se estabelece com elas. Para ele, a tarefa urgente seria, portanto, liberá-las do imperativo do rendimento.

Tratar as máquinas técnicas enquanto escravos não significa delegar a elas os trabalhos penosos necessários à nossa sobrevivência ou ao nosso conforto. Ninguém é escravo por realizar esta ou aquela tarefa determinada, mas, sobretudo, por ter sua existência desconsiderada, ou melhor, reconhecida apenas pelos seus resultados, por sua utilidade. Se, por um lado, ao longo de sua obra, Simondon nos convida a pensar na realidade técnica presente nas máquinas, por outro, não poderíamos deixar de fazer referência também ao livro de Mouhot (2011) – *Des esclaves énergétiques* – cuja ênfase está na fonte energética utilizada pelas máquinas técnicas. Ao empregar a expressão "escravos energéticos"[18] ele busca salientar o fato de não levamos em conta o modo pelo qual consumimos enormes quantidades de energia fóssil[19] causando profundas – e, talvez, até irreversíveis – mudanças em nosso mundo. Pensar nas máquinas como escravos energéticos seria, então, levar em conta dois aspectos que, por vezes, permanecem ocultos: por um lado, a tecnicidade das máquinas, e por outro, o custo energético envolvido.

[18] A expressão "escravo energético" teria sido empregada pela primeira vez por Richard Buckminster Fuller, no início dos anos de 1950. Desde então, houve várias tentativas de quantificar o número de escravos energéticos que, em média, um indivíduo teria a sua disposição (MOUHOT, 2011). Jancovici e Grandjean (2006, p.15, tradução nossa), por exemplo, calculam que cada europeu, por meio de seu consumo de energia, "dispõe de 100 empregados permanentemente, que são chamados de máquinas, trens e carros, navios e aviões, tratores, centrais de aquecimento, eletrodomésticos, cortadores de grama e teleféricos".

[19] As energias fósseis são aquelas cuja combustão emite dióxido de carbono contribuindo para o aquecimento global. Elas podem ser de matérias orgânicas (vegetais), transformadas quimicamente ou "fossilizadas". Os principais combustíveis fósseis são o carbono, o petróleo e o gás natural (MOUHOT, 2011).

Mas não são apenas as máquinas que podem ter sua realidade técnica ignorada. Os demais objetos técnicos – sejam eles mais ou menos complexos[20] – também podem participar de relações nas quais permanecem, de fato, desconhecidos quanto a sua essência. Sabe-se, por vezes, como operá-los, os botões que devem ser apertados para se obter determinados resultados, mas ignora-se tanto a maneira pela qual estão constituídos quanto seu funcionamento. Não seria assim que, em grande parte das vezes, nos relacionamos com o fogão, a geladeira, o celular, o notebook, o chuveiro, o relógio, o automóvel, os programas de computador etc.? Certamente há um problema que deve ser enfrentado: ninguém é capaz de sozinho conhecer a maior parte dos objetos técnicos com os quais se encontra no dia-a-dia. Felizmente, o próprio problema já traz consigo elementos para pensá-lo, ou seja, é necessário recolocá-lo não a partir do âmbito individual, mas do coletivo – ou, ainda mais especificamente, a partir da produção e da gestão do comum (temática que retomaremos mais detidamente na Terceira Parte desta tese). Por ora, importa afirmar que, mesmo sendo incapaz de conhecer todos os objetos técnicos em sua essência, ainda assim é possível manter uma certa atitude com eles, um certo olhar, um certo modo de com eles se compor.

O objeto tratado enquanto fechado não só está distante daquele que pode mantê-lo atualizado, mas também corre o risco constante de ser desprezado. Certamente os objetos técnicos não são seres viventes tal qual um escravo, porém nem por isso deixam de carregar consigo a cristalização de algo vivente – por um lado, as horas de trabalho humano, por outro, o esforço de invenção que permitiu concebê-los (SIMONDON, 2017g). E, sobretudo, todo objeto técnico carrega consigo um virtual, uma potência para atualização de aspectos que não foram efetuados e que, para isso, dependem do ato inventivo. Assim, o comprador – antes mesmo do usuário – ocupa uma posição bastante especial, pois

> [...] por seu poder de escolha ou rejeição, possui o poder despótico de dar vida ou morte à tradução materializada de um conjunto de gestos humanos do mesmo modo que o povo dominador podia conceder ou negar a vida ao gladiador derrotado nas arenas com um gesto do polegar para cima ou para baixo (SIMONDON, 2017g, p.63, tradução nossa).

[20] A abertura e o fechamento do objeto técnico não estão diretamente ligados à sua complexidade. Por exemplo, uma bicicleta Monark, apesar do grande número de elementos e das operações que eles realizam, é mais aberta do que um simples interruptor de luz, quando seus mecanismos e operações estão ocultos.

O produtor, ao fabricar um objeto técnico, além de empenhar-se no aperfeiçoamento da tecnicidade de seu produto, também passa a responder às normas e às exigências extra técnicas, acrescentando ao seu produto elementos que podem chegar a comprometer o seu progresso técnico[21]. E quanto mais tais elementos se destacam, mais se multiplicam e sobressaem, mais fechado se torna o objeto técnico. No limite, o objeto técnico totalmente fechado seria aquele só poderia ser utilizado, nunca conhecido ou atualizado. Não se deve esquecer, entretanto, que, apesar de sua constituição, um objeto devém aberto ou fechado por meio das relações das quais participa. É o que veremos no tópico a seguir.

1.4 O IBM 704, O TMRC E O TX-0

No final dos anos de 1950, o *Massachusetts Institute of Technology* (MIT) passou a contar com um modelo do IBM 704, também conhecido como *The Hulking Giant*. Assim como os demais computadores de sua época, ele ocupava um enorme espaço físico e exigia um sistema de ar-condicionado específico para mantê-lo funcionando. Era uma potente máquina que "entrava em pane apenas a cada oito dias e funcionava três vezes mais rápido que o modelo 701" (BRETON, 1990, p.109, tradução nossa). Havia uma espécie de ritualística que o envolvia. Apenas um grupo seleto de acadêmicos privilegiados – denominados acólitos – podiam submeter seus dados ao computador, porém sem poder acessá-lo diretamente. E somente os encarregados, comumente chamados de sacerdotes, é que de fato perfuravam cartões e os colocavam nos leitores, apertando botões e virando as chaves para receber os resultados que seriam, posteriormente, entregues aos solicitantes. Com regras rígidas e uma dura disciplina, o acesso ao IBM 704 era negado àqueles que não tinham autorização oficial.

O IBM 704 era mantido enclausurado, distante da maioria de seus usuários. A relação que lhes era proposta era basicamente aquela na qual entregavam os dados e recebiam os resultados. Toda a dinâmica e a operação que ocorriam entre os dois polos – o de entrada e o de saída – permaneciam ocultas, o que contribuía para criar certa

[21] Como nota Carrozzini (2016, p.97, tradução nossa), "em Simondon, a concretização de um objeto técnico [seu progresso técnico], enquanto *individualização*, é acompanhada – ou, ao menos, *deveria ser acompanhada* – de sua *abertura*".

mística em torno do computador. Não era difícil reconhecer a capacidade do computador para executar o árduo trabalho, efetuando complexos cálculos com grande rapidez e precisão. Para a maioria daqueles que o buscavam, pouco importava como ele realizava sua mágica, o importante era sua velocidade e confiabilidade. Se para tais o IBM 704 era feito objeto técnico fechado – uma caixa-preta –, outros estabeleciam com ele diferentes modalidades de relação.

Havia alguns estudantes que não se contentavam apenas com um uso distante do IBM 704. O que lhes interessava não era livrar-se da fastigiosa tarefa de realizar cálculos e mais cálculos. Eles não buscavam apenas delegar trabalho para o IBM 704, mas estavam ávidos, sobretudo, para colocar suas mãos na máquina. Tais jovens eram membros de uma organização fundada, em 1946, no MIT, o *Tech Model Railroad Club* (TMRC). Nela, os participantes dedicavam-se ao ferreomodelismo e suas atividades eram basicamente distribuídas em dois subgrupos. O primeiro, trabalhava na confecção tanto das réplicas de trens quanto dos cenários realistas nos quais elas eram colocadas para funcionar. O segundo, empenhava-se na manutenção, desenvolvimento e aprimoramento do sistema que permita aos modelos de trens circularem na maquete (LEVY, 2012b).

Enquanto o primeiro grupo tinha por preocupação principal o aspecto estético, ou seja, a beleza das réplicas produzidas, a identidade com os originais, o segundo era orientado pelo aspecto técnico, ou seja, a solução dos problemas para colocar os modelos de trens em movimento. Foram os estudantes mais produtivos do segundo grupo que, ao final da década de 1950, segundo Levy (2012b), passaram a utilizar o termo hacker de modo autoreferente, tendo por intuito se distinguirem dos demais, indicando por meio dele tanto o virtuosismo técnico quanto o espírito lúdico.

Quando, em 1959, o professor John MaCarthy ofereceu um novo curso de programação em computadores, os membros do TMRC que se autodenominavam hackers se matricularam e, assim, passaram a ter contato um pouco mais próximo com o IBM 704 (que foi atualizado para o IBM 709 e, depois, substituído pelo IBM 7090), tornando-se eles os maiores utilizadores de tempo de computador do Centro de Computação de todo MIT. Ainda assim, toda interação com a máquina era supervisionada e mediada pelos sacerdotes. Tudo o que lá se fazia deveria estar dentro

do roteiro previamente dado, buscando evitar ao máximo os imprevistos – que nem por isso deixavam de aparecer. Para os hackers do TRMC que tinham o hábito de tocar nas peças, manipulando-as e estabelecendo com elas uma relação de afeto entre corpos marcada pela experimentação e inventividade, as regras burocráticas em torno desses computadores eram fonte de grande frustração.

Tudo mudou quando um laboratório de desenvolvimento militar afiliado ao MIT emprestou, sem prazo definido para devolução, um computador chamado TX-0. Além de ser menor do que os IBMs, com ele estavam dadas condições para um outro tipo de relação. Não era necessário ter intermediários e esperar horas ou dias para saber o resultado de processamento de dados. O TX-0 não utilizava cartões, mas uma fita que era perfurada na Flexowriter, um equipamento semelhante a uma máquina de escrever. Assim, após gravar o programa, a fita era introduzida no TX-0 que rodava as instruções e permitia saber imediatamente quando algo estava errado com o programa. Além do uso dos botões e de lâmpadas que piscavam, também era possível ouvir uma espécie de ruído que saia dos altos-falantes. O TX-0 propiciava um tipo de interatividade que permitia, inclusive que os programas fossem modificados enquanto estavam sendo processados no computador. E, além disso, e certamente mais importante, não havia nem os sacerdotes nem a mesma burocracia do IBM 704 para utilizá-lo; era possível trabalhar nele sem supervisão (LEVY, 2012b).

Enquanto para a maioria dos Usuários Oficialmente Sancionados os computadores tinham finalidades claras e definidas: realizar cálculos, processar informações etc., para os hackers o TX-0 era uma máquina cujas possibilidades estavam em aberto. Havia uma aposta nos encontros com os computadores. Entendemos que o princípio hacker “Computadores podem mudar sua vida para melhor” (LEVY, 2012b, p.31) não diz respeito apenas ao que os computadores podem fazer por nós, mas, sobretudo, àquilo que podemos fazer com os computadores. Era como se aqueles hackers fizessem as seguintes questões: O que nós podemos fazer nos encontros, nas composições com os computadores? De que maneira afetamos e somos afetados pelos computadores e outros dispositivos? Os hackers do TX-0 testavam a potência de computadores, mas também eram testados em suas próprias potências pelos computadores. Como, em geral, não havia reservas no TX-0 para a madrugada, muitos

hackers alteraram seu ritmo biológico, tornando-se ativos principalmente durante a noite, quando poderiam desfrutar de longas horas na frente do console.

Tais hackers fizeram inúmeros experimentos, eram como que alquimistas transformando os computadores em máquinas de experiências de grande alegria. Para o hacker Peter Samson, por exemplo, não importava que o gigantesco TX-0, no qual ele operava, custasse três milhões de dólares. O que lhe interessava é que naquele momento o computador estava tocando uma melodia de Johann Sebastian Bach. Como ele conseguiu tal façanha? Antes de tudo, foi-lhe necessário “ouvir” o computador, deixar-se ser afetado por ele para compreender que dependendo do bit da décima-quarta posição na palavra de dezoito bits que o TX-0 acumulava em dado microssegundo, o som ligava ou desligava. Tudo dependia de um 0 ou 1 que ele aprendeu a manejar para que o TX-0 pudesse produzir os sons desejados (LEVY, 2012b).

Do encontro de Samson com o computador emergiu uma sinfonia porque entre ele o TX-0 estabelecia-se um novo sistema, no interior do qual a comunicação podia existir. O TX-0 não lhe era uma máquina totalmente aberta, mas ele tecia com ela uma relação com maior grau de abertura do que a que lhe era autorizada com o IBM 704. Assim como para seus colegas, o *hacking* consistia em uma certa atitude prática com os objetos técnicos – não importa se era o sistema que funcionava fazendo as réplicas de trens se deslocarem ou se era o IBM 704 ou TX-0. Com cada um deles, eles buscavam estabelecer uma relação pautada tanto no conhecimento dos objetos quanto na ação inventiva.

1.5 Uma Atitude Amistosa

O que os hackers parecem, por vezes, nos sugerir é que é possível estabelecer outras modalidades de relação com os objetos técnicos que escapem à dialética senhor-escravo. E com seria essa modalidade de relação na qual a máquina – ou qualquer outro objeto técnico – não ocupa nem a posição de dominante nem a posição de dominado? Uma das saídas, proposta por Simondon (2017i), é inspirada na ideia de convivialidade de Ivan Illich (1975). Este utiliza a expressão “objetos convivenciais” para se referir à disponibilização de objetos que estariam acessíveis às pessoas e, portanto, não estariam

restritos a um corpo de especialistas. Para ele, “as pessoas necessitam de novas ferramentas com as quais trabalhar ao invés de ferramentas que ‘trabalhem’ para elas. Elas necessitam de tecnologia para extrair o máximo de energia e imaginação que cada uma delas têm, ao invés de escravos energéticos bem programados” (ILLICH, 1975, p.23, tradução nossa).

Ou seja, os objetos técnicos poderiam ser feitos para o homem e não para servi-lo (SIMONDON, 2017i, p. 347). No lugar de uma relação vertical, uma relação horizontal – uma espécie de parceria. Para além da relação de propriedade, o que Simondon e Illich nos chamam a atenção é, sobretudo, para a relação na qual a realidade técnica não é dada pronta de antemão, mas na qual o usuário-consumidor – e não somente os *experts* – é, também, participante da constituição do objeto técnico:

> As pessoas não necessitam apenas obter coisas, elas precisam acima de tudo liberdade para fazer coisas através das quais elas podem viver, ou dar forma a elas de acordo com seus gostos, e utilizá-las para cuidarem uns dos outros. Prisioneiros em países ricos frequentemente têm acesso a mais coisas e serviços que membros de sua família, mas eles não podem decidir como as coisas devem ser feitas e nem o que fazer com elas. Sua punição consiste em serem privados daquilo que eu posso chamar de “convivialidade”. Eles são reduzidos ao status de meros consumidores (ILLICH, 1975, p.24, tradução nossa).

Para Simondon (2017c, p.389), trata-se de estabelecer uma relação marcada por uma “espécie de laço de amizade” no qual se possa “expressar uma certa amabilidade pelo antigo objeto que merece, se não a ternura, ao menos uma consideração em razão da sua idade, um respeito por sua autenticidade, o sentimento de sua densidade no tempo” (SIMONDON, 2017c, p.399, tradução nossa). Isto só é possível quando se compreende o objeto técnico, ou seja, quando se sabe como ele está constituído e qual foi sua gênese (seja diretamente ou pelo ensino). Ou seja, seu apelo vai na direção de reconhecer nos objetos técnicos tanto o esforço inventivo quanto a cristalização dos gestos humanos depositados – o que pressupõe, é claro, que o objeto não seja uma caixa-preta, não esteja fechado.

Entretanto, relacionar-se com um objeto técnico aberto exige um certo nível de competência técnica para poder utilizá-lo. Estabelecer uma relação amistosa com ele não se resume ao conhecimento racional, conceitual, abstrato ou teórico, ainda que possa vir a incluí-los. Não se trata apenas do conhecimento de suas especificações, da

inteligibilidade de seus esquemas. Antes, tal *savoir-faire* começa "*debaixo da razão,* começa com a percepção, começa com a ação do corpo" (SIMONDON, 2017b, p.426, tradução nossa). É no encontro com determinada realidade técnica, estabelecendo uma relação amistosa na qual se é capaz de ser afetado pelo objeto técnico, que se torna possível uma aprendizagem que não é meramente instrumental.

1.6 Wozniak, Jobs e os Apple I e II

No início da década de 1970, longe de uma relação amistosa com os computadores, a maioria das pessoas – de acadêmicos àqueles que participavam dos movimentos de contracultura – os desprezavam como símbolos de controle centralizado e orwelliano[22] (ISAACSON, 2014). À época, acessar um computador era privilégio de poucos, pois grande parte daqueles que existiam eram governamentais ou corporativos. Protegidos pelos muros institucionais, eles tinham sua realidade técnica desconhecida e, inacessíveis, tornavam-se alvo de projeção dos temores existentes.

Todavia alguns interessados nos objetos técnicos não se intimidavam com essas máquinas. Ao contrário, desejavam construir seus próprios computadores. Assim, lançaram um convite para que outras pessoas pudessem se juntar a eles nessa empreitada. O texto, distribuído em panfletos, dizia o seguinte:

> Você está construindo seu próprio computador? Seu terminal? Sua TV Typewriter? Seu dispositivo de entrada e saída? Ou alguma outra caixa-preta digital?
> Ou você está pagando por tempo em um serviço de tempo-compartilhado?
> Se estiver, talvez você possa querer participar de um encontro de pessoas com interesses parecidos.
> Trocar informações, ideias, falar de compras, ajudar em um projeto, seja lá o que for (MOORE, 1975, p.1, tradução nossa).

[22] No romance *1984*, de George Orwell (2005), há um dispositivo tecnológico denominado teletela. Capaz de capturar imagens e sons, aquele que se encontra em frente da teletela ou nas suas proximidades nunca está em condições de saber se está ou não sendo vigiado. Para além dessa função de vigilância permanente, a teletela, ao transmitir imagens e sons, cumpre também uma função pedagógica. Ao longo da distopia, a teletela é apresentada como um dispositivo de circulação de informações sempre a serviço do poder totalitário, nunca como instrumento de resistência. Assim, escrito em 1948, o romance logo alcançou o sucesso, contribuindo desde então na produção do imaginário social com a maneira de se pensar e associar os dispositivos tecnológicos e os regimes totalitários.

No primeiro encontro do que viria a ser denominado *Homebrew Computer Club*, ocorrido em março de 1975, estiveram presentes 32 (trinta e duas) pessoas, sendo que dessas seis já haviam construído seus próprios computadores (MARKOFF, 2005; MOORE, 1975). O tema principal foi o Altair 8800, fabricado pela *Micro Instrumentation and Telemetry System* (MITS) e anunciado pouco tempo antes, em janeiro de 1975, na *Popular Electronics,* como sendo o primeiro rival dos computadores comerciais e que poderia ser comprado por menos de US$ 400 (ROBERTS; YATES, 1975). Não era propriamente um computador pessoal pronto para utilizar, mas algo que lembrava um *Heathkit*. Quando alguém o comprava, recebia em seu endereço uma caixa com peças para soldar e, se tudo corresse bem, teria ao final uma máquina que podia receber informações por meio de alguns interruptores e que, ao processá-las, fazia algumas luzes piscar. Por mais rudimentar e menor que fosse a potência do Altair 8800, ele tinha um preço acessível e, assim, estavam dadas as condições para que algumas pessoas fizessem uso de um computador fora do controle das corporações, das universidades e dos militares (ISAACSON, 2014; MARKOFF, 2005).

Ainda no primeiro encontro, a seguinte questão surgiu conduzindo os participantes a inúmeras respostas diferentes: “O que as pessoas farão com um computador em suas casas?” (MOORE, 1975, p.1, tradução nossa). Tratava-se de questionar quais as aberturas que estavam dadas a partir do momento em que as pessoas passavam não só a ter um computador pessoal, mas, sobretudo, quando o uso desse computador não exigia mais a autorização e o controle de terceiros (que prescreviam para quê e como os computadores deveriam ser utilizados). O computador poderia ser uma ferramenta para que cada um levasse adiante os projetos que concebesse e não apenas os projetos vindos de cima para baixo por meio da hierarquia institucional e estruturada por meio da burocracia – ou seja, mais do que um utilitário para o trabalho, o computador poderia tornar-se um parceiro no ato inventivo. Ao redigir o boletim informativo acerca do primeiro encontro, Fred Moore (1975, p.1, tradução nossa) fez um interessante comentário à questão levantada: “Eu espero que computadores domésticos sejam usados de maneiras não convencionais – a maioria das quais ainda não foram pensadas por ninguém”.

Um computador, ao tornar-se um objeto convivencial, cria condições para a produção de novos mundos. Quem poderia prever os resultados de acoplamentos entre

seres humanos e máquinas abertas? Que novos modos de existência poderiam surgir de tais composições? Que novas práticas emergiriam?

Um daqueles que estiveram presentes desde o primeiro encontro foi um hacker bastante conhecido: Stephen Gary Wozniak (fundador da Apple juntamente com Steven Paul Jobs e Ronald Gerald Wayne). Mais do que o Altair 8800, o que lhe chamou a atenção foi um folheto com dados sobre um microprocessador que recebeu na reunião. As especificações técnicas que ele leu, lembraram-lhe de uma máquina muito semelhante – o Computador Cream Soda – que ele havia construído cinco anos antes. Inspirado pela possibilidade de produzir seu próprio computador e de compartilhá-lo com os demais, ele projetou e forneceu gratuitamente os diagramas esquemáticos para a montagem daquele que seria o Apple I. Ele não só distribuiu cópias com instruções, mas também ia às casas das pessoas para ajudá-las a construir seus próprios computadores (ISAACSON, 2014; WOZNIAK, 2017; WOZNIAK; SMITH, 2011). Era a posição do inventor e construtor que era, com isso, reafirmada. Mais do que ocupar a posição restrita de usuário, cada um poderia organizar seus encontros com um computador a partir da própria interioridade da relação. Entretanto, após algum tempo, Jobs que tinha em mente produzir e comercializar os computadores idealizados por Wozniack, acabou convencendo-o a deixar de dar cópias de seus esquemas (ISAACSON, 2011).

Tanto o Apple I quanto o Apple II foram projetados, segundo Wozniak (2017), como um hobby, para diversão e não para serem um produto de uma empresa. O que ele admirava neles, e reconhecia em suas invenções, era a sua tecnicidade e não um possível êxito comercial. Havia uma importante diferença de atitude entre ele e Jobs. Assim como outros hackers, Wozniak gostava de personalizar, modificar e conectar diferentes coisas em máquinas. Jobs, por sua vez, acreditava que a arquitetura teria que ser fechada, garantindo, assim, ao usuário uma experiência ininterrupta e controlada de ponta a ponta. No Apple II, por exemplo, Wozniak defendia que estivessem presentes oito slots, dando aos usuários a possibilidade de inserirem as placas de circuito e os periféricos que quisessem. Jobs, entretanto, insistia que apenas dois eram suficientes, um para a impressora e outro para o modem. Ao final, essa disputa foi vencida por Wozniak e os usuários puderam acoplar os dispositivos que desejavam (ISAACSON, 2011).

Retenhamos dessa história o embate entre Wozniak e Jobs. O primeiro não só estabelecia uma relação participativa e contínua com o objeto técnico, como também buscava disponibilizar aos demais as condições para uma experiência semelhante, ou seja, atuava para manter o Apple I e II enquanto objetos abertos. Tratava-se da afirmação de um modo de vida em que buscava garantir para si e oferecer aos demais a possibilidade de aprenderem por si mesmos. No fundo, estava pressuposta uma ética promotora de autonomia. O segundo, por sua vez, buscando comercializar os computadores, o fazia separando a função do produtor de um lado e a função do usuário[23] de outro. Para Jobs, importava controlar a experiência do usuário, garantindo que ela ocorresse de forma planejada e sem interferências. Desconhecedor dos esquemas que operavam nos computadores, o usuário era por ele considerado, antes de tudo, um consumidor. É para este sujeito – e não para *amateurs* e hackers tal como Wozniak – que um computador Apple deveria ser pensado e produzido. Tratava-se, portanto, ao entregar o Apple pronto, porém fechado, de restringir ao usuário a possibilidade de conhecer a realidade técnica presente no computador e, também, de nela intervir de modo inventivo. A ética pressuposta, neste caso, era a da heteronomia – ou seja, eram os fabricantes e *experts*, detentores do saber, que seriam os responsáveis por tomar as decisões que impactam na vida dos usuários. E, mais do que isso, que o produziam enquanto usuário.

A proposta de Jobs, que acabou tornando-se hegemônica na Apple, é, na terminologia simondoniana, alienante, pois produz a ruptura entre o ato produtor e o ato de utilização, aos quais já fizemos referência acima. De um lado, o usuário é mantido ignorante, e, de outro, o objeto técnico tem sua realidade técnica negada. Quanto mais fechado o objeto é feito, mais rápida pode ser a "curva de aprendizagem"[24] para seu uso, mas também mais afastado o usuário é mantido do ato inventivo que transforma a realidade técnica do próprio objeto. Como bem nota Simondon (2007, p.266, tradução

[23] Como nota Lazzarato (2014, p.28), "as funções de usuário, trabalhador e consumidor, e as divisões homem/mulher, pais/filhos, professor/estudante, entre outras, são investidas por conhecimento, práticas e normas – sejam elas sociológicas, psicológicas, de gerenciamento ou de polícia – que solicitam, encorajam e predispõem a produção de indivíduos alienados no interior da divisão do trabalho social e por gênero". A divisão usuário/produtor não opera no mesmo nível da ação inventiva. Enquanto aquela é molar – produzindo identidades e operando pela sujeição social – esta é um ato existencial. Ao introduzir e ampliar a distância entre usuários e produtores, o próprio grau de liberdade para ação inventiva é reduzido.

[24] Aqui o termo aprendizagem é utilizado no sentido corrente e não naquele que explicitamos na introdução.

nossa), “os objetos técnicos que mais produzem alienação são aqueles que também estão destinados a usuários ignorantes”. Afirmação que, segundo Blondeau (2004), não teria nenhuma objeção por parte dos hackers.

Ao se fechar os objetos mantendo-os opacos, as próprias relações de poder são transformadas (tema que abordaremos mais detidamente na Segunda Parte). Sujeitar o outro à condição restrita de usuário, negando-lhe participar ativamente da realidade técnica é um modo de conduzir condutas e, também, de produzir assujeitamento:

> Um aspecto mais impícito já aparece com certo tipo de dependência do usuário em relação ao produtor, que faz deste o educador, o professor, o homem que dá conselhos e regras de uso com prescrições mais ou menos misteriosas, justificadas em algumas poucas palavras, para o profano que é o usuário. Este último entra assim em uma relação assimétrica na qual é neófito, enquanto que o produtor é o iniciado que aceita revelar uma parte de seu saber – somente uma parte – porque o usuário seguirá sendo um profano, mas um profano que sabe certas regras e inclusive certas palavras: adquire um saber parcial, pouco coerente, mas que tem algum parentesco com o suposto saber verdadeiro, arquétipo da construção realizada (SIMONDON, 2017a, p.272–273, tradução nossa).

O apelo contido na proposta político-pedagógica de Simondon (2017f), à qual compartilhamos, é para repensarmos e transformarmos nossas relações com os objetos técnicos. Ele convida a cada um de nós para fazer parte do processo inventivo o que implica, necessariamente, recusar a modalidade de relação na qual, por um lado, o objeto técnico é feito e mantido fechado e, por outro, ocupamos unicamente a posição de usuários desconhecedores da realidade técnica. Para o filósofo, “o ser técnico deve ser considerado como um ser aberto” e “o usuário deve ocupar o lugar do construtor. Para isto, é necessário que ele corresponda com o esquematismo essencial inscrito no ser técnico, que seja capaz de pensá-lo, de compreendê-lo, de amá-lo como se ele o tivesse feito” (SIMONDON, 2017f, p.247, tradução nossa).

1.7 Possibilidades de Abertura

Mas nos dias de hoje ainda há condições para estabelecer uma relação amistosa com os objetos técnicos? Não estariam eles se tornando cada vez mais numerosos, complexos e difíceis de se compreender? Antes abordar estas questões, faz-se

necessário ressaltar que o objeto técnico não deve ser entendido enquanto uma totalidade isolada. Ainda que o objeto técnico possa ser entendido como algo separável (por exemplo, um fusível, uma bicicleta, um microfone, um computador, uma catedral), para Simondon (2007), deve-se levar em conta diferentes níveis de análise da realidade técnica, isto é: os elementos, os indivíduos e os conjuntos. Os primeiros são infra-individuais, integrando-se aos indivíduos técnicos. É possível compará-los "com o que é um órgão em um corpo vivo" (SIMONDON, 2007, p.86, tradução nossa). Os conjuntos técnicos, por sua vez, são compostos pelos indivíduos, mas não são o simples agrupamento ou reunião de indivíduos, eles "são um tecido de indivíduos técnicos em relação de interconexão" (SIMONDON, 2007, p.144, tradução nossa).

E o indivíduo técnico, como ele se caracteriza para além de ser constituído por elementos técnicos e estarem envolvidos na constituição dos conjuntos técnicos? No modo de produção artesanal era o ser humano quem cumpria a função de individualização técnica – ou seja, era ele quem coordenava as operações com as ferramentas, ele decidia o momento e o modo de utilizar uma ou outra de suas ferramentas, assegurando "através de seu corpo, a distribuição interna e a autoregulação da tarefa" (SIMONDON, 2007, p.97, tradução nossa). Porém, nas sociedades industriais tal função é substituída pela máquina. Já não é o ser humano que exerce a função de indivíduo técnico, mas é a máquina – ou seja, ela passa a ser "aquele que leva suas ferramentas e as dirige" (SIMONDON, 2007, p.98, tradução nossa).

Na produção artesanal não há, propriamente dito, peças separadas, pois cada uma delas é, ao longo da gênese do objeto técnico, continua e progressivamente talhada para adaptar-se às outras, de tal modo que cada peça é "como um órgão que leva a marca de todos os demais órgãos, e que então é o órgão de tal corpo, de tal organismo, e não de tal outro" (SIMONDON, 2017g, p.73, tradução nossa). Na produção industrial, por sua vez, "a totalidade separável existe em nível do elemento pré-fabricado" (SIMONDON, 2017g, p.73, tradução nossa) e, assim, os elementos tornam-se intercambiáveis – ou seja, podem ser transpostos de um objeto para o outro. Por exemplo, um resistor de um rádio pode ser substituído por outro proveniente de uma televisão ou ainda por outro que seja compatível.

Tal transformação teria criado condições, de acordo com Simondon (2007), para outras modalidades de relação com os objetos técnicos. O ser humano, sem ocupar o lugar de indivíduo técnico – função artesanal por excelência – poderia "converter-se seja em organizador do conjunto dos indivíduos técnicos, seja em ajudante dos indivíduos técnicos" (SIMONDON, 2007, p.98, tradução nossa).

Simondon (2017g) sugere que, nas sociedades pós-industriais, o poder de abertura desloca-se do individuo técnico para o elemento técnico. Para ele, a padronização das peças de reposição supõe uma nova modalidade de relação entre produtores e usuários. Dito de outra maneira, a comunicação material, por meio de uma rede de distribuidores representantes do produtor, permitiria ao usuário um novo tipo de vínculo com o produtor. O fechamento no nível do indivíduo técnico poderia, assim, ser acompanhado da abertura no nível dos elementos. Ainda que existam movimentos nesse sentido, Carrozzini (2016, p.97, tradução nossa) ressalta que os desenvolvimentos atuais da microeletrônica parecem completamente oposto à ideia de abertura dos objetos técnicos: "os objetos se *fecham* cada vez mais, e a modificação ou a reparação dos componentes, a substituição entre os *elementos* técnicos, são negadas para a maior parte dos homens, salvo aos experts".

Ainda que Carrozzini (2016) faça um diagnóstico coerente com o nosso tempo, não devemos ignorar a existencia de inciativas que oferecem objetos técnicos abertos, inclusive no campo da informática, como é o caso das plataformas do Arduino e do RaspberryPI, ambas criando condições para relações abertas e de inventividade. Na verdade, há todo um campo que emerge atualmente, sobretudo, na IoT em que elementos técnicos estão disponíveis para que os interessados possam produzir e alterar seus próprios objetos técnicos, inclusive contando com a colaboração de inúmeros outros por meio de fóruns, tutoriais, redes sociais etc.

No *hacking* não é o lugar do especialista – *expert* – que é ocupado, pois não se trata de afirmar uma verdade generalizável acerca de determinada categoria de objetos técnicos. Antes, importa a verdade que é intríseca a esta ou àquela relação singular. Não é a verdade científica que está em jogo, mas aquela que se produz no interior da relação. O que não significa, como já dito, que os conhecimentos científicos não possam estar presentes. Entretanto o que está em cena é, antes de tudo, o modo de relação inventivo

diante de uma situação problemática. Poderíamos dizer que o *hacking* aparece também naquilo que, no Brasil, por vezes é denominado de gambiarra.

Dentre outros sentidos, Bruno (2017, p.137-138) sugere que gambiarra "consiste numa relação despudorada e inventiva com os objetos técnicos, implicando também um modo de se relacionar com o mundo por meio dos entes técnicos que porta potencialidades cognitivas e políticas próprias". Dentre outros modos, a gambiarra pode aparecer como "prática cotidiana de solucionar um problema ou de reparar de forma improvisada e ágil um objeto quebrado ou que não funciona bem", ou enquanto "modo de produzir e usar tecnologias, objetos, serviços que não poderiam ser adquiridos ou comprados". Tecendo aproximações com Simondon, Bruno (2017) propõe que a gambiarra é justamente o avesso dos objetos industriais fechados, pois ela não está coberta por uma capa de sobredeterminação psicossocial, ou seja, não pesa sobre ela a "obrigação de usar um *véu* ou um *disfarce* para penetrar na cidadela da cultura" (SIMONDON, 2017g, p.45, tradução nossa). Na gambiarra, os elementos e o modo pelo qual estão interligados – suas conexões e emendas – são, geralmente, explícitos visualmente, sensorialmente e cognitivamente permitindo "que se leia em suas engrenagens e entranhas expostas os rastros de sua produção, dos gestos e acoplamentos que a constituem" (BRUNO, 2017, p. 141). Sem mostrar pudor, a gambiarra ingressa na cultura revelando-se tal como é, ou seja, sem ter a necessidade de ocultar sua realidade técnica para ser aceita.

E o que o objeto técnico aberto, a gambiarra e o *hacking* teriam em comum? Ainda que tenham suas especificidades, todos eles são marcados pela neotenia, pela reversibilidade e por uma espécie de *open knowledge* em sua própria materialidade. Se os articulamos, é justamente para ressaltar uma certa posição que, inúmeras vezes, é negada aos sujeitos designando-lhes a condição estrita de usuário. Ao recorrermos a Simondon, buscamos ressaltar uma relação com a realidade técnica na qual a divisão entre inventor, produtor e usuário tende a perder o sentido. Trata-se de ocupar um lugar – tal qual no *hacking* – no qual o sujeito pode retomar o ato de invenção e o ato de produção, atualizando virtualidades e fazendo derivar o objeto para novas direções.

Se buscamos ressaltar a inventividade no *hacking* é porque entendemos que as relações que temos com os objetos técnicos não são fixas – ainda que possam ser

fixadas – e, portanto, podem se atualizar de diferentes formas. Neste sentido, Maurente, Maraschin e Biazus (2008, p.107) afirmam:

> Se a relação se estabelecesse de uma vez por todas, fixando um modo de existência sujeito-máquina único, não haveria um espaço para o imprevisível e, tampouco, para a tomada de uma posição de autoria nas produções advindas de tal relação por parte do sujeito em questão.

No *hacking*, os objetos técnicos ingressam na relação de tal maneira que o germe de invenções futuras que carregam consigo pode ser novamente retomado – um virtual que pode vir a ser atualizado. O objeto técnico, longe de ser um simples utensílio, é, portanto, marcado pela transindividualidade. Isto significa que os objetos técnicos são uma espécie de interface entre os seres humanos, pois "quando entramos em uma relação direta com os objetos, nos comunicamos com essa capacidade, esse dinamismo mental que teve aquele que os inventou" (SANTAMARÍA, 2015, p.132, tradução nossa).

Portanto, nossas relações com os objetos técnicos não são estabelecidas com algo morto ou simplesmente físico, nem mesmo com algo que teria apenas a função utilitária. De fato, "cada vez que nós estabelecemos um vínculo com um objeto e esse objeto nos comove (nos afeta, condiciona, obriga ou direciona), o que estamos sentindo e o que está produzindo é uma realidade humana" (SANTAMARÍA, 2015, p.132, tradução nossa). Isto significa afirmar não apenas que os objetos técnicos não são neutros, mas, sobretudo, que eles têm "a capacidade de produzir e gerar mudanças em nós; nós sofremos processos de individuação na relação que estabelecemos com eles" (SANTAMARÍA, 2015, p.132, tradução nossa).

Eis que se nos apresenta uma questão: e o *hacking* enquanto programação, não seria ele de outra ordem? Ou ainda é possível pensá-lo a partir das noções aqui expostas?

2 ABRINDO OS CÓDIGOS

No capítulo anterior, salvo em duas ocasiões – quando nos referimos ao IBM 704 e ao TX-0 –, e ainda assim superficialmente, não abordamos o *hacking* enquanto modo de relação com um tipo de objeto técnico bastante peculiar: o software. É pela arte de programação – subversiva ou não – que a maior parte dos hackers são conhecidos. Mas o que é esse objeto tão especial e quais as possibilidades de relação que estão dadas quando nos encontramos com um software, seja ele livre ou proprietário[25], de código-fonte aberto ou fechado? Seria possível, tal qual no caso dos objetos técnicos tratados anteriormente – a caneta-chave e o videogame de Carlos C., o sistema telefônico, o sistema dos modelos de trem do TRMC, os computadores pessoais Apple I e o Apple II e as gambiarras – estabelecer uma relação inventiva e amistosa com os softwares? Ou antes, seria tal modalidade de relação privilégio dos *experts*?

Comecemos esclarecendo o que é um software[26]. Por vezes tratado como sinônimo de programa de computador, o software é composto também por outros elementos. Sommerville (2011, p.3) propõe que, além do programa em si, o software inclui "toda a documentação associada e dados de configurações necessários para fazer esse programa operar corretamente". O software não é, portanto, somente um executável, mas também algo que pode ser compreendido e alterado.

Mas nem todo software está sujeito às mesmas condições de existência. Faremos, portanto, uma breve retomada das linhas de forças que contribuíram para que os softwares chegassem a ser o que são atualmente, problematizando as relações que nos são propostas e as posições que nos são possíveis ocupar.

2.1 A EMERGÊNCIA DAS PRIMEIRAS LINGUAGENS DE PROGRAMAÇÃO

[25] Um software proprietário é aquele cuja cópia, redistribuição e/ou modificação só pode ser realizada mediante a permissão de seu proprietário. Na maioria dos casos, o usuário não compra o software proprietário, mas adquire uma licença, ou seja, a permissão de uso sob certas condições que lhe restringe direitos.

[26] Resumidamente, há basicamente dois tipos ou classes de softwares: de sistema e de aplicativo. Um software de sistema consiste em um conjunto de instruções que permite ao utilizador interagir com o computador e seus periféricos. Inclui a BIOS, drivers dos diferentes dispositivos e o sistema operacional (como, por exemplo, GNU-Linux, MAC OS, MS-DOS e Microsoft Windows). Os aplicativos, por sua vez, são programas que permitem executar tarefas específicas como, por exemplo, um processador de texto, um editor de imagem ou um *browser* para navegação na internet.

Até meados dos anos de 1950, pensava-se que o verdadeiro desafio da computação era o desenvolvimento do hardware e que o trabalho de codificação era apenas uma aplicação mecânica. Na prática, entretanto, descobriu-se que programar era mais difícil, demandava mais tempo e exigia mais recursos do que se imaginava (ENSMENGER, 2010). No *Eletronic Numerical Integrator and Computer* (ENIAC)[27], por exemplo, para efetuar os cálculos era necessário deslocar fiações, girar interruptores, modificar circuitos, interagir com painéis, enfim, alterar diretamente o modo pelo qual a máquina estava constituída (BRETON, 1990).

Programar, era, portanto, uma atividade muito localizada, pois inicialmente não só cada máquina era única, mas também, como nota Dijkstra (1972, p.860, tradução nossa), os programas desenvolvidos para elas "tinham apenas significância local". Era inconcebível que um programa escrito para uma máquina pudesse simplesmente ser executado em outra (KELTY, 2008) e, consequentemente, não havia portabilidade dos mesmos (MOOERS, 1975).

Em seus primórdios, a programação era tanto uma questão de lógica, de linguagem e de código quanto de conhecimento concreto da máquina (BRETON, 1990). Cada uma delas tinha um modo de manipular os zeros e os uns e, consequentemente, um software escrito para um computador IBM era amplamente incompatível com uma máquina Univac (FISHMAN, 1982). O fato dos computadores pertencerem ao mesmo fabricante não era garantia de portabilidade dos softwares, pois fazia-se necessário um grande trabalho de recodificação dos programas, isto quando era possível (BRETON, 1990).

Como em última instância os computadores digitais operam de modo binário, ou seja, eles seguem instruções dadas a partir de uma sequência de zeros e uns, escrever no código da máquina e nele operá-lo era demasiadamente trabalhoso. Assim, pouco a pouco, surgiram as linguagens de programação, que são mais próximas da linguagem humana, e cujas instruções poderiam ser traduzidas para a linguagem de máquina

[27] Sem manuais de instruções ou professores, as responsáveis por programar o ENIAC eram seis mulheres – Betty Jean Jennings, Elizabeth Snyder Holberton, Frances Bilas, Kathleen McNulty, Marlyn Wescoff e Ruth Lichterman – que tiveram que aprender a operá-lo, basicamente, por conta pória. O que elas fizeram nunca havia sido feito antes, isto é, programar um computador eletrônico (ENIAC PROGRAMMERS PROJECT, [s.d.]; ENSMENGER, 2010; ISAACSON, 2014; THE SECRET..., 2018).

(KNUTH; PRADO, 1976). O código-fonte[28] escrito em linguagem de “alto nível”, aquela mais amigável, poderia, portanto, ser traduzido em linguagem de “baixo nível”, aquela à qual a máquina estaria apta a operar. Tal processo de tradução, poderia dar-se de duas formas: antecipadamente, por intermédio do uso de um compilador, ou simultaneamente, por meio do uso de um interpretador.

Desenvolver programas deixava, então, de estar diretamente atrelado às especificidades da máquina e também de sua linguagem binária. Tornava-se possível pensar e redigir um programa numa espécie de linguagem que se pretendia universal e independe da máquina que o executaria. Em decorrência, o código-fonte poderia ser facilmente compartilhado e traduzido para os mais diferentes computadores. Assim, ao longo das décadas de 1950 e 1960, emergiram e se consolidaram linguagens de programação tais como a *Formula Translation* (FORTRAN), a *Algorithmic Language* (ALGOL), a *Programming Language 1* (PL/1) e a *Common Business-Oriented Language* (COBOL) (BRETON, 1990).

2.2 A COMODIFICAÇÃO DOS SOFTWARES

Paralelo ao desenvolvimento das linguagens de programação, importa também ressaltar as transformações das condições em que os softwares eram produzidos e circulavam entre fabricantes de computadores e seus clientes. Nas primeiras décadas da informática, como acabamos de mencionar, existia um grande desafio a ser superado: o problema da incompatibilidade entre as máquinas, inclusive aquelas procedentes do mesmo fabricante. Havia, portanto, todo um esforço para facilitar o desenvolvimento colaborativo de softwares e o compartilhamento dos mesmos. À época, era comum aos fabricantes de computadores ofertar, sem acréscimo no preço dos hardwares, os softwares (incluindo os códigos-fonte), pois a maioria dos executivos da indústria de computadores acreditava, pelo menos até o início da década de 1960, que não existia um mercado significativo para a comercialização dos softwares enquanto um produto (JOHNSON, 1998).

[28] O código-fonte consiste em “uma sequência de operações escritas em uma linguagem de programação compreensível por um humano e que lhe permite dar instruções ao computador” (BLONDEAU, 2004, p.94, tradução nossa).

A IBM[29], por exemplo, adotava no pós-guerra um modelo de negócios pautado, sobretudo, no aluguel de suas máquinas, estando incluído no preço uma variedade de outros serviços adicionais (FISHMAN, 1982). Ao adquirir um IBM, o cliente sabia que, mais do suporte técnico para a máquina, também teria todo o apoio necessário com os softwares (GOETZ, 2002). A empresa oferecia cursos e disponibilizava, sem custos adicionais, uma biblioteca, isto é, "uma coleção de rotinas padrão que podem ser inseridas em outros programas" (TAVARES, 1984, p.44). Nela, todos tinham acesso a aplicações comerciais e acadêmicas que teriam sido escritas tanto pela própria empresa quanto por seus clientes que, inclusive, eram incentivados a modificar os programas, adaptando-os às suas necessidades (INTERNATIONAL BUSINESS MACHINES, 1959; 1962).

O compartilhamento dos softwares não ocorria apenas verticalmente – entre a IBM e seus clientes –, mas também horizontalmente – entre os próprios clientes. Estes chegaram a constituir um grupo – denominado SHARE[30] – que tinha por intuito facilitar o intercâmbio de informações e de softwares. Havia à época também a *Univac Program Distribution Library*, uma biblioteca por meio da qual eram disponibilizadas ferramentas de programação e programas estatísticos escritos pelos programadores da Sperry e pelos usuários do Univac (GOETZ, 2002). Com certas ressalvas, pode-se dizer que se tratava de bibliotecas de uso comum, isto é, com as quais todos podiam tanto usufruir do que estava disponível quanto contribuir para incrementá-las.

Ao final da década de 1960, existia uma verdadeira cultura das práticas de compartilhamento tanto no ambiente comercial, quanto nas universidades. Mas sejamos

---

[29] Em 1967, pouco mais de 90% do mercado mundial de computadores estava nas mãos de apenas 8 (oito) companhias americanas, sendo que, dentre elas, a International Business Machines (IBM) destacava-se com 50% da produção mundial (BRETON, 1990). No início da década de 1970, a IBM era também conhecida pelo apelido de "Branca de Neve", pois estava acompanhada pelos "sete anões", ou seja, pelas outras 7 (sete) principais empresas: Honeywell Information Systems, Sperry Univac, Burroughs Corporation, National Cash Register and Control Data Corporation, General Electric e RCA (FISHMAN, 1982).

[30] Em 1952, a IBM lançou e concluiu a construção do primeiro computador comercial, o 701 (INTERNATIONAL BUSINESS MACHINES, 2003). Três anos mais tarde, em 1955, a IBM anunciou seus planos para o IBM 704. Como ambos os computadores não eram compatíveis, ao realizarem a troca de um pelo outro, os usuários teriam que recodificar toda a biblioteca de programas que possuíam. Diante de tal desafio, representantes dos 18 proprietários de IBMs 701 reuniram-se em agosto de 1955, na Rand Corporation, constituindo um grupo que passou a ser chamado SHARE. Apesar dos membros do grupo serem procedentes de firmas altamente competitivas, um forte senso de colaboração fazia-se presente (AKERA, 2001). No *SHARE Reference Manual for the IBM 704*, explicitava-se que a principal obrigação de quem participava do grupo era "ter um espírito cooperativo. Espera-se que todo membro participe de cada discussão com uma mente aberta e, tendo respeito pelas competências dos demais, esteja disposto a aceitar as opiniões dos outros mais frequentemente do que insiste em suas próprias" (EDSON et al., 1956, sem paginação, tradução nossa).

mais específicos, o que circulava não eram apenas os programas executáveis, ou seja, os programas já compilados, mas, sobretudo, os códigos-fonte, o que permitia tanto a compreensão de como os programas operavam, quanto modificá-los ou apropriar-se de parte deles para produzir ou alterar outros programas. Eram, portanto, objetos técnicos abertos, passíveis de serem conhecidos e transformados.

Nesse ambiente, poucas eram as empresas que se aventuravam no mercado desenvolvendo softwares com o intuito de vendê-los. Uma delas foi a *Applied Data Research (*ADR), que produziu e comercializou uma versão de um programa para elaboração automática de fluxogramas, o *Autoflow,* para os IBMs da série 1400, obtendo, assim, considerável sucesso de vendas. Isto, mesmo em um cenário em que muitos estavam habituados a ter os softwares da IBM gratuitamente (GOETZ, 2002).

Quando a ADR começou a comercializar o *Autoflow* para os computadores IBM, esta já disponibilizava um programa semelhante que, todavia, não era capaz de funcionar de modo automático. Com receio de que a IBM viesse a oferecer as mesmas funcionalidades, a ADR solicitou, em abril de 1965, e obteve, em abril. de 1968, a primeira patente de programas de computador da história (GOETZ, 2002, 2016). Goetz (2002, p.49, tradução nossa), que à época trabalhava na ADR, relata:

> Nossa primeira grande batalha foi com a IBM e seu produto livre [free product], o IBM *Flowcharter*, que competia com o *Auto ow*. Essa batalha entre ADR e IBM evoluiu para uma batalha da indústria para forçar a IBM a *unbundle* [desagregar a venda conjunta de softwares e hardwares]. A ADR tinha que proteger seus investimentos em novos produtos que estava construindo ou que planejava construir. Paralelamente com essas batalhas, nós começamos a reconhecer a necessidade de proteger nossa propriedade intelectual, e nós lutávamos para poder patentear e também usar o *copyright* no software. Curiosamente, a IBM – uma grande proponente do sistema de patentes em geral e de patentes de hardware de computador em particular – foi contra o patenteamento de software.

Com o lançamento de computadores que seriam compatíveis, inclusive com aqueles de outras marcas, o cenário mudou. No caso da IBM, que dominava o mercado, instaurava-se o risco iminente de ter os softwares que havia desenvolvido (não raro em comum com seus clientes) sendo executados nos computadores fabricados pelos seus concorrentes sem, porém, receber por isso. Para que ela pudesse cobrar pelos softwares era necessário vendê-los separadamente dos hardwares, pois se assim não o fizesse corria o risco de ser condenada por prática anticompetitiva. O *unbundle*, ou seja, a

desagregação de softwares e hardwares na comercialização, passou a ser seriamente considerado na IBM. Programas e serviços de engenharia de sistemas não seriam mais incluídos no preço do hardware, mas oferecidos separadamente (HUMPHREY, 2002).

Mas como comercializar os softwares de tal forma a manter sobre eles e sobre os clientes o controle? Esta passou a ser uma importante questão para a IBM. Diferentemente dos recursos materiais, cujo uso por alguém rivaliza, ao mesmo tempo, com o uso por outrem, os softwares podem ser executados por inúmeras pessoas sem nunca se esgotar. A implicação é clara: a venda de um único software poderia significar sua multiplicação no mercado – por intermédio de cópias – sem que a empresa que o desenvolveu recebesse por isso. Em decorrência de interesses comerciais, fazia-se necessário à IBM desenvolver estratégias não só para garantir que a propriedade do software permanecesse com ela, mas também para evitar que usos não autorizados de seus softwares viessem a ocorrer.

O modelo de negócios da IBM estava em vias de modificar-se. A estratégia que estava sendo considerada era a de comercializar não o software propriamente dito, mas uma licença paga, uma autorização com regras específicas acerca de questões como cópia e utilização. Em acréscimo à licença, dando-lhe suporte, também haveria o registro de *copyright* do software. Desse modo, tanto por razões competitivas quanto para prevenir uma ação judicial antitruste, em junho de 1969, a IBM anunciou o *unbundle*[31] (HUMPHREY, 2002).

No decorrer dos anos de 1970 teve-se, cada vez mais, a comodificação do software. Assim como a IBM, outras empresas de informática também passaram a comercializar seus programas separadamente do hardware. Duas principais estratégias, que buscavam se amparar de alguma forma na legislação vigente, eram utilizadas: o segredo comercial [*trade secret*] e a proteção por meio de patentes [*patent protection*]. Havia, entretanto, falta de clareza no âmbito jurídico, que se expressava por uma confusa série de decisões judiciais para a concessão de patentes de softwares (MOOERS, 1975).

[31] De acordo com Moglen (2001, p.180, tradução nossa), o *unbundle* teve menos efeitos imediatos "sobre as práticas sociais da fabricação de programas do que a gente poderia supor". Para reforçar seu argumento, ele explica que, entre 1979 e 1984, quando era o corresponsável pelos aperfeiçoamentos técnicos de uma linguagem informática produzida na IBM, ele era capaz de considerar o produto como "quase livre", discutindo com os usuários as modificações que eles haviam proposto ou efetuado nos programas, inclusive engajando-se com eles no desenvolvimento cooperativo de produtos para todos os demais usuários.

Às duas estratégias, uma terceira passou a ser utilizada de modo crescente, especialmente a partir das grandes mudanças realizadas na legislação de propriedade intelectual norte-americana nos anos de 1976 e 1980: a aplicação do *copyright*. Com as alterações na legislação, não só o escopo dos materiais protegidos foi ampliado, como também a exigência de registro foi eliminada (KELTY, 2008).

Há diferenças importantes em relação ao funcionamento e aos efeitos da lei de patentes e da lei de *copyright*. Esta estabelece o controle sobre as cópias e adaptações dos códigos dos programas, mas não protege as ideias. Ou seja, o *copyright* não proíbe que alguém se utilize de ideias que encontrou em programas já existentes, implementando-as em seus próprios softwares por meio de novos códigos – é o caso da engenharia reversa [*reverse engineering*]. Já as patentes de softwares são obtidas quando uma ideia considerada inovadora é registrada garantindo ao detentor o monopólio de sua aplicação por, no mínimo, 20 anos. O que está em jogo é o direito de proibir outros de se utilizarem da ideia patenteada, impedindo, inclusive, o uso de engenharia reversa (WILLIAMS, 2010).

Assim, o software que antes circulava enquanto objeto aberto – seu código-fonte era, geralmente, disponível e não havia imposições legais restritivas –, tornava-se, cada vez mais, um objeto fechado. Das práticas de produção de software que eram uma espécie de contínuo entre fabricantes de computadores e clientes, ou seja, havia sempre a possibilidade de se retomar os softwares a partir de uma posição de inventor (seja conhecendo-o, seja modificando-o, seja atualizando-o), passava-se para uma condição em que apenas os fabricantes e seus designados – técnicos especializados com autorização – poderiam ocupar tal posição, o que era, de certo modo, comum tornava-se, assim, propriedade privada. Ao mesmo tempo, fortalecia-se a posição do cliente-consumidor-usuário, daquele que adquire, por meio de uma licença de uso, um programa executável, mas que não tem o direito legal de relacionar-se com o software enquanto um inventor. Ou seja, não pode conhecer seu código-fonte, saber quais atos inventivos estão ali cristalizados e, nem mesmo, pode modificá-lo, dando-lhe novos destinos. O software tornava-se, assim, cada vez mais, um utensílio, um objeto a ser utilizado e não a ser conhecido.

2.3 O Caso "EMACS"

Foi nesse território nebuloso, em que as condições de relação com os softwares estavam se transformando, especialmente por meio dos atravessamentos jurídicos e econômicos, que uma série de disputas passaram a se dar em torno de um importante programa desenvolvido entre hackers no MIT, *EMACS,* o *the extensible, customizable self-documenting display editor* um dos mais famosos editores de texto na virada dos anos de 1970 para 1980. Sendo uma ferramenta altamente customizável, o usuário podia alterá-lo, adaptando-o conforme seus interesses e necessidades, sempre que desejasse e sem a necessidade de ter habilidades em programação:

> A extensibilidade torna o EMACS mais flexível que qualquer outro editor. Usuários não são limitados pelas decisões feitas pelos implementadores do EMACS. O que nós decidimos que não vale a pena adicionar, o usuário pode prover para si próprio. Ele pode com bastante facilidade fornecer sua própria alternativa para um recurso se ele não gosta do modo como algo funciona no sistema padrão (STALLMAN, 1981, sem paginação, tradução nossa).

Com o EMACS, em uma mesma interface, tornava-se possível ao usuário-programador não apenas escrever seus programas, mas também depurá-los, compilá-los, executá-los, enviá-los para outros e escrever extensões para serem executadas no próprio EMACS (KELTY, 2008). Para facilitar, inúmeras outras funções poderiam ser encontradas em uma biblioteca que criava condições para que cada um publicasse e compartilhasse as extensões desenvolvidas, as quais poderiam vir a ser integradas ao sistema básico (STALLMAN, 1981).

Inicialmente, em 1974, quando Stallman desenvolveu o EMACS, este era um novo recurso para o editor de textos TECO, que havia sido desenvolvido no MIT e aprimorado por hackers (RAYMOND, 2003b; WILLIAMS, 2010). O nome, inclusive, fazia referência ao acrônimo *Editing MACroS for* TECO. Assim, derivado de uma versão do TECO, que era executada no *Incompatible Time-sharing System* (ITS), no Laboratório de Inteligência Artificial do MIT, o EMACS recebeu contribuições de diversas pessoas e, ao longo dos anos, tornou-se bastante popular (KELTY, 2008).

Uma das expressões-chave para Stallman era "comuna de compartilhamento". Os usuários eram convidados a copiar, modificar e compartilhar suas contribuições – ou seja,

a estabelecerem modos de relação com EMACS que não fossem restritos à posição usuário *stricto sensu*. Havia uma espécie de contrato social que, sem ingressar no âmbito da legalidade, indicava as condições para fazer parte da comuna de ajuda mútua idealizada por Stallman. Em 1980, no *EMACS Manual for ITS Users*, ele afirma:

> Ele [o EMACS] não custa nada. Como alternativa, você deve se juntar à comuna de compartilhamento de software EMACS. As condições de associação são que você deve enviar de volta todos os aperfeiçoamentos que você faz para o EMACS, incluindo bibliotecas que você escreve, e que você não deve redistribui-lo, exceto se for exatamente como você conseguiu: completo (você também pode distribuir suas personalizações, separadamente). É patético ouvir de lugares que receberam cópias incompletas sem as fontes me perguntando anos depois se as fontes estão disponíveis (STALLMAN, 1980, p.1–2, tradução nossa).

Deixemos de lado por enquanto a questão específica da “comuna” e detenhamo-nos um pouco na crítica que Stallman (1980) faz daqueles que tendo acesso ao código-fonte, alteram-no, compilam e distribuem aos demais apenas a versão executável, ou seja, o código-fonte já compilado, compreensível por uma máquina, mas não por um ser humano. Ainda que a circulação da versão executável permita aos demais a utilização do programa, a ausência do código-fonte é de suma importância. Sem ele, boa parte da gênese, da intenção fabricadora – que não pode ser confundida com a intenção de utilização – acaba sendo ocultada. O software, enquanto um objeto técnico, desprovido dos elementos que fazem dele compreensível, torna-se uma espécie de caixa-preta, ou seja, é feito objeto técnico fechado. Isto porque é justamente o código que é “por excelência o portador do esquema técnico original de invenção que autoriza a prolongar esta atividade de invenção e de construção” (BLONDEAU, 2004, p.96, tradução nossa).

O código-fonte não se comunica apenas com a máquina para fazê-la operar. Há um aspecto transindividual, uma comunicação que se dá também entre seres humanos. Por um lado, ele contém a resolução de problemas por meio de um ato inventivo transcrito nas linhas de instrução do código. Por outro, os códigos-fonte são, frequentemente, acompanhados de comentários que ainda que sejam, geralmente, direcionados para outros programadores, também podem ser úteis para os usuários sem conhecimento técnico. Na verdade, afirma Moglen (2001, p.153, tradução nossa), nós nos surpreenderíamos em “descobrir que a maior parte das informações contidas na maioria dos programas é, do ponto de vista do compilador ou dos processadores de linguagem,

constituída de comentários, uma substância não funcional". Ao que acrescenta "na maior parte das linguagens informáticas, muito mais espaço é consagrado para explicar aos outros o que programa pode fazer, do que para dizer ao computador como executá-las".

Entretanto, apesar da condição imposta por Stallman (1980) – ou seja, a de que as modificações fossem a ele remetidas para serem integradas –, vários programadores portaram, reescreveram e imitaram o EMACS, que passou a ter inúmeras versões existindo ao mesmo tempo e em diferentes sistemas operacionais e em variadas arquiteturas. As regras da comuna EMACS não se aplicavam, todavia, a essas novas versões. Uma delas era o GOSMACS, escrito em C para UNIX[32] por James Gosling, em 1981 (WILLIAMS, 2010).

Assim como Stallman, Gosling também recebeu muitas contribuições que passavam a fazer parte do programa que ele mantinha e distribuia. Em abril de 1983, entretanto, Gosling decidiu vender sua versão do EMACS para a UniPress, que passaria a mantê-lo e disponibilizá-lo comercialmente, o que significava que o GOSMACS não estaria em domínio público, mas teria seus direitos autorais ligados a uma empresa.

Com a venda do GOSMACS, os usuários do UNIX deixavam de ter uma versão do EMACS não proprietária para utilizar. Além disso, os proprietários do UNIX, que até então circulava de forma quase que gratuita e sem grandes restrições, passavam a demonstrar interesse em torná-lo um sistema operacional prioritariamente comercializável (KELTY, 2008). É nesse cenário que Stallman (1983) anuncia o projeto GNU, ressaltando que ele seria fornecido gratuitamente para quem quisesse utilizá-lo. Como justificativa, ele afirma: "Eu considero que a regra de ouro requer que se eu gosto de um programa eu devo compartilhá-lo com outras pessoas como eu" (STALLMAN, 1983, sem paginação, tradução nossa).

Durante os anos de 1984 e 1985 Stallman, juntamente com outros, trabalhou no GNU EMACS, uma versão *free* para ser executada em sistemas UNIX. Ao lançá-la, um acalorado debate se iniciou em decorrência do fato de que Stallman utilizou partes do código de uma antiga versão do GOSMACS que, no momento, já pertencia à UniPress. Preocupado com o fato de que muitas pessoas poderiam deixar de utilizar o GNU EMACS

[32] O Unix é um sistema operacional proprietário criado no início da década de 1970, sendo utilizado amplamente por universidades, grandes indústrias e pelo governo americano.

devido a ameaças legais, ele reescreveu novos códigos suprimindo as partes que eram provenientes do GOSMACS. A grande ironia é que pairava sobre Stallman a acusação de ter infringido o *copyright* de um software que ele mesmo teria inventado – lembrando que o GOSMACS era derivado do EMACS, derivado, por sua vez, do TECO, e que, além disso, todos eles teriam sido produzidos por meio da contribuição de inúmeras pessoas (KELTY, 2008; WILLIAMS, 2010).

Um contrato informal, tal como o da comuna EMACS, não era suficiente para garantir que os softwares do projeto GNU permanecessem livres para serem distribuídos, copiados, modificados e redistribuídos com as alterações realizadas. A opção de deixar os códigos em domínio público também era insuficiente, já que alguém poderia utilizar parte dos códigos transformando-os em proprietários. A solução encontrada foi jogar no próprio campo da legalidade, inicialmente, em 1985, com a *GNU Emacs General Public License* que posteriormente, com algumas alterações, tornou-se, em 1989, a GPL. Diferentemente do que se pedia no contrato da comuna EMACS, na GPL os programadores só eram obrigados a publicar as modificações realizadas se os softwares fossem redistribuídos. Em síntese, o que se buscava impedir eram as ramificações proprietárias de códigos livres (WILLIAMS, 2010).

Stallman, fundador da *Free Software Foundation*, não estava, portanto, lutando para extinguir as leis ou os aparatos legais que ele considerava capaz de restringir direitos que afetavam a sua vida e de outros. Como ressalta Williams (2010, p.128, tradução nossa), “implícito no preâmbulo da GPL estava uma mensagem profunda: em vez de ver a lei de *copyright* com suspeita, os hackers deveriam vê-la como um sistema perigoso que poderia ser hackeado”. Tratava-se, assim, de subverter o sistema, não de aniquilá-lo, fazendo-o trabalhar em benefício do comum.

Com a GPL, o que estava sendo colocado em xeque era o próprio modo dominante de se produzir e se relacionar com os softwares. Ao ser questionado se o movimento do software livre é vital para outros movimentos no mundo, Stallman (2004, sem paginação, tradução nossa) respondeu:

> Bem, nós não somos contra o capitalismo como um todo. Nos somos contra subjugar pessoas que usam computadores, uma determinada prática de negócios. [...] *free software* é um movimento contra a dominação, não necessariamente contra a dominação corporativa, mas contra qualquer dominação. Os usuários de software não devem ser

> dominados pelos desenvolvedores do software, sejam tais desenvolvedores corporações, indivíduos, universidades ou outros. Os usuários não devem ser mantidos divididos e desamparados. E é isto que o software não livre [*nonfree*] faz; ele mantém os usuários divididos e desamparados. Divididos porque você está proibido de compartilhar cópias com qualquer outra pessoa e desamparado porque você não recebe o código-fonte. Então você não pode nem mesmo dizer o que o programa faz, muito menos mudá-lo.

Neste trecho, Stallman (2004) esclarece que o movimento do software livre tem caráter político. Sua luta não é contra um inimigo localizado – o capitalismo ou uma grande corporação –, mas contra qualquer tipo de dominação. O termo *free*, que inglês apresenta dois sentidos – gratuito e livre – teria aqui, sobretudo, o significado de liberdade. É interessante que Stallman (2004) aponta um caso concreto, bem particular, para dar clareza ao que está propondo. Ele faz referência às relações entre desenvolvedores de softwares e usuários, aqueles que produzem os programas e aqueles que deles fazem uso. No EMACS, como vimos, tal separação não era tão clara. Ou melhor, havia um espaço comum de ação, isto é, havia continuidade entre os atos do programador e os do usuário, sendo que estes atos não eram, necessariamente, divididos e designados para dois sujeitos distintos. O usuário poderia estar sempre contribuindo no aperfeiçoamento do código, seja alterando-o diretamente, seja dando sugestões, seja relatando os *bugs* com os quais se deparava – processo muito importante na programação e denominado *debugging*.

Não custa reafirmar que o que define o software livre não é a gratuidade, mas a proposição de uma situação na qual o usuário está em condições de agir inventivamente, contribuindo no devir do software. Neste sentido, Lazzarato (2006, p.138) esclarece:

> Existem softwares gratuitos que não são livres. O acesso gratuito a um 'software proprietário' aumenta a dependência do usuário diante da gama de outros softwares propostos pela empresa fabricante, ao passo que o acesso, mesmo que pago, a um software livre garante condições de sua independência. O software livre coloca o usuário em uma situação potencial – ao demandar um engajamento específico por parte deste mesmo usuário – de liberdade e independência. Já o software proprietário, mesmo que tenha sido adquirido gratuitamente, deixa o usuário em uma condição de dependência e passividade.

Assim, se, por um lado, o aparato jurídico e a própria constituição dos softwares proprietários podem contribuir no sentido de instaurar uma divisão entre usuários e

programadores, entre clientes e fabricantes; por outro, com a GPL busca-se garantir condições para outras modalidades de relação com os softwares. A licença do software proprietário designa ao sujeito, basicamente, duas posições a serem ocupadas: a de consumidor – alguém que opera no mercado econômico –, e a de usuário definida pelos termos legais que acompanham a licença do produto comprado. O software nesse caso é um produto a ser utilizado. Já o software que está sob a licença GPL, denominado *free software*, cria outras possibilidades, pois o usuário pode acessar o código-fonte e estudá-lo, pode copiar o programa e compartilhá-lo. Além disso, ele também tem a possibilidade de ser um colaborador sugerindo mudanças no código, contribuindo na tradução do programa ou enviando sugestões aos desenvolvedores. Por fim, como tem acesso ao código-fonte, dependendo das competências técnicas que possui, o usuário pode ocupar a posição de programador, daquele que altera diretamente o próprio código e o modo pelo programa se comporta. Trata-se, portanto, com os softwares livres de contribuir na construção "das condições de neutralização da clivagem entre invenção e reprodução, entre criadores e usuários, entre experts e não-experts, imposta pelos modelos de gestão da propriedade intelectual" (LAZZARATO, 2006, p.144).

2.4 O GNU-LINUX

Na virada de 1970 para 1980, os softwares proprietários tornaram-se maioria. Desde o anúncio de Stallman (1985), no *Manifesto GNU*, o projeto da criação de um sistema operacional livre e semelhante ao Unix avançou consideravelmente, mas ainda faltava um componente essencial: o núcleo ou *kernel*. Em 1991, Linus Torvalds desenvolveu um núcleo compatível, o Linux, e em 1992 ele o tornou software livre. Fruto de uma combinação surgiu um sistema operacional livre e completo: o GNU-Linux (STALLMAN, 2011).

Mas de que maneira se produziu o GNU-Linux? Para Sennett (2013), o desenvolvimento do sistema GNU-Linux deu-se a partir de uma comunidade de artífices, programadores que trabalharam de modo colaborativo buscando encontrar maneiras de conciliar a qualidade dos códigos escritos e o livre acesso aos códigos produzidos. Tal modo artífice de se trabalhar implicaria, para o sociólogo, "uma aguda posição crítica na

sociedade" (SENNETT, 2013, p.56). Ele propõe comparar os programadores do GNU-Linux aos burocratas. Estes, para ele, "não se abalançam a dar um passo sem que todos os procedimentos, metas e resultados visados de determinadas diretrizes sejam antecipadamente mapeados" (SENNETT, 2013, p.37). Os desenvolvedores do GNU-Linux, por sua vez, trabalhariam em caráter experimental, sendo o código produzido continuamente revisto, nunca um objeto acabado ou fixo. Ou seja, como nos referimos anteriormente, um objeto quase.

Mais do que remeter os hackers à imagem do artesão e mesmo de opô-la à simples imagem dos burocratas, importa-nos pensar que tipo de práticas, que modalidade de composições os hackers buscavam tecer ao produzirem os softwares. Sem afirmar um binarismo, buscamos, com Kelty (2008), traçar dois modos – dentre tantos outros possíveis – de compor com os softwares. Para ele, havia um tensionamento constante entre o modo dos advogados e o modo dos programadores de estabilizar o objeto denominado UNIX. Para os advogados, a estabilidade implicava encontrar maneiras para fazer do UNIX um produto que poderia se adequar e tirar as maiores vantagens do marco legal existente, garantindo à *American Telephone and Telegraph Company* (AT&T) a propriedade sobre ele e suas possíveis ramificações. Já para os programadores que nele trabalhavam, a estabilidade era alcançada pela constante redistribuição de inovações e de atualizações do sistema operacional. Enquanto os advogados buscavam fazer o UNIX legalmente estável, os programadores buscavam fazê-lo tecnicamente estável e compatível consigo mesmo.

Pode-se dizer que um software nunca está pronto, pois, apesar da realização de testes e da depuração [*debugging*], é impossível prever de antemão todas as possíveis falhas. Como afirma Dijkstra (1970, p.7, tradução nossa), "efetuar testes de programas pode mostrar a presença de *bugs*, mas nunca a ausência deles!". Em decorrência, sempre pode ser demandada a ação do programador para intervir no programa, para aperfeiçoá-lo e para corrigir os bugs. Se por questões técnicas, o software é um devir, por questões jurídico-comerciais, pode-se fazer necessário impor-lhe uma parada, fixando-lhe a identidade à qual servirá de parâmetro no sistema legal. Enquanto muitas empresas de softwares vinculam-se especialmente ao modo de produzir estabilidade dos advogados que impõe uma existência dura aos códigos, os hackers do software livre

aproximam-se do modelo de estabilidade do programador. Ao problematizar a naturalização dos direitos de propriedade dos softwares, Santos (2007, p. 48) afirma:

> Os 'atributos especiais do *software*', contudo, fazem que ele nunca seja um produto acabado, mas sim um verdadeiro *work in progress* cuja natureza processual se corporifica particularmente na modulação, isto é, na sua capacidade de ir se inventando em sintonia com o fluxo de *inputs* que recebe na interação com outras máquinas e outros seres humanos, sob a forma de informações, ou seja, de diferenças que fazem a diferença. Em suma: a invenção de um *software* só se cristaliza e se 'completa' graças a uma violência arbitrária que impede a continuidade das operações de recombinação e de modulação.

Até aqui, buscamos ressaltar que diferentes softwares – proprietários ou livres – possibilitaram distintos modos de composição. Quando Stallman (c2009-2019], sem paginação, tradução nossa) aborda as "4 liberdades" a serem garantidas aos usuários, ele afirma que no software livre "os usuários (individualmente e coletivamente) controlam o programa e o que ele faz para eles", já no caso do software proprietário o programa, segundo ele, "controla os usuários, e o desenvolvedor controla o programa; isto faz do programa um instrumento de poder injusto". Apesar de pensarmos que nunca há controle total de um dos participantes nas relações de poder – isso seria o caso da violência, tal como compreende Foucault (1995) –, não deixa de ser notável que, na prática, o software proprietário geralmente apresente linhas mais duras, delimitando com mais intensidade os modos dos usuários se comportarem, enquanto que um software livre estaria mais aberto a modificações, permitindo ao usuário alterá-lo e, assim, transformar as condições que o produzem enquanto usuário.

Se escolhemos acompanhar Stallman é justamente para poder problematizar um modo de produção de subjetividade que se faz hegemônico – efeito da naturalização do software proprietário –, o que não significa afirmar que o software livre seria a escolha correta – há muitas outras licenças existentes e a serem inventadas. Portanto, são distintas convocações: o comerciante do software proprietário age para que o usuário seja, sobretudo, um cliente-consumidor, alguém que utilize o software tal como ele está (modificações não autorizadas são consideradas pirataria). Já no caso do software livre, o usuário é incitado a ser um contribuidor do software do qual faz uso. São diferentes posições a serem ocupadas, cada uma delas com implicações na produção das subjetividades.

2.5 O SOFTWARE COMO OBJETO NEOTÉNICO

Na década de 1980, quando o modelo de software proprietário havia se tornado hegemônico, os hackers também passaram a ser mais conhecidos, especialmente após a publicação, em 1984, do livro do jornalista Levy (2012b). No mesmo ano, ocorreu em Marin County, Califórnia, a primeira conferência hacker, a partir da qual foi produzido o documentário *Hackers: Wizards of the Electronic Age*. Neste, Levy faz uma interessante afirmação acerca dos hackers. Ele diz que "um hacker nunca termina os programas" (HACKERS..., 1986, tradução nossa). Mas o que isto nos diz? Pensamos que tal proposição diz respeito, sobretudo, à atitude que o hacker apresenta para com os softwares, uma relação segundo a qual se busca restituir e manter nos softwares sempre a potência para devir algo outro. Ao invés de fazer do software um produto (e apenas um produto), cujas possibilidades estão inscritas em definitivo no seu código-fonte, o hacker faz do software um campo de experimentações, uma obra de arte que só pode produzir seus efeitos porque nunca é concluída. É justamente o inacabamento, o inconcluso, que carrega a potência de novas combinações, de outras composições, enfim, da emergência de criações outras.

Um software, constituído enquanto objeto técnico aberto, é aquele que é legível, que pode ser conhecido, ou seja, que não só tem seu código-fonte disponível, mas também é acompanhado de comentários, de documentos e outros aspectos que o tornam acessível. Tudo isso contribui para que ele possa ser sempre retomado, seja para se aprender com ele, seja para aperfeiçoá-lo ou para derivá-lo em algo outro. Já o software constituído enquanto objeto técnico fechado é, no limite, aquele que não pode ser mais alterado, pois resta apenas sua versão executável, imobilizada por aparatos técnicos, jurídicos e comerciais. Ele é produzido para ser usado tal qual está feito. Ao cliente-usuário é negado conhecer o modo pelo qual ele está constituído e, consequentemente, não lhe é possível acessar suas entranhas. É justamente diante de tal fechamento do objeto técnico que o *hacking* surge novamente. Por meio de práticas – consideradas, por vezes, ilegais – como a engenharia reversa [reverse engineering], tais softwares podem ser novamente abertos.

Hackear é, portanto, tensionar as relações de poder, não só resistindo à posição estrita de usuário-consumidor oferecida e incitada pelos fabricantes de softwares, mas, também, assumindo a posição do inventor. Como ressalta Jollivet (2003, p.205, tradução nossa), os hackers do software livre "por meio de suas práticas cotidianas de conceptores-programadores-utilizadores, afirmam-se como figuras políticas de utilizadores-produtores da técnica, como atores e produtores da sociedade técnico-política na qual vivem".

Não podemos ignorar que a técnica é, ela mesma, desde sempre política, pois é atravessada "por relações de forças, por linhas de fuga, de dobras e redobras que podem assim ser alavancas para promover uma 'nova política da tecnologia' e pode ainda, *in fine*, da democracia (BLONDEAU, 2004, p.92, tradução nossa). Trata-se de compreender de que, inclusive as redes digitais, não são, por natureza, propiciadoras de espaços democráticos, conectando "tudo" e a "todos" de modo isonômico e não hierárquico. Antes, são como esferas de relações de poder às quais se faz necessário tensionar e problematizar (MOZZINI; HENNIGEN, 2016).

Assim, o convite de Simondon – de reconsiderarmos o modo como nos relacionamos com os objetos técnicos – não está caduco, mas se renova em meio à multiplicação dos novos dispositivos que emergem em nossos dias. Tal desafio ético-político, coloca-se ainda mais urgente, não só por desconhecermos a gênese ou mesmo como tais objetos técnicos funcionam, mas, sobretudo, porque chegamos inclusive a ignorar sua existência – caso que ocorre em relação a inúmeros softwares (o que veremos mais detidamente na Segunda Parte).

2.6 O Problema da Visisbilidade

Antes de passarmos ao próximo capítulo, faz-se necessário algumas considerações acerca da visibilidade dos objetos técnicos. Esta é uma das condições (necessárias, mas não suficientes) de sua abertura. Quando o objeto técnico é legível – como no caso do trabalho do artesão ou da gambiarra –, ele atua, como disse Norman (2006, p.217), enquanto "uma sugestão, recordando ao usuário as possibilidades e convidando à exploração de novas ideias e métodos". Ou seja, a visibilidade do objeto,

seu modo de apresentar-se tem efeitos nos usuários, incita modos de existência, intervém nos processos de subjetivação individuais e coletivos.

Dentre outros objetos técnicos, Simondon (2013) descreve o convento de *la Tourette*, projetado por Le Corbusier, ressaltando o fato de os materiais terem sido empregados sem dissimulação. O cimento aparece como cimento, não há uma camada de reboco. Os tubos e cabos não estão escondidos nas paredes, teto ou chão, mas estão suspendidos em calhas de T invertido, à vista e acessíveis. Assim, é possível acompanhar o caminho que percorrem, saber de onde provém e para onde vão, ver quando se agrupam e quando se separam. Desse modo, a visibilidade dos materiais assegura a intuição dos esquemas existentes. Além disso, as calhas permanecem abertas, capazes de acolher novos cabos e tubos, multiplicando-se os fluxos que por ela transitam. A própria concepção modular do convento permite que ele venha a ser prolongado sem ruptura, ou seja, não apenas recebendo o acréscimo de objetos complementares e/ou secundários, mas integrando ao seu próprio modo de ser novas realidades.

Aproximando-se da abordagem de Simondon (2013) quanto ao convento dominicano de *Sainte-Marie de la Tourette*, Norman (2006) também propõe uma espécie de autenticidade dos objetos técnicos, ou seja, que eles possam se mostrar sem esconder o modo pelo qual estão constituídos e funcionam. Neste sentido, ele argumenta em favor de um design que transmita a “essência da operação do aparelho; a maneira como ele funciona, as ações possíveis que podem ser executadas” (NORMAN, 2006, p.11). Para Norman (2006, p.11) – o que não estaria muito longe de Simondon –, “o design é na verdade um ato de comunicação”. Ao longo de seu livro, ele sustenta que um bom design é aquele que está feito de tal maneira que o usuário é capaz de compreendê-lo facilmente, inclusive dispensando, salvo raras exceções, os manuais e outras instruções externas, ou seja, o próprio objeto é meio e conteúdo de comunicação.

Além disso, o design “assume uma importância política; na verdade, as filosofias do design variam de maneira importante nos diferentes sistemas políticos” (NORMAN, 2006, p.252). Como temos visto, o modo pelo qual o objeto está constituído não é neutro. Se é mais ou menos visível, se mostra este ou aquele lado, uma parte ou outra, enfim, o

objeto técnico produz efeitos. A luta pela visibilidade é, de certo modo, uma luta pelas condições de abertura dos objetos técnicos, inclusive dos softwares.

O problema que se nos coloca, entretanto, não diz respeito mais somente a esta dimensão da visibilidade que temos abordado. Há todo um jogo que se produz na distribuição da luminosidade que, por vezes, faz aparecer alguns objetos técnicos – as câmeras de video vigilância, por exemplo – e desaparecer completamente outros – como algoritmos de rastreamento presentes na internet. Assim, a questão já não é mais somente ampliar a visibilidade dos objetos técnicos que já conhecemos, mas, sobretudo, começar inclusive por tomar consciência da existência de objetos técnicos com os quais nos encontramos sem nos dar conta.

SEGUNDA PARTE - GOVERNAMENTALIDADE ALGORÍTMICA

1 A PRODUÇÃO EXPONENCIAL DE DADOS

Evitar, ao máximo, o uso de cartões de crédito é uma prática de liberdade valorizada por Richard Stallman. É diante de uma vigilância distribuída, constante e que se amplifica cada vez mais, que ele afirma: “quase nunca uso meu cartão de crédito a não ser como último recurso para pequenas despesas inesperadas. E, se um sítio [site] quer um pagamento pelo acesso, não o uso, pelo menos não até que possa pagar de maneira anônima” (PACIFICI, 2011, sem paginação). Que modo de vida é este que procura escapar aos registros das ações realizadas no campo econômico (e em tantos outros)? O que Stallman, assim como outros hackers, buscam evitar com tais práticas de anonimato? Ou melhor, que modalidades de composição com os objetos técnicos eles procuram tecer?

Em 2012, uma reportagem do *The New York Times* causou perplexidade em seus leitores, pois revelava que a Target – uma rede de lojas de varejo norte americana – havia desenvolvido e fazia uso de um algoritmo capaz de detectar quando uma cliente estava grávida e, também, de prever o mês de gestação do bebê. Muito antes do ocorrido, a empresa já mantinha a prática de recolher e armazenar todos os dados possíveis a respeito de seus clientes. A cada um deles era reservado um número de identificação ao qual os diversos dados eram associados. Se um cliente comprou com um cartão de crédito ou com um cupom, se devolveu algum produto e solicitou ressarcimento, se preencheu um formulário, se visitou o site da Target ou se abriu um e-mail enviado pela empresa, tudo era registrado no banco de dados. Também estavam presentes dados demográficos tais como: idade, estado civil, número de filhos, endereço, estimativa de salário e mudanças de residência. É provável ainda que a empresa tenha adquirido no mercado dados adicionais como etnia, história de trabalho, revistas lidas, tópicos de discussão on-line, marcas de alimentos preferidas, tendências políticas, hábitos de leitura, entre tantos outros (DUHIGG, 2012).

Foi em 2002, logo após ser contratado pela Target, que Andrew Pole, fazendo uso dos dados acima mencionados, levou adiante um projeto para responder à questão proposta por dois de seus colegas do departamento de marketing. Eles queriam saber se era possível descobrir se uma consumidora estava grávida, mesmo se ela não quisesse

que a Target soubesse. Utilizando-se de técnicas estatísticas, os dados foram analisados em computadores e alguns padrões foram encontrados. Por exemplo, os analistas perceberam que mulheres no início do segundo trimestre de gravidez estavam comprando grandes quantidades de loção sem cheiro. Também observaram que nas primeiras 20 semanas as mulheres grávidas estavam adquirindo suplementos como cálcio, magnésio e zinco. Com a análise informatizada de 25 produtos em conjunto, o algoritmo desenvolvido era capaz de prever dentro de uma pequena janela quando a cliente daria à luz ao bebê, o que permitia à Target direcionar o marketing apresentando produtos e enviando cupons de desconto cronometrados para estágios específicos da gravidez (DUHIGG, 2012). Na reportagem é apresentado um exemplo hipotético oferecido por um dos empregados da Target:

> Tomemos uma compradora fictícia da Target chamada Jenny Ward, 23 anos, que vive em Atlanta e que em março comprou uma loção de manteiga de cacau, um bolsa suficientemente grande para ser utilizada também como uma bolsa de fralda, suplementos de zinco e magnésio e um tapete azul brilhante. Digamos que existe 87 por cento de chance que ela está grávida e que vai dar à luz em algum momento ao final de agosto. Além disso, por causa dos dados atrelados ao seu número de identificação [*Guest ID number*], a Target conhece o gatilho para disparar os hábitos de consumo da Jenny. Eles sabem que se ela recebe um cupom via e-mail, este a incitará a comprar on-line. Eles sabem que se ela recebe uma propaganda no seu e-mail na sexta-feira, ela frequentemente a usará para ir na loja no fim da semana (DUHIGG, 2012, sem paginação, tradução nossa).

Com o modelo preditivo em mãos, a Target direcionava seu *marketing* buscando conduzir a conduta de seus clientes. O uso do algoritmo dava-lhe uma considerável vantagem, aumentando suas chances de sucesso no tocante ao produzir ações de consumo. Desconhecedores das estratégias da empresa, muitos tinham ciência apenas dos efeitos que neles se produziam – ou seja, a inclinação para comprar este ou aquele produto.

O que a Target fez só foi possível em decorrência de novas condições que passaram a permitir a recolha de quantidades massivas de dados. Este é um fator que não deve ser negligenciado. Em entrevista à BBC Mundo, Martin Hilbert (2017 apud LISSARDY, 2017) ressalta que em 2016 a maior coleção de dados registrados era a da biblioteca do Congresso americano. Se em 2014 o volume de dados registrados

disponível no mundo equivalia à coleção dessa biblioteca por cada 15 pessoas, em 2017, segundo ele, deve haver uma biblioteca do Congresso dos EUA para cada sete pessoas. E em 2022, ele estima que haverá uma para cada indivíduo.

Como logo veremos, estamos diante de uma nova realidade – geralmente referenciada pela expressão Big Data – na qual o crescente volume, variedade e velocidade da produção de dados não podem mais ser ignorados nas novas formas de exercício do poder. Conforme já se afirmou:

> Target sabe. Apple Computer também sabe. Então, Linked In, Netflix, Facebook, Twitter, Expedia, campanhas políticas nacionais e locais, e dezenas de outras organizações que geram enormes valores econômicos, socais e políticos também sabem. Eles sabem que a era do Big Data está aqui e está aqui para ficar (DAVIS; PATTERSON, 2012, p.1, tradução nossa).

Assim, cabe a nós fazermos a seguinte pergunta: como podemos compor com tais objetos técnicos que não só registram dados acerca do mundo e de nossas vidas, mas também produzem saberes sobre nós? Que práticas de liberdade podemos ter em meio às novas formas de exercício do poder? Buscaremos, a partir de agora, abrir algumas dessas caixas-pretas, descrevendo tanto alguns objetos técnicos quanto as redes das quais participam, apontando, também, práticas hackers que se encaminharam para tecer outros modos de composição.

1.1 Coleta e Armazenamento de Dados

Algumas décadas atrás os dados digitais eram produzidos em poucos dispositivos – basicamente mainframes e alguns computadores pessoais. Porém, com a miniaturização, o aumento da capacidade e o barateamento dos aparatos tecnológicos, criaram-se condições para a disseminação de inúmeros objetos técnicos capazes de produzir dados a partir de fontes heterogêneas e de forma massiva (AMARAL, 2016; GOMES, 2017).

Além disso, se antes o custo de armazenamento era uma variável de extrema relevância – obrigando a selecionar os dados criteriosamente, sobretudo considerando seu valor imediato –, atualmente os baixos preços de armazenamento contribuem para que os dados sejam coletados e armazenados de forma indiscriminada (AMARAL, 2016).

Em uma rara explicação pública, Gus Hunt, chefe da divisão técnica da CIA, esclareceu que como o valor de cada dado não é conhecido a não ser no momento no qual ele é conectado a outro dado, o que pode ocorrer apenas em uma ocasião futura, e como não é possível vincular dados que não se possui, então a CIA passou a se esforçar por "[...] coletar tudo, e de o conservar para sempre" (BERNARD, 2013, sem paginação, tradução nossa).

Assim, governos, empresas privadas, cientistas e, inclusive, os próprios indivíduos contribuem recolhendo e armazenando dados, seja para fins de gestão de recursos, de prevenção de crimes, de otimização de processos, de segurança, de marketing e de publicidade, de aquisição e avanço dos conhecimentos ou, o que apesar de paradoxal é ainda mais marcante, sem ter uma finalidade clara ou previamente definida (ROUVROY; BERNS, 2013).

Além da capacidade de armazenamento teoricamente ilimitada, há de se ressaltar a condição de tais dados serem potencialmente acessados a qualquer momento e de qualquer lugar, sendo necessário apenas um computador conectado na rede. Por mais que se diga que os dados estão na "nuvem", dando a impressão de serem desmaterializados, eles possuem uma localização física e, além disso, por vezes não estão distribuídos, mas fortemente centralizados em gigantescos *datacenters* (ROUVROY, 2014; ROUVROY; BERNS, 2013).

Dentre os dados coletados e armazenados há aqueles que estão estruturados, como no caso da Target. Ou seja, estão organizados em tabelas com linhas e colunas. Por exemplo, cada linha pode dizer respeito a um indivíduo e a série de colunas às diferentes características ou atributos associados ao indivíduo em questão. Porém, a maior parte dos dados acumulados nos dias de hoje não teria por centro de gravidade os indivíduos. Ou seja, não seria no nível dos indivíduos que a maior parte dos dados seriam coletados e nem mesmo seria no nível dos indivíduos que o poder se exerceria com mais intensidade. Ao menos esta é a tese lançada por Rouvroy ([s. d.] apud COLLE; LEDOX; VLAJCIC, 2017, p. 58, tradução nossa) que afirma: "O desafio atualmente é menos a proteção dos dados pessoais que o desaparecimento da pessoa, do sujeito".

Para a pesquisadora, os dados produzidos no Big Data são amnésicos quanto às condições de sua produção, isto é, eles são despersonalizados, descontextualizados e

desprovidos de significação (ROUVROY, 2016a, 2016b). Isto porque o real, ao ser transcrito em termos digitais, é convertido em zeros e uns, sendo incapaz de carregar consigo o sentido, as forças que atravessavam e contribuíam para a emergência do fenômeno do qual ele é a transcrição reduzida. No Big Data, o que interessa é desenvolver modelos de predição: "você só precisa saber que algo funciona, não o porquê" (STEPHENS-DAVIDOWITZ, 2018, p. 71). A novidade histórica, segundo Rouvroy e Berns (2013, p.169, tradução nossa), consiste em

> [...] conservar o traço de uma compra, de um deslocamento, do uso de uma palavra ou de uma língua, cada elemento é restabelecido à sua natureza mais bruta, quer dizer estando ao mesmo tempo totalmente abstraído do contexto do qual ele emergiu e reduzido à condição de simples 'dado'. Um dado não é nada mais que um sinal expurgado de toda a significação própria.

São dados, em sua grande maioria, não estruturados, tais como aqueles gerados em mídias sociais (Facebook, Twitter, Youtube e outros), documentos em geral, páginas da internet, e-mails, trocas de mensagens em aplicativos de bate-papo, imagens, vídeos, arquivos de áudio, plantas de engenharia, sensores, etiquetas RFID, câmeras de vídeo etc (AMARAL, 2016; STEPHENS-DAVIDOWITZ, 2018; TAURION, 2015). A esta recolha e conservação automatizada e massiva de dados não triados, Rouvroy e Berns (2013) denominam de *dataveillance* (vigilância de dados). Para Amaral (2016, p.10), estamos diante do "registro eletrônico de um fenômeno qualquer, como o movimento do celular, o acionamento do freio do veículo, uma fotografia do céu ou gravação de câmera de segurança". Mesmo o que é, aparentemente insignificante, está sujeito a ser capturado e registrado digitalmente.

Para se ter uma ideia inicial do volume de dados que está em jogo, basta-se dizer que aproximadamente metade da população mundial utiliza a internet (INTERNATIONAL TELECOMMUNICATION UNION, 2017). E, de acordo com o site *Internet Live Stats*[33], o número de usuários ativos no Twitter seria de aproximadamente 310 milhões, enquanto que no Facebook já teria ultrapassado 2 bilhões. Por dia, tais usuários enviam mais de 200 bilhões de e-mails, realizam mais de 65 milhões de postagens no Instagram e

[33] E como a *Real Time Statistics Project ([S. d.], sem paginação, tradução nossa)*, responsável pelo site *internet Live Stats*, consegue seus dados? Por meio de mais de 250 diferentes fontes, que trabalham os dados por meio de "um avançado algoritmo com a finalidade de produzir uma estimativa que é tão acurada quanto possível". Disponivel em: http://www.internetlivestats.com/faq/. Acesso em: 11 jan. 2019.

efetuam mais de 5 trilhões de pesquisas no Google. Dados que, certamente, já estão desatualizados, pois o crescimento vertiginoso nos permite apenas apresentar um retrato sempre já ultrapassado.

É necessário acrescentar ainda os 10 bilhões de sensores conectados à rede mundial de computadores e que são capazes de coletar e transmitir dados (MORE THAN..., 2013). São objetos de todas as formas e que capturam dados como imagens, temperatura, localização, sons, dentre outros (GOMES, 2017).

Qualquer uso de serviço – seja aqueles do Google, do Facebook, um GPS, um cartão de débito e/ou crédito, ou mesmo de uma linha telefônica em aparelho fixo ou celular – é, ao mesmo tempo, uma potencial fonte para a coleta e registro de dados. Em outras palavras, ao utilizarmos eles estamos, frequentemente, também alimentando o Big Data. Ou melhor, pelo simples fato de existirmos e nos encontrarmos com determinados objetos técnicos, fluxos de dados estão sendo produzidos. E, ainda, são dados produzidos a respeito do mundo e acerca de nós que, em sua esmagadora maioria, desconhecemos. Como afirma Antoun (2008, p.24), “a mina de dados é completamente opaca, completamente invisível para o sujeito”. Isto é, no geral, não estamos cientes nem que tais dados estão sendo coletados e registrados, nem que tais dados podem dizer especificamente acerca de nossa existência, nossos hábitos, nossas relações sociais, nossos interesses e afinidades, etc.

1.2 SENSORES

Ocupando papel central na produção de dados estão os sensores. Mas o que é um sensor? É um objeto técnico capaz de “*sentir* a variação de uma grandeza física qualquer” sendo, geralmente, também um transdutor, ou seja, possuindo “a capacidade de correlacionar essa variação com alguma outra grandeza” (STEVAN JUNIOR; SILVA, 2015, p.24). Um termômetro de mercúrio é um clássico exemplo de um sensor transdutor, pois a variação de temperatura no ambiente exterior afeta diretamente o volume do mercúrio em seu interior. Assim, com uma câmara de expansão graduada, torna-se possível ler a temperatura em função da escala, seja ela em Celsius, seja ela em Kelvin ou em Fahrenheit.

Outro exemplo é o fotorresistor, também denominado de *Light-Dependent Resistor* (LDR), que é o sensor mais simples para detecção de luz. Em síntese, ele tem sua resistência alterada de acordo com a quantidade de luz que nele incide. Na ausência de luminosidade, ele apresenta resistência extremamente alta, porém quando recebe iluminação sua resistência ao fluxo de corrente elétrica cai drasticamente. É possível utilizá-lo, em conjunto com outros elementos técnicos, para realizar uma ação sobre o mundo como, por exemplo, ligar a luz de um poste ao anoitecer[34].

Existem também sensores capazes de perceber variações no campo magnético devido à presença de algum elemento metálico. Quantos de nós não tivemos em algum momento da vida a dificuldade para acessar o interior de um banco, a sala de espera de um aeroporto ou, até mesmo, um museu simplesmente por estarmos portando algumas chaves ou moedas no bolso da calça? É bem provável que um ou mais sensores tenham detectado a presença dos metais acionando um sinal de alarme e/ou mesmo fornecendo dados para o travamento das portas de acesso.

Variações de temperatura, de luminosidade, de campos magnéticos, dentre tantas outras grandezas físicas analógicas podem ser percebidas e quantizadas, ou seja, transformadas em valores discretos e, assim, facilmente processadas por máquinas digitais. Deste modo, o mundo percebido pela vasta imensidão de sensores espalhados torna-se um conjunto de sequências de zeros e uns. Mundos heterogêneos encontram, portanto, uma forma de equivalência, um campo comum de tratamento. Ou seja, é em uma mesma linguagem – a numérica – que poderão ser tratados os dados provenientes de sensores de umidade, de pressão, de vazão, de gases, de tensão e de corrente elétrica, acelerômetros e giroscópios, além de tantos outros.

Se ainda não é realidade, não tardará muito para que a maior parte dos dados existentes venha a ser composta por aqueles provenientes dos sensores acoplados a objetos, superfícies físicas ou organismos vivos (SADIN, 2015). Mesmo sem estarmos cientes, dificilmente temos um dia no ambiente urbano sem que nos encontremos com algum sensor. Para utilizarmos a televisão com o controle remoto, acionamos um sensor infravermelho. Mesmo que escutemos um rádio antigo, é um sensor resistivo, mais

[34] Neste caso, em específico, a inversão do efeito do LDR pode ser realizada utilizando-se um transistor. Assim, ao invés de a luz do poste acender-se quando estiver claro, ela poderá ser acessa quando houver ausência de luminosidade.

especificamente um potenciômetro, que nos permite aumentar o volume. Se carregamos conosco um *smartphone*, possivelmente ele terá um acelerômetro e um giroscópio que, em conjunto, possibilitam "o conhecimento completo de aceleração, velocidade, posição e orientação de um objeto" (STEVAN JUNIOR; SILVA, 2015, p.84) – no caso, do próprio *smartphone* e daquele que o porta. Isso sem falar do GPS, que também pode estar integrado no *smartphone*, e que permite localizar a sua posição no globo terrestre. Nossos carros estão repletos de sensores que indicam a velocidade, a temperatura interna e externa, o nível de combustível e outros fluídos, a necessidade de realizar manutenções, etc. Para passar a catraca de um ônibus pode ser necessário apresentar um cartão magnético que é lido por um sensor. Se utilizamos um notebook ou um desktop lá estão presentes sensores nos dispositivos de entrada como mouses, teclados, *touchscreen* e *touchpad*. Ainda que saíamos de casa apenas para passear na rua, provavelmente nos defrontaremos com algum sensor captando nossos movimentos.

A difusão dos sensores não teria o mesmo impacto se muitos deles não estivessem conectados, ou seja, mais do que permitirem alguns objetos técnicos funcionarem de maneira automática – o que por si só já é bastante relevante –, também estão em condições de transmitir dados a outros objetos técnicos, podendo estar conectados entre si, em redes locais e/ou com a internet. É a esta modalidade de objetos interconectados, frequentemente operando em tempo real, que tem se denominado IoT.

Multiplicam-se, assim, os objetos técnicos que podemos carregar conosco, vestir ou mesmo ingerir[35] e que são capazes de coletar dados acerca de nossa fisiologia e comportamentos. São *smartphones*, relógios, pulseiras e outros tantos que possuem sensores integrados e estão permanentemente conectados, produzindo e transmitindo dados. Frequência cardíaca, temperatura, taxa de glicose, grau de hidratação, calorias queimadas, aspectos relacionados ao sono e à performance sexual, nível de stress, enfim, as inúmeras modalidades de variação no corpo humano passam a estar em condições de serem observadas por sensores (SADIN, 2015). Alguns são postos sobre a pele, outros permanecem, mais ou menos, à distância e há ainda aqueles que podem atuar dentro de nossos corpos. Até o simples ato de escovar os dentes, se feito com a

[35] O *Ingestible Micro-Bio-Electronic Device*, por exemplo, é um protótipo já testado em porcos, cujo sistema digestivo é semelhante ao de seres humanos. Ao ingeri-lo, é possível identificar um sangramento gastrointestinal, assim como diferentes tipos de doenças, tudo por meio de transmissão de dados sem fio (MIMEE et al., 2018).

Kolibree – a primeira escova de dentes inteligente –, pode produzir dados. Ao fazer a higiene bucal com ela, a duração e a frequência das escovadas são registradas, assim como a quantidade de tártaro eliminado e as zonas que merecem mais atenção. A Kolibree analisa a maneira que o usuário escova os dentes, a pressão que exerce e oferece conselhos para uma melhor escovação (COLOMBAIN; LECOMTE; SOREL, 2015; KOLIBREE, 2015).

A multiplicação indefinida de uma variedade crescente de sensores conectados e transmitindo dados em tempo real[36] transforma profundamente o mundo em que vivemos. Ainda que não estejamos cientes, dados sobre nós estão sendo permanentemente coletados a não ser que tenha ocorrido alguma falha ou que apresentemos alguma resistência bem-sucedida. A produção ininterrupta de variados fluxos de dados torna-se a regra e sua ausência a exceção. Além disso, nos dias de hoje, não é mais necessariamente o indivíduo (nem as populações) o alvo principal da coleta dos dados, mas todo e qualquer aspecto dos indivíduos e do mundo. Observam-se indivíduos, mas também o número de peças que percorrem uma esteira, a temperatura e a umidade dentro de um laboratório, a presença/ausência de objetos e pessoas em determinado lugar, o tipo de material que circula ou permanece parado, a concentração de gás carbônico ou de álcool etc.

É esta modalidade de coleta de dados que também está em jogo naquilo que ocorre na internet. É como se uma infinidade heterogênea de sensores fosse produzida através de linhas e linhas de códigos, sendo programados para coletar dados acerca dos dispositivos e a respeito do modo pelo qual os usuários interagem entre si, com os próprios programas e com o mundo.

1.3 As Plataformas-Sensores

A função de coleta de dados, não raro, torna-se até mais importante do que os serviços prestados pelas plataformas. Para designar esse aspecto peculiar, utilizamos a expressão plataformas-sensores. Dentre as plataformas consideradas por Stephens-

[36] A expressão “tempo real” mereceria uma análise mais detida, pois não se trata da duração enquanto experiência psicológica – tema que Deleuze (2012) retoma e desenvolve a partir de Bergson –, mas de instantes recortados no tempo, unidades discretas, isto é, da justaposição sucessiva de instâncias do “agora”.

Davidowitz (2018) como “minas de ouro digitais” – aquelas que teriam armazenado e continuam a coletar dados acerca da conduta humana – estariam o Wikipédia, o Facebook, o PornHub e, a mais importante de todas, o Google. Como ele demonstra, cada ação na rede é também um *input* que pode ser analisado. Ele chega a comparar o mecanismo de busca do Google a um confessionário, no qual as pessoas expressariam pensamentos que não cogitariam em expor em nenhum outro lugar – pesquisas a respeito de sexo, de suicídio, de ilegalidades, tendo por temas anseios e temores.

O Google – assim como outras redes sociais tal como o Facebook – faz da internet um grande laboratório. Enquanto os experimentos sociais tradicionais – aqueles realizados com questionários, entrevistadores, observações, Termos de Consentimento Livre e Esclarecido etc – podem demorar meses para serem concluídos e necessitar de elevada quantidade de recursos econômicos, humanos, entre outros, os experimentos no mundo digital podem ser bem mais baratos e rápidos. Expressando certo fascínio por tais mecanismos, Stephens-Davidowitz (2018, p.208) chega a afirmar que basta codificar um programa que automatize os processos e, além disso, “não precisa contatar ninguém. Nem mesmo contar aos usuários que estão participando de um experimento”. Em suas palavras, que bem resumem o momento atual, “na era do Big Data, o mundo todo é um laboratório”. E, poderíamos acrescentar que todos nós somos – estejamos cientes ou não –, em maior ou menor medida, as cobaias.

Levy (2012a) chega a comparar os usuários do Google a ratos de laboratório que seriam submetidos a contínuas experiências por meio do “teste A/B”. Neste, uma pequena parcela de usuários – geralmente 1% – é exposta às mudanças sugeridas, tendo suas ações coletadas, analisadas e comparadas com as dos demais usuários. Assim, o Google avalia cada alteração em seus produtos e serviços, “desde a tonalidade das cores de sua interface até o número de resultados apresentados em uma consulta” (LEVY, 2012a, p.83).

Se há algo que interessa ao Google, bem como a outras plataformas, é a participação do usuário, pois como assinala o coletivo Ippolita (2010, p.106, tradução nossa):

> o motor de busca ‘bom por definição’ explora e registra por inteiro e de forma contínua os comportamentos dos usuários que utilizam seus serviços, a fim de identificar seus costumes e inserir em suas atividades

> (navegação, correio eletrônico, gerenciamento de arquivos, etc.) anúncios personalizados, contextuais, leves, onipresentes e, possivelmente, em condição de gerar *feedback*, de modo que os usuários ofereçam informações úteis para os vendedores e até cheguem a aprimorar por si mesmos 'as sugestões publicitárias', expressando suas 'preferências'.

O Google armazena, portanto, não apenas uma cópia, ainda que parcial, dos conteúdos existentes na internet. Ele coleta e registra também "as relações humanas, emocionais e profissionais dos usuários do serviço" (IPPOLITA, 2010, p.133, tradução nossa). O mesmo faz o Facebook ao atentar-se a cada postagem, a cada curtida, a cada comentário, enfim, a cada clique do mouse ou caractere digitado. A prática de coletar e registrar os dados é corrente nas diversas plataformas (Instagram, Airbnb, Amazon, Netflix etc.), seja ela de rede social, de comércio, de transporte, de hospedagem ou de outra finalidade. O que buscamos assinalar não é se determinada organização coleta dados de determinado tipo, mas que é uma tendência, cada vez mais presente, que qualquer ação na rede ou fora dela seja capturada e transcrita em forma de dado capaz de ser processado em computadores.

Uma experiência interessante pode ser visitar o site interativo ClickClickCLick[37]. Nele, o internauta pode acompanhar, em tempo real, algumas de suas ações que são capturadas, registradas e exibidas. Mesmo algo que, a princípio, seria irrelevante, como arrastar lentamente o ponteiro do mouse para o canto inferior direito, é passível de ser monitorado. A proposta do site é mostrar algumas de nossas ações on-line que, não raro, são coletadas quando navegamos em sites destinados ao comércio, à divulgação de notícias, ao entretenimento etc. É com base nesses e outros dados que se produzem saberes e se conduzem condutas. Apesar de simples, o ClickClickCLick é capaz de colocar diante dos nossos olhos aquilo com o qual nos deparamos cotidianamente sem nos darmos conta – isto é, algoritmos de vigilância (prevenção e zelo) e monitoramento (acompanhamento e avaliação).

1.4 *DEFAULT*, OU REGRAS PADRÃO

[37] Disponível em: https://clickclickclick.click/. Acesso em: 26 fev. 2019.

Se muitos dos dados produzidos são oferecidos benevolentemente pelos usuários – como nas ativas postagens nas redes sociais e nos blogs –, outros parecem apenas ter a aparência de consentimento. Por exemplo, ao se logar em uma conta do Google[38], por *default*, o histórico de pesquisas realizadas em seu motor de busca e as páginas visitadas a partir dos resultados encontrados são, automaticamente, registrados na nuvem. Ainda que estejam disponíveis, em alguma medida, opções para alterar o modo pelo qual compartilhamos nossos dados com o Google, a maioria de nós as desconhece. Assim, por *default*, estamos sempre oferecendo nossos dados.

Por um lado, o *default* não é impositivo – ou seja, não obriga o usuário a compartilhar ou deixar de compartilhar seus dados –, entretanto, por outro, o modo pelo qual está arquitetado pode produzir efeitos bem diferentes[39]. Por exemplo, suponha que uma instituição – pública ou privada – esclareça que os dados de navegação na internet – como os sites visitados – não serão compartilhados com ninguém a menos que se clique em um botão concordando com o compartilhamento (é a lógica do *opt-in*, do colocar-se dentro, da adesão à funcionalidade). Suponha agora que a mesma instituição especifique que a menos que o usuário proíba, os dados serão compartilhados (é a lógica do *opt-out*, do colocar-se fora, da recusa à funcionalidade). Sunstein (2013) afirma que, considerando os dois casos, os resultados não serão os mesmos. No primeiro, os usuários tendem a ignorar a questão ou a recusar o compartilhamento de seus dados, mantendo assim sua privacidade. No segundo, os usuários tendem a ignorar a questão ou a recusar-se em deixar de compartilhar seus dados, ainda mais se a decisão do *opt-out* passa pela leitura de algo complicado como, por exemplo, um texto técnico que o usuário não domina. É justamente o segundo caso – no qual por *default* os movimentos dos usuários são visíveis e podem ser monitorados – que é o mais comum entre os *browsers* disponíveis atualmente. Assim, por *default*, muitos dados estão sendo continuamente coletados.

Em alguns casos o *default* pode ser facilmente alterado pelas empresas que oferecem os aplicativos. Isto significa que os termos da relação podem ser modificados,

---

[38] Caso o leitor queira acessar dados acerca de alguma conta do Google que possui, basta efetuar o login e visitar a página disponível em: https://myactivity.google.com/myactivity

[39] O artigo de Johnson e Goldstein (2003) mostra, por exemplo, que na Alemanha, em que a política de doação de órgãos se dá na condição de *opt-in*, apenas 12% são doadores; enquanto na Áustria, cujo *default* é ser doador e para não o ser é necessário *opt-out*, 99,98% são doadores.

de certo modo, unilateralmente – basta ao desenvolvedor alterar alguns poucos parâmetros e as regras passam a ser outras. Por exemplo, de 2004 a 2010, o Facebook utilizou largamente do *default* para modificar as configurações de privacidade sem que muitos de seus usuários estivessem cientes e/ou compreendessem o que estava ocorrendo. Se em 2004 não havia dados compartilhados com toda a rede da internet, e um número muito restrito deles era compartilhado com todos os demais usuários do Facebook, em 2010 o cenário era bem diferente: o nome, a foto pessoal, o gênero, os likes, as fotos e imagens postadas, os amigos, além de uma série de outros dados passaram a estar disponíveis por *default* a qualquer um que se interessasse (IPPOLITA, 2012; MCKEON, [2010]). Tratava-se, assim, por meio da lógica de alteração do *opt-out* de instaurar uma relação tecnocrática, que supõe o usuário como aquele cuja posição a ser ocupada é a de quem se adapta:

> Quando se modificam os parâmetros de *default* de milhões de pessoas, sem comunicar a mudança, e se fala disto de forma enigmática ou *a* posteriori, é que implicitamente se considera que os usuários não sabem o que querem, ou pelo menos que quem oferece o serviço sabe mais do que eles (IPPOLITA, 2012, p.63, tradução nossa).

Tais mudanças no *default* quando ocorrem em grande velocidade têm implicações ainda mais importantes. Trata-se da questão do saber. Ao aprendermos a nos relacionar com um objeto técnico – uma bicicleta, por exemplo – sua constância no mundo permite-nos retomar a relação e continuá-la sem que toda a história que temos com ele seja descartada a cada vez. É sempre um recomeço que é também continuidade. Porém, como bem assinala o coletivo Ippolita (2012, p.41, tradução nossa), no caso dos softwares cujo *default* é constantemente alterado, tal como no Facebook, o usuário tem seu saber tornado rapidamente obsoleto, exigindo-lhe a atualização constante “por meio de uma formação continuada que não estratifica nem ensina nada mais que a adequação ao sistema”. Tais transformações excluem o usuário da condição de um aprendizado quanto à própria tecnicidade do objeto técnico, designam-lhe a posição de conformidade, ou seja, trata-se de uma relação de heteronomia com reduzido grau de liberdade. É neste sentido que Ippolita (2012, p.41, tradução nossa) apresenta a questão: “O que se pode opor à obsolescência programada das capacidades, se nada do que existe aí fora depende verdadeiramente de nós?”. Ou seja, se estamos sujeitos a regras do jogo que

não podem ser por nós modificadas – e, em alguns casos até mesmo conhecidas –, qual é o espaço de liberdade que nos é proposto/designado?

1.5 *SOCIALBOTS*

Em pouco mais de uma década da criação das redes sociais on-line (o Orkut e o Facebook em 2004, o Twitter em 2006 e o Instagram em 2010), muitos de nós nos acostumamos a delas participar. Além de nos relacionarmos com outros seres humanos, tendo ciência ou não, também podemos nos encontrar com alguns seres técnicos bastante peculiares que são capazes de mimetizar os comportamentos humanos: os *social bots*. Trata-se de algoritmos de computador que "produzem automaticamente conteúdo e interações com humanos e mídias sociais, tentando emular e possivelmente alterar seus próprios comportamentos" (FERRARA et al., 2016, p.96, tradução nossa).

O nível de automatização dos processos pode ir desde a criação de contas e de perfis associados em redes sociais até a "gestão" destas e outras contas existentes, postando mensagens e efetuando solicitações de amizade. Por vezes, é impossível distinguir quando uma conta é operada por um ser humano ou por um software, seja ele parcialmente ou totalmente automatizado. E à medida que os *social bots* adotam níveis ainda maiores de Inteligência Artificial (IA), torna-se ainda mais difícil de distinguir suas ações e aquelas levadas à cabo por seres humanos (ADAMS, 2017; FERRARA et al., 2016; GRIMME et al., 2017). Em pesquisa recente, Varol et al. (2017, p.6, tradução nossa) estimaram que são *bots* entre 9% e 15% das contas ativas no Twitter, considerando apenas usuários que se comunicam em inglês, isto sem deixar de fazer a ressalva que

> [...] *bots* muitos sofisticados podem sistematicamente escapar ao julgamento de um anotador humano. Estes complexos *bots* podem estar ativos no Twitter, e consequentemente em nosso conjunto de dados, e podem ter sido incorretamente classificados como humanos, fazendo mesmo os 15% uma estimativa conservadora.

No experimento levado adiante por Boshmaf et al. (2011), os pesquisadores fizeram uso de um grupo de 102 *social bots* reprogramáveis para se infiltrarem no Facebook (que à época contava com "apenas" 750 milhões de usuários). Cada um dos

social bots controlava uma conta na rede social e todos eles eram coordenados, recebendo suas instruções e transmitindo dados, por meio de um *botmaster* – um software de controle.

Ao longo de 8 semanas foram enviadas um total de 8.570 solicitações de amizade, das quais 3.055 foram aceitas. E, além dos "amigos", passaram a fazer parte da rede estendida também os contatos indiretos, ou seja, os "amigos dos amigos", totalizando 1.085.785 perfis com os quais os *social bots* puderam interagir e coletar dados. Ainda que pudessem acessar dados relacionados ao perfil, às publicações no *feed* de notícias e às postagens no mural, os pesquisadores focaram naqueles mais sensíveis e que teriam valor econômico. Diante de si, os *social bots* podiam coletar dados tais como endereços de e-mail, número de telefone, endereço, gênero, data de nascimento, local de trabalho e/ou estudo, dentre outros dados privados (BOSHMAF et al., 2011).

Para nós, a questão não é tanto saber quantos dentre os nossos "amigos" no Facebook, Twitter ou outras redes sociais são *social bots*, mas de compreender como eles podem agir, o que podem fazer e os efeitos que estão em condições de produzir. Ou seja, não apenas, como denuncia IPPOLITA (2012, p.33, tradução nossa), que eles "fingem saber coisas que não sabem, enganam, mentem", mas, sobretudo, que em nossos encontros com tais objetos técnicos não são neutros. Isto porque podemos ter nossas vidas transcritas em dados que podem ser posteriormente – ou, até mesmo, em tempo real – utilizados para a produção de saberes e, consequentemente, nas relações de poder.

1.6 RASTREADORES

A coleta e registro de dados na web não se restringe e nem se focaliza apenas nos conteúdos divulgados, de forma mais ou menos pública e voluntária, pelos usuários como, por exemplo, os dados de sua conta, as postagens e as conversações em redes sociais. Antes, qualquer vestígio, qualquer traço das atividades realizadas on-line são, cada vez mais, objeto de captura. Para isso, diversos sites utilizam quantidades expressivas de rastreadores no intuito de identificar seus visitantes, coletando e arquivando dados acerca de suas ações on-line. Como sublinha Bruno (2016, p.35),

> [...] toda ação efetuada na rede – navegação, busca, simples cliques em links, downloads, produção ou reprodução de conteúdo – deixa potencialmente um rastro, um vestígio, uma inscrição mais ou menos explícita, suscetível de ser capturada, recuperada, classificada.

Cao, Li e Wijmans (2017) ressaltam o rápido desenvolvimento dos métodos de rastreamento na web e os distinguem entre três gerações. A primeira, adota identificadores *statefull* definidos pelo servidor como, por exemplo, *cookies* e *evercookie*. Já a segunda geração, chamada de *fingerprinting*, ao invés de configurar um novo identificador, explora identificadores *stateless*, tais como versões de plug-in (ou módulo de extensão) e *user agent*, que já existem nos navegadores. Enquanto os métodos de rastreamento de primeira e segunda geração estão restritos a um único *browser*, os métodos de terceira geração, que estão emergindo, buscam rastrear o usuário através de diferentes dispositivos (*smartphones*, smart TVS notebooks, desktops, tablets etc), independentemente dos *browsers* utilizados.

Os *cookies* – que ainda são utilizados por inúmeros sites – podem ser definidos como pequenos arquivos de texto armazenados no dispositivo do usuário. Eles foram criados para facilitar a navegação*,* evitando a necessidade de que a cada visita a um determinado site fosse preciso refazer um longo processo de identificação. Por meio dos *cookies*, tornou-se possível introduzir uma espécie de memória que armazena dados de personalização, permitindo ao usuário encerrar a conexão com um determinado site e retomá-la a partir do estado no qual a havia deixado. Os *cookies* têm papel fundamental em sites de compra, por exemplo, quando podemos navegar entre diferentes páginas, sair do site de vendas e retornar mais tarde, mas mantendo no carrinho de compras os itens já adicionados.

Em um primeiro estágio, os *cookies* são gerados pelo servidor Web e transmitidos ao dispositivo do usuário que os armazena juntamente ao *browser*. Já em um segundo estágio, quando o usuário faz uma requisição por meio de seu *browser* para visualizar certa página de um determinado servidor, o *browser* automaticamente transmite *cookies* com os dados para esse servidor. Os *cookies* podem conter dados como o número de vezes que alguém acessa determinada página, o nome da pessoa, seu endereço, sua senha, cliques em determinados botões da página, itens no carrinho de compras etc.

Porém, como esclarece Grande (2006, p.31), um determinado dispositivo pode conter *cookies* de páginas que nunca foram acessadas pelo usuário:

> Isso ocorre devido ao fato de existirem sites que são assinantes de algum serviço de personalização de alguma organização. Esses sites podem possuir em sua página principal uma requisição de cookie para os servidores dessa organização. Por exemplo, o usuário pode encontrar diversos cookies do site da DoubleClick sem tê-lo visitado, mas alguns dos sites que foram visitados são assinantes do serviço da DoubleClick. Quando se acessa um site semelhante a esse descrito anteriormente, ele requisita o cookie armazenado no computador do usuário. Através dessa requisição, ele obtém as informações para saber quem está visitando-o e qualquer outra informação contida no arquivo do cookie. Então, é enviada uma requisição para um outro servidor, o qual promove esse serviço de personalização, informações de propagandas a respeito de quem visitou o site. Com a resposta dessa requisição o site pode promover propagandas personalizadas para um usuário específico.

Mas é possível rastrear os rastreadores e *watch the watchers*, abrir a caixa-preta, saber como ela funciona e quem está nos monitorando. A extensão *Firefox Lightbeam*[40,41], por exemplo, permite visualizar de modo gráfico parte do caminho que os nossos dados de navegação percorrem, desde os sites que acessamos e coletaram nossos dados até aqueles pelos quais não navegamos, mas com os quais nossos dados estão sendo compartilhados. Por exemplo, apenas ao acessar as páginas principais do portal de notícias Globo.com e das lojas Americanas é suficiente para ter os dados compartilhados com 25 outros sites e serviços de terceiros.

É por meio do rastreamento, através de *cookies*, que ao demonstrar interesse por um determinado livro – seja por digitar seu nome em um motor de pesquisa, seja clicando em uma imagem ou botão – que inúmeras propagandas podem ser apresentadas ao internauta como se o estivessem seguindo ao longo de sua navegação na web. Entretanto, ainda que os *cookies* armazenados digam respeito à um determinado dispositivo (um desktop, um tablet, um smartphone etc.) e não a um internauta em particular, organizações empenham-se associar os *cookies* – a princípio, anônimos – com

---

[40] A extensão *Firefox Lightbeam* está disponível atualmente apenas em inglês, o que pode acabar sendo, em um primeiro momento, um impeditivo para a grande maioria dos internautas que não estão familiarizados com este idioma. Entretanto, seu layout é bastante intuitivo, tornando o uso da extensão mais acessível. Como nem sempre as as traduções acompanham a velocidade de criação e das transformações dos programas que têm por finalidade problematizar as relações de poder na internet, seria importante buscar, na medida do possível, oferecer um layout capaz de se comunicar de forma mais direta, inclusive, dispensando o uso da linguagem escrita e priorizando os esquemas, diagramas, símbolos, etc.

[41] Disponível em: https://github.com/mozilla/lightbeam-we . Acesso em: 26 fev. 2019.

dados provenientes de fora da web, isto é, com dados de pessoas e seus nomes reais (ANGWIN, 2014).

Na prática, quanto mais dados são obtidos – por meio de *cookies* e através de outros rastreadores – mais fácil se torna identificar um determinado dispositivo como sendo único. Mas há margem de negociação, ou seja, é possível estabelecer outras composições com os *cookies* que não somente aquela na qual o usuário fica à deriva das implementações que não foram por ele programadas. Podemos, por exemplo, apagar com regularidade os *cookies* que nosso *browser* armazena e que são utilizados para nos identificar. Para isto, na maioria dos *browsers* basta acessar o menu “Configurações” ou “Preferências”, depois “Privacidade e Segurança” e então apagar em “Limpar Dados”. É possível ainda selecionar e configurar os *cookies* que serão mantidos, o tempo que serão preservados e, até mesmo, bloquear alguns deles.

Já o *evercookie* é, por definição, muito mais difícil de remover do que os *cookies,* pois ele armazena dados em, ao menos, dez diferentes lugares no dispositivo do usuário. Na página do projeto do seu criador, Samy Kamkar (2010, sem paginação, tradução nossa), a pergunta “*What is the point of evercookie?*” é respondida assim:

> Evercookie é projetado para fazer os dados persistentes realmente persistentes. Armazenando o mesmo dado em vários locais nos quais um cliente pode acessar, se qualquer dado é perdido definitivamente (por exemplo, por meio da limpeza de *cookies*), o dado pode ser recuperado e então restabelecido e reutilizado. Simplesmente pense nisso como *cookies* que nunca desaparecerão.

O *Evercookie* é uma espécie de experimento fruto da curiosidade de Kamkar acerca dos modos pelos quais os anunciantes o rastreavam. É ao realizar suas explorações, catalogando o que ele encontrava em seu computador, que “ele fez o *Evercookie* para demonstrar justamente como computadores pessoais podem ser completamente infiltrados pela mais recente tecnologia da internet” (VEGA, 2010, sem paginação, tradução nossa).

Ao criar o *Evercookie*, Kamkar abre a caixa-preta dos rastreadores com os quais se deparava. Ele os hackeia, levando a cabo a máxima hacker de que “toda a informação deve ser aberta e gratuita” (LEVY, 2012b, p.26). Assim, ao publicar seu código, ele expõe o funcionamento dos rastreadores – conhecimento que até então era restrito a alguns *experts* e organizações. Ao deixar o código-fonte disponível para que outros o conheçam

e o utilizem, criam-se condições tanto para que o *Evercookie* seja capturado e empregado para acentuar o controle quanto para produção de estratégias de contra-controle, que buscam escapar, driblar ou enfrentar o *Evercookie*.

Enquanto os métodos de rastreamento da primeira geração necessitam do envio de um arquivo de texto a ser armazenado pelo dispositivo do usuário, os métodos de segunda geração o dispensam. Seu modo de operação é outro, pois apenas solicita ao *browser* do visitante que lhe forneça alguns dados e/ou realize algumas tarefas. No caso do método *canvas fingerprinting*, por exemplo, Vasilyev (2013, sem paginação, tradução nossa) esclarece: "um *browser* é questionado acerca de seu *agent string*, sobre a profundidade da cor de sua tela, de seu idioma, dos plugins instalados com suporte de *mime types*, de seu fuso-horário e de outras capacidades, tais como *local storage* e *session storage"*.

Isoladamente, cada um desses dados tem pouco a dizer acerca do dispositivo do usuário, mas no conjunto tais dados podem ser utilizados para identificá-lo com alto grau de acerto. Basicamente, o que o *canvas fingerprinting* faz é instruir o *browser* do visitante a desenhar uma imagem não visível. Como cada computador realiza a tarefa de modo diferente, do resultado extrai-se "uma persistente e durável impressão digital [*fingerprint*] sem o conhecimento do usuário" (ACAR et al., 2014, p.674, tradução nossa). O mesmo procedimento já vem sendo testado com outras tarefas, tornando os resultados ainda mais precisos e permitindo, inclusive, identificar o dispositivo mesmo quando o usuário alterna entre diferentes *browsers* (CAO; WIJMANS, 2017).

E quanto aos métodos de terceira geração? Sabe-se que estão em franco desenvolvimento, no horizonte não tão distante de muitas organizações. Sem dúvida, há muitos outros mecanismos de rastreamento que estão permanentemente coletando dados on-line. Não pretendemos esgotar o assunto, apenas colocar em evidência alguns desses objetos técnicos que, ordinariamente, são invisíveis e, quando deles se toma ciência, geralmente são caixas-pretas, objetos fechados dos quais pouco se compreende. Assim, é necessário hackeá-los – isto é, trazê-los à luz, abri-los e explorá-los para poder criar outras possibilidades de composição.

1.7 VIGILÂNCIA GENERALIZADA E DISTRIBUÍDA

No início da década de 1990, na *Phrack,* uma popular revista eletrônica hacker, Niel (1993) evocava a figura orwelliana do *Big Brother* para denunciar a vigilância realizada pelo governo norte-americano destacando que, já naquela época, o volume dos dados coletados e armazenados acerca de indivíduos específicos era consideravelmente grande. Cabe notar que a vigilância não recaía sobre todos – escolhiam-se alguns e não outros para serem observados – e nem era contínua – apenas algumas situações eram dignas de serem registradas –, sendo realizada, basicamente, pelo Estado. Como ele explica:

> Uma vez que você comete um crime, eles estão observando você. Eles atualizam o seu arquivo cada vez que há uma grande ocorrência em sua vida, ou seja, casamento, hospitalização, ingresso no exército, prática de outro crime etc. Se eles acham a menor probabilidade de suspeita, eles te investigam profundamente para acrescentar ainda mais ao seu arquivo. As pessoas nem sequer percebem quão grande é o arquivo que o FBI tem sobre elas (NIEL, 1993, sem paginação, tradução nossa).

Com os atentados de 11 de setembro de 2001, nos EUAs, tem-se uma importante reorganização das relações entre segurança e vigilância, já que esta não focaliza mais "populações e espaços classificados como perigosos ou suspeitos, mas se dirige a toda sorte de espaço público, semipúblico e privado" (BRUNO, 2013, p. 8). As ações e comunicações cotidianas tornam-se, cada vez mais, sujeitas a coleta, registro e análise. Ainda que alguns indivíduos e populações continuem a ganhar atenção especial, a vigilância não está mais restrita a eles, mas se difunde em todo o tecido social. Além disso, a vigilância não pode mais ser localizada apenas em um ou outro Estado, pois passa, cada vez mais, a envolver complexas tramas que podem incluir diferentes Estados, organizações e indivíduos. Outro aspecto a ser considerado é que, nas sociedades contemporâneas, a vigilância é distribuída, ou seja, "tende a tornar-se incorporada em diversos dispositivos, serviços e ambientes que usamos cotidianamente, mas que se exerce de modo descentralizado, não hierárquico e com uma diversidade de propósitos, funções e significações nos mais diferentes setores" (BRUNO, 2010, p.156). Assim, sua onipresença é tal que há aqueles que chegam a afirmar que não nos é mais possível escapar dos atuais mecanismos digitais de vigilância (HIJMANS, 2016).

Sem dúvida, o governo norte-americano ainda é um dos mais importantes atores a serem considerados quando se fala de vigilância. Neste sentido, as revelações de Edward Snowden acerca das práticas da Agência de Segurança Nacional dos Estados Unidos (NSA) não devem ser negligenciadas. Segundo ele, por meio do programa Prism, a NSA tinha acesso aos servidores de empresas como Microsoft, Yahoo, Google, Facebook, YouTube, Skype e Apple. Com o programa, a NSA poderia acessar e vasculhar as comunicações armazenadas e também acompanhar em tempo real as que estivessem ocorrendo (GREENWALD; MACASKILL, 2013). Além disso, como a internet depende de cabos de fibra óptica, os EUAs estariam em situação bastante favorável para realizar a interceptação de fluxos de dados de outros países latino-americanos, pois, como afirma Assange (2013, p.20-21):

> Não é segredo algum que, na internet, todos os caminhos que vão e vêm da América Latina passam pelos Estados Unidos. A infraestrutura da internet direciona a maior parte do tráfego que entra e sai da América do Sul por linhas de fibra óptica que cruzam fisicamente as fronteiras dos Estados Unidos. O governo norte-americano tem violado sem nenhum escrúpulo as próprias leis para mobilizar essas linhas e espionar seus cidadãos. E não há leis contra espionar cidadãos estrangeiros.

Como já dito, se antes as comunicações interceptadas eram restritas, selecionando aqueles que seriam alvo de vigilância, atualmente “se intercepta tudo e se armazena tudo permanentemente” (ASSANGE, 2013, p.57). Certamente, o Centro de Processamento de Dados de Utah, gerenciado pela NSA, cumpre um papel capital, pois é capaz de conservar volumes de dados equivalente à vários séculos do atual tráfego da internet e, também, de processá-los em velocidade inimaginável. De acordo com Bernard (2013, sem paginação, tradução nossa), seu propósito é “armazenar o conjunto das comunicações trocadas no planeta, desde e-mails e telefonemas particulares a buscas no Google, compra de livros, viagens aéreas, transações comerciais, além de segredos comerciais ou diplomáticos”.

1.8 Estratégias de Composição

Ainda que a vigilância seja distribuída – opera na internet, mas também fora dela por meio dos sensores, das câmeras de video-vigilância, etc –, os dados coletados são,

geralmente, armazenados de forma centralizada estando acessíveis a um número bastante restrito de atores, o que altera significativamente as relações de poder. Assim, muitos hackers levaram e ainda levam adiante práticas de anonimato que visam escapar às tentativas de identificação, cumprindo, não raro, um papel estratégico, inclusive no âmbito da resistência política. Para Bordeleau (2018, p.14, tradução nossa), essas práticas – que ele reconhece estarem presentes no *Anonymous*[42] – buscam "maximizar a eficácia de uma intervenção, escapar a possíveis perseguições judiciais ou evitar se expor em condições consideradas desfavoráveis".

Dentre tais práticas, está a dissimulação da identidade por meio de pseudônimos e até mesmo a tentativa de não ter a sua presença notada. Porém, o anonimato não implica estar escondido, deixar de ser visto. É justamente neste aspecto que, de acordo com Coleman (2012), desde a década de 1970, hackers, sem deixar de fazer uso do anonimato, estabelecem um modo bastante peculiar de composição com os mecanismos de vigilância. Cientes de estarem sendo acompanhados, inclusive por agentes governamentais que tinham interesse em capturá-los, eles deixam rastros para que sejam vistos, percebidos, escrevem mensagens direcionadas aos vigias, enfim, produzem performances. O espetáculo que criam deixa claro de que sabem que estão sendo vigiados e que, além disso, também estão vigiando aqueles que os vigiam. Assim, produz-se uma espécie de "jogo de gato e rato de vigilância e contra-vigilância" (COLEMAN, 2012, p.108, tradução nossa).

Uma problematização semelhante dos mecanismos de vigilância é levada a cabo pelo grupo *Surveillance Camera Players* ([1996]) que realiza performances diante das câmeras que estão dispostas em lugares públicos. Assumindo a posição de vigiados e realizando suas intervenções, o grupo cria condições para a produção de rupturas no modo pelo qual os transeuntes e os vigilantes se compõe com as câmeras, pois simultaneamente "perturbam não só a unilateralidade do olhar da câmera (que vê sem ser visto) como a relativa indiferença dos passantes e do fluxo

[42] *Anonymous* não atua sempre com o mesmo grupo de pessoas, "não é uma organização, não tem estrutura nem dirigentes [...] não é mais que o avatar de uma identidade coletiva" (PADILLA, 2012, p. 65, tradução nossa). É uma espécie de coletivo, ou melhor, multidão que se constitui para ações específicas na internet – e em outros espaços – por meio da adesão daqueles que concordam com o(s) objetivo(s) proposto(s), agindo de maneira coordenada, descentralizada e fazendo uso do anonimato.

urbano em relação a elas, produzindo uma perturbação no estado atencional regular dos espaços vigiados" (BRUNO, 2013, p. 115).

Assim como as performances do *Surveillance Camera Players* (Figura 01), há práticas hackers que também convocam uma experiência subjetiva que, não raro, está ausente da nossa relação cotidiana com os objetos técnicos. Isto é, são práticas que trazem tais objetos novamente para o nosso campo de sensibilidade, que nos colocam em movimento para (re)pensar o modo pelo qual nos relacionamentos com eles.

Figura 1 - Performances do *Surveillance Camera Players*

Fonte: Disponivel em: http://www.notbored.org/you-are-watching-me.jpg. Acesso em: 15 abr. 2019

Projetos como *Panopticlick*[43] – da *Eletronic Frontier Foundation* – e *Am I unique?*[44] – conduzido pelos pesquisadores Laperdrix, Rudametkin e Baudry (2016) também colocam os mecanismos de vigilância, e em especial os de rastreamento, em questão. São como que convites para que venhamos a tomar conhecimento tanto da existência quanto do modo como operam certos objetos técnicos com os quais frequentemente nos encontramos on-line. Nos sites dos projetos é possível verificar o quão único é o dispositivo por meio do qual estamos navegando, isto é, o quão fácil é identificá-lo entre tantos outros.

Uma série de elementos servem como subsídios para a análise e a identificação do internauta: dados do *user agent*, de fuso horário, de resolução de tela, *cookies*, fontes instaladas, *canvas fingerprinting*, etc. Por exemplo, como resultado de um teste realizado no *Am I unique?*, podemos descobrir que nosso *browser* está em condições de ser identificado unicamente entre outros 815.516, o que é um número expressivo. Apenas com o uso do *Tor Browser*[45] – um software livre e de código aberto – é possível alterar para 7.503 *browsers* entre 815.516, ocultando-se na massa e tornando a navegação um pouco mais anônima. Há, ainda muitas outras ferramentas – como, por exemplo, as extensões *NoScript*[46] e *Ghostery*[47] – que são produzidas e compartilhadas, contribuindo para transformar as relações com os rastreadores e mecanismos de identificação. Mais do que elencar as ferramentas existentes, nosso intuito é afirmar que outras modalidades de relação estão em nosso campo de possibilidades e que, além disso, tantas outras restam a ser inventadas.

Se o controle realizado por meio dos objetos técnicos é, progressivamente, naturalizado, os hackers, por meio de suas práticas, têm o potencial de nos deloscar, produzindo desvios e diferenças que podem transformar o nosso modo de perceber o mundo, que podem transformar a nossa sensibilidade. Ao resistirem aos mecanismos de poder e controle, objetos técnicos que antes nos passavam desapercebidos, podem receber luminosidade. E, ao abrirem os objetos técnicos fechados e disponibilizarem suas

[43] Disponível em: https://panopticlick.eff.org/. Acesso em: 26 fev. 2019.
[44] Disponível em: https://amiunique.org/. Acesso em: 26 fev. 2019.
[45] Disponível em: https://www.torproject.org/. Acesso em: 26 fev. 2019.
[46] Disponível em: https://noscript.net/. Acesso em: 26 fev. 2019.
[47] Disponível em: https://www.ghostery.com/. Acesso em: 26 fev. 2019.

criações, passamos a ter novas condições para outras composições que possam aumentar o nosso grau de liberdade.

2 TRATAMENTO DE DADOS, PRODUÇÃO DE CONHECIMENTO E GOVERNAMENTALIDADE

Neste capítulo, daremos prosseguimento à tarefa de descrever/mapear algumas redes de objetos técnicos, buscando compreender melhor como operam e de que modo participam de uma nova modalidade de governamentalidade que, por mais paradoxal que possa ser, é capaz de nos prometer bons encontros, desde que para isso, renunciemos à crítica e ao exercício deliberado de nossa autonomia. O que nos é proposto é que confiemos cegamente em tais objetos técnicos – geralmente opacos –, delegando-lhes àqueles que lhes programam/controlam grande parte de nossas decisões.

Caberia, sem dúvida, retomarmos uma das máximas hackers que diz: “Desconfie da autoridade” (LEVY, 2012b, p.27). O que os primeiros hackers questionavam, de acordo com Levy (2012b), eram os burocratas que ocupavam uma posição na qual davam ordens que deveriam ser seguidas sem questionamentos. É o princípio da crítica, em uma das suas modalidades, que os hackers atualizavam e, por vezes, continuam a atualizar. Trata-se de problematizar aquilo que produz efeitos sobre nós, que nos constitui, aquilo que visa conduzir nossas condutas. Desconfiar da autoridade não é, portanto, a simples negação de toda e qualquer autoridade. Antes, o que está em jogo são os modos pelos quais queremos ou não ser conduzidos, as forças pelas quais queremos ou não ser afetados.

2.1 A *CAMBRIDGE ANALYTICA*

Os rumos de dois grandes eventos políticos, o referendo do Brexit e a eleição presidencial norte-americana, ambos em 2016, não teriam sido os mesmos sem a ativa participação da *Cambridge Analytica*, uma empresa que atuou de modo a combinar a mineração de grandes quantidades de dados, a produção de perfis psicológicos e o marketing elaborado e direcionado de acordo com a personalidade do público-alvo.

O algoritmo utilizado pela *Cambridge Analytica* foi produzido a partir do modelo *Big Five*, que aponta a existência de cinco grandes dimensões da personalidade analisadas por meio dos seguintes fatores: Extroversão, Neuroticismo, Socialização,

Realização e Abertura à experiência. Enquanto características psicológicas, tais traços podem ser usados, de acordo com Silva e Nakano (2011, p.52), para “resumir, prever e explicar a conduta de um indivíduo”.

Mas como produzir tal saber acerca dos sujeitos? Tradicionalmente a psicologia tem utilizado testes psicométricos, situação na qual o avaliador e o avaliado encontram-se presencialmente em um mesmo lugar previamente preparado e adequado ao procedimento em questão. O primeiro orienta e instrui enquanto o segundo realiza as tarefas, responde a questões e/ou produz textos ou desenhos. A determinação espaço-temporal é clara e, na grande maioria dos casos, ambos têm ciência da finalidade da atividade realizada.

Com o lançamento no Facebook, em 2007, do aplicativo *myPersonality*, os internautas passaram a poder se submeter a um teste psicométrico on-line – um questionário padrão *Big Five* – que lhes dava o resultado instantaneamente. Eles também eram convidados, por meio do *opt-in*, a compartilhar, com os pesquisadores que mantinham o teste, suas respostas e dados de seus perfis no Facebook (THE PSYCHOMETRICS CENTRE, [*s. d*.], sem paginação; MYPERSONALITY..., 2018). Os dados cedidos foram então agregados formando um grande conjunto que Bachrach et al. (2012, p.1, tradução nossa) analisaram e puderam constatar a existência de correlação entre a

> [...] personalidade dos usuários e as propriedades de seus perfis no Facebook, tais como o tamanho e a densidade da sua rede de relacionamentos, o número de fotos enviadas, o número de comparecimento em eventos, o número de grupos dos quais é membro e o número de vezes em que o usuário foi marcado em fotos.

A pesquisa de Kosinski, Stillwell e Graepel (2013) também fez uso dos dados compartilhados pelos pesquisadores que criaram o *myPersonality*. Eles mostraram que os likes – isto é, curtidas – no Facebook poderiam predizer de forma bastante precisa, além dos traços de personalidade, atributos pessoais tais como: orientação sexual, etnia, visão religiosa e política, uso de substâncias (álcool, drogas, cigarro), separação parental, satisfação com a vida, idade, gênero, status de relacionamento etc. E não são necessários muitos likes de um usuário para que um algoritmo possa encontrar resultados satisfatórios. Youyou, Kosinski e Stillwell (2015), a partir de seus achados,

argumentam que com apenas dez likes o algoritmo que desenvolveram é capaz de avaliar uma pessoa melhor que seu colega de trabalho; com 70 likes, melhor que um amigo; e com 300, melhor que seu cônjuge.

A ferramenta que a *Cambridge Analytica* fez uso nas eleições em que Trump foi eleito e no referendo em que o Brexit foi aprovado é uma caixa-preta. A maior parte de suas engrenagens não estão disponíveis, mas podemos inferir que ela possui grandes semelhanças com os programas utilizados nas pesquisas acima citadas. Inclusive, Michal Kosinski suspeita de que Aleksandr Kogan tenha copiado e revendido à *Cambridge Analytica* as ferramentas que ele e sua equipe desenvolveram e faziam uso em 2014 (GRASSEGGER; KROGERUS, 2017). Com elas, a *Cambridge Analytica* foi além do modo tradicional de conduzir condutas nas eleições, isto é, abordando os eleitores a partir de recortes sociodemográficos (sexo, faixa etária, grau de escolaridade, renda familiar etc). Na verdade, a partir dos dados analisados foram produzidos conteúdos publicitários (sites, blogs, correspondências, e-mails, vídeos, postagens em mídias sociais) de modo direcionado a vilas, a bairros e, até mesmo, a indivíduos considerando, através do *Big Five*, a personalidade de seus alvos (GRASSEGGER; KROGERUS, 2017; ALEXANDER NIX..., 2017).

O próprio CEO da *Cambridge Analytica*, Alexander Nix, referindo-se a uma imagem publicitária na qual alguém está quebrando uma porta ou janela de vidro com sua mão, utilizando uma luva preta – dando a entender que se trata de um intruso –, esclarece: "Para um público altamente neurótico e consciente, apresentamos a ameaça de um roubo e comparamos uma arma à uma apólice de seguro" (CAMBRIDGE..., 2016). E, ao indicar outra imagem, na qual um homem e uma criança estão no campo, ao pôr do sol, com um clima afetivo aparentemente agradável, ambos portando armas de caça, ele diz: "Por outro lado, essa é a propaganda que apresentamos para um público fechado e amável, pessoas que se preocupam com tradições, hábitos e família" (CAMBRIDGE..., 2016).

De acordo com Alexander Nix – o que pode ser exagerado –, com dados obtidos das mais diversas fontes, todos os adultos dos Estados Unidos – 220 milhões de pessoas – tiveram, em maior ou menor medida, sua personalidade avaliada pela *Cambridge Analytica* (CAMBRIDGE..., 2016; GRASSEGGER; KROGERUS, 2017). Mesmo que esse

número não seja real, a dimensão daqueles que podem ter sido avaliados pelos algoritmos da *Cambridge Analytica* é surpreendente, isto se consideramos apenas os dados (subestimados) das contas do Facebook que foram violados: 87 milhões de contas, sendo que destas 443.117 são de usuários brasileiros (VAZAMENTO..., 2018).

Para se ter uma ideia do fluxo de dados que produzimos na plataforma do Facebook, assim como tais dados podem estar sendo analisados, basta instalar no *browser* a extensão *Data Selfie*[48]. Quando ativado, o programa roda em *background* enquanto o internauta interage na rede social. Ele grava dados tais como: o que é digitado, o tempo gasto nas postagens dos amigos e em outras páginas, o que é visualizado, os cliques e likes. Em uma segunda etapa, todos os dados são primeiramente anonimizados para remover informações pessoais e, depois, submetidos pelos servidores do *Data Selfie* a dois programas de *machine learning*: o *IBM Watson* e o *Apply Magic Sauce*. O primeiro é utilizado para analisar os seguintes aspectos:

- *Personality Insights* que, por meio de dados de mídias sociais e transacionais, identifica "traços psicológicos que determinam decisões de compra, intenção e traços comportamentais" (IBM Cloud, 2016a);
- *Tone Analyzer* que, por meio da análise linguística, detecta "três tipos de sinais, incluindo emoção (raiva, repugnância, medo, alegria e tristeza), propensões sociais (sinceridade, escrupulosidade, extroversão, amabilidade e faixa emocional) e estilos de texto (analítico, confiante e hesitante)" (IBM Cloud, 2016b).

Com base nos *digital footprints*, o segundo programa – o *Apply Magic Sauce* – prevê características psico-demográficas tais como personalidade, satisfação com a vida, inteligência, visões políticas e religião (UNIVERSITY OF CAMBRIDGE PSYCHOMETRICS CENTRE, [s.d.]).

O *Data Selfie*, segundo seus criadores, tem por intenção "fornecer uma perspectiva pessoal sobre mineração de dados, analítica preditiva e nossa identidade de dados online – incluindo informações inferidas a partir de nosso consumo" (DATA X, [s.d.], tradução nossa). Diferentemente do Facebook e outras plataformas, o *Data Selfie*

[48] Disponível em: https://dataselfie.it. Acesso em: 26 fev. 2019.

não retém e nem armazena os dados de seus usuários. Além disso, o programa é gratuito e o código-fonte é aberto, ou seja, está disponível para a comunidade (DATA..., [2018]).

O caso da *Cambridge Analytica* nos coloca de imediato a questão da condução de condutas por meio desses novos objetos técnicos que são os algoritmos que mineram dados do Big Data. Lembrando que se pesquisadores como Kosinski solicitaram o consentimento dos usuários do Facebook para trabalharem com seus dados, "hoje muitos aplicativos e questionários online requerem acesso a dados privados como pré-condição para realizar testes de personalidade" (GRASSEGGER; KROGERUS, 2017, sem paginação, tradução nossa). Isto é, muitas vezes antes mesmo de saber do que se trata o aplicativo, o usuário precisa aceitar os "Termos e Condições", submetendo-se à situação de ter seus dados coletados e, frequentemente, minerados, compartilhados, revendidos etc.

O jogo satírico *Cow Clicker*[49]*,* por exemplo, foi um experimento-intervenção cuja atividade consistia, basicamente, em clicar na imagem de uma vaca e também convidar os amigos para participar do jogo. Bogost (2018), o criador do jogo, relata que mesmo sem ter otimizado o *Cow Clicker* para coletar dados, o próprio Facebook disponibilizava e enviava para ele dados sensíveis dos jogadores. Neste caso, a proposta não era coletar dados e ainda assim o desenvolvedor os recebia. Mas e quanto aos inúmeros apps que têm por função principal a coleta de dados, ao que eles têm acesso? Que dados acerca de nós, de nossos hábitos, de nossos comportamentos, de nossas relações sociais eles possuem?

Sem dúvida, há uma infinidade aplicativos gratuitos e pagos que estão cobrando o seu preço: nossos dados. E uma vez que os tenhamos fornecido, ainda que venhamos a revogar as permissões anteriormente concedidas, não há nenhuma garantia de que os dados armazenados serão excluídos. Até porque, como afirma Pariser (2012, p.189), "os dados são facilmente vendidos no mercado negro, pois não carregam consigo nenhum indício sobre o local de onde vieram ou por onde passaram pelo caminho". Koebler (2018, sem paginação) chega a afirmar que "é tarde demais. Se seus dados já foram obtidos, o Facebook não possui mecanismos nem energia para fazer com que as pessoas o excluam". E mesmo que nunca tenhamos fornecido os nossos dados, é bem provável

[49] Disponível em: http://www.cowclicker.com/. Acesso em: 26 fev. 2019.

que, mesmo sem saber, algum amigo ou conhecido tenha compartilhado parte deles nas redes sociais. Assim, seria sensato supor que muitos de nossos dados já circulam pelo mercado, sendo negociados, minerados, utilizados para ações de marketing digital etc.

É quase nulo o número de pessoas que chega a ler os termos na totalidade e com dedicação antes de aceitá-los. Quem já passou, ao menos, os olhos nos termos do Facebook, do Gmail e do WhatsApp? Segundo um levantamento publicado na Folha de São Paulo (HERNANDES, 2017), apenas para ler os termos desses três seriam necessárias quatro horas e meia – o que não garante a compreensão, pois a linguagem em que estão escritos é bastante técnica, escapando àquela que a maioria das pessoas estão habituadas. Os termos cumprem assim, dentre outras funções, a de barreiras que tornam tais plataformas e aplicativos objetos técnicos fechados. Ao invés de esclarecerem aos usuários as regras do jogo, eles as escondem, tornando-as obscuras.

2.2 A Mineração de Dados e a Produção de Perfis

A produção, a coleta e o armazenamento de fluxos de dados, mesmo que em um grande volume, teriam poucos efeitos na condução de condutas se não estivessem articulados aos processos de mineração de dados [*data mining*] e da produção de perfis [*profiling*]. Por mineração de dados, podemos entender, de acordo com o relatório do *United States General Account Office* (2004, p.1, tradução nossa), “a aplicação de tecnologia e técnicas de banco de dados – tais como análise estatística e modelagem – para descobrir padrões ocultos e relacionamentos sutis nos dados e para inferir regras que permitem predizer resultados futuros”.

Assim, com o *data mining* quantidades massivas de dados podem ser tratadas automaticamente – ou com um mínimo de intervenção humana – por meio de algoritmos, fazendo emergir correlações que só se tornam visíveis a partir do processamento computacional e que, além disso, permitem antecipar eventos futuros. Estamos, sem dúvida, diante da produção de saber que, como todo saber, “acarreta efeitos de poder” (FOUCAULT, 1979, p.142).

Trata-se de um uso muito peculiar da estatística, isto é, não se trata de descrever amostras ou populações – como na epidemiologia – e, nem mesmo, de testar hipóteses

que podem ser comprovadas ou invalidadas – como na aplicação de modelos de regressão. Antes, a produção de saber, indiferente às causas dos fenômenos, é ancorada, sobretudo, na observação de correlações estatísticas entre dados, geralmente não triados, e coletados de variados contextos heterogêneos (ROUVROY, 2012; ROUVROY; BERNS, 2010).

Assim, torna-se possível, em alguma medida, antecipar as ações humanas como votar ou deixar de votar, comprar ou deixar de comprar, pagar ou deixar de pagar etc. Uma das áreas nas quais a mineração de dados tem sido utilizada é na análise preditiva e preventiva de crimes. O filme Minority Report (2002) – no qual três videntes, denominados “precogs”, são capazes de prever a ocorrência de crimes, dando condições para que policiais possam agir antecipadamente para evitá-los – já não é mais apenas ficção. O Departamento de Polícia de Santa Cruz possui e faz uso de um programa capaz prever quando e onde crimes poderiam vir a ser cometidos (GOODE, 2011).

Não se está em questão qual é a causa dos crimes, nem o porquê de se comprar determinados produtos e não outros, nem mesmo as motivações para se escolher um candidato, o outro ou nenhum deles. Não há referência a hipóteses exteriores e, se há hipóteses, como na aprendizagem de máquina [*machine learning*], elas emergem dos próprios dados – são a eles imanentes. Nada a explicar, apenas a produção de saberes acompanhada da ação sobre ações que não existem a não ser em forma de germe, seja no intuito de efetuá-las, seja de evitá-las. Por exemplo, no caso da *Cambridge Analytica* buscava-se tanto produzir votos para Trump como agir para reduzir as possibilidades de que pessoas que pretendiam votar em Hillary concretizassem sua intenção.

Como já temos indicado, o registro dos dados por *default* não incide apenas nos indivíduos, mas também coletivamente e, ainda mais, em todo e qualquer aspecto do mundo. É a partir dos inúmeros rastros, dos traços que não precisam estar atrelados a indivíduos específicos e identificáveis, que se produzem os perfis. Para a produção de perfis, o que se faz necessário são justamente os fragmentos infra-pessoais da existência cotidiana – a frequência de um determinado ato, a trajetória de um corpo, a presença ou ausência de algum elemento etc. É a partir de vários dados que não estão no nível individual, mas infra-individual, que se produzem “modelos de comportamentos, ou perfis,

aos quais correspondem, por certas combinações de traços a cada vez específicos, uma multidão de pessoas" (ROUVROY, 2014, p.3, tradução nossa).

Para Rouvroy (2014), não é a história individual, a trajetória pessoal, as conquistas e fracassos que alguém tem em sua vida que seriam os dados de maior valor no novo tipo de governo que está emergindo. Isto é, a discussão acerca do anonimato e da evitação dos mecanismos de identificação – que vínhamos fazendo até o momento – encontra seus limites quando comparada ao que se pode fazer com os fluxos de dados produzidos em nossos encontros com os objetos técnicos.

Para a autora, mesmo a NSA, a Amazon, o Google e o Facebook estão menos interessados em nós enquanto indivíduos do que enquanto "agregados de dados temporários exploráveis em massa, à escala industrial, uma vez descontextualizados, purificados de tudo aquilo que poderia relacioná-los a isto que faz a singularidade de uma vida" (ROUVROY, 2014, p.3, tradução nossa). É indiferente se são os nossos dados ou de nosso vizinho, o que está em jogo na construção dos modelos ou perfis não são os dados advindos desta ou daquela pessoa em específico, mas o volume, a grande quantidade de indivíduos dos quais os dados são provenientes.

O que tem relevância nesse plano de análise não são mais apenas os dados sensíveis – a idade, o sexo, a renda, o estado de saúde, opiniões políticas, a religião etc. –, mas todo e qualquer dado, inclusive aqueles mais triviais aos quais não nos importamos em ceder ou compartilhar. Mesmo garantindo-se o anonimato individual, por meio da mineração de dados e da produção de perfis é possível produzir um saber de outra ordem, isto é, que ao fazer uso de dados infra-pessoais produz modelos supra-individuais, de categorizações impessoais, pautados, sobretudo, em correlações. Um perfil não é uma pessoa, ninguém corresponde totalmente a um perfil e, ao mesmo tempo, nenhum perfil visa unicamente a uma única pessoa identificável. Antes, os perfis são saberes que "permitem modelizar os comportamentos, atitudes, trajetórias e eventos do mundo de modo mais detalhado e preciso à medida que a quantidade de dados disponíveis cresce" (ROUVROY, 2014, p.10, tradução nossa).

Estamos diante de uma nova forma de operação do poder que, segundo Deleuze (1992a, p.220), poderá nos fazer parecer os confinamentos mais duros – característicos do poder disciplinar – "um passado delicioso e benevolente". Ele próprio, ao descrever

as transformações que vivemos, afirma que “por toda parte o *surf* já substituiu os antigos *esportes*” (DELEUZE, 1992b, p.227). Isto é, enquanto as disciplinas tinham por principal técnica o confinamento, no qual os sujeitos eram moldados em formas específicas (a prisão fabricando o prisioneiro, a escola o estudante, a fábrica o operário etc.), nas novas formas de poder – que operam por controle contínuo e comunicação instantânea – os moldes deixam lugar para a modulação, ou seja, são como “uma moldagem autodeformante que mudasse continuamente, a cada instante, ou como uma peneira cujas malhas mudassem de um ponto a outro” (DELEUZE, 1992b, p.225). E, além disso, enquanto nas disciplinas as estratégias e técnicas de governo eram mais facilmente localizáveis, em nossos dias “por seu caráter sutil, indireto e plural, subjetivam-nos sem que nos apercebamos da sua atuação” (HENNIGEN, 2006, p.47).

Assim, pode-se dizer que os perfis mais eficazes não aqueles que possuem moldes duros, ou seja, associados às características sócio-demográficas mais estáveis. Antes, são os perfis produzidos por meio de aprendizagem de máquina*,* a partir de dados infra-individuais e continuamente ajustados, que são mais úteis na condução de condutas. Tais perfis são capazes de acompanhar o movimento das ondas, exigindo-nos práticas de liberdade que, por vezes, não são mais aquelas que funcionavam diante do poder disciplinar. Isso não significa que o exercício da liberdade não possa ocorrer. Deleluze (1992a), em entrevista à Antonio Negri, faz uma rápida menção ao aparecimento de novas formas de delinquência e resistência, das quais oferece como exemplo a pirataria e os vírus de computador, práticas comumente associadas aos hackers. O filósofo imagina que essas “substituirão as greves e o que no século XIX se chamava de 'sabotagem' (o tamanco – *sabot* – emperrando a máquina)” (DELEUZE, 1992a, p.221). Trata-se não só de afirmar que as antigas estratégias de luta contra as disciplinas têm seus limites como também que nos cabe compreender “que poderes é preciso enfrentar e quais são as nossas possibilidades de resistência hoje” (DELEUZE, 2005, p.123).

2.3 NETFLIX E OS SISTEMAS DE RECOMENDAÇÃO

A Netflix está no Brasil desde 2011 e, atualmente, oferta o serviço de *streaming* para mais de 130 países. Muito do seu sucesso pode ser explicado pelos seus algoritmos de recomendação de filmes, séries e documentários. O usuário, ao acessar a Netflix, recebe uma espécie de matriz – com linhas e colunas – na qual constam sugestões para assistir. Decidir o que será exibido ao usuário não é uma tarefa fácil, pois há milhares de possibilidades no catálogo e é justamente nisto que os algoritmos trabalham: selecionado aqueles conteúdos que mais poderiam agradar a cada um dos seus mais de 75 milhões de assinantes (BARRETT, 2016b).

Percorrer título por título para encontrar algo que interesse pode ser uma tarefa enfadonha para quem está buscando algo para assistir. Boas indicações são, portanto, cruciais para que o usuário encontre algo que lhe agrade, e isto da forma mais rápida possível. De acordo com Gomez-Uribe e Hunt (2015, p.2, tradução nossa),

> Pesquisas sobre consumidores sugerem que um típico usuário da Netflix perde o interesse após aproximadamente 60 a 90 segundos de pesquisa, tendo visto de 10 a 20 títulos (talvez 3 em detalhe) em uma ou duas telas. O usuário ou encontra alguma coisa interessante ou o risco de ele abandonar nosso serviço cresce substancialmente. O problema de recomendação é garantir que nas duas telas, cada usuário, na diversidade de sugestões oferecidas, encontrará algo atrativo para assistir e saberá porque tal escolha poderá ser interessante.

Supõe-se, assim, que a melhor situação é aquela na qual o tempo entre o acesso à plataforma e o início da exibição do conteúdo seja próximo de zero. O usuário ideal seria aquele que nem se daria ao trabalho de procurar um filme, uma série ou um documentário, mas que apenas se conectasse a uma transmissão ininterrupta e continuamente personalizada para ele. O que a Netflix busca capturar e manter é a nossa atenção, ligando-a diretamente aos seus conteúdos e mantendo-nos em uma situação de excitação visual e sonora permanente. Mas não seria justamente assim – continuamente atravessados pelos estímulos, sempre mobilizados – que nos tornamos incapazes de silêncio, distantes daquelas situações nas quais algo nos acontece, isto é, quanto o inusitado nos assalta, nos pega desprevenidos? Como sugere Bondía (2002, p.21), “dir-se-ia que tudo o que se passa está organizado para que nada nos aconteça”. E ele acrescenta que para que haja experiência, e algo nos toque, algo se passe com a gente, é requerido

> um gesto de interrupção, um gesto que é quase impossível nos tempos que correm: requer parar para pensar, parar para olhar, parar para escutar, pensar mais devagar, olhar mais devagar, e escutar mais devagar; parar para sentir, sentir mais devagar, demorar-se nos detalhes, suspender a opinião, suspender o juízo, suspender a vontade, suspender o automatismo da ação, cultivar a atenção e a delicadeza, abrir os olhos e os ouvidos, falar sobre o que nos acontece, aprender a lentidão, escutar aos outros, cultivar a arte do encontro, calar muito, ter paciência e dar-se tempo e espaço (BONDÍA, 2002, p.19).

É esta pausa, ou redução de velocidade, que dificilmente encontramos nos algoritmos de recomendação, pois, em sua grande maioria, estão, a cada passo, incitando-nos a preencher nosso tempo e a nossa vida, agitando-nos sem parar. Os algoritmos de recomendação buscam organizar, cada vez mais, os nossos encontros, conduzindo-nos e deixando pouco espaço para que o imprevisto aconteça.

As respostas nos são dadas antes mesmo que possamos formular as perguntas, a busca e seu resultado tendem a confundir-se de tal maneira que o trajeto da busca tende a desaparecer em proveito dos achados que nos são oferecidos. Talvez fosse interessante não encontrar nada para que pudéssemos permanecer submersos na busca, para que pudéssemos nos demorar na procura, criando condições para encontros inusitados.

Importa esclarecer ainda que os algoritmos de recomendação criam um universo de informações e experiências exclusivo para cada um de nós, reduzindo o espaço para encontros fortuitos que nos trazem novas percepções e aprendizados. Trata-se daquilo a que Pariser (2012) denomina de “bolha dos filtros”, ou seja, a construção desses mundos que tendem a priorizar a apresentação daquilo que interessa àqueles que possuem perfis semelhantes aos nosso. Neste sentido, ele assinala o risco que tais algoritmos de recomendação trazem consigo ao selecionarem o iremos ver, ler, ouvir, fazer, etc.:

> Por definição, um mundo construído a partir do que é familiar é um mundo no qual não temos nada a aprender. Se a personalização for excessiva, poderá nos impedir de entrar em contato com experiências e ideias estonteantes, destruidoras de preconceitos, que mudam o modo como pensamos sobre o mundo e sobre nós mesmos (PARISER, 2012, p.19).

Assim, as chances de nos depararmos com que é muito diferente de nós é cada vez menor. Quanto mais eficazes forem os filtros de recomendação, maiores são as

chances de que sejamos reforçados nos pontos de vista que já temos, apresentando-nos ideias com as quais já estamos familiarizados (e que, provavelmente, também concordamos). Em última instância, o que se excluí do campo da experiência são os encontros radicais, aqueles que são capazes de nos deslocar de nossas certezas, de nossos hábitos e de nossos enraizamentos. A abertura à alteridade deixa de ser estimulada e, dentre a infinidade dos bons encontros, somente alguns passam a estar disponíveis, isto é, aqueles com os quais já estamos acostumados.

De modo simples, o problema da recomendação realizada pela Netflix pode ser pensado como equivalente ao problema de predizer o número de estrelas, em uma escala de 1 a 5, que uma pessoa poderia dar para um vídeo após assisti-lo. Produzir algoritmos capazes de realizar o feito com precisão e acurácia é tão importante que, em 2009, a Netflix lançou um concurso oferecendo o prêmio de 1 milhão de dólares para quem apresentasse uma solução que fosse apenas 10% melhor do que o algoritmo que ela já empregava. Parte dos algoritmos desenvolvidos no concurso é, inclusive, utilizada até hoje na empresa para prever classificações (GOMEZ-URIBE; HUNT, 2015; NETFLIX, 2009).

Poderíamos cogitar que a empresa valoriza traços individuais como o sexo, a idade e a localização de seus clientes para filtrar os conteúdos que lhes serão sugeridos. Tal suposição, entretanto, é falsa (BARRETT, 2016b). Isto porque um jovem, brasileiro e universitário, pode ter seu interesse por documentários muito mais próximo de uma senhora indiana que já passou dos 80 anos e que cuida de seus netos, do que de seu colega de turma que mora na mesma cidade que ele.

Não são apenas as avaliações realizadas – as estrelas dadas a algum conteúdo – que servem de *input* para os algoritmos da Netflix. Os dados a partir dos quais os algoritmos são desenvolvidos são variados e em grande quantidade. Dizem respeito aos conteúdos assistidos, o dispositivo utilizado para assistir, o dia e a hora em que o usuário assistiu os conteúdos, a frequência que assiste, as pesquisas/buscas realizadas etc. Para produzir o perfil de um usuário, um modelo capaz de predizer o que irá lhe agradar, a Netflix faz uso não de um, mas de vários algoritmos: o *Personalized Video Ranker*, o *Top-N Video Ranker*, o *Trending Now*, o *Continue Watching*, o *Video-Video Similarity*, o *Page Generation*, entre outros (GOMEZ-URIBE; HUNT, 2015).

Apenas no ano de 2015 a Netflix realizou 160 testes A/B, sobretudo com novos consumidores, cada um representando de 2 a 20 experiências diferentes (BARRETT, 2016a). A cada teste os algoritmos podem se transformar, tornando-se mais eficazes em realizar predições. Tais objetos técnicos não são engessados, mas altamente dinâmicos, flexíveis, aptos a terem seu próprio modo de operar modificado. Eles evoluem junto com aqueles sobre os quais agem, seus acertos e erros são incorporados, sempre no sentido de aperfeiçoá-los. Em 2015, o sistema de recomendações da Netflix já era responsável por aproximadamente 80% dos conteúdos assistidos, sendo que apenas os outros 20% são acessados a partir das buscas realizadas pelo usuário na plataforma. Além disso, 2 de cada 3 horas de conteúdo assistido são decorrentes das recomendações apresentadas pelos algoritmos na tela inicial (GOMEZ-URIBE; HUNT, 2015).

Apesar da complexidade da metodologia utilizada pela Netflix – que ainda é, em sua maior parte, uma caixa-preta –, Wheelan (2016, p.88) esboça um "quadro geral", um desenho esquemático do modo pelo qual seus mecanismos operam:

> No nível mais básico, a Netflix está explorando o conceito de correlação. Primeiro, eu avalio um conjunto de filmes. A Netflix compara minhas avaliações com as de outros clientes para identificar aqueles cujas avaliações estejam altamente correlacionadas com as minhas. Esses clientes tendem a gostar dos filmes que eu gosto. Uma vez estabelecido isso, a Netflix pode recomendar filmes que receberam alta avaliação de clientes de mentalidade semelhante à minha, mas que eu ainda não assisti.

Eis o ponto crucial: a produção de saberes a partir de correlações estatísticas. Não há implicação de causalidade, pois uma associação positiva ou negativa entre duas variáveis não significa necessariamente que a variação em uma delas esteja causando a variação na outra – apenas se mede o grau em que dois fenômenos estão relacionados entre si. A correlação não demanda um outro plano explicativo, não faz menção a algo anterior, a um fundamento precedente. Antes, é no mesmo plano que ela se afirma[50]. Se, por um lado, a correlação não tem poder explicativo, por outro, tem poder preditivo. É preciso esclarecer que não se trata apenas de previsão, mas também, e sobretudo, de intervenção, de condução de condutas.

[50] Para Taurion (2015, p. 24), ao lidarmos com grandes volumes de dados no Big Data, "saímos do modelo '*hypothesis-driven*', onde tentamos provar nossa hipótese analisando dados específicos com perguntas específicas, para '*data-driven*', onde submetemos um imenso e variado volume de dados a algoritmos de correlação".

Sistemas de recomendação não são utilizados apenas pela Netflix. Quase todos os serviços de *streaming*, de pesquisa, as redes sociais, os *e-commerce* e diversas outras plataformas os utilizam. Sob as palavras “personalização” e “customização” ocultam-se mecanismos de governamentalidade. Como bem assinala Alexander (2016, p.87, tradução nossa),

> [...] esses processos [levados adiante pelos algoritmos] estão longe de ser transparentes; de fato, a maioria dos usuários ou desconhecem o fato que seus hábitos de visualização estão sendo constantemente documentados, ou são incapazes de traçar, acessar e compreender os numerosos modos nos quais suas ações estão sendo traduzidas em recomendações.

O que encontramos nas plataformas são arquiteturas de escolha construídas pelos desenvolvedores que não são, necessariamente, alinhadas com os interesses dos utilizadores. São mecanismos por meio dos quais o usuário é incitado “a não se distanciar da regra por padrão [*par défaut*]” (ROUVROY, 2014, p.7, tradução nossa). Isto não significa que não possam existir bons encontros. A Netflix e a Amazon, assim como outras plataformas que utilizam sistemas de recomendação, podem sugerir filmes, documentários, livros, entre outros produtos com os quais podemos ter encontros alegres, tecendo boas composições. A questão que queremos problematizar, entretanto, é outra: qual é o espaço de liberdade que temos para selecionar tais encontros, já que as escolhas já são previamente feitas pelos algoritmos (a partir de um conjunto de possibilidades já dadas)? E, como cada escolha é, ao mesmo tempo, a exclusão de tantas outras, o que está sendo retirado do nosso campo de possibilidades? São os algoritmos que fazem uma pré-seleção dos conteúdos com os quais poderemos ou não compor, e que irão ou não se articular aos nossos aspectos infra-individuais, com nossa sensibilidade e nossa atenção.

2.4 Servidão Maquínica e Sujeição Social

Como já nos ensinou Foucault (2010, p.30), não há produção de “saber que não suponha e não constitua ao mesmo tempo relações de poder”. Tais relações de poder-saber, na governamentalidade algorítmica, são, de acordo com o pensamento de Rouvroy, inassimiláveis aos regimes de poder da soberania e da disciplina analisados

pelo filósofo. Essa nova modalidade de poder não se baseia nem na lei nem na norma. Na verdade, ela não tem por alvo nenhum sujeito individuado, pois

> [...] ela contorna e evita os sujeitos humanos reflexivos, ela se alimenta de dados infra-individuais insignificantes neles mesmos, para produzir modelos de comportamento ou perfis supra-individuais, sem jamais convocar o sujeito, sem jamais o obrigar a dar conta por si mesmo daquilo que ele é nem daquilo que ele poderia vir a ser (ROUVROY; BERNS, 2013, p.174, tradução nossa).

A governamentalidade algorítmica não se dirige nem ao sujeito individuado nem à pessoa, pois para governar – isto é, para estruturar o campo de ações possíveis –, indivíduos capazes de entendimento, de vontade, de reflexão, de enunciação não são mais nem pressupostos nem requeridos (ROUVROY, 2011; FROIDEVAUX; ABITEBOUL, 2016). Se os sujeitos existem na governamentalidade algorítmica é “de maneira infra-individual (fragmentada em diversos bancos de dados) ou supra-individual (os ‘perfis’ não se endereçam jamais a não ser para conjuntos de indivíduos, ou, mais exatamente, para conjuntos de comportamentos) ” (ROUVROY, 2011, sem paginação, tradução nossa).

Nem mesmo o sujeito produzido no modo de governo neoliberal é interpelado pela governamentalidade algorítmica. Esta não o incita a ser empresário de si mesmo, a se autocontrolar, a avaliar-se continuamente. Antes, ela ignora a consciência e o pensamento, operando, por meios dos perfis, em indivíduos e grupos, no modo de alerta e de respostas reflexas. A governamentalidade algorítmica atua, portanto, em um “sujeito” supra-individual – constantemente reconfigurado – feito de traços digitais heterogêneos, impessoais e infra-individuais. As recomendações automatizadas funcionam frequentemente sobre as lógicas relativamente opacas, dificilmente traduzíveis em uma forma narrativa e inteligível, e buscam “curto-circuitar os processos através dos quais nós construímos e revisamos nossas escolhas” (ROUVROY, 2016 apud FROIDEVAUX; ABITEBOUL, 2016, sem paginação, tradução nossa).

O modo de funcionamento da governamentalidade algorítmica, descrita por Rouvroy e Berns (2013), guarda bastante proximidade com o conceito de servidão maquínica, que Lazzarato (2014) retoma dos escritos de Deleuze e Guattari. Tal conceito aparece em conjunto com o de sujeição social, sendo que, por meio de ambos, os autores buscam pensar a produção de subjetividade no capitalismo. Mas o que são a servidão maquínica e a sujeição social? Esta diz respeito aos processos pelos quais somos

dotados de “uma subjetividade, atribuindo a nós uma identidade, um sexo, um corpo, uma profissão, uma nacionalidade e assim por diante […] ela fabrica sujeitos individuados, sua consciência, representações e comportamentos”, aquela, por sua vez, “desmantela o sujeito individuado, sua consciência e suas representações, agindo sobre os níveis pré-individual e supraindividual” (LAZZARATO, 2014, p. 17).

A servidão maquínica consiste, conforme Lazzarato (2008, p.114, tradução nossa),

> [...] na modulação dos componentes pré-individuais, pré-cognitivos e pré-verbais da subjetividade, fazendo funcionar os afetos, as percepções, as sensações ainda não individuadas, ainda não atribuíveis a um sujeito, etc., como elementos de uma máquina.

Quando anteriormente abordamos a relação entre usuários e desenvolvedores, clientes e fabricantes, estávamos discorrendo acerca de processos de sujeição social aos quais, como vimos, encontravam resistências entre os hackers que, com suas práticas, desestabilizam as relações de poder assim constituídas. Com os hackers, não se tratava de recusar-se a ocupar a posição de usuário para ocupar a posição de desenvolvedor, mantendo a relação assimétrica entre ambas. Antes, tratava-se de afirmar um outro modo de vida que desfaz tal divisão. É contrapondo-se às relações de sujeição que Nelson (1974) lança *Computer Lib/Dream Machine*, considerado “o épico da revolução dos computadores, a bíblia do sonho hacker” (LEVY, 2012b, p.164). O livro tem por subtítulo “Você pode e deve compreender os computadores AGORA” (NELSON, 1974, tradução nossa), um chamado para que as pessoas deixem de se submeter aos especialistas da área, tornado-se mais autônomas e relacionando-se de modo amigável e inventivo com os computadores.

A sujeição social fabrica um indivíduo vinculado a um objeto externo, do qual faz uso. Nela, “o indivíduo trabalha ou se comunica com outro sujeito individuado via uma máquina-objeto, que funciona como ‘meio’ ou medição de sua ação ou uso” (LAZZARATO, 2014, p. 29). Trata-se da interação entre entes globais, individualizados. Diante dos objetos, a sujeição social designa aos sujeitos funções como a de usuário, a de telespectador, a de consumidor etc. É sempre o sujeito enquanto totalidade que é convocado, incitado, induzido, solicitado, encorajado, impedido, alertado, estimulado a agir ou deixar de agir.

Diferentemente, na servidão maquínica dualismos como homem e máquina, sujeito e objeto inexistem. Como dizia Deleuze (1992b, p.226), nas sociedades de controle os "indivíduos tornam-se 'dividuais', divisíveis, e as massas tornam-se amostras, dados, mercados ou 'bancos'". Na servidão maquínica, não há diferença no modo de "funcionamento" do dividual e dos componentes "não humanos" dos objetos técnicos, tais como os dados, os protocolos, os botões, os softwares etc. O dividual não se opõe às máquinas nem faz uso de um objeto externo, antes ele é adjacente às máquinas. Seres humanos e máquinas, juntos, constituem um agenciamento, um dispositivo, no qual são "meras partes recorrentes e intercambiáveis de um processo de produção, de comunicação, de consumo etc. que os excede" (LAZZARATO, 2014, p.29).

É no âmbito da servidão maquínica que a governamentalidade algorítmica atua. Isto é, ela estrutura o campo de ações de agentes humanos e não-humanos, entendendo-os sempre enquanto um agenciamento, enquanto híbridos. É por isso que os sistemas de recomendação mais do que se dirigirem aos sujeitos, buscam conectar-se com os divíduos, com os componentes da subjetividade (atenção, memória, sensações, cognição, força física). Estes não são mais unificados em um "eu", não possuem um sujeito referente, mas são "conectados" diretamente. Os processos de servidão maquínica "conectam um órgão, um sistema de percepção, uma atividade intelectual, e assim por diante, diretamente à máquina, a procedimentos, a signos, ignorando a representação de um sujeito (funcionamento diagramático)" (LAZZARATO, 2014, p. 39).

Sujeição social e servidão maquínica não são excludentes. E, apesar de serem processos heterogêneos, são interdependentes e complementares. Se Rovroy e Berns (2013) dão especial relevo à governamentalidade algorítmica não é por desconhecerem os processos de sujeição social. Antes, é porque buscam lançar luz para a emergência de uma nova modalidade de funcionamento do poder (o que não exclui as anteriores, é claro). Na governamentalidade algorítmica, o que está em jogo não é a ação sobre corpos ou almas no presente, mas, sobretudo, a ação sobre a potência de ser afetado e de agir:

> Ter seu perfil produzido de tal ou qual maneira, afeta as oportunidades que nos são disponíveis e, assim, o espaço de possibilidades que nos definem: não somente isto que nós temos feito ou fazemos, mas isto que nós teríamos podido fazer ou poderíamos fazer no futuro. Com a produção de perfis algorítmicos, o poder mudou de alvo: não o provável, mas o potencial, a potencialidade pura, a dimensão de virtualidade no real (ROUVROY, 2014, p.14, tradução nossa).

É no âmbito do virtual, seja para atualizá-lo, seja para evitar sua atualização, que esta modalidade de poder opera buscando, assim, reduzir a incerteza, operando uma espécie de gerenciamento do acontecimento. Não se trata de abolir o imprevisível, mas de gerenciá-lo, de governar o ingovernável. Com bastante sintonia, o Comitê Invisível – um grupo anônimo de pensadores e ativistas sediados na França – esclarece que "a gestão do governo cibernético [expressão que aproximamos da governamentalidade algorítmica] não é apenas, como no tempo da economia política, prever para orientar a ação, mas agir diretamente sobre o virtual, estruturar os possíveis" (COMITÊ INVISÍVEL, 2016, p. 137).

2.5 O Espaço da Crítica e as Práticas de Liberdade

Desde o princípio temos afirmado um certo modo de existência que se esforça para compor a vida por meio dos bons encontros. Mas não seria justamente os encontros alegres que as plataformas como o Netflix e a Amazon nos prometem ou nos fazem acreditar que teremos seguindo suas sugestões? Que basta confiarmos em seus algoritmos e que eles farão todo o trabalho por nós? Não apenas os algoritmos de recomendação, mas tantos outros que parecem ser capazes de fazer boas escolhas em nosso lugar. A grande questão não é se vamos ou não seguir as sinalizações dos algoritmos, mas como nos relacionamos com eles, isto é, sob que condições, com que finalidade e sob que efeitos em nossos modos de existência os fazemos de nossos mestres, daqueles que conduzem as nossas condutas.

Se ignoramos o que são tais algoritmos, como funcionam, qual a sua essência técnica, e, mesmo assim, nos sujeitamos aquilo que nos recomendam, então não sabemos que efeitos eles podem ou não produzir em nós. Trata-se de ter um modo de vida – na relação com tal rede de objetos técnicos – no qual permanecemos no domínio das paixões, isto é, permanecemos sob a primazia dos afetos passivos. Mas o que são os afetos passivos? Em síntese, de acordo com a leitura que Deleuze (2008, p.245, tradução nossa) faz de Spinoza, "o afeto é paixão ou passivo na medida em que é provocado por algo distinto de mim". Ao que acrescenta: "quando sou eu quem me afeto,

o afeto é uma ação". É por meio do afeto de si para consigo que o sujeito pode praticar a liberdade, que pode dar contornos a própria existência (DELEUZE, 2005).

No caso das recomendações dos algoritmos, que buscam nos manter no âmbito dos afetos passivos – sejam elas, alegres ou tristes – pouco aprendemos além de aceitar o que nos é sugerido. Programas de navegação como Waze, por exemplo, nos indicam a rota a ser percorrida, os momentos de sairmos de uma pista e entrarmos em outra e, até mesmo, avisam quando há acidentes ou policiamento. Toda a nossa trajetória é organizada pelo programa com a finalidade de otimizar o percurso. Teríamos que nos perguntar do que se trata tal otimização, o que ela supõe e implica. Quando o principal aspecto a ser considerado é a economia de tempo – um tempo atravessado pela lógica econômica –, provavelmente programas como Waze sejam as melhores soluções. Mas a vida pode ser muito mais do que economizar, poupar ou investir tempo. Não poderíamos ter outras modalidades de relação com o tempo, tal como nos lembra Bondía (2002), ao qual já fizemos referência neste capítulo? Para isso, seria necessário tecermos outras relações com os sistemas de recomendação, relações essas que escapem ao modo de resposta reflexo.

Para Sant'Anna (2011), é preciso distinguir reflexo e reflexão, termos que apesar de semelhantes dizem respeito a conteúdos muito diferentes. O reflexo tende a ser mais rápido, barato e leve do que a reflexão, já esta "incomoda mais do que acomoda, desestabiliza mais do que apazigua, o que torna as coisas ainda mais difíceis para quem quer continuar refletindo" (SANT'ANNA, 2011, p.87). A reflexão assume riscos e está aberta ao imprevisto, não tem garantias de chegar a alguma solução.

Por que sugerir que podemos ter outras relações com os algoritmos de recomendação que não aquelas pautadas no reflexo imediato, isto é, quando acatamos rapidamente o que nos foi sugerido e que, não raro, nos é gratificante? Por que arriscar? Se nossa relação com o Waze – assim como outros sistemas de recomendação – se resume em seguir suas orientações – por vezes apresentando-se até como imperativos ("vire à direita", "vire à esquerda", "siga em frente por 2 quilômetros") –, então aprenderemos muito pouco acerca de como organizar nossos encontros. E além disso, e talvez mais importante, tais algoritmos não agem apenas em situações pontuais – esta ou aquela escolha –, antes procuraram estruturar nossas ações ao longo de um trajeto –

de deslocamento, de consumo, de afetos, de pensamentos, de encontros etc. E o fazem a partir de critérios que, na maior parte das vezes, não consideramos se seriam aqueles por meio dos quais gostaríamos de dar contornos às nossas vidas.

Assim, pouco contribuem para aumentar a nossa potência de agir e de sermos afetados. Ou seja, não aprendemos a selecionar, a escolher, a organizar nossos encontros. E se não há aprendizado, se não há experimentação, não há como nos apropriarmos da nossa potência, de aprendermos o que podemos, o que nos convém e o que não nos convém.

Ao não se dirigir aos sujeitos humanos reflexivos, a governamentalidade algorítmica evita a emergência da crítica. Ela não provoca a liberdade e, assim, não suscita recalcitrâncias (ROUVROY, 2011). Sejamos um pouco mais claros: não é a liberdade que é excluída: os sujeitos continuam livres, permanecem participando de relações de poder. Entretanto, e aí está a sutileza da artimanha, o que se torna rarefeito é o exercício refletido da liberdade. Comentando o pensamento de Rovroy, Colle, Ledox e Vlajcic (2017, p. 58, tradução nossa) esclarecem:

> A Governamentalidade Algorítmica não faz nada a não ser curto-circuitar nossos desejos: ela torna também mais difícil a racionalização *a posteriori* de nossas escolhas. Com efeito, a opacidade das recomendações algorítmicas que nos induzem a comprar não nos ajudam nem a fazer escolhas mais esclarecidas, nem a identificar melhor ou a nos dar conta, depois de termos comprado, a razão de nossa escolha. Então é precisamente nessa capacidade que reside nossa (única) liberdade. Por que compramos tal coisa? Porque ela nos foi sugerida. Por que ela nos foi sugerida? Porque nós compramos uma outra coisa parecida. E assim por diante.

Se não há espaço para recalcitrâncias, para resistências no âmbito da governamentalidade algorítmica, estaríamos condenados a servidão maquínica por meio da qual ela opera? Estaríamos, portanto, um passo atrás de podermos, inclusive, abordar, assim como Foucault (2012), a seguinte questão: é inútil revoltar-se? Certamente não, pois precisamos esclarecer que se as resistências se produzem no âmbito das sujeições sociais, no âmbito das servidões maquínicas o que é importante é a política dos afetos. É justamente sobre esses que tais algoritmos de recomendação intentam agir, isto é, por meio da ação sobre o pré-individual.

Assim, importa traçar estratégias, inventar dispositivos que nos levem a participar de outros agenciamentos, criando condições para outros afetos, abrindo-se, inclusive, para encontros dos quais não sabemos muito bem o que nos acontecerá, pois, como lembra o Comitê Invisível (2016, p.52), “ninguém pode antecipar a potência de um encontro”. As práticas de liberdade que ocorrem na dimensão dos seres individuados repercutem na dimensão maquínica dos agenciamentos. Como produzir condições que transformem nossos afetos, sobretudo, quando a variedade e complexidade dos objetos tecnológicos aumenta a cada dia? Tal qual os objetos técnicos – que cada vez mais operam em rede – torna-se imprescindível constituir redes de resistência, espaços comuns que nos permitam escapar ao modo hegemônico de nos relacionar com os objetos técnicos.

TERCEIRA PARTE – A CRIAÇÃO DE NOVOS MUNDOS

1 A PRODUÇÃO DO COMUM

Dentre outros embates nos quais podemos encontrar hackers envolvidos estão aqueles que se dão em torno do comum. São lutas tanto para que as informações circulem sem se tornarem propriedade exclusiva de alguns, quanto lutas nas quais há um certo modo de colaboração pautado pelo fazer comum. Como escreve Levy (2012b, p.26), dentre as máximas que hackers encarnam estão: “O acesso aos computadores – e a tudo que possa ensinar algo sobre o funcionamento do mundo – deve ser ilimitado e total” e “Toda informação deve ser aberta e gratuita”. Insurgência, portanto, quanto às expropriações do comum.

Pensamos que hackers estão entre os novos enciclopedistas, isto é, se compreendemos o enciclopedismo, enquanto o fazer comum dos conhecimentos e das técnicas, e que, nos dias de hoje, passa a dizer respeito também ao fazer comum dos próprios objetos técnicos. Buscaremos abordar, portanto, neste capítulo, hackeações nas quais o comum está em jogo. Para isto, comecemos esclarecendo o que entendemos por comum.

1.1 DEFININDO O COMUM

Em *Império*, Hardt e Negri (2002, p.224) já apontavam para a necessidade de se criar um novo corpo social, um projeto político que não estivesse pautado somente na recusa, mas que fosse afirmativo: “Nossas linhas de fuga, nosso êxodo precisam ser constituintes e criar uma alternativa real. Além da simples recusa, ou como parte dessa recusa, precisamos construir um novo modo de vida e, acima de tudo, uma nova comunidade”. Mas é, sobretudo, em *Multidão* (HARDT; NEGRI, 2014) e *Bem-estar Comum* (HARDT; NEGRI, 2016) que eles levam adiante uma primeira teoria “do comum” (no singular), avançando em relação às elaborações já existentes acerca dos comuns [*the commons*].

Tal deslocamento teórico tem importância, pois o termo comuns (no plural) remete, segundo eles, a “espaços de partilha pré-capitalista que foram destruídos pelo advento da propriedade privada” (HARDT; NEGRI, 2014, p. 14). Assim, o comum – apesar de ser

um termo um tanto desajeitado – remete a um princípio político, um regime de práticas e lutas, cuja perspectiva não está no passado, mas no presente. O comum não é o que teria sido destruído pelo capitalismo, mas o que ele explora e, em certa medida, o que produz: “Nossa comunicação, colaboração e cooperação não se baseiam apenas no comum, elas também produzem o comum, numa espiral expansiva de relações” (HARDT; NEGRI, 2014, p.14).

Para tentar delinear melhor o que os autores compreendem por comum, retomemos os quatro significados que eles apresentam. O primeiro deles, diz respeito “à riqueza comum do mundo material – o ar, a água, os frutos da terra e todas as dádivas da natureza –, o que nos textos políticos europeus clássicos em geral é considerado herança da humanidade como um todo, a ser compartilhada por todos” (HARDT; NEGRI, 2016, p.8). Pensar o comum, restrito a esse modo, é manter-se atrelado à perspectiva teológica, isto é, entendendo-o enquanto dádiva divina, o “comum natural”. A este, os autores acrescentam o “comum artificial”, que seria constituído pelos “resultados da produção social que são necessários para a interação social e para mais produção, como os conhecimentos, as imagens, os códigos, a informação, os afetos e assim por diante” (HARDT; NEGRI, 2016, p.8). Nem dádiva divina, nem dado natural, o comum passa a designar a atividade humana tanto como condição quanto como resultado. Mas tal divisão – entre o comum natural e o comum artificial –, como lembram os autores, logo desaparece, pois não se sustenta na realidade (HARDT, 2010). Isto é, “o comum é ao mesmo tempo natural e artificial; ele é nossa primeira, segunda, terceira e enésima natureza” (HARDT; NEGRI, 2014, p.436).

De acordo com Dardot e Laval (2017), Hardt e Negri não se contentam em resgatar esses dois significados antigos e heterogêneos do comum. Eles acrescentam um terceiro sentido, este sim original e estreitamente relacionado às características daquilo a que alguns autores têm denominado de “capitalismo cognitivo”[51] e de “trabalho imaterial”[52]. Trata-se de notar que a exploração do capitalismo incide não apenas em tudo o que se refere ao comum – nos dois primeiros sentidos previamente definidos –, mas também,

[51] O capitalismo cognitivo diz respeito a um novo regime de produção marcado pela informatização, no qual a “lógica de reprodução é substituída pela lógica da inovação, e o regime da repetição, pelo da invenção” (MALINI; ANTOUN, 2013, p.48).

[52] O trabalho imaterial é, para Hardt e Negri (2002, p.311), aquele cuja produção não resulta em bem material e durável, mas “produz um bem imaterial, como serviço, produto cultural, conhecimento ou comunicação”.

que cada vez mais, precisa ter acesso livre aos recursos “imateriais” comuns que estão em plena expansão na atualidade. Paradoxalmente, é justamente no comum, que se baseia na produção imaterial, que reside a potência de resistências inventivas: “o conteúdo daquilo que é produzido – inclusive ideias, imagens e afetos – pode ser facilmente reproduzido e assim tende a ser comum, resistindo fortemente a todas as tentativas legais e econômicas de privatizá-lo ou submetê-lo ao controle público” (HARDT; NEGRI, 2016, p.10).

Toda produção de ideias, de conhecimentos, de linguagem, de software, etc., tem por pressuposto e, ao mesmo tempo, por resultado o comum. Ninguém pensa isoladamente, pois cada pensamento é produzido na relação com o pensamento passado e presente de outros. Cada uma dessas produções enriquece o comum e serve de base para outras (HARDT; NEGRI, 2014). Como vimos no caso do EMACS, não há programa que seja criado do zero e, além disso, todo programa pode ser desenvolvido, transformado ou ter partes reaproveitadas para outros programas. Na verdade, como apontam Hardt e Negri (2014, p.196), o comum “manifesta-se não só no início e no fim da produção, mas também no meio, já que os próprios processos de produção são comuns, colaborativos e comunicativos”.

E, por fim, um quarto significado do comum na obra de Hardt e Negri, apontado por Dardot e Laval (2017), diz respeito à esfera de luta social e política, sendo o comum compreendido como o fazer coletivo de singularidades[53] irredutíveis ao Uno, isto é, uma verdadeira multiplicidade. Nesse mesmo viés, Curcio e Roggero (2017, p.11) afirmam que o comum põe em questão relações de força e de antagonismo e, portanto, “não há comum sem luta pelo comum”. Luta esta que antes mesmo de ter por objeto o comum, busca defender as condições de produção do comum – isto é, a própria possibilidade de cooperação e de interdependência produtiva (MENDES; CAVA, 2017; NEGRI; HARDT, 2016). São lutas, ao mesmo tempo, econômicas, políticas e culturais, lutas constituintes que criam novas formas de vida e de viver em comum (HARDT; NEGRI, 2002).

Não se trata, portanto, de compreender o comum enquanto um bem comum original que foi ou está sendo perdido/destruído e que precisa ser resgatado/recuperado.

[53] Ao abordarem o conceito de multidão, que seria composta por um conjunto de singularidades, Hardt e Negri (2014, p.139) definem singularidades enquanto “um sujeito social cuja diferença não pode ser reduzida à uniformidade, uma diferença que se mantém diferente”.

Antes, o comum é o que está continuamente sendo produzido nas práticas concretas do cotidiano, no seio das próprias relações sociais, ou seja, ele é devir e não ser (HARDT; NEGRI, 2014, 2016).

Não deixamos de reconhecer, juntamente com Dardot e Laval (2017), que os quatro significados do comum, presentes na obra de Hardt e Negri (2014), acima mencionados, articulam-se com certa dificuldade, ou melhor, que não há uma unidade, mas um amálgama no qual

> [...] encontram-se, ao mesmo tempo, o que é dado desde sempre pela natureza, o que é engendrado de modo universal pela vida social, o que é resultado de um trabalho imaterial historicamente dominante na época do capitalismo cognitivo e, por fim, o que caracteriza as lutas mais recentes (DARDOT; LAVAL, 2017, p.205).

Se para Dardot e Laval (2017) tal amálgama é sinal da fragilidade do conceito elaborado por Hardt e Negri (2014), para nós trata-se, antes, de uma potência, com a qual buscaremos operar. Isto é, transitaremos, com certa liberdade, entre os diversos significados reconhecendo que eles não se atualizam de modo independente, mas enquanto mistos, híbridos que apenas em um esforço teórico e didático podem ser separados com alguma clareza.

1.2 Para Além do Privado e do Público: o Comum

A partir do discurso econômico-jurídico, pode-se dizer que os bens privados são exclusivos e rivais. Um bem é feito exclusivo quando seu detentor ou produtor está em condições de exercer o direito de propriedade impedindo que qualquer outra pessoa tenha acesso a ele, ou seja, ele está reservado para determinado sujeito. E pode ser considerado rival quando sua compra ou uso diminui a quantidade do bem disponível para outras pessoas. Há bens, entretanto, que não são exclusivos e nem rivais, como, por exemplo, a luz de uma vela que ao ser compartilhada com outras, acendendo-as, multiplica as velas acesas. Muitos podem dela desfrutar sem que com isso a quantidade disponível aos outros seja reduzida. Geralmente, esses bens que não são rivais ou exclusivos são produzidos e/ou geridos pelo Estado, sendo caracterizados como públicos (DARDOT; LAVAL, 2017).

Não devemos, entretanto, confundir o comum com o público. Dois casos são citados por Negri e Hardt (2016) para elucidar a questão: a chamada guerra da água em Cochabamba, na Bolívia, em 2000, e o referendo sobre a água na Itália, em 2011. Em ambas as situações, as lutas empreendidas foram capazes de evitar a privatização da água, mas, ao invés de torná-la um recurso comum, como os cidadãos pretendiam, contribuíram para reforçar o controle público existente.

A ação direcionada para o próprio bem – a água – foi insuficiente, pois era necessário também levar em conta a rede da qual a água fazia parte, isto é, toda a infraestrutura de apoio envolvida (canos, bombas, sistemas de gestão etc.). Para a água se tornar comum, de acordo com Negri e Hardt (2016, p.96), "o conhecimento das necessidades sociais e também os requisitos técnicos de processamento e distribuição não devem permanecer sob domínio de especialistas. [...] mas devem ser difundidos amplamente entre os cidadãos".

O conhecimento é, portanto, uma condição prévia da participação democrática e da gestão do comum. O que não significa, é claro, que todos devem se tornar especialistas. Aqui reside um mito que tem por efeito afastar as pessoas da ação política e de encontros potentes com os objetos técnicos. Pressupõe-se que para uma participação ativa é necessário ser um *expert*, ter qualidades especiais, ser portador de segredos que estariam reservados apenas aos iniciados. Negri e Hardt (2016, p.96) afirmam que "as pessoas foram educadas na apatia e na ignorância, estimuladas a suprimir seu apetite pela participação democrática e a considerar os sistemas sociais como tão complexos que somente os especialistas podem entendê-los". Pensamos que, semelhantemente, muitas pessoas também foram ensinadas a relacionar-se com os objetos técnicos como se eles tivessem a natureza de uma caixa-preta que deve ser acessada apenas por especialistas, por aqueles que "realmente" saberiam o que estão fazendo.

Portanto, fazer da água um recurso comum não é torná-la pública, atribuindo sua regulamentação e administração a instituições locais e estatais nas quais atuam representantes eleitos e especialistas. Antes, um bem comum – seja a água, um software ou qualquer outro – é "algo que deve ser construído, possuído, administrado e distribuído por todos" (NEGRI; HARDT, 2016, p. 98). O público não é de todos, mas designa algo

que está submetido à posse do Estado que, por definição e constituição, é transcendente aos cidadãos. Quem nele governa são representantes que cumprem tanto a função de síntese – ligando e associando os cidadãos ao governo – quanto a função disjuntiva – separando e apartando os cidadãos do governo (HARDT; NEGRI, 2014).

Hackear máquinas fechadas – sejam elas técnicas ou sociais – é um ato político que pode contribuir para a produção do comum. Ao abri-las, reproduzi-las e compartilhá-las é o comum que se enriquece. A distribuição pirata de um software sujeito à lei de *copyright* não ameaça a propriedade em si. O software não é subtraído do seu proprietário tal qual nas tradicionais formas de roubo, apenas "passa a haver mais propriedade para alguém mais" (HARDT; NEGRI, 2014, p.235). Isto porque o software – assim como outros bens imateriais – não está sujeito à lógica da escassez, isto é, a não ser que essa lhe seja imposta por meio de restrições que lhe tornam fechado como, por exemplo, os aparatos jurídicos e técnicos (já abordados na Primeira Parte desta tese). Assim, não há transferência de propriedade de um proprietário a outro, antes o que é violado é o próprio caráter privado da propriedade.

1.3 O Enciclopedismo e a Produção do Comum

A produção do comum implica a constituição de um plano de imanência, inclusive no campo dos saberes. Ou seja, a criação de condições para que o comum seja gerido de forma democrática e não por meio de representantes ou intermediários que excluam os cidadãos de participarem. Não estamos com isso querendo introduzir a alternativa na qual o comum é gerido pelos cidadãos ou por especialistas, mas por cidadãos e especialistas, por todos. Assim, faz-se importante retomar o movimento do enciclopedismo, sobretudo, porque nele há não só o questionamento de certas relações hierárquicas do saber, mas também a constituição de um plano de imanência no qual as multiplicidades de saberes singulares podem coabitar. No enciclopedismo, o fazer comum dos saberes é, ao mesmo tempo, condição e efeito. Isto é, o enciclopedismo produz saberes enquanto comum que são, ao mesmo tempo, condição (e ferramenta) para produção do comum. Retomemos, em linhas gerais e rapidamente, o que foi o movimento do enciclopedismo.

Na Idade Média, a cátedra não era encontrada só nos templos, mas também nas universidades. Era assentado na cadeira professoral que, estando mais elevado que seus alunos, o catedrático transmitia os ensinos dos grandes mestres e filósofos da Antiguidade. Na virada do século XIV para o XV e, especialmente no XVI, os saberes tradicionais estavam sendo questionados não apenas no âmbito religioso, mas também fora dele. Multiplicavam-se os escritos de técnicos e artesãos, por meio dos quais os saberes eruditos eram colocados em xeque. É para além dos muros da universidade, às margens da cultura oficial, e muitas vezes contra ela, que outra abordagem para a produção de verdades acerca do mundo ganhava espaço. A tão duradoura concepção sacerdotal do saber, na qual este é privilégio de poucos e uma espécie de sabedoria oculta e secreta, estava sendo confrontada por outra concepção, em que a colaboração, a publicidade dos resultados e o bem-estar de todos afirmam-se no lugar do interesse de apenas um pequeno grupo social. Por meio de diversas publicações filosóficas, artísticas, literárias e técnicas que assumem uma posição ético-política, afirmava-se o conhecimento advindo da relação direta do homem no mundo (ROSSI, 1989).

Tornava-se possível todo um campo comum de colaboração entre humanistas e literatos, técnicos e artesãos, entre o saber científico e o saber técnico, entre a teoria e o trabalho manual. Tratava-se de colocar em xeque as formas de sabedoria espiritual solitária por meio da constituição de um modo de pensamento que privilegiava a transmissibilidade do saber, sua circulação entre a ciência e a técnica. Como ressalta Rossi (1989, p.85), “desse ideal de um saber resultante da colaboração originam-se as constantes relações entre os eruditos, os grandiosos epistolários, as grandes academias e sociedades científicas do século XVII”. Insurreição, portanto, dos saberes que alargou o campo de trocas, de composições, de coexistência das contradições fazendo com que diferentes mundos pudessem ser afirmados ao mesmo tempo.

Tem-se, então, no Século das Luzes a multiplicação do gênero das enciclopédias, das quais a *Encyclopédie,* ou *Dictionnaire raisonné des sciences, des arts et des métiers,* organizada por Diderot e d'Alambert é, sem dúvida, a mais conhecida. Publicada entre 1751 e 1775, a extensa obra francesa é composta por mais de 70 mil verbetes e 600 pranchas com ilustrações e esquemas – um verdadeiro feito para a época. Nela, o escrito

e o imagético, o saber abstrato e o concreto, o erudito e o artesanal coexistem e estão articulados (PIMENTA; SOUZA, 2015).

Tal trabalho só foi possível porque contou com a contribuição de 160 colaboradores identificados, além, é claro, daqueles que preferiram o fazer na condição de anonimato – o que é compreensível, dado o caráter subversivo e polêmico dessa enciclopédia que despertou entre as autoridades grandes temores a ponto de ter sua publicação proibida por mais de uma vez, passando a circular na clandestinidade.

Para d'Alambert (1751 apud PIMENTA; SOUZA, 2015, p.107), não havia superioridade das artes liberais em relação as artes mecânicas, pois, segundo ele, “a sociedade, que justamente venera os grandes gênios que a iluminam, não deve aviltar as mãos que a servem”. Sendo um trabalho colaborativo, participaram da *Encyclopédie* com seus conhecimentos: matemáticos, filósofos, advogados, professores, cientistas, membros de academias, artífices, dentre outros. Cada um contribuiu a partir de sua especialidade sem que uma hierarquia entre os saberes fosse constituída.

Simondon (2007, p.112-113, tradução nossa) defende que a grande força da *Encyclopédie* não reside nos verbetes, mas, sobretudo, nas pranchas com ilustrações, pois

> [...] a informação está ali [nas ilustrações da *Encyclopédie*] suficientemente completa para constituir uma documentação prática utilizável, de tal modo que todo homem que possuía a obra era capaz de construir a máquina descrita, ou de fazer avançar, por meio da invenção, o estado alcançado pela técnica nesse domínio, fazendo sua investigação começar no ponto em que haviam concluído os homens que o precederam.

Mesmo os iletrados poderiam obter proveito das pranchas nas quais os esquemas apresentados eram suficientemente claros. O texto e a imagem estavam abertos, disponíveis sem necessidade de que um intermediário se colocasse como única condição para o aprendizado, pois, com a *Encyclopédie,* o mestre se tornava uma opção a mais entre outras. Tratava-se de um outro modo de relação com os saberes que “supõe um sujeito adulto, capaz de dirigir-se a si mesmo e de descobrir totalmente sua própria normatividade sem um ser que o dirija: o autodidata é necessariamente um adulto” (SIMONDON, 2007, p.113, tradução nossa).

A *Encyclopédie* não é constituída de uma unidade fechada, encerrada em si mesma, cujos elementos estão cristalizados. Antes é dinâmica e, como assinala Simondon (2018, p.113, tradução nossa), é “necessariamente inacabada; não busca substancializar-se, mas encarnar-se no devir”. Sua potência não está no objeto-livro atualizado, mas, sobretudo, pelo virtual que carrega consigo, por criar possíveis: “A Enciclopédia de Diderot não é um livro obsoleto, mas uma força que faz nascer fábricas, máquinas, laboratórios” (SIMONDON, 2018, p.113, tradução nossa).

A *Encyclopédie*, sem excluir as relações de poder-saber, mas antes nelas operando, publicizou o que antes era exclusivo, fazendo com que o segredo das especialidades pudesse circular e, assim, constituiu “um 'cosmos' de relações, um cosmos 'onde tudo está ligado' ao invés de ser 'ciumentamente guardado em uma corporação'” (ARAY, 2002, p.125, tradução nossa). Trata-se, para Simondon (2007), no caso do pensamento enciclopédico, de um grandioso movimento de fraternidade no qual a tolerância é um valor decorrente da abertura informacional. Constituem-se, assim, relações de poder-saber móveis, nas quais as situações de dominação são tensionadas ao mesmo tempo em que as composições entre os diferentes são favorecidas. Poderíamos dizer que a *Encyclopédie* é uma das expressões da luta pelo comum.

Deve-se lembrar que, como ressaltou Foucault (2014, p.8-9), não há sociedade em que a produção do discurso não seja

> [...] ao mesmo tempo controlada, selecionada, organizada e redistribuída por certo número de procedimentos que têm por função conjurar seus poderes e perigos, dominar seu acontecimento aleatório, esquivar sua pesada e temível materialidade.

Seja no jogo da produção discursiva, seja na circulação dos saberes, as relações de poder sempre se fazem presentes. No enciclopedismo, as relações de forças não são desfeitas de tal maneira com que todos possam falar de um mesmo lugar. Na verdade, criam-se espaços alternativos, multiplicam as posições a partir das quais os discursos podem ser produzidos. Não se deve nas práticas de resistência e liberdade visualizar a realização de um ideal de igualdade para todos, mas sim a potência de criação da diferença. Abertura, portanto, para a heterogeneidade e não a homogeneização dos diferentes, tornando-os iguais uns aos outros.

Podemos, então, definir o “espírito enciclopédico” como uma atitude que problematiza um modo fechado de se lidar com as informações, ou seja, quando estas permanecem localizadas e restritas a uma minoria que as utiliza ou tem a condição de utilizá-las para estabelecer, manter ou aprofundar situações de dominação. Tendo por tarefa multiplicar as informações, tornando-as difusas e fazendo-as circular no tecido social, esse modo de pensar, sentir e agir, opera por meio de produções colaborativas e pela abertura para as diferenças. O espírito enciclopédico, portanto, atualiza-se em práticas de produção do comum, práticas de liberdade nas quais se torna possível a coexistência de singularidades.

1.4 SOFTWARE LIVRE E A *GENERAL PUBLIC LICENSE*

Simondon (2018, p.123, tradução nossa), em meados de 1950, realiza um diagnóstico bastante preciso ao afirmar que os novos enciclopedistas “são os sábios construtores de centros automáticos de documentação, isto é, os cibernéticos, esses técnicos da informação que trabalham em equipe e pensam em comum”. Ainda que àquela altura não existisse a internet e, nem mesmo, a Arpanet, o filósofo já era capaz de vislumbrar os primeiros traços do campo no qual o espírito enciclopedista passava a se expessar. Concordamos com Hardt e Negri (2014, 2016) quando eles defendem que é no comum do conhecimento que as lutas atuais passam a se atualziar de forma privilegiada.

No campo dos softwares, como já tivemos oportunidade de abordar, a produção do comum passou a ser ameaçada pela comodificação dos softwares que teve por efeito, ao menos em um primeiro momento, tanto a redução do espaço ocupado por sistemas livres como da restrição do modo cooperativo pelo qual eles eram produzidos. É neste contexto que, face às regras jurídicas que protegiam a propriedade privada, emergiu a GPL, um novo regime de proteção jurídica que definiu “uma propriedade comum ‘aberta’, isto é, baseada na abertura do código fonte” (DARDOT; LAVAL, 2017, p.176–177). Para Aigrain (2005, p.109, tradução nossa), a própria *Free Software Foundation*, criada por Stallman, tinha por objetivo “construir o conjunto de ferramentas de software necessárias

para os usos gerais da informática, garantindo que essas ferramentas fossem e permanecessem disponíveis em regime de bens comuns".

De acordo com Dardot e Laval (2017, p.177), a GPL "cria um verdadeiro comum a partir da definição dos direitos e deveres dos usuários". Ao invés de garantir direitos de restrição de cópia e uso, ela garante os direitos de acesso, cópia, modificação e redistribuição dos programas – as chamadas "4 liberdades" básicas do software livre (FREE SOFTWARE FOUNDATION, 1989). Em termos legais, a GPL não é uma negação da propriedade intelectual, mas um uso subversivo da mesma. Há, inclusive, um interessante trocadilho feito com o termo *copyright* que passou, no caso da GPL, a ser referenciado como *copyleft* (termo que, segundo Dardot e Laval (2017), foi criado por Don Hopkins, amigo de Stallman). O "direito de cópia" tornou-se o "deixar copiar", a "cópia de direita" virou "cópia de esquerda" (EVANGELISTA, 2010). Quando utilizada em um programa, a licença *copyleft* exige que todas as versões modificadas ou estendidas, ao serem publicadas, continuem sob a mesma licença e nisso consiste seu aspecto viral.

Assim, a GPL protege o direito de uma comunidade de usuários-produtores, garantindo que todos possam fazer uso dos resultados acumulados pela comunidade, inclusive para usos comerciais. Entretanto, ao mesmo tempo, ela garante que ninguém possa "reservar para si a exclusividade dos resultados dos desenvolvimentos, porque estes são comuns" (DARDOT; LAVAL, 2017, p.178, grifo do autor). Em suma,

> [...] o *copyleft exclui a exclusão*, e é nisso, aliás, que se distingue da entrega pura e simples ao domínio público, visto que impõe aos usuários a regra de livre acesso às alterações introduzidas. O *copyleft* não é uma negação da propriedade, mas um uso paradoxal do direito do criador sobre sua criação, o qual é livre para utilizá-la como quiser e decidir como distribuí-la, com o intuito de assegurar o enriquecimento contínuo do comum.

Deve-se ter em mente que "o direito sempre foi um terreno privilegiado para identificar e estabelecer controle sobre o comum" (HARDT; NEGRI, 2014, p.263), o que torna as lutas no campo jurídico ainda mais importantes. Talvez o maior mérito da GPL, enquanto um *hack*, tenha sido afirmar que a criação de outros mundos é possível. Após ela, muitas outras licenças vieram a existência como as variações da *Creative Commons* (CREATIVE COMMONS BR, [2019]), a Arte Livre (COPYLEFT ATTITUDE, 2007) e a RobinRight (LICENÇA..., 2013). Cada licença cumpre uma função estratégica,

contribuindo para a atualização de mundos divergentes, que escapam à hegemonia do poder – o que não significa, é claro, que não possam ser capturados por ele em algum momento. Tal qual Fonseca (2012), pensamos que o próprio licenciamento pode ser visto como um espaço criativo, ou seja, mais do que recusar o *copyright*, estamos em condições de produzir nossas próprias licenças, dando a elas os contornos que desejamos.

1.5 UM NOVO ENCICLOPEDISMO: *LIBRARY GENESIS, REDDIT SCHOLAR* E *SCI-HUB*

Abordarmos, na Segunda Parte desta tese, algumas plataformas-sensores, isto é, plataformas que são capazes de se apropriar dos fluxos que nela circulam. Podemos agora afirmar que em muitas delas, sobretudo nas redes sociais, a produção do comum se faz presente de forma privilegiada. O Facebook, por exemplo, é um espaço no qual conteúdos são produzidos continuamente por seus usuários. O comum nelas produzido, entretanto, é logo capturado e expropriado, isto é, feito propriedade privada de tal modo que, em muitos casos, os próprios usuários não têm acesso aos dados que são produzidos por eles e acerca deles. Vimos também que a partir da mineração de dados e da produção de perfis, criam-se condições para agir sobre os sujeitos, tanto enquanto indivíduos quanto como divíduos, modulando, assim, seus comportamentos, emoções, percepções etc. Trata-se da plataforma-atuador, isto é, de sua função de agir sobre o mundo.

Agora, porém, gostaríamos de tratar de outras plataformas e estratégias que exercem a função de criar condições para o compartilhamento do comum, inclusive ultrapassando barreiras legais. Abordaremos a produção do comum nas plataformas/serviços *Library Genesis, Reddit* e *Sci-Hub.* Sem dúvida, há na internet muitas outras práticas de produção do comum, seja em plataformas especificamente construídas para isso, seja em outros serviços que têm sua finalidade original desviada ou subvertida para a produção, defesa e gestão do comum (como, por exemplo, o *Twitter*). Interessa-nos, porém, apenas indicar algumas práticas já existentes ressaltando a potência de produção do comum em encontros entre seres humanos e objetos técnicos.

A pergunta que Cabanac (2016, p.1, tradução nossa) apresenta no início do seu artigo sobre a *Library Genesis*, mais conhecida pela abreviação *LibGen*, nos dá uma boa noção acerca do que consiste tal plataforma: “E se aqueles que são chamados hackers se infiltrassem nas bibliotecas digitais das principais editoras baseadas em assinaturas, fizessem o download de artigos científicos em massa e os divulgassem por meio de redes *peer-to-peer*[54] anônimas?”. Na LibGen, por meio de um de motor de busca de artigos, o internauta pode pesquisar e baixar dezenas de milhares de documentos que vão desde artigos, livros (científicos, didáticos, de literatura, de ficção, dentre outros), revistas até histórias em quadrinhos. Basicamente, todo esse material passa a estar disponível na plataforma a partir de dois caminhos: (1) vazamentos massivos de documentos que são *uploaded* na plataforma; e (2) *upload* de documentos isolados por meio de *crowdsourcing*, termo que Cabanac (2016, p.2, tradução nossa) utiliza para “qualificar a colaboração explícita de pessoas que criam uma coleção distribuída de itens que podem ser compartilhados entre usuários”.

Já o *reddit.com* é uma plataforma semelhante a um fórum no estilo *bulletin board system* (BBS), no qual os internautas criam categorias ou áreas de interesse, denominadas de *subreddits* e nas quais são realizadas as postagens de links e comentários. Um desses *subreddits* é o *r/Scholar* e nele é possível solicitar e compartilhar artigos específicos de vários de bancos de dados. Para isto, basta registrar-se no site e seguir as orientações de postagem que incluem, basicamente, *tags* (indicando se é um livro, um artigo, um capítulo de livro etc.), o título, o autor e o identificador (DOI/PMID/ISBN)[55]. Uma vez feita a solicitação, outro internauta que tenha acesso ao arquivo pode fazer o *upload* para o *LibGen* e postar o hiperlink na plataforma de compartilhamento.

Uma das recomendações que o *bot* do *r/Scholar* nos apresenta é: “se você receber uma mensagem privada de alguém pedindo para você pagar pelo livro, por favor compreenda que isto é contra o espírito desta subcategoria e nós não toleramos. Avise os moderadores se você acredita que isso é um *scam*” (“Scholar”, [s.d.]). Trata-se,

[54] *Peer-to-peer* (P2P) significa par a par ou, simplesmente, ponto a ponto. Nessa arquitetura de redes, os arquivos são permutados diretamente entre os computadores dos usuários. Cada nó – ou ponto – pode funcionar tanto como cliente quanto como servidor, permitindo o compartilhamento, sem a necessidade de um servidor central.
[55] Disponivel em: https://www.reddit.com/r/Scholar/. Acesso em: 15 abr. 2019.

portanto, de fazer um uso da plataforma de tal modo que os conteúdos possam circular sem grandes restrições, inclusive econômicas. Não significa, neste caso, que a plataforma ignore as leis, pois ela mesma adverte que todos os conteúdos ali presentes são fornecidos sob o *fair use*, uma exceção legal ao *copyright*, que permite "o uso de materiais protegidos por direitos autorais sem obter permissão, desde que o uso possa ser considerado justo" (PURDUE UNIVERSITY, 2018, tradução nossa). Sem entrar nas minúcias, esclarecemos que para ser considerado um uso justo quatro fatores devem ser pesados: (1) o caráter e o propósito do uso do material; (2) a natureza do trabalho (quanto mais criativo maior é a proteção que lhe é garantida); (3) a quantidade de trabalho que está sendo utilizada; e (4) o impacto no mercado (PURDUE UNIVERSITY, 2018).

O *Sci-Hub*, por sua vez, está em operação desde 2011, tendo emergido enquanto uma crítica à cobrança para o acesso a artigos científicos, compartilhando-os gratuitamente. Logo na página inicial da plataforma, esclarece-se que se trata do "primeiro site pirata do mundo a fornecer acesso em massa e ao público a dezenas de milhões de trabalhos de pesquisa" (SCI-HUB..., [2019], sem paginação, tradução nossa). São mais de 70 milhões de artigos disponibilizados, driblando *paywalls* e outras restrições de acesso. São três os princípios norteadores do *Sci-Hub*: conhecimento para todos, recusa de *copyright* e acesso aberto. Para obter o artigo desejado, basta inserir a URL, o PMID/DOI ou digitar as palavras que se deseja buscar. Desse modo, o internauta pode obter acesso não autorizado aos documentos que procura (SCI-HUB..., [2019]).

Há também um uso subversivo Twitter por meio da *hashtag* #icanhazpdf. Com ela internautas solicitam e compartilham documentos científicos que, na maior parte dos casos, estão protegidos por *copyright* e só têm acesso mediante pagamento de taxas. O uso da *hashtag* começou com Andrea Kuszewski, uma cientista para quem tais práticas de compartilhamento são atos de desobediência civil não necessariamente agressivos, mas capazes de dizer que mudanças são necessárias (MOHDIN, 2015, sem paginação, tradução nossa).

> Ela [Kuszewski] explica que muitas pessoas estão ficando cada vez mais frustradas com um modelo de negócios – no qual o trabalho é produzido por acadêmicos, editado por seus pares e muitas vezes financiado pelo contribuinte – que está escondido atrás de um *paywall*. Se alguém não quiser pagar o preço da assinatura, digamos, no New York Times, ela diz, muitas vezes eles podem ler as notícias em outro lugar, mas esse não é

> o caso de trabalhos acadêmicos por trás de um *paywall*, porque esse é o único lugar para encontrar o trabalho completo.

Harding (2015a, 2015b), em um dos mais importantes eventos hackers – o *Chaos Communication Camp* –, apresentou uma palestra intitulada “Driblando o *Paywall* – como compartilhar pesquisas livremente sem ser preso”. Nela, ele abordou diversas maneiras pelas quais “hipoteticamente” é possível superar as barreiras técnicas e legais para acessar e distribuir conteúdos científicos protegidos. Dentre as estratégias para obter conteúdos, ele sugere o uso de fontes que requerem identificação apenas como última alternativa. Algo muito semelhante ao que já vimos com Stallman quanto ao uso dos cartões de crédito. Aqui, novamente, vigora o zelo pela preservação da privacidade, buscando, assim, evitar que sejam registrados fluxos de dados associados ao indivíduo. Deixar traços é criar condições para ser vigiado e monitorado e, portanto, evitá-los é uma forma – ainda que limitada – de preservar-se nas relações de poder e dominação. Por exemplo, se a instituição universitária requer que seja feito login com credenciais individuais (usuário e senha), ele recomenda que primeiro se procure o documento em todos os outros lugares. Dentre as alternativas, ele sugere a LibGen, o SciHub, o *Reddit Scholar*, o #IcanHazPDF – recém abordados –, o Google Scholar, que às vezes disponibiliza gratuitamente arquivos pagos e, por fim, visitar às páginas pessoais e de trabalho dos autores ou, até mesmo, entrar em contato direto com eles. E, se tudo falhar, então pode-se tentar acessar via repositório das instituições universitárias como visitante (acesso aberto) e, somente em última instância, acessar o conteúdo realizando o login.

Além de obter os documentos eletrônicos, Harding (2015a, 2015b) preocupa-se também em explicar como torná-los irrastreáveis antes de compartilhá-los. Por exemplo, ele apresenta práticas como remover proteções do conteúdo, marcas d’água e metadados. E, claro, além disso, ao publicar na internet, navegar anonimamente (com o Tor, por exemplo) e evitar realizar ações muito próximas que possam ser correlacionadas (por exemplo, baixar os arquivos e publicá-los pouco tempo depois).

Há importantes aproximações entre essas práticas e a elaboração da *Encyclopédie*. Em ambas, temos presente aquilo a que denominamos o espírito enciclopédico. São práticas que estão localizadas em um campo de lutas pela produção do comum, tornando acessíveis conhecimentos que antes tinha acesso restrito àqueles

que detinham os privilégios necessários (status social, recursos econômicos etc.). Uma diferença importante, entretanto, está no alcance. Enquanto a *Encyclopédie* por seus esquemas tornava-se mais universal, as práticas às quais fizemos referência neste tópico são mais localizadas àqueles que participam do meio acadêmico e possuem um mínimo de conhecimentos técnicos. Ainda assim, consideramos que a sua validade não está tanto no seu alcance, mas, sobretudo, na constituição de dispositivos de produção e gestão do comum.

Que mundos outros poderiam emergir na composição com tais plataformas? Para alguém que não tem condições de pagar mais de $ 30,00 por cada artigo que baixar diretamente no site da revista *Annual Review of Psychology,* uma série de outros mundos passam a estar ao alcance. Outros encontros, que antes estavam fora do campo de possibilidades, passam a estar em condições de serem atualizados. E, mesmo para um acadêmico ou para um pesquisador vinculado a uma universidade de ponta ou a um centro de pesquisa de referência, nos quais já se têm acesso livre ou subsidiado a artigos, a livros, a documentos e a tantos outros materiais, compor com tais plataformas pode ser interessante. Se as produções que circulam por meio de *paywalls* têm um circuito bastante restrito, ao serem integradas ao comum em tais plataformas, passam a estar em condições de alcançar uma série de outros leitores e interlocutores.

1.6 Pirataria e Compartilhamento

Se as licenças atuam no campo jurídico, a pirataria lhe escapa ou, ao menos, habita suas margens. Para alguns a pirataria é assumida enquanto prática positiva, marcada principalmente pela criação de espaços de liberdade e cooperação (TARIN; BELISÁRIO, 2012). Machado (2012), por exemplo, ao traçar um breve resgate histórico da pirataria nos séculos XVII e XVIII, afirma que a mera existência dos piratas representava um risco às autoridades muito menos pelos roubos do que por seus modos de vida e as regras de comunidade que praticavam, pois assim colocavam em xeque os regimes de governo existentes à época.

Reconhecendo que o campo da produção imaterial é um espaço de disputas e defendendo que as produções da mente humana sejam consideradas bens comuns,

Belisário (2012, p.79) apresenta o termo *copyfight* referindo-se, por meio deste, a um fluxo crítico, no qual se trata de "antropofagizar a cultura hacker e a tecnologia em nome da autonomia e livre circulação do conhecimento", ao que acrescenta que

> [...] a desobediência civil, a criação de plataformas de comunicação em código-aberto, a radicalização da apropriação tecnológica e da democratização da comunicação, o desenvolvimento de redes federadas e sistemas de comunicação eletrônica independentes e locais desempenham papéis fundamentais de resistência aos mecanismos de vigilância e sistemas de restrição ao acesso à informação (BELISÁRIO, 2012, p.79).

O que torna os softwares (assim como muitos dos documentos eletrônicos) valiosos é sua reprodutibilidade. Paradoxalmente, é justamente a mesma qualidade que ameaça seu caráter privado. Assim, a cópia pirata – aquela feita sem autorização infringindo o *copyright* –, ao ser compartilhada, acaba sendo associada, pela publicidade e a indústria do entretenimento, ao roubo. Inclusive há aqueles que sustentam que cada cópia pirata seria uma venda a menos realizada, premissa que certamente carece de fundamento (BELISÁRIO, 2012).

Produzido de forma colaborativa em comunidade, muitos softwares acabam sendo expropriados, isto é, apropriados de tal modo a se tornarem propriedade privada (HARDT; NEGRI, 2014). Mas o que sustenta o regime do *copyright*? Seguindo a tradição de Étienne de La Boétie, poderíamos supor que é o nosso consentimento que lhe dá força. Assim, nosso caminho começa por uma política da recusa, pois como afirmam Hardt e Negri (2002, p.223), leitores do jovem filósofo francês, "o repúdio ao trabalho e à autoridade, ou o repúdio à servidão voluntária é o começo da política libertadora". É necessário, portanto, inventarmos novas formas de resistência capazes de criar condições para outros mundos. Tais estratégias em ação vão desde a criação e uso de licenças alternativas até outras que extrapolam as práticas restritas ao âmbito jurídico.

Não há uma regra geral de como fazer. Cada caso é singular, sendo necessário compreender a situação atual e nela descobrir/criar mecanismos para administrar, desenvolver e sustentar a riqueza comum mediante a participação democrática, sendo a tarefa que nos cabe "não é só prover acesso aos campos e rios para que os pobres possam se alimentar, mas também criar meios para a livre troca de ideias, imagens, códigos, músicas e informações" (NEGRI; HARDT, 2016, p. 138).

Na *Encyclopédie,* como resultado da produção comum tínhamos saberes comuns. Além dos verbetes, também havia a representação das máquinas e das ferramentas, os esquemas de funcionamento dos objetos e o modo de utilizá-los (SIMONDON, 2018). Atualmente – e esta é uma grande novidade histórica que assinalamos –, a internet e as tecnologias digitais nos permitem ir além e compartilhar os próprios objetos técnicos. Isto é, estão em condições de circular desde músicas e filmes até softwares como editores de texto, navegadores, jogos etc.

Malini e Antoun (2013) abordam uma série de sistemas de trocas de arquivos digitais que começa com o Napster, passa pelo Gnutella, pelo Kazaa, pelo eDonkey, pelo eMule e vai até o BitTorrent, sendo todos eles, em maior ou menor medida, sistemas P2P. Para eles, tais sistemas envolvem práticas de gestão do comum que despertaram a fúria do capital que permaneceu inerte, mas reagiu, sobretudo, no âmbito jurídico com a publicação, por exemplo, do *Digital Millenium Copyright Act* (DMCA) – uma lei norte-americana que criminaliza a produção e a distribuição de tecnologias que permitam evitar as medidas de proteção dos direitos autorais.

Ainda citando os sistemas de trocas de arquivos digitais, não poderíamos deixar de mencionar, mesmo que rapidamente, o site *The Pirate Bay*, que se autodefine como o tracker BitTorrent mais resiliente da galáxia. Apesar das inúmeras controvérsias e polêmicas que rondam sua história, é o modo pelo qual funciona que nos interessa. Sem armazenar nenhum arquivo torrent em seus servidores, *The Pirate Bay* atua simplesmente como um indexador. Nele, o internauta pode fazer uso de um motor de busca e encontrar os mais variados tipos de arquivos: músicas, textos, jogos, pornográficos, programas, dentre outros. Ainda que existam algumas pessoas à frente do projeto, ele só é possível porque a multidão o sustenta, isto é, porque há aqueles que continuamente disponibilizam seus arquivos para serem compartilhados.

Não estamos dizendo que basta ingressar em redes P2P, baixar os arquivos digitais e tudo está resolvido. Sabe-se bem que há riscos, inclusive, de que o arquivo baixado tenha incorporado a si códigos para apropriar-se de senhas do usuário, de dados pessoais etc. Como não sabemos de antemão o que pode vir de um encontro, ao tecer relações é sempre importante levar em conta a recomendação da prudência.

Portanto, flertando com a ilegalidade – por vezes ultrapassando os limites da lei – essas práticas de hackeamento, pautadas no fazer comum, constituem outros mundos nos quais o fluxo dos dados desafia as tentativas – jurídicas, políticas, técnicas etc. – de fechamento dos objetos técnicos e do controle das informações.

2 O VIRTUAL

Para Castells (2001, sem paginação, tradução nossa), os hackers são "simplesmente pessoas com conhecimentos técnicos em informática cuja paixão é inventar programas e desenvolver novas formas de processamento da informação e comunicação eletrônica". Ainda que discordemos do requisito que envolve conhecimentos técnicos em informática – pois o *hacking* pode estar presente em qualquer área –, estamos de acordo quanto às práticas de invenção, sobretudo, cooperativas que se fazem presentes entre os hackers. Sem dúvida, hackers tiveram e ainda têm papel fundamental no desenvolvimento da internet tal qual o sociólogo espanhol apresenta por meio da seguinte retomada histórica:

> Foram *hackers* acadêmicos que projetaram os protocolos da Internet. Um *hacker*, Ralph Tomlinson, trabalhador da empresa BBN, inventou o correio eletrônico em 1970 para uso dos primeiros internautas, sem comercialização alguma. *Hackers* da Bell Laboratories e da Universdade de Berkeley desenvolveram o UNIX. *Hackers* estudantes inventaram o modem. As redes de comunicação eletrônica inventaram os quadros de aviso, os chats, as listras eletrônicas e todas as aplicações que hoje estruturam a Internet. E Tim Berners-Lee e Roger Cailliau projetaram o *browser/editor World Wide Web* por paixão de programar, escondidos de seus chefes no CERN de Genebra, em 1990, e o difundiram na rede sem direitos de propriedade a partir de 1991. Também o *browser* que popularizou o uso da *World Wide Web*, o Mosaic, foi projetado na Universidade de Illinois por outros dois *hackers* (Marc Andreesen e Eric Bina) em 1992. E a tradição continua: no momento, dois terços dos servidores de web utilizam Apache, um programa servidor desenhado e mantido em software aberto e sem direitos de propriedade por uma rede cooperativa (CASTELLS, 2001, sem paginação, tradução nossa).

Mesmo que todos os casos acima citados façam referência a *hacks* de complexidade relativamente grande, não podemos deixar de reforçar que o *hacking* pode ocorrer mesmo com um mínimo de conhecimentos técnicos, pois o que está em jogo mais do que a *expertise* é a inventividade. Por exemplo, buscando preservar a privacidade algumas pessoas cobrem a câmera de seus notebooks com *post-it* ou algo semelhante. Certamente, não é essa a função imaginada inicialmente para se utilizar o *post-it*, e nem mesmo essa é uma das soluções/alternativas projetadas para que as câmeras dos notebooks não captem imagens. Trata-se, assim, de uma gambiarra, de uma resolução inventiva de uma situação problemática que traz consigo algo da ordem do não previsto.

Uma das mais interessantes definições do verbo hackear está em *A hacker manifesto*, de Wark (2004, § 74, tradução nossa), e diz o seguinte: “hackear é liberar o virtual no atual”. Para que possamos compreendê-la melhor, faz-se necessário esclarecer filosoficamente os conceitos de virtual, atual, real e possível. Começaremos pelos dois últimos e, após isso, abordaremos dois *hacks* – isto é, atualizações de campos problemáticos, de tensões de forças – que são o *DuckduckGo* e o sistema Bitcoin. Cada um deles envolve uma atualização de virtuais que, ao serem produzidos, passam também a ocuparem uma função estratégica nas lutas em torno da privacidade e no fluxo das informações.

2.1 O REAL E O POSSÍVEL

A execução de um software, por mais complexo que ele seja, é puramente lógica e, como assinala Lévy (1996, p.17), “tem a ver com o par possível/real”. Tomemos, por exemplo, um algoritmo funcional do jogo Jokenpô. Neste, basicamente, dois adversários enfrentam-se ao longo de sucessivos lances independentes. A cada lance, ambos os jogadores devem escolher uma entre três possibilidades: Pedra, Papel ou Tesoura. Na sequência, ambas as escolhas são comparadas e o resultado é exibido (“Jogador A venceu”, “Jogador B venceu” ou “Empate”). As regras são bastante simples: (1) Pedra empata com Pedra e ganha de Tesoura; (2) Tesoura empata com Tesoura e ganha de Papel; e (3) Papel empata com Papel e ganha de Pedra.

No caso em questão, as três possibilidades de escolha do “Jogador A” e as três possibilidades de escolha do “Jogador B” podem produzir nove diferentes combinações, cada uma delas já prevista, de algum modo, no algoritmo do programa. Os resultados, derivados das nove composições possíveis, são os seguintes:

Quadro 1 - Composições Possíveis

	Jogador A	**Jogador B**	**Resultado**
1	Pedra	Pedra	Empate

2	Pedra	Papel	Vence Jogador B
3	Pedra	Tesoura	Vence Jogador A
4	Papel	Pedra	Vence Jogador A
5	Papel	Papel	Empate
6	Papel	Tesoura	Vence Jogador B
7	Tesoura	Pedra	Vence Jogador B
8	Tesoura	Papel	Vence Jogador A
9	Tesoura	Tesoura	Empate

Fonte: O próprio autor (2019)

Portanto, antes mesmo que um lance seja realizado, todas as possibilidades já estão dadas. Analisemos um lance específico, entendendo-o como processo de realização, ou seja, quando uma possibilidade passa a ter realidade. A única diferença entre a Pedra enquanto possibilidade (a ser escolhida) e a Pedra enquanto realidade (escolhida e) realizada é que neste último caso foi a ela conferida existência. O processo de realização está, como assinala Deleuze (2012, p.84), submetido à regra da semelhança: “estima-se que o real seja à imagem do possível que ele realiza (de modo que ele, a mais, só tem a existência ou a realidade, o que se traduz dizendo que, do ponto de vista do conceito, não há diferença entre o possível e o real)”.

A escolha é feita entre um conjunto predeterminado, entre possíveis estáticos e já constituídos. Quando um jogador faz sua escolha entre as três possibilidades, realizando-a – isto é, fazendo-a passar à existência, tornando-a real –, as outras duas possibilidades não se realizam. Trata-se daquilo a que Deleuze (2012, p.84) refere-se como regra da limitação, pois “como nem todos os possíveis se realizam, a realização implica uma limitação, pela qual certos possíveis são considerados rechaçados ou impedidos, ao passo que outros ‘passam’ ao real”. A realização só confere existência a certas

possibilidades em detrimento de outras, trata-se de uma eleição ou de uma seleção (LÉVY, 1996).

A mesma linha de pensamento quanto à execução dos programas poderia ser utilizada para um jogo da velha, para o xadrez ou para o sorteio da Mega-Sena. Isto é, mesmo nos casos nos quais as possibilidades consideradas são numericamente imensas, ainda assim, trata-se de conjuntos numericamente finitos tratados a partir do par possível/real.

Ao comentar o texto *O esgotamento*, de Deleuze, Zourabichvili (2000, p.335) afirma que o possível pode ser entendido "ou como uma alternativa ou como uma potencialidade". Ou melhor, reconhecendo a inspiração bergsoniana no pensamento de Deleuze, ele ressalta que "há uma diferença entre o possível que se realiza e o possível que se cria" (ZOURABICHVILI, 2000, p. 337). Quanto ao primeiro, isto é, o possível como alternativa (já dada) que se realiza, vimos que se trata de uma imagem que pode (ou não) vir a existência. É deste que ele distingue um outro possível, ou seja, puras potências, puros dinamismos, puros componentes problemáticos aos quais podemos designar melhor por meio do termo virtual. É de acordo com este sentido que Zourabichvili (2000, p.343, p.346) afirma:

> Tudo é possível, mas nada ainda está dado, segundo a nova definição do possível, já que ele precisa ser criado: o possível é o que devém, e a potência ou potencialidade merece o nome de possível na medida em que abre o campo de criação (a partir daí tudo está por se fazer). O possível é o *virtual*. [...] O possível enquanto novidade, à diferença das alternativas atuais ou dos projetos de futuro, é objeto de efetuação, não de realização. A efetuação concerne a um ato de criação, inseparável, desde então, de uma atualização.

Portanto, para evitar confusões, passemos a falar, de um lado, do virtual ou de criação de possíveis e, de outro, apenas do possível (que pode ou não ser realizado). Mas o que é o virtual?

2.2 O Atual e o Virtual

No uso corrente, o termo virtual é empregado com uma ampla gama de significados que vão desde a ausência de existência, de algo que pode ser ilusório,

imaginário, simulado, ou, até mesmo, falso, até a designação daquilo que é processado através de meios eletrônicos (“jogos virtuais”, “namoro virtual”, “dinheiro virtual”). Há, portanto, diversos sentidos para o virtual: o sentido comum, o sentido tecnológico etc (LÉVY, 1996, 2010). Aqui, todavia, adotaremos o conceito filosófico de virtual, tal qual acabamos de fazer com o par possível/real.

Não raro, confunde-se o possível e o virtual, o que pode ser explicado por um traço em comum que ambos possuem, isto é, “ambos são latentes, não manifestos. Anunciam antes um futuro do que oferecem uma presença” (LÉVY, 1996, p. 137). Mas como são distintos, cabe a nós dar mais clareza quanto ao que se diferem. Se o possível, como vimos, diz respeito a alternativas que, ao serem escolhidas ou selecionadas, podem vir a se realizar, o virtual é “como o complexo problemático, o nó de tendências ou de forças que acompanha uma situação, um acontecimento, um objeto ou uma entidade qualquer, e que chama um processo de resolução: a atualização” (LÉVY, 1996, p. 16).

Enquanto ao possível corresponde o processo de realização, ao virtual corresponde o processo de atualização. Quando o possível se realiza, nada nele muda, apenas lhe é acrescentada a existência. Já o virtual, ao atualizar-se, diferencia-se. Entre o virtual e sua atualização não há correspondência no sentido do idêntico ou do semelhante, pois, como explica Deleuze (2012, p.36), na esteira de Bergson, “a atualização se faz por diferenciação, por linhas divergentes, e cria pelo seu movimento próprio outras tantas diferenças de natureza”. O exemplo clássico da atualização é o problema da semente em tornar-se uma árvore. É a partir das coerções que lhe são próprias que a semente deverá inventar a árvore, isto é, coproduzi-la com as circunstâncias que encontrar (LÉVY, 1996). A semente não realiza uma árvore já dada, antes, atualiza um complexo problemático, que parte e considera as necessidades da situação presente.

Portanto, duas são as regras da atualização de acordo com Deleuze (2012): a diferença ou a divergência – isto é, há diferença entre o virtual de que se parte e os atuais aos quais se chega – e a criação – isto é, ao atualizar-se, há uma resolução criativa do complexo problemático. O resultado de uma atualização, como lembra Kastrup (2012), não está dado de antemão – ou seja, é da ordem da imprevisibilidade.

Assim, se a execução de um software diz respeito à realização, a invenção de um objeto técnico, inclusive a escrita do próprio software, diz respeito ao processo de atualização (LÉVY, 1996). Não é sem razão que Wark (2004, p. § 74) afirma que um "*hack* toca o virtual – e transforma o atual", hackear é, para ele, a produção da diferença, a atualização de virtualidades. Produzir um *hack* é inventar, atualizar uma solução criativa e não prevista para uma dada situação problemática. Isso não significa que uma vez tendo sido produzido o *hack* ele não possa ser copiado, repetido, reutilizado. Mas, neste caso – o da simples cópia/repetição –, se formos fiéis à definição, já não se trata de hackear. Claro que, mesmo seguindo uma receita, frequentemente faz-se necessário algum grau de improvisação, isto é, a atualização de algumas virtualidades – como já vimos, com Carlos C., na Segunda Parte desta tese.

A simples aplicação de uma solução existente não é hackear. Inclusive, no universo da informática, aqueles que buscando serem reconhecidos enquanto hackers e que utilizam soluções já prontas, dadas de antemão, sem compreendê-las, sem contribuir singularmente para modificá-las, recebem diferentes denominações: *lamer*, *luser*, *script kiddies* etc. (cf. cada uma dessas definições em Raymond (1991)). É claro que cada um desses tem sua especificidade, mas todos eles têm em comum o fato de que lhes está ausente a ação inventiva, apenas fazendo uso de objetos técnicos que, para eles, são caixas-pretas. São sujeitos que seguem as instruções, que assujeitam-se aos códigos sem subvertê-los.

Geralmente, quando se aprende a programar, o primeiro código que se é ensinado é aquele que imprime/exibe na tela a mensagem "Olá, Mundo!" ou "Hello, World!". Em HTML, de forma bem básica, o código-fonte poderia ser o seguinte:

```
<!DOCTYPE html>
<html lang="pt-br">
<head>
   <meta charset="UTF-8">
   <title>Olá, Mundo!</title>
</head>
<body>
   <h1> Olá, Mundo!</h1>
</body>
</html>
```

De linguagem para linguagem, o código irá variar. E, mesmo em uma mesma linguagem, há inúmeras formas de escrevê-lo. O mais importante para quem está aprendendo, entretanto, não é copiar o código e executá-lo, mas dar-se conta que novos mundos podem ser criados, que novos mundos podem ser atualizados. Neste sentido, Pariser (2012, p.149) afirma:

> Não é por coincidência que a carreira de todo programador começa com o 'Olá, Mundo!'. Esse poder de criar novos universos é o que costuma atrair as pessoas para a programação. Escreva algumas linhas, ou alguns milhares, aperte uma tecla e algo parece ganhar vida em sua tela – um novo espaço se abre, um novo motor começa a funcionar.

Programar é, sobretudo, resolver problemas, criar soluções, atualizar virtuais. Sempre quando se começa a escrever um código, a tela em branco – na qual a problemática já se faz presente – está preenchida por virtuais que poderão ser atualizados. Por exemplo, o que fazer diante dos mecanismos de vigilância e monitoramento quando queremos simplesmente buscar algum conteúdo na internet? É diante de um campo problemático como este que emerge, dentre outras, uma solução criativa, isto é, o *DuckDuckGo*.

2.3 DUCKDUCKGO

Em 2010, o motor de buscas *DuckDuckGo*[56] passou por uma importante transformação: deixou de acompanhar o histórico de pesquisa de seus usuários, oferecendo uma ferramenta que não fazia uso de rastreadores. Para além de um ato de marketing, o *outdoor* colocado em São Francisco – que tinha a mensagem "O Google rastreia você. Nós não. Procure melhor com DuckDuckGo.com" (tradução nossa) – indica-nos a presença de um complexo problemático (e, portanto, virtual) em torno de questões relacionadas à privacidade.

A leitura da Política de Privacidade do *DuckDuckGo* pode ser bastante elucidativa quanto aos tensionamentos que estão em questão. Um primeiro ponto problematizado é referido nela como sendo o "vazamento de pesquisa", ou seja, quando uma pesquisa é realizada e os termos buscados são compartilhados não apenas com o motor de busca,

[56] Disponivel em: https://duckduckgo.com/privacy. Acesso em: 15 abr. 2019.

mas também com todos os sites cujos links exibidos nos resultados foram clicados. Como ao visitar qualquer site o dispositivo utilizado compartilha dados que podem ser utilizados para o identificar, o resultado é que o site recebe dados não apenas acerca dos termos pesquisados que levaram o internauta até ele, mas também acerca de quem pesquisou aqueles termos.

Outro ponto, é que muitos motores de pesquisa salvam e armazenam o histórico de pesquisa de seus usuários, não raro acompanhado de uma série de outros dados tais como: a data/hora da pesquisa, dados do dispositivo e do *browser* e, em alguns casos, quando conectado ao serviço, o endereço de e-mail e nome do usuário. Assim, o serviço que oferece as pesquisas na internet é capaz de conhecer não apenas uma pesquisa isolada, mas tudo o que cada um dos usuários pesquisou.

É diante desses dois pontos, desses dois aspectos a serem evitados/superados que o *DuckDuckGo* é produzido enquanto resolução de um campo problemático. Para preservar a privacidade, o *DuckDuckGo* impede o vazamento de pesquisa por padrão, isto é, ainda que os sites visitados a partir do motor de pesquisa possam saber que o internauta o visitou, eles não terão acesso aos termos utilizados na pesquisa. Além disso, ele também não coleta nenhuma informação pessoal, inclusive, por padrão, não utiliza nenhum *cookie*, impossibilitando qualquer tentativa de vinculação dos usuários às pesquisas realizadas.

Mas, como se sabe, o problema da privacidade não está restrito às buscas que realizamos. E, tendo ciência disso, e dos desafios que se apresentam àqueles que não possuem conhecimentos técnicos, o *DuckDuckGo* lançou em 2018 uma extensão para *browser* e um app para dispositivos móveis que, além de permitirem fazer as buscas de modo anônimo, também são capazes de aumentar o nível de privacidade da navegação na internet – isto é, bloqueando rastreadores, oferendo uma criptografia mais inteligente, etc. Um dos aspetos mais interessantes da extensão/app é que ao visitar um site, é-lhe atribuída uma classificação de privacidade que vai de “A” até “F” que considera se a conexão é criptografada (por meio de HTTPS), os rastreadores que estão sendo bloqueados e as informações acerca das práticas de privacidade do site (PROTECTING..., 2018).

De modo simples, porém bastante instrutivo, a extensão/app do *DuckDuckGo* é capaz de oferecer ao internauta uma outra condição de navegação, pois não só evita muitos rastreadores, mas também cumpre uma função pedagógica, isto é, apresenta, a cada site visitado, uma cartografia dos elementos que podem aumentar/reduzir seu nível de privacidade.

Navegar na internet por meio do motor de pesquisa *DuckDuckGo* ao invés do Google, por exemplo, leva o internauta a experienciar outros mundos. Ao pesquisar, os resultados exibidos não serão personalizados de acordo com o histórico de pesquisa e/ou outros dados já coletados sobre o internauta. Podemos, assim, nos deparar com sites e conteúdos que os algoritmos não selecionaram especialmente para nós. Por um lado, ao pesquisar o a palavra-chave “futebol” talvez nosso time do coração não seja o primeiro a aparecer, por outro lado, poderemos nos deparar com tantas outras informações que nunca imaginaríamos sequer a existência. Ao não termos nossos interesses e gostos reafirmados, passamos a estar sujeitos a outros encontros que carregam consigo sua potência de nos fazer diferir.

Os próprios anúncios que também estão presentes no *DuckDuckGo* podem, não raro, dar a impressão de serem muito generalistas – e o são. Se na maior parte dos motores de pesquisa somos constantemente incitados com ofertas personalizadas, como se estivéssemos caminhando na rua e os vendedores nos chamassem pelo nome, apresentando-nos produtos e serviços tão direcionados que nem as pessoas mais próximas saberiam que estamos neles interessados, no *DuckDuckGo* os anúncios parecem mais com *outdoors* impessoais.

Ao utilizar o *DuckDuckGo* podemos ter inicialmente a impressão de que algo não vai bem. Um dos motivos é que estamos tão acostumados com os mecanismos de personalização e de recomendação – e que, cada vez mais, nos oferecem resultados em um espaço de tempo menor – que demorar-se na busca pode ser desconfortável. Entretanto, é no demorar-se ao longo do processo de busca que o imprevisível pode ter o seu lugar, isto é, que algo pode nos acontecer, que podemos nos encontrar com aquilo que nos desloca de nosso centro de referência.

2.4 O SISTEMA BITCOIN

Ao longo de 2007 e 2008, durante a crise do *subprime*, em vários lugares do mundo, diversas instituições financeiras quebraram, inclusive o centenário banco Lehman Brothers. Sob a justificativa de evitar maiores danos, os próprios bancos centrais de vários países passaram a oferecer socorro aos bancos que necessitavam. É em meio a esse sistema financeiro instável, com elevado nível de intervenção estatal, em relação ao qual a desconfiança e a perda da privacidade das pessoas eram crescentes, que emerge o que Ulrich (2014, p.44) bem designa como sendo o "experimento Bitcoin".

Apesar de ser conhecido como sendo criação de Satoshi Nakamoto – pseudônimo de um programador ou de grupo de programadores anônimo (s) – o Bitcoin é, na verdade, o resultado da atividade em comum de diversas pessoas. Trata-se de uma moeda digital, *peer-to-peer*, de código aberto e que não depende de nenhuma autoridade central.

Até a invenção do Bitcoin, em 2008, todas as transações on-line tinham por requisito a presença de um terceiro intermediário de confiança. Este era responsável por manter um registro histórico das transações evitando, assim, o problema do "gasto duplo", isso é, quando alguém consegue gastar as mesmas moedas digitais mais de uma vez em diferentes transações. A entidade que realiza o papel de intermediário – por exemplo, a Visa, a Mastercard ou o Paypal – é quem verifica se a moeda já foi gasta, validando ou não a transação. Assim, o funcionamento do sistema é centralizado, o que exige que todos os participantes confiem na autoridade central, sendo dela dependentes. E, além disso, por ser centralizado, qualquer erro/problema na autoridade central pode colocar em xeque o funcionamento de todo o sistema.

Ao escrever acerca de sua proposta para o Bitcoin, Satoshi Nakamoto (2008) esclarece que ele estava trabalhando em um sistema totalmente *peer-to-peer*, sem a presença de uma terceira parte confiável, e que permitiria aos participantes o anonimato. Para ele, a questão problemática girava em torno da confiança na entidade central:

> O problema básico da moeda convencional é toda a confiança necessária para que ela funcione. O banco central deve ser confiável para não depreciar a moeda, mas a história das moedas fiduciárias está cheia de violações dessa confiança. Os bancos devem ser confiáveis para manter nosso dinheiro e transferi-lo eletronicamente, mas eles o emprestam em ondas de bolhas de crédito com apenas uma fração de reserva. Temos que confiar neles com nossa privacidade, confiar neles para não deixar que os ladrões de identidade drenem nossas contas. Seus enormes

> custos indiretos tornam os micropagamentos impossíveis (NAKAMOTO, 2009, sem paginação, tradução nossa).

Eis o complexo problemático com o qual ele se deparava: como garantir que as transações econômicas possam ocorrer na ausência de um intermediário confiável sem que, com isso, o gasto duplo possa ocorrer a ponto de colocar em xeque o próprio sistema? Para Ulrich (2014), duas tecnologias, em especial, estão envolvidas na criação do Bitcoin: a distribuição de um banco de dados por meio de uma rede *peer-to-peer* e a criptografia.

Diferentemente das redes nas quais há um servidor central ao qual os nós – clientes – se conectam, na rede *peer-to-peer* cada um dos nós funciona tanto como cliente quanto como servidor, tornando desnecessária a figura de um servidor central. Assim, a rede *peer-to-peer* é descentralizada e a força computacional é distribuída. No caso do Bitcoin, é o *blockchain* – uma espécie de livro de registro – que é distribuído para todos nós, que possuem, assim, cada um deles, uma cópia atual e fidedigna do histórico de transações (ULRICH, 2014).

Não faz sentido para o Bitcoin, portanto, ter um banco central ou qualquer instituição financeira centralizada, seja para autenticar as transações seja para manter um histórico das mesmas. Além disso, enquanto os bancos mantêm a maior parte dos registros das transações reservadas, o *blockchain* é público, isto é, qualquer um pode ter acesso a todas as transações já realizadas, desde a primeira até a mais recente.

A criptografia, por usa vez, cumpre, de acordo com Ulrich (2014, p.45-46), tanto a função de “impossibilitar que um usuário gaste os bitcoins da carteira de outro usuário (autenticação e veracidade das informações)”, quanto a de “impedir que o *blockchain* seja violado e corrompido (integridade e segurança das informações, evita o gasto duplo)”.

Em relação à primeira função, trata-se da implementação da dupla de chaves privada e pública, que são combinações de letras e números. Se a chave privada permite gastar os bitcoins de um endereço, é a partir da chave pública que se geram endereços para se receber bitcoins. São os endereços que são compartilhados no *blockchain* que podem ser vistos por todos. Mesmo que cada endereço seja público, não é possível, de antemão, identificar a quem ele pertence. E, além disso, apenas quem possuí a chave privada a ele associado pode realizar transações.

Em relação à segunda função, é por meio da criptografia que as transações são validadas. Para que um novo bloco de transações seja acrescentado à cadeia de blocos – o *blockachain* – é necessário resolver um problema criptográfico, isto é, encontrar uma determinada função *hash*. Este trabalho se torna tanto mais difícil quanto mais blocos já fazem parte do *blockchain*. Desse modo, o consenso descentralizado substituí a confiança em uma entidade centralizada.

Obviamente, apenas traçamos linhas gerais, bastante imprecisas, o que é o sistema Bitcoin. Nosso interesse não é nem seremos detalhistas nem exaustivos. Antes, o que queremos apontar é que diante de um complexo problemático – que envolve vários aspectos como centralização/descentralização, o problema do duplo gasto, anonimato – o Bitcoin é uma atualização marcada por inventividade, um *hack* que cria novas condições para transações financeiras.

Que mundo é criado quando se opta por realizar transações por meio do sistema Bitcoin? Dentre outros aspectos, destacamos que as instituições financeiras – como os bancos e as operadoras de cartão de crédito – deixam de ter acesso privilegiado ao histórico das transações realizadas pelos indivíduos. No *blockchain* é possível visualizar que um determinado valor saiu de um endereço e foi enviado a outro, mas não se sabe ao que se refere, isto é, se é a uma compra, a uma prestação de serviço, a um empréstimo ou ao pagamento de uma antiga dívida. É possível saber quando as transações ocorreram, mas não quem nelas esteve envolvido.

Sem dúvida, ao aumentar o anonimato, criam-se condições para transações ilegais. Mas também se criam condições para escapar, em maior ou menor medida, das estratégias e dos mecanismos que dependem do contínuo controle e monitoramento das ações no mercado financeiro, e que operam por meio da servidão maquínica e da sujeição social. Neste sentido, o uso do sistema Bitcoin aproxima-se do uso do papel moeda, pois tal como este deixa poucos rastros que podem contribuir para identificar indivíduos relacionando-os às transações ocorridas e, ao mesmo tempo, reduzem a produção de dados para a elaboração de perfis.

Portanto, com o sistema Bitcoin a posição de sujeito enquanto cliente bancário é, de certo modo, colocada em xeque, desestabilizando relações de saber-poder constituídas. Isto porque cada usuário é, a princípio, responsável por gerenciar sua

própria carteira de Bitcoin. Ou seja, a função de zelar pelas moedas digitais não cabe a um terceiro – a não ser que seja delegada como alguns fazem com *exchanges* –, mas é o próprio sujeito que administra sua carteira e seus recursos, é ele quem tem a chave privada para poder acessar suas moedas e realizar transações. É como se ele possuísse seu próprio banco escapando, de certo modo, à identidade de cliente do sistema bancário que geralmente lhe é atribuída em nossa sociedade. Sem sair do mercado financeiro e nem mesmo do capitalismo, o usuário do Bitcoin pode experienciar outros mundos – outras modalidades de relação – e participar de outros processos de subjetivação.

2.5 Potência de Afetar e Ser Afetado

Ainda que tenhamos dado ênfase ao processo de atualização, os fenômenos são bem mais complexos. Vimos dois processos, o de atualização – que vai do virtual ao atual – e o de realização – que vai do potencial ao real. Além desses, há também os processos de virtualização – que vai do atual ao virtual – e o de potencialização – que vai do real ao potencial. Sem adentrarmos em muitos detalhes quanto aos dois últimos, apenas apontaremos que, de acordo com Lévy (1996), tratam-se de distinções conceituais e não de um princípio de classificação exclusivo, pois na análise de um fenômeno concreto e particular tais processos aparecem, quase sempre, operando juntos através de mistos.

Há situações nas quais alguns desses processos podem ocupar o primeiro plano. É o caso da hackeação quando as virtualizações – enquanto remontar inventivo de uma solução a uma problemática – e as atualizações – enquanto resolução inventiva de um complexo problemático – tendem a ser mais presentes. Em outras situações, segundo Lévy (1996), as virtualizações podem ser bloqueadas – transformando maquinações vivas e abertas em mecanismos mortos – e as atualizações cortadas – tornando os problemas estéreis, incapazes de ação inventiva.

A criação, seja pela resolução ou pela invenção de problemas, não coloca em movimento apenas a emergência de novos objetos, mas, sobretudo, de novas possibilidades de vida, de novos mundos. Mas a própria ação inventiva só pode ocorrer quando o campo de sensibilidade é transformado, isto é, quando uma nova maneira de ser afetado se faz presente. Trata-se de ver o que já estava aí, mas não era visto. Se o

vidente não é aquele que vê o futuro, mas aquele que “aprende o intolerável em uma situação” (ZOURABICHVILI, 2000, p.340), o hacker, enquanto visionário, não é alguém que está à frente de seu tempo, tal qual concebe Levy (2012b). Antes, o que está em jogo nas práticas de hackeação é a potência de ser afetado, a presença de uma sensibilidade outra.

No encontro com os mecanismos de vigilância e monitoramento, por exemplo, muitos hackers são profundamente afetados. Não porque eles se dão conta de que já não possuem tanta privacidade – algo restrito a uma tomada de consciência –, mas porque juntamente com a maquinaria de vigilância e monitoramento também apreendem algo que ultrapassa a atualidade da situação, isto é, não só “as potencialidades que ela atualiza, mas [também] que poderiam se atualizar de outro modo” (ZOURABICHVILI, 2000, p.341). A ênfase deve ser dada ao “se atualizar de outro modo”, é justamente aquilo com o qual nós nos encontrávamos cotidianamente, mas que não nos afetava que afeta o hacker. É por isso que o *hacking* não diz respeito, em um primeiro momento, ao campo da *expertise*, pois o que está em jogo antes de tudo é a distribuição dos afetos, o campo de sensibilidade.

Peter Samson, ao qual fizemos referência na Primeira Parte, tinha a potência de ser afetado pelas diferentes vibrações sonoras produzidas pelo TX-0. Foi isso, e não um conhecimento técnico extenso e aprofundado, que lhe deu condições de “ouvir” o computador nele operar atualizando-o de tal maneira a tocar a melodia de Bach. É claro que também se fez presente sua potência de afetar, mas esta, no caso da hackeação, é secundária em relação à potência de ser afetado. Antes de criar algo – atualizando virtuais – o hacker é aquele capaz de inventar problemas, isto é, efetuando a passagem da solução dada no aqui e agora em direção ao campo problemático, desmontando o que é dado como resolvido, multiplicando os olhares e perspectivas, torcendo saberes instituídos e hegemônicos.

CONSIDERAÇÕES FINAIS

Ao longo desta tese, conspiramos com alguns hackers modos outros de compor com os objetos técnicos existentes na contemporaneidade. Nos deparamos com mecanismos de poder que agem sobre nós, afetando-nos e produzindo-nos. E, ainda que tenhamos abordado algumas práticas de liberdade, em momento algum tivemos a pretensão de responder à pergunta “o que fazer?”, isto é, trançando um programa ou projeto de ação concreta.

Ao abrir algumas caixas-pretas, dando visibilidade ao modo pelo qual operam e descrevendo seus esquemas de funcionamento, buscamos criar condições para outros acoplamentos nos quais possamos participar de modo mais inventivo. Não ignoramos a complexidade das redes de objetos técnicos das quais participamos cotidianamente. Temos ciência de que ninguém, isoladamente, pode compreendê-las em sua totalidade. E nem é nossa intenção que alguém o faça. Neste sentido, estamos em sintonia com o Comitê Invisível quando este declara:

> Ora, ninguém pode dominar individualmente o conjunto de técnicas que permitem ao sistema atual se reproduzir. Apenas uma força coletiva pode fazer isso. Construir uma força revolucionária, nos dias de hoje, é justamente isto: articular todos os mundos e todas as técnicas revolucionariamente necessárias, agregar toda a inteligência técnica numa força histórica, e não num sistema de governo (COMITÊ INVISÍVEL, 2016, p.115–116).

Assim, afirmamos a potência da produção e do fazer comum. Trata-se de compor uns com os outros, assim como com os objetos técnicos, constituindo corpos mais potentes.

Simondon (2007) há muito já abordava o modo como, majoritariamente, nos relacionamos com os objetos técnicos, isto é, reconhecendo-os, basicamente, por sua utilidade e por seus resultados. De fato, o caráter técnico do nosso mundo vivido tende a nos escapar e, não raro, apenas nos salta aos olhos quando nos deparamos ou com alguma invenção ou quando há uma pane, um “apagão”, algo quebra ou para de funcionar (COMITÊ INVISÍVEL, 2016). Salvo nestes casos, tendemos a ignorar a realidade técnica, parte essencial das condições de nossa existência, que produzimos e na qual somos engendrados.

Sabemos que os objetos técnicos podem parecer ameaçadores e, até mesmo, nos despertar um sentimento de incompetência, levando-nos a ignorar suas condições de funcionamento e delegando as decisões aos *experts* das áreas de informática, de engenharia, de estatística etc., entretanto, quanto mais nos relacionamos com os objetos técnicos como sendo fechados, mais urgente se torna a difusão de uma cultura técnica.

Estaríamos convidando a todos para experienciar práticas hackers? Sim, é justamente isto, ou seja, que nossos leitores possam se deixar afetar pelos objetos técnicos, experienciando novos territórios existenciais, afetivos, cognitivos, políticos etc. É preciso reforçar que uma existência hacker – com suas práticas – não é uma alternativa entre ser músico, advogado – ou qualquer outro ofício – e ser hacker. Também não se trata de uma diferença de grau que iria daqueles sem conhecimentos técnicos até aqueles que seriam os *experts*. Talvez ainda tenha ficado ao leitor a sensação de que ser hacker é algo reservado apenas para uma suposta elite – tal qual compreende Flichy (2017), por exemplo. Sem dúvida, muitos hackers são conhecidos por suas proezas que, não raro, exigem conhecimentos técnicos avançados. Entretanto, pensamos que a existência hacker é sempre derivada das práticas hackers, isto é, só podemos denominar alguém de hacker a partir do reconhecimento de suas práticas de hackeação. Samson (2005b), responsável pela redação do *TMRC Dictionary,* já definia hacker enquanto "alguém que hackeia, ou faz *hacks*", explicando que o hacker evita a solução padrão e que um hacker é definido por seus *hacks*.

Claro que há práticas que se fundamentam em conhecimentos técnicos que exigem longos anos de aprendizado, mas há também aquelas cujos requisitos são bem menos exigentes. Uma existência hacker está longe de ser algo que está apenas ao alcance de *geeks*, de aficionados por tecnologia ou *experts* em suas áreas. O que está em jogo na hackeação é um saber que é capaz de instalar-se no devir interior das coisas, e que com elas se compõe atualizando virtuais, criando novos mundos.

Apesar das divergências que possuímos com Raymond (2015, tradução nossa) – por exemplo, na diferenciação que ele realiza entre hackers e crackers –, não podemos deixar de concordar que o modo de existência hacker não é restrito à cultura dos hackers de software, mas pode ser encontrado em "qualquer ciência ou arte". Ou seja, é possível ser advogado e hackear as leis – tal qual o fez Stallman –, músico e hackear o conteúdo

musical – tal como Gilberto Gil. Se não há "*hacker* sem máquina", como afirma Cardoso (2016, p.136), é preciso compreender a máquina do modo mais amplo possível, isto é, que ela não é só técnica, mas, tal qual ele define a partir de Deleuze e Guattari (2010, p.7), que a "máquina é qualquer coisa que se conecte a outra". Há máquinas de todos os tipos, das composições mais heterogêneas, de conexões das mais diversas.

Quando alguém almeja tornar-se um hacker – fazendo de si um hacker – o que se busca é dar contornos a sua vida, de tal modo que as práticas de hackeação se façam presentes frequentemente. Isso implica a ação criativa, composições inusitadas com os objetos técnicos, a invenção de novos mundos, a abertura para novas percepções, a produção e a defesa do comum. Uma ética hacker é um modo de existência no qual hackear é uma maneira de viver e habitar o mundo, criando possíveis.

Então toda e qualquer prática hacker é bem-vinda? Ora, estamos longe de afirmar isso. O *hacking* não é, por si só, garantia de aumento dos graus de liberdade, da ampliação dos espaços individuais e coletivos de liberdade. No encontro com a realidade técnica há experimentações que aumentam a potência de afetar e de ser afetado, assim como há aquelas que reduzem a potência de afetar e de ser afetado. Privilegiamos, ao longo da tese, compartilhar aquelas que, para nós, constituem-se de encontros alegres. Porém, ao leitor, cabe fazer seu caminho e, como não sabemos de antemão, o que pode um corpo (no encontro com outros corpos), resta apostar (prudentemente) na experimentação e na abertura ao inusitado.

REFERÊNCIAS

ACAR, G. et al. The Web Never Forgets: Persistent Tracking Mechanisms in the Wild. *In:* ACM SIGSAC - CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, 21., 3-7 nov. 2014. **Proceedings...** Disponivel em: https://doi.org/10.1145/2660267.2660347 Acesso em: 15 abr. 2019.

ADAMS, T. AI-Powered Social Bots. **arXiv:1706.05143v1,** 16 jun. 2017.. Disponivel em: http://arxiv.org/abs/1706.05143. Acesso em: 15 abr. 2019.

AIGRAIN, P. **Cause Commune:** L'information entre bien commun et propriété. Paris: Fayard, 2005.

AKERA, A. Voluntarism and the Fruits of Collaboration: The IBM User Group, Share. **Technology and Culture**, v. 42, n. 4, p. 710–736, 2001. Disponivel em: https://doi.org/10.1353/tech.2001.0146. Acesso em: 15 abr. 2019.

ALEXANDER NIX, CEO, Cambridge Analytica - Online Marketing Rockstars Keynote | OMR17. OMR (Online Marketing Rockstars), 10 mar. 2017. 1 vídeo (30 min). Disponível em: https://www.youtube.com/watch?v=6bG5ps5KdDo. Acesso em: 15 abr. 2019.

ALEXANDER, N. Catered to Your Future Self: Netflix's "Predictive Personalization" and the Mathmatization of Taste. *In:* MCDONALD, K.; SMITH-ROWSEY, D. (org.). **The Netflix Effect:** Technology and Entertainment in the 21st Century. [*S. l.*]: Bloomsbury Publishing USA, 2016. p. 81–97.

AMARAL, F. **Introdução à ciência de dados:** mineração de dados e Big Data. Rio de Janeiro: Alta Books, 2016.

ANGWIN, J. Why Online Tracking Is Getting Creepier. **Propublica,** 12 jun. 2014. Disponivel em: https://www.propublica.org/article/why-online-tracking-is-getting-creepier. Acesso em: 21 jun. 2018.

ANTOUN, H. De uma teia à outra: a explosão do comum e o surgimento da vigilância participativa. In ANTOUN, H. (org.). **Web 2.0:** participação e vigilância na era da comunicação distribuída. Rio de Janeiro: Mauad X, 2008. p. 11–28.

ARAY, N. Ethos Technicien et Information: Simondon reconfiguré par les hackers. *In:* ROUX, J. (org.). **Gilbert Simondon:** une pensée opérative. Saint-Étienne: Université de Saint-Etienne, 2002. p. 109–130.

ASSANGE, J. **Cypherpunks:** liberdade e o futuro da internet. Tradução de Cristina Yamagami. São Paulo: Boitempo, 2013.

BACHRACH, Y. et al. Personality and Patterns of Facebook Usage. *In:* WEB SCIENCE'12 - INTERNATIONAL ACM WEB SCIENCE CONFERENCE, 12., 22-24

June 2012. **Proceedings...** Disponivel em: https://doi.org/10.1145/2380718.2380722. Acesso em: 15 abr. 2019.

BARRETT, B. Netflix Isn't Made for the US Anymore - It's for the Whole World. **Wired,** 13 jan. 2016a. Disponivel em: https://www.wired.com/2016/01/in-the-us-were-now-watching-the-worlds-netflix/. Acesso em: 15 abr. 2019.

BARRETT, B. (2016b, março 27). Netflix's Grand, Daring, Maybe Crazy Plan to Conquer the World. **Wired,** 27 mar. 2016b. Disponivel em: https://www.wired.com/2016/03/netflixs-grand-maybe-crazy-plan-conquer-world/. Acesso em: 15 abr. 2019.

BARTHÉLÉMY, J. H. **Simondon, ou, l'encyclopédisme génétique**. Paris: Presses universitaires de France, 2008.

BARTHÉLÉMY, J. H. Glossaire Simondon: les 50 grandes entrées dans l'œuvre. **Appareil,** n. 16, 2015. Disponivel em: https://doi.org/10.4000/appareil.2253. Acesso em: 15 abr. 2019.

BARTHÉLÉMY, J.H. Genèse, histoire et <<normativité technique>>. *In:* M. Centre culturel international. *In:* BONTEMS, V. (org.). **Gilbert Simondon ou l'invention du futur:** actes de la décade des 5-15 août 2013 du Centre culturel international de Cerisy-la-Salle. Paris: Klincksieck, 2016. p. 17–32.

BELISÁRIO, A. Sobre guerrilhas e cópias. *In:* TARIN, B.; BELISÁRIO, A. (org.). **Copyfight**. Rio de Janeiro: Beco do Azougue, 2012. p. 75–92.

BERGSON, H. **A evolução criadora.** São Paulo: UNESP, 2010.

BERNARD, P. Grandes oreilles: A l'automne doit être inauguré le centre d'interception des communications de la NSA près de Bluffdale, dans l'Utah. Un «big data center» aux capacités titanesques, construit dans le secret. **Le Temps,** 28 ago. 2013. Disponivel em: https://www.letemps.ch/societe/grandes-oreilles. Acesso em: 15 abr. 2019.

BEWARE: HACKERS AT PLAY. (1983). Newsweek. Disponivel em: http://www.ismlab.usf.edu/isec/files/Beware_HackersAtPlay_Newsweek_09_05_1983.docx. Acesso em: 15 abr. 2019.

BLONDEAU, O. Des hackers aux cyborgs: le bug simondonien. **Multitudes,** v. 18, n. 4, p. 91, 2004. Disponivel em: https://doi.org/10.3917/mult.018.0091. Acesso em: 15 abr. 2019.

BOGOST, I. My Cow Game Extracted Your Facebook Data. The Atlantic website, 22 mar. 2018. Disponivel em: https://www.theatlantic.com/technology/archive/2018/03/my-cow-game-extracted-your-facebook-data/556214/. Acesso em: 20 jan. 2019.

BONDÍA, J. L. (2002). Notas sobre a experiência e o saber de experiência. **Revista Brasileira de Educação**, v. 19, p. 20–28, 2002. Disponivel em: https://doi.org/10.1590/S1413-24782002000100003. Acesso em: 15 abr. 2019.

BONTEMS, V.¡ Esclavos y máquinas, el mismo combate! La alienación según Marx y Simondon. *In:* BLANCO, J.; PARENTE, D.; RODRÍGUEZ, P. (org.). **Amar a las máquinas:** cultura y técnica en Gilbert Simondon. Buenos Aires: Prometeo Libros, 2015. p. 195–210.

BORDELEAU, É. **Foucault anonimato.** Cidade Autónoma de Buenos Aires: Cactus, 2018.

BOSHMAF, Y. et al. The socialbot network: when bots socialize for fame and money. *In:* ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE, 27., 2011. ACM. **Proceedings...** Orlando, USA: ACM, 2011. p. 93–102.

BRETON, P. **Une histoire de l'informatique.** Seuil: Éditions du Seuil, 1990. (Collection Points: Série Sciences).

BRUNO, F. Mapas de crime: vigilância distribuída e participação na cultura contemporânea. *In:* BRUNO, F.; KANASHIRO, M.; FIRMINO, R. (org.). **Vigilancia e visibilidade:** espaco, tecnologia e identificação. Porto Alegre: Sulina, 2010. p. 155–173.

BRUNO, F. **Máquinas de ver, modos de ser:** vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013.

BRUNO, F. Rastrear, classificar, performar. **Ciência e Cultura**, v. 68, n. 1, p. 34–38, 2016. Disponivel em: https://doi.org/10.21800/2317-66602016000100012. Acesso em: 15 abr. 2019.

BRUNO, F. Objetos técnicos sem pudor: gambiarra e tecnicidade. **Revista ECO-Pós,** v. 20, n. 1, p. 136–149, 2017. Disponivel em: https://revistas.ufrj.br/index.php/eco_pos/article/view/10407. Acesso em: 15 abr. 2019.

CABANAC, G. Bibliogifts in LibGen? A study of a text-sharing platform driven by biblioleaks and crowdsourcing. **Journal of the Association for Information Science and Technology,** v. 67, n. 4, p. 874–884, 2016. Disponivel em: https://doi.org/10.1002/asi.23445. Acesso em: 15 abr. 2019.

CAMBRIDGE Analytica - The Power of Big Data and Psychographics. [*S.l.*]: Concordia, 2016. 1 Video [11 min]. Disponivel em: https://www.youtube.com/watch?v=n8Dd5aVXLCc. Acesso em: 15 abr. 2019.

CAO, Y., LI, S.; WIJMANS, E. **(Cross-) Browser Fingerprinting via OS and Hardware Level Features**. 1 jan. 2017. Disponivel em: https://doi.org/10.14722/ndss.2017.23152. Acesso em: 15 abr. 2019.

CARDOSO FILHO, C. A. **Máquinas, Mônadas, Daemons:** uma breve história e filosofia da máquina universal de Turing. 2016. 271 f. Tese (Doutorado em Psicologia Social e Institucional) – Instituto de Psicologia, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2016.

CARROZZINI, G. Simondon et le design du futur. *In:* BONTEMS, V. (org.). **Gilbert Simondon ou l'invention du futur.** Paris: Klincksieck, 2016. p. 89–99.

CASTELLS, M. **Hackers, crackers, seguridad y libertad.** out. 2001. Disponivel em: https://www.uoc.edu/web/esp/launiversidad/inaugural01/hackers.html#bibliografia. Acesso em: 18 fev. 2019.

COLEMAN, E. G. Phreake, Hackers, and Trolls: The Politics of Transgression and Spectacle. *In:* MANDIBERG, M. (org.). **The social media reader.** New York: New York University Press, 2012. p. 99-119.

COLEMAN, E. G. **Coding freedom:** the ethics and aesthetics of hacking. Princeton: Princeton University Press, 2013.

COLLE, J.; LEDOX, L.; VLAJCIC, C. Gouvernementalité algorithmique: arme ultime pour ne pas changer le monde? **Peoplesphere,** n. 211, p. 56–58, mar. 2017. Inclusive está disponível em: https://philoma.org/wp-content/uploads/docs/2016_2017_Algorithmes/Ledoux_-_Vlajcic_-_Rouvroy_-_Gouvernemantalite_algorithmique_-_Peoplesphere_-_PSFR211-Opinion.pdf. Não sei se seria o caso de incluir o link. A princípio, não vejo necessidade. Mas foi lá que acessei.

COLOMBAIN, J.; LECOMTE, Y.; SOREL, F. **Ces objets connectés qui vont changer votre vie.** Paris: First Interactive, 2015.

COMITÊ INVISÍVEL. **Aos nossos amigos:** crise e insurreição. [*S.l.*]: N-1 edições, 2016.

COPYLEFT ATTITUDE. Licença da Arte Livre 1.3. 2007. Disponivel em: http://artlibre.org/licence/lal/pt/. Acesso em: 3 jan. 2019.

CREATIVE COMMONS BRASIL. **Sobre as Licenças.** Disponível em: https://br.creativecommons.org/licencas/. Acesso em: 3 jan. 2019.

CURCIO, A.; ROGGERO, G. Prefácio. *In:* MENDES, A. F.; CAVA, B. **A constituição do comum:** antagonismo, produção de subjetividade e crise no capitalismo. Rio de Janeiro: Revan, 2017. p. 7–12.

DARDOT, P.; LAVAL, C. **Comum:** ensaio sobre a revolução no século XXI. São Paulo: Boitempo, 2017.

DATA Selfie: a browser extension to track yourself on Facebook and analyze your data. [2018]. Disponivel em: https://github.com/d4t4x/data-selfie. Acesso em: 15 abr. 2019.

DATA X. Data Selfie. Disponivel em: https://dataselfie.it. Acesso em: 3 set. 2018.

DAVIS, K.; PATTERSON, D. **Ethics of Big Data.** [*S.l.*]: O'Reilly Media, Inc., 2012.

DELEUZE, G. Controle e Devir. *In:* DELEUZE, G. **Conversações.** Tradução de Peter Pál Pelbart. 2. ed. São Paulo: Editora 34, 1992a. p. 213–222.

DELEUZE, G. Post-Scriptum sobre Sociedade do Controle. *In:* DELEUZE, G. **Conversações.** Tradução de Peter Pál Pelbart. 2. ed. São Paulo: Editora 34, 1992b. p. 209–226.

DELEUZE, G. **Diferença e Repetição.** Lisboa: Relógio D'Água, 2000.

DELEUZE, G. **Espinosa:** filosofia prática. São Paulo: Escuta, 2002.

DELEUZE, G. **Foucault.** São Paulo: Brasiliense, 2005.

DELEUZE, G. **En medio de Spinoza.** Buenos Aires: Cactus, 2008.

DELEUZE, G. **Bergsonismo**. Tradução de Luiz B. Lacerda Orlandi. São Paulo: Editora 34, 2012.

DELEUZE, G.; GUATTARI, F. **O Anti-Édipo:** capitalismo e esquizofrenia. São Paulo: Editora 34, 2010.

DELEUZE, G.; GUATTARI, F. **Kafka:** por uma literatura menor. Belo Horizonte: Autêntica Editora, 2015.

D'ALAMBERT, J. le R. Discurso preliminar dos editores (Junho de 1751). *In:* PIMENTA, P. P.; SOUZA, M. G. (org.). **Enciclopédia, ou Dicionário razoado das ciências, das artes e dos ofícios - Diderot e d'Alambert.** Tradução de Fulvia M. L. Moretto. São Paulo: Unesp, 2015. p. 43–265. (Volume I: Discurso preliminar e outros textos).

DIJKSTRA, E. W. **Notes On Structured Programming**. 1970. Disponível em: https://www.cs.utexas.edu/users/EWD/ewd02xx/EWD249.PDF. Acesso em: 13 nov. 2016.

DIJKSTRA, E. W. The humble programmer. **Communications of the ACM**, v. 15, n. 10, p. 859–866, 1972.

DUCKDUCKGO website. Disponível em: https://duckduckgo.com/privacy. Acesso em: 9 fev. 2019.

DUHIGG, C. How Companies Learn Your Secrets. **The New York Times,** 12 fev. 2012. Disponível em: http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html. Acesso em: 15 abr. 2019.

EDSON, J. et al. (org.). **SHARE Reference Manual:** For the IBM 704. [*S. l.*]: IBM, 1956. Disponível em: http://www.piercefuller.com/scan/share59.pdf?id=share59. Acesso em: 15 abr. 2019.

ENIAC PROGRAMMERS PROJECT. See The Film. [*S. l.*]: Eniac programmers, [s. d]. Disponível em: http://eniacprogrammers.org/see-the-film/. Acesso em: 04 mar. 2019.

ENSMENGER, N. **The computer boys take over:** computers, programmers, and the politics of technical expertise. Cambridge: MIT Press, 2010. (History of computing).

EVANGELISTA, R. A. **Traidores do movimento:** política, cultura, ideologia e trabalho no Software Livre. 2010. 121 f. Tese (Doutorado em Pós-Graduação em Antropologia Social) - Universidade Estadual de Campinas, Campinas, 2010.

FERRARA, E. et al. The rise of social bots. **Communications of the ACM**, v. 59, n. 7, p. 96–104, jul. 2016. Disponível em: https://doi.org/10.1145/2818717. Acesso em: 15 abr. 2019.

FISHMAN, K. D. **The computer establishment.** New York; Montréal: McGraw-Hill, 1982.

FLICHY, P. **Les nouvelles frontières du travail à l'ère numérique.** Paris: Éditions du Seuil, 2017.

FONSECA, F. Por licenças mais poéticas. *In:* TARIN, B.; BELISÁRIO, A. (org.). **Copyfight**. Rio de Janeiro: Beco do Azougue, 2012. p. 151–152.

FOUCAULT, M. Sobre a Prisão. *In:* MACHADO, R. (org.). **Microfísica do poder**. Rio de Janeiro: Graal, 1979. p. 129-143.

FOUCAULT, M. O Sujeito e o Poder. *In:* DREYFUS, H. L.; RABINOW, P. **Michel Foucault, uma trajetória filosófica:** para além do estruturalismo e da hermenêutica. Rio de Janeiro: Forense Universitária, 1995. p. 231–249.

FOUCAULT, M. **Vigiar e punir:** nascimento da prisão. Tradução de R. Ramalhete. Petrópolis: Vozes, 2010.

FOUCAULT, M. 1979 - É Inútil Revoltar-se? *In:* MOTTA, M. B. (org.). **Ética, sexualidade, política**. 3. ed. Rio de Janeiro: Forense Universitária, 2012. p. 76–80.

FOUCAULT, M. **A ordem do discurso:** aula inaugural no Collège de France, pronunciada em 2 de dezembro de 1970. São Paulo: Edicoes Loyola, 2014.

FOUCAULT, M. 1984 – O que São as Luzes? *In:* MOTTA, M. B. (org.). Traduçaão de E. Monteiro. **Arqueologia das ciências e história dos sistemas de pensamento.** Rio de Janeiro: Forense Universitária, 2015. p. 351-368.

FREE SOFTWARE FOUNDATION. O Sistema Operacional GNU. 1989. Disponível em: https://www.gnu.org/licenses/old-licenses/gpl-1.0.html. Acesso em: 19 jan. 2017.

FROIDEVAUX, C.; ABITEBOUL, S. Autour de l'informatique: les algorithmes et la disparition du sujet. **The conversation,** 22 jan. 2016. Disponível em: http://theconversation.com/autour-de-linformatique-les-algorithmes-et-la-disparition-du-sujet-53515. Acesso em: 15 abr. 2019.

GALLOWAY, A. R. **Protocol how control exists after decentralization.** Cambridge; London: MIT Press, 2004.

GOETZ, M. Memoirs of a Software Pioneer: Part 1. **IEEE Annals of the History of Computing**, v. 24, n. 1, p. 43–56, 2002.

GOETZ, M. 50 Years of Controversy Rages On: A Closer Look at Computer-Implemented Inventions. **Patents & Patent Law**, 11 out. 2016. Disponível em: http://www.ipwatchdog.com/2016/10/11/50-years-controversy-computer-implemented-inventions/id=73560/. Acesso em: 2 nov. 2016.

GOMES, R. D. P. **Big Data:** desafios à tutela da pessoa humana na sociedade da informação. Rio de Janeiro: Lumen Juris, 2017.

GOMEZ-URIBE, C. A.; HUNT, N. The Netflix Recommender System: Algorithms, Business Value, and Innovation. **ACM Trans. Manage. Inf. Syst.**, v. 6, n. 4, p. 13:1–13:19, jan. 2015. Disponível em: https://doi.org/10.1145/2843948. Acesso em: 15 de abr. 2019.

GOODE, E. Data-Crunching Program Guides Santa Cruz Police Before a Crime. **The New York Times,** 15 ago. 2011. Disponível em: https://www.nytimes.com/2011/08/16/us/16police.html. Acesso em: 15 abr. 2019.

GRANDE, R. E. D. Sistema de Integração de Técnicas de Proteção de Privacidade que Permitem Personalização. 2006. 141 f. Dissertação (Mestrado em Ciência da Computação) - Universidade Federal de São Carlos, São Carlos, 2006. Disponível em: http://www2.dc.ufscar.br/~zorzo/pagina_mestrado_robson/dissertacao_robson.pdf. Acesso em: 15 abr. 2019.

GRASSEGGER, H.; KROGERUS, M. The Data That Turned the World Upside Down. **Motherboard**, 28 jan. 2017. Disponível em: https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win. Acesso em: 19 ago. 2018.

GREENWALD, G.; MACASKILL, E. NSA Prism program taps in to user data of Apple, Google and others. **The Guardian**, 7 jun. 2013. Disponível em: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data. Acesso em: 15 abr. 2019.

GRIMME, C. et al. Social Bots: Human-Like by Means of Human Control? **Big Data**, v. 5, n. 4, p. 279–293, 2017. Disponível em: https://doi.org/10.1089/big.2017.0044. Acesso em: 15 abr. 2019.

GROSMAN, J. Simondon et l'informatique II. *In:* BONTEMS, V. (org.). **Gilbert Simondon ou l'invention du futur:** actes de la décade des 5-15 août 2013 du Centre culturel international de Cerisy-la-Salle. Paris: Klincksieck, 2016. p. 247-254.

GUATTARI, F. **Revolução molecular:** pulsações políticas do desejo. Tradução de Suely Belinha Rolnik. São Paulo: Brasiliense, 1985.

HACKERS: Wizards of the Electronic Age. Direção: Fabrice Florin. Atores: Steve Wozniak, Andy Hertzfeld, Bill Atkinson, Lee Felsenstein, Richard Stallman. Sausalito, California: [s. n.], 1986. 1 DVD (26 min.). (Documentary).

HAFNER, K.; MARKOFF, J. **Cyberpunk:** outlaws and hackers on the computer frontier. New York; London: Touchstone, 1995.

HARDING, S. Jumping the Paywall. **Chaos Communication Camp 2015**, 16 ago. 2015a. 1 Video (16 min.). Disponível em: https://media.ccc.de/v/camp2015-6766-jumping_the_paywall#video. Acesso em: 6 jan. 2019.

HARDING, S. lecture: Jumping the Paywall. **Schedule Chaos Communication Camp 2015**, 13-17 ago. 2015b. Disponível em: https://fahrplan.events.ccc.de/camp/2015/Fahrplan/events/6766.html. Acesso em: 6 jan. 2019.

HARDT, M. The Common in Communism. **Rethinking Marxism**, v. 22, n. 3, p. 346–356, 2010. Disponível em: https://doi.org/10.1080/08935696.2010.490365. Acesso em: 15 abr. 2019.

HARDT, M.; NEGRI, A. **Império**. 4. ed. Tradução de B. Vargas. Rio de Janeiro: Record, 2002.

HARDT, M.; NEGRI, A. **Multidão.** Rio de Janeiro: Record, 2014.

HARDT, M.; NEGRI, A. **Bem-estar e comum**. Rio de Janeiro: Record, 2016.

HENNIGEN, I. Subjetivação como produção cultural: fazendo uma outra psicologia. **Psicologia & Sociedade,** v. 18, n. 2, p. 47–53, 2006. Disponível em: https://doi.org/10.1590/S0102-71822006000200007. Acesso em: 15 abr. 2019.

HERNANDES, R. Ler Contrato de Internet exige 4,5 horas. **Folha de S.Paulo**, ano 97, n. 32.407, p. A16-A17, 24 dez. 2017. Disponível em: http://acervo.folha.com.br/leitor.do?numero=48112&anchor=6074679&origem=busca&pd=f22066b36d16fed3a4d34fafce0d192d. Acesso em: 17 abr. 2019.

HIJMANS, H. **The European Union as Guardian of Internet Privacy**. [S. l.]: Springer, 2016. (Law, Governance and Technology Series - v. 31). Disponível em: https://doi.org/10.1007/978-3-319-34090-6. Acesso em: 15 abr. 2019.

HUMPHREY, W. S. Software unbundling: a personal perspective. **IEEE Annals of the History of Computing,** v. 24, n. 1, p. 59–63, 2002. Disponível em: https://doi.org/10.1109/85.988582. Acesso em: 15 abr. 2019.

IBM - INTERNATIONAL BUSINESS MACHINES. IBM 1401 Programming Systems. 1959. Disponível em: http://archive.computerhistory.org/resources/text/IBM/IBM.1401.1959.102646282.pdf. Acesso em: 29 out. 2016.

IBM - INTERNATIONAL BUSINESS MACHINES. IBM 1440: New low cost Data Processing System. 1962. Disponível em: http://archive.computerhistory.org/resources/text/IBM/IBM.1440.1962.102646250.pdf. Acesso em: 29 out. 2016.

IBM - INTERNATIONAL BUSINESS MACHINES. **Personality Insights** - IBM Cloud. 01 maio 2016. Disponível em: https://console.bluemix.net/catalog/services/personality-insights?env_id=ibm:yp:us-south. Acesso em: 05 set. 2018.

ILLICH, I. **Tools for conviviality.** Glasgow, UK: Fontana/Collins, 1975.

INTERNATIONAL TELECOMMUNICATION UNION - ITU. **ICT Facts & Figures 2017.** Jul. 2017. Disponível em: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf. Acesso em: 6 mar. 2018.

IPPOLITA. **El lado oscuro de Google:** Historia y futuro de la industria de los metadados. Barcelona: Virus editorial, 2010.

IPPOLITA. **En el acuario de facebook:** el resistible ascenso del anarco-capitalismo. Madrid: Enclave de Libros, 2012.

ISAACSON, W. **Steve Jobs:** a biografia. Tradução de B. Vargas, D. G. Bottmann e P. M. Soares. São Paulo: Companhia das Letras, 2011.

ISAACSON, W. **The innovators:** how a group of hackers, geniuses, and geeks created the digital revolution. New York: Simon & Schuster, 2014.

JANCOVICI, J.M.; GRANDJEAN, A. **Le plein, s'il vous plaît!:** la solution au problème de l'énergie. Paris: Ed. du Seuil, 2006.

JOHNSON, E. J.; GOLDSTEIN, D. Do defaults save lives? **Science,** n. 302, p. 1338–1339, 2003.

JOHNSON, L. A view from the 1960s: how the software industry began. **IEEE Annals of the History of Computing**, v. 20, n. 1, p. 36–42, 1998. Disponível em: https://doi.org/10.1109/85.646207. Acesso em: 15 abr. 2019.

JOLLIVET, P. Les multitudes seront techniques ou ne seront pas? **Multitudes**, v. 11, n. 1, p. 201, 2003. Disponível em: https://doi.org/10.3917/mult.011.0201. Acesso em: 15 abr. 2019.

KAMKAR, S. **Applied Hacking**. 11 out. 2010. Disponível em: https://samy.pl/evercookie/. Acesso em: 22 jun. 2018.

KASTRUP, V. Virtualizar/Atualizar. *In:* FONSECA, T. M. G.; NASCIMENTO, M. L.; MARASCHIN, C. (org.). **Pesquisar na diferença:** um abecedário. Porto Alegre: Sulina, 2012. p. 245–246.

KELTY, C. M. Two Bits-The Cultural Significance of Free Software. [*S. l.*]: Duke University Press 2008. Disponível em: https://twobits.net/pub/Kelty-TwoBits.pdf. Acesso em: 15 abr. 2019.

KNUTH, D. E.; PRADO, L. T. The early development of programming languages. [*S. l.*]: Stanford University, 1976. Disponível em: http://bitsavers.trailing-edge.com/pdf/stanford/cs_techReports/STAN-CS-76-562_EarlyDevelPgmgLang_Aug76.pdf. Acesso em: 31 out. 2016.

KOEBLER, J. It's Too Late. **Motherboard**, 21 mar. 2018. Disponível em: https://motherboard.vice.com/en_us/article/59jpa8/its-too-late-to-protect-your-facebook-data-cambridge-analytica. Acesso em: 20 jan. 2019.

KOLIBREE. **Features of the new Magik Toothbrush**. 2015. Disponível em: https://www.kolibree.com/en/. Acesso em: 17 jun. 2018.

KOSINSKI, M.; STILLWELL, D.; GRAEPEL, T. Private traits and attributes are predictable from digital records of human behavior. **Proceedings of the National Academy of Sciences of the United States of America**, v. 110, n. 15, p. 5802–5805, 2013. Disponível em: https://doi.org/10.1073/pnas.1218772110. Acesso em: 15 abr. 2019.

LAPERDRIX, P.; RUDAMETKIN, W.; BAUDRY, B. Beauty and the Beast: Diverting Modern Web Browsers to Build Unique Browser Fingerprints. *In:* IEEE SYMPOSIUM ON SECURITY AND PRIVACY (SP), 22-24 maio 2016. **Proceedings...** San Jose, CA, USA: IEEE, 2016. Disponível em: https://doi.org/10.1109/SP.2016.57. Acesso em: 15 abr. 2019.

LAPSELY, P. More on the Origin of "Phreak". **The History of Phone Phreaking Blog**, 4 abr. 2010. Disponível em: http://blog.historyofphonephreaking.org/2010/04/more-on-origin-of-phreak.html. Acesso em: 12 mar. 2017.

LAZZARATO, M. **As revoluções do capitalismo**. Tradução de L. Corsini. Rio de Janeiro: Civilizacao brasileira, 2006.

LAZZARATO, M. Postfacio. *In:* RAUNIG, G. **Mil máquinas:** breve filosofía de las máquinas como movimiento social. Tradução de M. Expósito. Madrid: Traficantes de sueños, 2008. p. 109-118.

LAZZARATO, M. **Signos, Máquinas, subjetividades.** São Paulo: Sesc São Paulo, 2014.

LÉVY, P. **O que é virtual.** São Paulo: Ed. 34, 1996.

LÉVY, P. **Cibercultura.** 3. ed. São Paulo: Ed. 34, 2010.

LEVY, S. **Hackers:** Heroes of the Computer Revolution - 25th Anniversary Edition. [*S. l.*]: O'Reilly Media, 2010.

LEVY, S. **Google a biografia.** São Paulo: Universo dos Livros, 2012a.

LEVY, S. **Os heróis da revolução**. São Paulo: Editora Évora, 2012b.

LICENÇA RobinRight. Istituto Recivitas, 2013. Disponível em: https://www.recivitas.org/licenca-robinright. Acesso em: 3 jan. 2019.

LISSARDY, G. Despreparada para a era digital, a democracia está sendo destruída, afirma guru do "big data". **BBC New Brasil,** 9 abr. 2017. Disponível em: http://www.bbc.com/portuguese/geral-39535650. Acesso em: 15 abr. 2019.

MACHADO, J. Sonho pirata ou realidade 2.0? *In:* TARIN, B.; BELISÁRIO, A. (org.). **Copyfight**. Rio de Janeiro: Beco do Azougue, 2012. p. 31–39.

MALINI, F.; ANTOUN, H. **[at] Internet e [hashtag] rua:** ciberativismo e mobilização nas redes sociais. Porto Alegre: Editora Sulina, 2013.

MARKOFF, J. **What the Dormouse said:** How the Sixties Counterculture Shaped the Personal Computer Industry. London: Penguin Books, 2005.

MAURENTE, V.; MARASCHIN, C.; BIAZUS, M. C. Modulações de Acoplamento Tecnológico Como Estratégia de Pesquisa e Intervenção. **Educação & Realidade**, v. 34, n. 1, 2008. Disponível em: https://seer.ufrgs.br/educacaoerealidade/article/view/8460. Acesso em: 15 abr. 2019.

MCKEON, M. **The Evolution of Privacy on Facebook**. [2010]. Disponível em: http://mattmckeon.com/facebook-privacy/ Acesso em: 17 fev. 2018.

MENDES, A. F.; CAVA, B. **A constituição do comum:** antagonismo, produção de subjetividade e crise no capitalismo. Rio de Janeiro: Revan, 2017.

MIMEE, M. et al. An ingestible bacterial-electronic system to monitor gastrointestinal health. **Science**, v. 360, n. 6391, p. 915–918, 2018. Disponível em: https://doi.org/10.1126/science.aas9315. Acesso em: 15 abr. 2019.

MINORITY Report. Direção: Steven Spielberg. Los Angeles: 20th Century Fox; DreamWorks SKG, c2002. 1 DVD (146 min.). widwscreen, color.

MOGLEN, E. L'anarchisme triomphant: Le logiciel libre et la mort du copyright. **Multitudes**, v. 5, n. 2, p. 146, 2001. Disponível em: https://doi.org/10.3917/mult.005.0146. Acesso em: 15 abr. 2019.

MOHDIN, A. Academics have found a way to access insanely expensive research papers—for free. **Quartz,** 21 out. 2015. Disponível em: https://qz.com/528526/academics-have-found-a-way-to-access-insanely-expensive-research-papers-for-free/. Acesso em: 6 jan. 2019.

MOOERS, C. N. Computer software and copyright. **ACM Computing Surveys (CSUR)**, v. 7, n. 1, p. 45–72, 1975.

MOORE, F. **Amateur Computer User Group HomeBrew Computer Club... you name it.** 15 mar. 1975. Disponível em: http://www.digibarn.com/collections/newsletters/homebrew/V1_01/homebrew_V1_01_p1.jpg. Acesso em: 15 abr. 2019.

MORE THAN 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020. **Abiresearsh,** 9 maio 2013. Disponível em: https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne/. Acesso em: 6 mar. 2018.

MOUHOT, J.-F. **Des esclaves énergétiques:** réflexions sur le changement climatique. Seyssel: Champ Vallon, 2011.

MOZZINI, C.; HENNIGEN, I. Redes digitais: um local de produção de verdades no contemporâneo? **Psicologia & Sociedade**, v. 28, n. 3, p. 412–422, 2016. Disponível em: https://doi.org/10.1590/1807-03102016v28n3p412. Acesso em: 15 abr. 2019.

MURPHY, J. Computers: A Threat from Malicious Software. **Time,** 18 abr. 2005. Disponível em: http://content.time.com/time/magazine/article/0,9171,1050549,00.html. Acesso em: 15 abr. 2019.

MYPERSONALITY PROJECT. **myPersonality.org.**, maio 2018. Disponível em: https://sites.google.com/michalkosinski.com/mypersonality. Acesso em: 20 ago. 2018.

NAKAMOTO, S. Bitcoin P2P e-cash paper. 31 out. 2008. Disponível em: http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html. Acesso em: 15 abr. 2019.

NAKAMOTO, S. Bitcoin open source implementation of P2P currency. **P2P Foundation**, 11 fev. 2009. Disponível em: http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source. Acesso em: 12 fev. 2019.

NEGRI, A.; HARDT, M. **Declaração - Isto não é um manifesto**. 2. ed. São Paulo: N-1 edições, 2016.

NELSON, T. H. **Computer Lib e Dream Machines.** South Bend: Theodor H Nelson, 1974.

NETFLIX. **Netflix Prize:** Home. 21 set. 2009. Disponível em: https://www.netflixprize.com/. Acesso em: 9 set. 2018.

NIEL, V. The Freedom of Information Act and You. **Phrack Magazine**, v. 4, n. 42, p. 12-14, 01 mar. 1993. Disponível em: http://phrack.org/issues/42/12.html#article. Acesso em: 15 abr. 2019.

NORMAN, D. A. **O design do dia-a-dia**. Rio de Janeiro: Rocco, 2006.

ORWELL, G. **1984.** 29. ed. São Paulo: Ed. Nacional, 2005.

PACIFICI, G. **O mundo após a civilização que nega a transparência:** Entrevista com Richard Stallman. Tradução de Benno Dischinger. 2 fev. 2011. Disponível em: http://www.ihu.unisinos.br/noticias/40351-o-mundo-apos-a-civilizacao-que-nega-a-transparencia-entrevista-com-richard-stallman. Acesso em: 15 abr. 2019.

PADILLA, M. **El kit de la lucha en Internet.** Madrid: Traficantes de sueños, 2012.

PARISER, E. **O filtro invisível:** o que a internet está escondendo de você. Rio de Janeiro: Zahar, 2012.

PROTECTING Your Personal Data Has Never Been This Easy. 23 jan. 2018. Disponível em: https://spreadprivacy.com/privacy-simplified/. Acesso em: 09 fev. 2019.

PURDUE UNIVERSITY. Fair Use. 2018. Disponível em: https://www.lib.purdue.edu/uco/CopyrightBasics/fair_use.html. Acesso em: 04 jan. 2019.

RAUNIG, G. **Mil máquinas:** breve filosofía de las máquinas como movimiento social. Tradução de M. Expósito. Madrid: Traficantes de sueños, 2008.

RAYMOND, E. S. **The New hacker's dictionary.** Cambridge: MIT Press, 1991.

RAYMOND, E. S. **Cracker.** 2003a. Disponível em: http://www.catb.org/jargon/html/C/cracker.html. Acesso em: 16 jan. 2017.

RAYMOND, E. S. **TECO**. 2003b. Disponível em: http://www.catb.org/jargon/html/T/TECO.html. Acesso em: 22 fev. 2017.

RAYMOND, E. S. **How To Become A Hacker**. 2015. Disponível em: http://www.catb.org/esr/faqs/hacker-howto.html. Acesso em: 03 nov. 2016.

REAL TIME STATISTICS PROJECT. FAQ. **Internet Live Stats.** [*S. d.*]. Disponivel em: http://www.internetlivestats.com/faq/. Acesso em: 11 jan. 2019.

ROBERTS, H. E.; YATES, W. Altair 8800 Minicomputer, Part I: the most powerful minicomputer project ever presented - for under $ 400. **Popular Electronics**, v. 7, n.1, jan. 1975. Disponível em: https://www.imsai.net/download/PopTronics_Jan-1975.pdf. Acesso em: 15 abr. 2019.

ROSENBAUM, R. Secrets of the little blue box. **Esquire Magazine**, v. 76, p. 117–125, 1971.

ROSSI, P. **Os Filosofos e as maquinas, 1400-1700.** São Paulo: Companhia das Letras, 1989.

ROUVROY, A. Pour une défense de l'éprouvante inopérationnalité du droit face à l'opérationnalité sans épreuve du comportementalisme numérique. **Dissensus**, n. 4, 2011. Disponível em: https://popups.uliege.be:443/2031-4981/index.php?id=963. Acesso em: 15 abr. 2019.

ROUVROY, A. The end(s) of critique: data-behaviorism vs. due-process. *In:* HILDEBRANDT, M.; DE VRIES, E. (ed.). **Privacy, Due Process and the Computational Turn.** [*S. l.*]: Rouledge, 2012. Cap. 5.

ROUVROY, A. **Des données sans personne:** le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des Big Data. [*S. l.*]: [*s. n.*], 2014. (Contribution en marge de l'Étude annuelle du Conseil d'État. Le numérique et les droits et libertés fondamentaux).

ROUVROY, A. L'art de ne pas changer le monde: Entretien avec Antoinette Rouvroy. **La Revue Nouvelle**, n. 8, p. 44–50, 2016a.

ROUVROY, A. Les algorithmes remplacent l'idée de projet par des processus d'optimisation. **TANK**, n. 15, 2016b.

ROUVROY, A.; BERNS, T. Le nouveau pouvoir statistique. Ou quand le contrôle s'exerce sur un réel normé, docile et sans événement car constitué de corps «numériques »...». **Multitudes**, v. 40, n. 1, p. 88–103, 2010. Disponível em: https://doi.org/10.3917/mult.040.0088. Acesso em: 15 abr. 2019.

ROUVROY, A.; BERNS, T. Gouvernementalité algorithmique et perspectives d'émancipation, faced with algorithmic governmentality. **Réseaux**, v. 177, p. 163–196, 2013. Disponível em: https://doi.org/10.3917/res.177.0163. Acesso em: 15 abr. 2019.

SADIN, É. **La vie algorithmique:** critique de la raison numérique. Paris: Éditions l'Échappée, 2015.

SAMSON, P. R. TMRC Dictionary. [*S. l.*]: Tech Model Railroad Club, 2005a. Disponível em: http://www.gricer.com/tmrc/dictionary1959.html. Acesso em: 19 jan. 2017.

SAMSON, P. R. TMRC Dictionary. 2. ed. [S. l.]: Tech Model Railroad Club, 2005b. Disponível em: http://www.gricer.com/tmrc/dictionary1960.html. Acesso em: 19 jan. 2017.

SANT'ANNA, D. B. Michel Foucault e os paradoxos do corpo e da história. *In:* VEIGA-NETO, A.; SOUZA FILHO, A.; ALBUQUERQUE JÚNIOR, D. M. (org.). **Cartografias de Foucault.** 2. ed. Belo Horizonte: Autêntica Editora, 2011. p. 83–91.

SANTAMARÍA, J. W. M. El individuo técnico: un objeto inevitable. *In:* BLANCO, J.; PARENTE, D.; RODRÍGUEZ, P. (org.). **Amar a las máquinas:** cultura y técnica en Gilbert Simondon. Buenos Aires: Prometeo Libros, 2015. p. 121–137.

SANTOS, L. G. dos (org.). Paradoxos da Propriedade Intelectual. *In:* VILLARES, F. **Propriedade intelectual:** tensões entre o capital e a sociedade. São Paulo: Paz e Terra S/A., 2007. p. 41–57.

SAWAYA, M. R. **Dicionário de Informática e Internet:** inglês - português. São Paulo: Nobel, 1999.

SCHOLAR. Disponível em: https://www.reddit.com/r/Scholar/. Acesso em: 04 jan. 2019.

SCI-HUB: removing barriers in the way of science. Disponível em: https://sci-hub.tw/. Acesso em: 05 jan. 2019.

SENNETT, R. **O artífice.** 4. ed. Rio de Janeiro: Record, 2013.

SILVA, I. B.; NAKANO, T. C. modelo dos cinco grandes fatores da personalidade: análise de pesquisas. **Aval. psicol.**, Porto Alegre, v.10, n.1, p. 51-62, abr. 2011. Disponível em: http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S1677-04712011000100006. Acesso em: 15 abr. 2019.

SIMONDON, G. **El modo de existencia de los objetos técnicos.** Buenos Aires: Prometeo Libros Editorial, 2007.

SIMONDON, G. **Imaginación e invención**: (1965-1966). Buenos Aires: Cactus, 2013.

SIMONDON, G. **La individualización:** a la luz de las nociones de forma y de información. Buenos Aires: Cactus, 2015.

SIMONDON, G. El efecto de halo en materia técnica: hacia una estrategia de la publicidad. *In:* SOBRE LA técnica: 1953-1983. Cidade Autónoma de Buenos Aires: Cactus, 2017a. p. 271–284.

SIMONDON, G. Entrevista sobre la mecanología: Gilbert Simondon y Jean Le Moyene (1968). *In:* SOBRE LA técnica: 1953-1983 Cidade Autónoma de Buenos Aires: Cactus, 2017b. p. 391–427.

SIMONDON, G. Entrevista sobre la tecnlogía con Yves Deforge (1965). *In:* SOBRE LA técnica: 1953-1983 Cidade Autónoma de Buenos Aires: Cactus, 2017c. p. 385–389.

SIMONDON, G. La mentalidad técnica (1961?). *In:* SOBRE LA técnica: 1953-1983. Cidade Autónoma de Buenos Aires: Cactus, 2017d. p. 285–302.

SIMONDON, G. Lugar de una iniciación técnica en una formación humana compelta (1953). *In:* SOBRE LA técnica: 1953-1983. Cidade Autónoma de Buenos Aires: Cactus, 2017e. p. 201–220.

SIMONDON, G. Prolegómenos para una reconstitución de la ensenãza (1954). *In:* SOBRE LA técnica: 1953-1983. Cidade Autónoma de Buenos Aires: Cactus, 2017f. p. 229–248.

SIMONDON, G. Psicosociología de la tecnicidad (1960-1961). *In:* SOBRE LA técnica: 1953-1983. Cidade Autónoma de Buenos Aires: Cactus, 2017g. p. 35–130.

SIMONDON, G. Respuesta a las objeciones (1954). *In:* SOBRE LA técnica: 1953-1983. Cidade Autónoma de Buenos Aires: Cactus, 2017h. p. 221–228.

SIMONDON, G. Salvar el objeto técnico (1983). *In:* SOBRE LA técnica: 1953-1983. Cidade Autónoma de Buenos Aires: Cactus, 2017i. p. 431–439.

SIMONDON, G. Las enciclopedias y el espíritu enciclopédico. *In:* SOBRE LA filosofia: 1950-1980. Cidade Autónoma de Buenos Aires: Cactus, 2018. p. 111–123.

SOMMERVILLE, I. **Engenharia de software.** São Paulo: Pearson Prentice Hall, 2011.

STALLMAN, R. **EMACS manual for ITS users**. [S. l.]: MIT, 1980. Disponível em: http://www.dtic.mil/dtic/tr/fulltext/u2/a093186.pdf. Acesso em: 15 abr. 2019.

STALLMAN, R. **EMACS:** The Extensible, Customizable Display Editor. [S. l.]: MIT, 1981. Disponível em: https://www.gnu.org/software/emacs/emacs-paper.html. Acesso em: 20 fev. 2017.

STALLMAN, R. **new UNIX implementation**. Cambridge, MA: MIT AI Lab, 1983. Disponível em: http://linux.topology.org/gnustart.txt. Acesso em: 15 abr. 2019.

STALLMAN, R. **The GNU Manifesto.** Boston, MA, USA: Free Software Foundation, 1985. Disponível em: https://www.gnu.org/gnu/manifesto.html. Acesso em: 19 jan. 2017.

STALLMAN, R. **Interview with Richard Stallman, Edinburgh, 2004**. Boston, MA: Free Software Foundation, 2004. Disponível em: https://www.gnu.org/philosophy/rms-interview-edinburgh.html. Acesso em: 22 jan. 2017.

STALLMAN, R. **O Projeto GNU.** 15 dez. 2018. Disponível em: https://www.gnu.org/gnu/thegnuproject.html. Acesso em: 2 fev. 2017.

STALLMAN, R. **What is free software?** [GNU Operating System]. C2009-2019. Disponível em: https://www.gnu.org/philosophy/free-sw.en.html. Acesso em: 24 fev. 2017.

STEPHENS-DAVIDOWITZ, S. **Todo mundo mente:** O que a internet e os dados dizem sobre quem realmente somos. Rio de Janeiro: Alta Books, 2018.

STEVAN JUNIOR, S. L.; SILVA, R. A. **Automação e instrumentação industrial com arduino:** teoria e projetos. São Paulo: Érica, 2015.

SUNSTEIN, C. **Impersonal default rules vs. active choices vs. personalized default rules:** A triptych. [*S. l.*]: Harvard, 2013.

SURVEILLANCE Camera Players: completely distrustful of all government. **Notbored**, 1996. Disponivel: http://www.notbored.org/the-scp.html. Acesso em: 10 jan. 2019.

TARIN, B.; BELISÁRIO, A. (org.). **Copyfight**. Rio de Janeiro: Beco do Azougue, 2012.

TAURION, C. **Big Data.** Rio de Janeiro: Brasport, 2015.

TAVARES, H. F. F. **Dicionário do Computador.** [*S.l.*]: Rio Gráfica Ltda, 1984.

THE PSYCHOMETRICS CENTRE. myPersonality database. Disponível em: https://www.psychometrics.cam.ac.uk/productsservices/mypersonality. Acesso em: 20 ago. 2018.

THE SECRET History of The ENIAC Women. Por Kathy Kleiman. TEDx Talks. 16 fev. 2018. 1 Video (13 min. 42 s.). Disponível em: https://www.youtube.com/watch?v=Zevt2blQyVs. Acesso em: 15 abr. 2019.

TONE ANALYZER. IBM Cloud. 1 maio 2016. Disponível em: https://console.bluemix.net/catalog/services/tone-analyzer?env_id=ibm:yp:us-south. Acesso em: 5 set. 2018.

ULRICH, F. **Bitco*ln:*** a moeda na era digital. São Paulo: Instituto Ludwig von Mises Brasil, 2014.

UNITED STATES GENERAL ACCOUNTING OFFICE. Data Mining: Federal Efforts Cover a Wide Range of Uses. [S. l.]: GAO, 2004. Disponívl em: https://www.gao.gov/new.items/d04548.pdf. Acesso em: 15 abr. 2019.

UNIVERSITY OF CAMBRIDGE PSYCHOMETRICS CENTRE. Apply Magic Sauce - Prediction API. Disponivel em: https://applymagicsauce.com/. Acesso em: 11 jan. 2019.

VAROL, O. et al. Online Human-Bot Interactions: Detection, Estimation, and Characterization. **arXiv:1703.03107**, 2017. Disponível em: http://arxiv.org/abs/1703.03107. Acesso em: 15 abr. 2019.

VASILYEV, V. **Fingerprintjs:** Anonymous browser fingerprint. Github, 2013. Disponível em: https://github.com/Valve/fingerprintjs. Acesso em: 15 abr. 2019.

VAZAMENTO de dados do Facebook atinge 443.117 usuários brasileiros. **Folha de S.Paulo**, 5 abr. 2018. Disponível em: https://www1.folha.uol.com.br/mundo/2018/04/vazamento-de-dados-do-facebook-atinge-443117-usuarios-brasileiros.shtml. Acesso em: 21 ago. 2018.

VEGA, T. Web Upgrade HTML 5 May Weaken Privacy. **The New York Times**, 10 out. 2010. Disponível em: https://www.nytimes.com/2010/10/11/business/media/11privacy.html. Acesso em:15 abr. 2019.

WARK, M. **A hacker manifesto**. Cambridge, MA: Harvard University Press, 2004.

WHEELAN, C. **Estatística:** o que é, para que serve, como funciona. Rio de Janeiro: Zahar, 2016.

WILLIAMS, S. **Free as in Freedom (2.0) Richard Stallman and the Free Software Revolution.** Boston, Ma: Free Software Foundation, 2010.

WOZNIAK, S. **Homebrew And How The Apple Came To Be.** Disponível em: http://www.atariarchives.org/deli/homebrew_and_how_the_apple.php. Acesso em: 30 mar. 2017.

WOZNIAK, S.; SMITH, G. **iWoz:** a verdadeira história da Apple segundo seu cofundador Steve Wozniak e Gina Smith. São Paulo: Évora, 2011.

YOUYOU, W.; KOSINSKI, M.; STILLWELL, D. Computer-based personality judgments are more accurate than those made by humans. **Proceedings of the National Academy of Sciences**, v. 112, n. 4, p. 1036–1040, 2015. Disponível em: https://doi.org/10.1073/pnas.1418680112. Acesso em: 15 abr. 2019.

ZOURABICHVILI, F. Deleuze e o possível (sobre o involuntarismo na política). *In:* ALLIEZ, E. (org.). **Gilles Deleuze:** uma vida filosófica. São Paulo: Editora 34, 2000. p. 333–335.