



## **Cultura Hacker e Controle de Informações na Internet<sup>1</sup>**

Drielle Furtado dos SANTOS<sup>2</sup>

Rafael Rodrigues da COSTA<sup>3</sup>

Universidade Federal do Ceará, Ceará, CE

### **Resumo**

Este artigo busca analisar as relações entre o poder do Estado no contexto da era informacional em que vivemos, destacando o surgimento de novas culturas dentro da internet e citando casos de violação da privacidade dos usuários. A partir de pesquisas bibliográficas e documentais (dentre as quais estão presentes obras de Manuel Castells, Michel Foucault e ainda Francisco Rüdiger) o artigo destaca a importância de cultura hacker, relacionando-a a criação da internet até os dias atuais e contextualizando-a aos recentes acontecimentos.

### **Palavras-chave**

cibercultura; cultura hacker; espionagem; internet; marco civil da internet; panóptico; vigilância.

### **Introdução**

Pensar as relações em rede é algo indispensável nos dias atuais. Com o advento da Internet, novas culturas, maneiras de agir e pensar surgem, trazendo todo um novo leque de costumes que passam a fazer parte da cultura rede de computadores. Esse mesmo ciberespaço onde a liberdade de expressão foi cultivada fez com que a soberania nacional fosse deixada à margem da rede, mas logo os governos trataram de desenvolver dispositivos para a retomada do controle de informações. Afinal, essa é a melhor maneira que o Estado tem para assegurar o seu poder diante a sociedade, como Foucault já havia observado na década de 1980.

O resultado é que novas questões vão sendo levantadas como, por exemplo, a quem essa nova tecnologia dará maior poder e liberdade? O poder e liberdade de quem

---

<sup>1</sup> Trabalho apresentado no DT 1 – Jornalismo do XVI Congresso de Ciências da Comunicação na Região Nordeste realizado de 15 a 17 de maio de 2014.

<sup>2</sup> Estudante de Graduação 5º. semestre do Curso de Jornalismo da UFC, email: driellefurtado@gmail.com

<sup>3</sup> Orientador do trabalho. Professor do Curso de Jornalismo da UFC, email: rafaelrg@ufc.br



serão reduzidos com ela? Como Neil Postman comenta no seu livro *Tecnopólio*, “as mudanças forjadas pela tecnologia são sutis, quando não são completos mistérios; e poder-se-ia dizer que são imprevisíveis” (1994) e, por isso, devem ser analisadas com atenção.

No entanto, as novas culturas emergentes não poderiam deixar o governo ou qualquer outro tipo de organismo se impor diante da liberdade de expressão que se cultivou no ciberespaço desde o princípio. É nesse contexto que hackers e ciberativistas de toda a rede passam a lutar de todas as formas para subverter o Estado. A exemplo disso, Edward Snowden, um hacker que se vê trabalhando para uma grande agência do governo norte-americano e se depara com documentos secretos que viriam mudar a forma como os usuários viam a segurança na rede. Ele não foi o primeiro, nem será o último, mas, de toda forma, serviu para chamar atenção do resto do mundo para os problemas de privacidade na Internet

Francisco Rüdiger, autor do livro *"As teorias da Cibercultura"*, ressalta a forma como o ciberespaço é controlado, sendo regulado não apenas de acordo com a classe política ou pelas elites empresariais, mas, sobretudo, "pelas forças do mercado e sua dinâmica". Essas companhias que recolhem, processam e exploram os dados das pessoas no ciberespaço são cada vez mais opacas em relação as suas práticas e intenções, enquanto as informações dos usuários, gradativamente, configuram-se mais transparentes. O autor ainda afirma que

voluntariamente ou não, as pessoas estão se tornando prisioneiras de redes telemáticas que permitem saber, por quem conduz o processo e ou paga pela informação, cada vez mais sobre sua identidade, relações, desejos e movimentos. Queiramos ou não, estamos nos tornando fornecedores de informações que podem ser coletadas, reunidas, analisadas, vendidas e exploradas como propriedade de organizações e indivíduos sobre as quais temos muito pouco conhecimento e praticamente nenhuma autoridade. (RÜDIGER, 2009, p.47)

No Brasil muito se tem avançado em relação as questões envolvendo privacidade e liberdade dentro da rede passaram a ser discutidas pelo poder legislativo. Um exemplo disso é a criação do Marco Civil da Internet que, se aprovado<sup>4</sup>, muito vem a favorecer os usuários brasileiros.

---

<sup>4</sup> No período e finalização do trabalho, o Marco Civil da Internet ainda não havia sido aprovado.



## **Origens e Cultura da Internet**

Desde a antiguidade, grandes chefes de Estado utilizam a espionagem como estratégia de inteligência na busca por informações privilegiadas, seja pela utilização de espiões para obter conhecimento ou até a criação de aparatos técnicos como satélites. Ao longo dos séculos, os governos aperfeiçoaram essa técnica, deixando de lado os espiões infiltrados em território inimigo e passando a dar lugar às novas tecnologias. É no ápice da Guerra Fria que a idealização de novos suportes tecnológicos torna-se ainda mais frenética. A competição entre as duas potências mundiais da época, EUA e União Soviética, em busca da afirmação de superioridade sobre o rival acabou por desencadear uma série de avanços tecnológicos que foram incorporados às telecomunicações e a informática.

É em meio a este conflito ideológico que surge a Internet. Com o intuito de desenvolver novas tecnologias, o Departamento de Defesa dos EUA criou em 1958 a ARPA (Advanced Research Projects Agency) a fim de arrecadar recursos oriundos das universidades. O objetivo desse departamento, segundo a definição do seu primeiro diretor, Joseph Licklider, era estimular a investigação no campo da informática interativa. A partir de então é criada a ARPANET, uma rede de computadores estabelecida pela agência de projetos de investigação. Posteriormente, ela se transforma em um sistema usado exclusivamente para a investigação militar.

É importante ressaltar que a tecnologia usada para a criação das redes de computadores era aberta ao domínio público, e dessa forma era possível que outros desenvolvedores criassem suas próprias conexões. Assim, a Internet poderia se desenvolver em velocidades ainda maiores, uma vez que qualquer pessoa tinha acesso aos protocolos de comunicação. Tanto as redes contraculturais como as redes privadas, providas de mais aparato científico, convergiam nas universidades. Como consequência, surgiram várias outras redes de computadores, entre elas o sistema BBS (Bulletin Board System), o UNIX, a FIFONET e a BITNET, criados dentro de centros universitários na década de 1970.

Para entender a cultura da Internet, é importante destacar a importância desses sistemas. Eles se baseavam na livre distribuição de seus códigos-fonte (chaves para acesso e modificação de softwares, programas executáveis de computadores). Assim, os estudantes que utilizavam a rede desenvolviam versões melhoradas de programas e distribuíaam para outros usuários, que por sua vez faziam outras melhorias nos



programas e voltavam a disponibilizá-los, como num constante ciclo de inovação tecnológica baseada na livre circulação de conhecimento. Isso representou uma tendência decisiva no surgimento da cultura de rede. O uso e o desenvolvimento de *free softwares* (*softwares* livres) e do compartilhamento de informações tornaram-se os códigos de conduta daqueles que viriam ser os primeiros *hackers*.

Em a “Galáxia da Internet”, Manuel Castells discute o assunto:

A cultura da liberdade individual que se gerou nos campi universitários, nos anos 60 e 70, utilizou a ligação informática em rede para os seus próprios fins, na maior parte dos casos, procurando inovação tecnológica pelo puro prazer de descobrir. As universidades tiveram um papel fundamental no apoio às redes comunitárias [...] Sem a contribuição cultural e tecnológica dessas novas redes informáticas de base, Internet teria um aspecto muito diferente e, muito provavelmente não teriam alcançado todo o mundo ou, pelo menos, não tão rapidamente. (CASTELLS, 2004, p.41)

O autor explica que a cultura estudantil se apoderou da ligação informática, utilizando-a como uma ferramenta de comunicação livre, uma forma de libertação que, juntamente com o *Personal Computer* (PC), deu a todos o poder da informação, para que se libertassem tanto dos governos como das empresas.

Apesar de a Internet ter sido desenvolvida graças a recursos públicos e de projetos de investigação de interesse nacional, a liberdade de pensamento e a inovação não foram reprimidas. Isso era extremamente necessário para que a criatividade se sobrepujasse aos interesses militares de segurança. Dessa maneira, foi possível o desenvolvimento da rede de comunicação entre computadores que conhecemos hoje.

Por ser uma tecnologia demasiado ousada, cara e arriscada, a Internet não teve sua origem no mundo das grandes empresas privadas. Castells afirma que ela nasce, portanto, de um extraordinário vínculo entre a investigação militar, a ciência nos campi universitários e a cultura libertária, “uma ideologia baseada na defesa dos princípios de liberdade individual como valor supremo, frequentemente contra o governo, mas às vezes com a colaboração de alguns governos, como a defesa da privacidade perante interesses comerciais” (CASTELLS, 2004, p.34)

O sociólogo define a cultura da Internet como “a cultura dos seus criadores [...] um conjunto de crenças e valores que formam o comportamento de seus próprios criadores”. Isso acaba gerando uma série de costumes que se impõem diante das organizações sociais informais. Ele a divide em quatro estratificações culturais que são dispostos hierarquicamente em: cultura tecnomeritocrática (dos cientistas), *hacker*, comunitária virtual e empreendedora.



A seguir, será feita uma análise um pouco mais minuciosa sobre o conceito de cultura *hacker* e sua influência dentro da rede de computadores, tanto no âmbito do ciberativismo quando sua relação reacionária à prática de espionagem por parte dos governos.

### **A cultura *hacker***

Em linhas gerais, o termo *hacker* é utilizado para designar um indivíduo hábil em enganar os mecanismos de segurança de sistemas e de computadores, além de conseguir acesso não autorizado aos recursos do mesmo. No entanto, sua acepção vai muito além disso. A tradicional descrição de *hacker* é a de um programador de computador talentoso que se dedica em grande intensidade a conhecer e modificar dispositivos, programas e redes. Ele resolve problemas rapidamente usando meios não-convencionais. Esses indivíduos compartilham de uma série valores e crenças que tiveram origem em redes onde programadores informáticos interagem em torno de projetos de programação criativa. Eles têm bastante autonomia nos projetos em relação àqueles institucionais e sua base tecnológica e matéria são provenientes das redes informáticas.

McKenzie Wark discute em seu livro "A hacker manifesto" (2004) as origens do termo *hacker*. Segundo ele essa designação emerge das engenharias elétricas e da computação, pois são áreas de produção criativa onde representam atividades mais ampla em um "mundo vetorial". "The hacking of new vectors of information has indeed been the turning point in the emergence of a broader awareness of the creative production" (WARK, 2004, p.44)<sup>5</sup>

Em "A galáxia da Internet", Castells ressalta que a cultura *hacker* está diretamente ligada à cultura tecnomeritocrática (Cultura dos Cientistas). Essa última constitui-se como cultura *hacker*, contudo seus costumes giram em torno de normas geradas nas redes de cooperação relacionadas a projetos tecnológicos. Sem a cultura dos cientistas, os *hackers* seriam apenas uma comunidade contracultural específica "cheia de *geeks* e *nerds*".

A origem dos costumes nasce a partir da sede de conhecimento dos estudantes que buscavam aprender e entender a relação dos computadores com os homens. A corrente

---

<sup>5</sup> "O *hacking* (ou "raqueamento", se traduzido ao pé da letra) de novos vetores de informação tem, de fato, sido um ponto de decisivo na emergência de uma consciência mais ampla da produção criativa"



de pensamento dominante nesse grupo girava em torno da Internet e não se preocupava com a comercialização de produtos. Um dos símbolos dessa cultura é o movimento pelo software livre, que era a favor da liberdade de expressão, partindo do princípio da comunicação livre, em que o uso do software significaria um direito inalienável.

Entretanto, liberdade não o único valor levado em consideração por esse grupo, o prazer de cada um pela criatividade e o objetivo máximo do alcance à excelência tecnológica são componentes essenciais para a manutenção de suas atividades como *hackers*. Para Wark, os *hackers* podem se comportar de diferentes maneiras quando suas habilidades e conhecimentos são requisitados. "*Hackers use their knowledge and their wits to maintain their autonomy. Some take the money and run. (We must live with our compromises.) Some refuse to compromise. (We live as best we can).*"<sup>6</sup> (WARK, 2004, p.15). Eles estão constantemente criando novas possibilidades e desenvolvendo novos produtos. Nem sempre esses produtos são de qualidade ou bem intencionados, entretanto, não muda o fato de que estão continuamente inovando. "It is in the nature of hacking to discover freely, to invent freely, to create and produce freely".<sup>7</sup> (WARK, 2004, p.45)

Um dos principais símbolos da luta pelo direito ao software livre foi o *hacker* Linus Torvalds, um estudante da Universidade de Helsínque, na Finlândia, que em 1993 criou o sistema operativo Linux. Baseado no próprio UNIX, a ideia de Linus era publicar as atualizações que ia fazendo e estimular outras pessoas a fazerem o mesmo. O resultado foi que uma centena de *hackers* foram se envolvendo no projeto, aperfeiçoando-o cada vez mais. A publicação de cada nova atualização permitiu que as falhas do Linux fossem eliminadas de maneira que o tornou um dos sistemas mais operativos existentes. McKenzie Wark explica:

Outra característica importante dessa contracultura é a necessidade comum de partilha e manutenção desses códigos abertos de softwares. A comunidade baseia-se nesse sistema com o objetivo de aumentar a qualidade e operatividade dos sistemas. No entanto, sublinha Castells,

quando essa excelência está desligada de instituições que ofereçam uma recompensa em troca, exige a adesão a uma série de valores que combinem o prazer da criatividade com a reputação entre colegas. Um valor fundamental

---

<sup>6</sup> "Hackers usam seu conhecimento e suas habilidades para manter sua autonomia. Alguns deles pegam aceitam o dinheiro e correm (Nós devemos viver com nossos compromissos). Outros recusam se comprometer (Vivemos da melhor maneira possível)."

<sup>7</sup> "É da natureza dos *hackers* descobrir livremente, inventar livremente, criar e produzir livremente."



nesse contexto é o da liberdade. Liberdade para criar, liberdade para absorver os conhecimentos disponíveis e liberdade para redistribuir sob a forma e o canal eleitos pelo *hacker* (CASTELLS, 2004, p.67).

Para o sociólogo, o surgimento desses costumes desempenhou um papel crucial na construção da Internet.

Por um lado, é terreno de cultivo onde surgiram diversas inovações tecnológicas importantes e, por outro, serve de conexão entre os conhecimentos da cultura tecnomeritocrática e os projetos empresariais que difundem a Internet no conjunto da sociedade. (CASTELLS, 2004)

Na literatura, a representação do hacker chega a ser bastante próxima daquilo que ele é a realidade. As tramas sempre os trazem em conflito com governos, megacorporações e até mesmo inteligências artificiais. As características são quase sempre as mesmas: descritos como heróis solitários possuidores de uma genialidade invejável que, acima de tudo, combatem a tirania e a injustiça de grandes empresas. Normalmente são assinalados como pessoas desprivilegiadas de alguma forma e que buscam na cultura hacker uma forma de libertação. Uma das tramas mais atuais é a da trilogia Millennium, escrita por Stieg Larsson, que tem como personagens principal uma jovem hacker, Lisbeth Salander que também utiliza todas suas habilidades como um meio de vida. Na série, ela se vê colocada no meio de intrigas envolvendo grandes conspirações, juntamente com seu amigo Mikael Blomkvist.

### **Relações de controle na Internet**

Em uma de suas análises sobre o poder do Estado, Michael Foucault (1987) baseia-se no conceito de Panóptico do filósofo Jeremy Bentham, cuja ideia consiste em uma prisão circular onde todo e qualquer detento era observado do alto por uma sentinela posicionado o centro, possibilitando assim a vigilância e controle de todos os presos.

O dispositivo panóptico organiza unidades espaciais que permitem ver sem parar e reconhecer imediatamente. Em suma, o princípio da masmorra é invertido; ou antes, de suas três funções — trancar, privar de luz e esconder — só se conserva a primeira e suprimem-se as outras duas. A plena luz e o olhar de um vigia captam melhor que a sombra, que finalmente protegia. A visibilidade é uma armadilha. (FOUCAULT, 1987)

Na Era da Informação, onde a comunicação se dá por meio da mediação por computadores, a liberdade de expressão e a possibilidade de anonimato aumentaram o contato das pessoas com a um público ainda maior, permitindo-lhes expressar suas



opiniões, angústias e esperanças. Tais fatores vieram trazer atenção redobrada por parte de empresas, redes criminosas e, principalmente o Estado.

Nos primeiros anos do surgimento da Internet, o governo podia fazer pouquíssimo para controlar os fluxos de comunicação, pois além de transcender as fronteiras geográficas, a rede ultrapassava as barreiras políticas nacionais. Nesse sentido, a rede de informática contribuiu decisivamente para que o controle do Estado e a soberania nacional fossem restringidos dentro do ciberespaço. Uma vez que o surgimento da Internet vulnerabilizou, de certa forma, o comando dos governos em relação ao ciberespaço, a obtenção dessas informações contidas na rede tornou-se umas das maiores prioridades dos governos.

. Como o controle da informação sempre foi uma das principais estratégias governamentais para garantir o poder do Estado ao longo da História, as primeiras medidas tomadas pelo congresso estadunidense foi garantir instrumentos legais para a intervenção sobre a rede. No entanto a proposta foi negada nos tribunais, tornando ainda mais difícil que os EUA impusessem qualquer tipo de regulamentação da comunicação, uma vez que a natureza da rede é global.

Não obstante, os EUA buscaram softwares que pudessem identificar rotas de comunicação e conteúdo, possibilitando o monitoramento dos dados contidos na Internet. Com alternativas tecnológicas de vigilância ampliadas, o comportamento e o cotidiano dos cidadãos passam a ser facilmente rastreados e monitorados. O controle de redes de comunicação permite a transformação de diversos interesses e valores em normas orientadas de comportamento humano. Castells argumenta que:

Através do uso dessas tecnologias pode-se transgredir a privacidade e, enquanto se chega a relacionar determinados indivíduos com processos de comunicação específicos em contextos institucionais concretos, é possível utilizar todas as formas tradicionais de controle político e organizativo contra o indivíduo ligado à rede (CASTELLS, 2004).

Nesses novos tempos em que a vigilância adquire novas características, as possibilidades de observação debruçam-se sobre todos. Como Foucault constatou, o efeito prioritário do Panoptico é a vigilância generalizada. Isso se reflete no dias atuais em que, não só agências de inteligência nacional, mas grandes empresas nos monitoram constantemente. O Panóptico é uma máquina de dissociar o par “ver/ser visto”: no anel periférico se é totalmente visto, sem nunca ver; na torre central, vê-se tudo, sem nunca ser visto.



Daí o efeito mais importante do Panóptico: induzir no detento um estado consciente e permanente de visibilidade que assegura o funcionamento automático do poder. Fazer com que a vigilância seja permanente em seus efeitos, mesmo se é descontínua em sua ação; que a perfeição do poder tenda a tornar inútil a atualidade de seu exercício (FOUCAULT, 1987)

Nessa nova era da informação, em que a liberdade e a possibilidade do anonimato são um fator chave, o controle do estado sobre os cidadãos fica ameaçado. Hackers e ativistas de todo o mundo almejam que a liberdade e acima de tudo a privacidade permaneçam assegurados como direitos inalienáveis. Dessa maneira, tudo o possível é feito para desmascarar os governos ou instituição que ameacem esse preceito. No últimos anos, vários casos vieram a tona quando documentos secretos de grandes agencias de vigilância foram divulgados. O mais recente foi no ano passado (2013).

### **Vigilância e vazamento de informações**

No início de junho de 2013, o jornal britânico The Guardian publicou informações reveladoras sobre os poderes de vigilância do governo Norte-Americano. Foram divulgados documentos que comprovam a utilização de complexos programas de monitoramento das comunicações, tanto digitais quanto telefônicas, pela Agência Nacional de Segurança (NSA – National Security Agency) dos Estados Unidos.

Os arquivos foram vazados por Edward Snowden, que trabalhava como consultor de inteligência da NSA. O delator atuava como uma espécie de *hacker* testando diversas redes e sistemas de computadores a fim de encontrar suas vulnerabilidades e comunicá-las às empresas. No período em que trabalhou para a agência norte-americana, sua missão era barrar ataques aos sistemas do governo, atuando assim como *hacker* defensivo em favor da NSA. Durante esse período, Snowden se deparou com os arquivos e decidiu divulgá-los, pois julgava ser importante que a população soubesse que estava sendo monitorada.

O programa Prism, utilizado para a quebra de sigilo eletrônica, coletava dados importantes, não só de indivíduos de todas as localidades do mundo, como também arquivos sigilosos de Estados. Essas informações eram colhidas através de bancos de dados de empresas renomadas como Google, Facebook, Microsoft, entre outros. O Brasil foi um dos países atingidos por essa vigilância de forma que, além de milhares de usuários terem tido e-mails, fotos e videoconferências interceptados, a própria presidenta Dilma Rousseff foi vítima da espionagem norte-americana.



Edward Snowden não foi o único que tentou trazer a tona os projetos de vigilância dos EUA. Em 2005, O jornal *The New York Times* divulgou que o então presidente George W. Bush havia autorizado NSA a executar milhares de escutas telefônicas sem consentimento judicial, alegando o que a Lei *USA Patriot* permitiria tal ação a favor da segurança nacional no combate ao terrorismo.

Esses e outros casos parecidos alertam-nos para o grande poder de vigilância que têm alguns países, e principalmente os Estados Unidos. Além disso, e levanta discussão sobre as regras e leis adequadas a serem aplicadas no ciberespaço e o questionamento sobre até que ponto a soberania de um país se estendo dentro da Internet.

### **Marco Civil da Internet no Brasil**

No âmbito nacional, as relações entre legislação e internet vêm evoluindo nos últimos anos. Um exemplo disso é projeto de regulamentação da Internet através da implantação do Marco Civil da Internet cuja intenção é funcionar como uma espécie de Constituição para a rede de computadores e normatizar a navegação em rede no Brasil. Se aprovado, o projeto reunirá uma série de preceitos que guiarão a criação de leis e decisões futuras envolvendo a Internet no país.

Com a aprovação do marco alguns princípios básicos serão criados. Ele prevê uma série de direitos e garantias aos usuários da rede, além da indicação de diretrizes para uma correta atuação do Estado. Um dos principais é a política de não-intervenção desse Estado no ambiente cibernético, tornando-o mais livre e democrático. O projeto de lei foi elaborado em parceria com a população de forma que a mesma tinha o poder de fazer várias observações, através da Internet, sobre o conteúdo do Marco. Tramitando na Câmara dos Deputados, uma comissão especial tem o encargo de realizar audiências públicas e discutir a proposta para, enfim, levá-la a votação.

A demora para a votação do projeto é devido a vários pontos polêmicos no mesmo. Uma das questões da retirada de conteúdos da internet que ainda envolve direitos de liberdade de expressão. Um desses pontos polêmicos é a proposta relacionada às determinações sobre o que deve ser feito em caso de vazamento indevido de conteúdos na rede, de forma que os provedores de conteúdo só serão responsabilizados pela retirada de conteúdos se a vítima.

Há ainda algumas umas questões ausentes no texto do Marco Civil que foi submetido à comissão especial. O projeto não aborda, por exemplo, o assunto dos



crimes cibernéticos, algo importante nos dias atuais, e ainda o tema dos direitos autorais, que permanecem sem resolução no Brasil.

Atualmente o projeto tramita na Câmara dos Deputados, onde aguarda por um acordo que possam, enfim, fazer a votação. Se aprovado o Marco representará um novo momento para as relações de Estado e internet no país com, sem dúvida, mais facilidades para aqueles que sofreram crimes cibernéticos, mas também mais responsabilidades civis para os usuários.

### **Considerações Finais**

Podemos, certamente, dizer que desde a criação da ARPANET até a internet que conhecemos hoje, muito se tem evoluindo nas relações entre tecnologia, Estado e a população em geral. Contudo, observa-se a dificuldade em garantir o respeito à privacidade dos usuários. Escutas telefônicas e a violação do anonimato são apenas a “ponta do iceberg”. A internet deixa de ser simplesmente um instrumento de propagação do conhecimento para se tornar uma rede de vigilância que busca obter não só informações, mas subjugar os usuários, retendo dados e conteúdo de foro íntimo.

Ademais, a contribuição da cultura hacker para a o desenvolvimento da Internet foi, de fato, muito importante na maneira como se evoluiu as relações na internet. A cultura (ou como alguns costumam chamar: contracultura) que essa comunidade constituiu, baseada em preceitos de liberdade, influenciou no comportamentos dos usuários até os dias atuais. É por essa e outras razões que a questão da liberdade dentro da rede de computadores ainda é um elemento de intensa discussão.

### **Referências bibliográficas**

CASTELLS, Manuel. *A galáxia da Internet: reflexões sobre a Internet, os negócios e a sociedade*. Lisboa, Portugal: Fundação Calouste Gulbenkian, 2004. 325p.

FOUCAULT, Michel. *Vigiar e punir: nascimento da prisão*. Petrópolis: Vozes, 1987. 288p.

POSTMAN, Neil. *Tecnopólio: a rendição da cultura à tecnologia*. São Paulo: Nóbél, 1994. 221p.

RÜDIGER, Francisco. *As teorias da Cibercultura*. 2 ed. São Paulo: Sulina, 2013. 319p.



SILVEIRA, Sérgio Amadeu da. *Ciberativismo, cultura hacker e o individualismo colaborativo*. Revista USP. São Paulo, n.86, p. 28-39, junho/agosto 2010.

WARK, McKenzie. *A hacker manifesto*. United States of America: Harvard University Press, 2004. 209p.