

Quando transgredir vira profissão: uma análise do processo de institucionalização da atuação hacker

Olivia Hirsch

Em março de 2009, Owen Thor Walker, um hacker de 19 anos que cumpriu pena por desenvolver um vírus que invadiu 1,3 milhão de computadores em todo o mundo e causou prejuízos da ordem de US\$ 20 milhões, foi contratado pela operadora de telecomunicações neozelandesa TelstraClear. Segundo a polícia, Owen criou um vírus único indetectável pelos programas antivírus que permitia acesso aos nomes, às senhas e aos números de cartões de crédito dos usuários. O jovem, que na internet usava o pseudônimo “Akill”, não chegou a tirar dinheiro da conta bancária dos usuários, mas vendeu o software desenvolvido por ele por cerca de US\$ 30 mil. O hacker foi detido em novembro de 2007, depois de uma investigação que durou 18 meses e envolveu a polícia local e o FBI. De acordo com os investigadores que trabalharam no caso, o programa era um dos “mais avançados” já vistos no mercado. Owen ganhou a liberdade e logo foi admitido pela empresa, para a qual passou a atuar como consultor de segurança, além de ministrar palestras a executivos e clientes da operadora. “Ele dá conselhos sobre como reduzir os riscos e sobre o que motiva os cibercriminosos”, explicou Chris Mirams, diretor da TelstraClear¹.

Trajetória semelhante teve Mikeyy Mooney, de 17 anos. Ele foi contratado por uma empresa de desenvolvimento de aplicativos para a web para trabalhar como consultor de segurança, depois de ter infectado pelo menos 190 contas do site de microblogs Twitter. Nos dias 11 e 12 de abril de 2009, Mikeyy espalhou no Twitter um *worm*² criado por ele e, mais tarde, assumiu a autoria das invasões. O jovem americano alegou três motivos para ter cometido os ataques: tédio, intuito de promover seu nome e intenção de avisar o Twitter sobre as falhas de segurança, de acordo

com informações do site de tecnologia *CNet*. O hacker afirmou ter tentado contatar o Twitter previamente para alertar sobre as vulnerabilidades, mas, sem sucesso, resolveu usar o *worm* para chamar a atenção. Travis Rowland, diretor da empresa *exqSoft Solutions*, que desenvolve aplicativos para a web, ficou impressionado com suas habilidades e ofereceu-lhe uma vaga de programador e consultor de segurança, segundo o site *ABCNews*. Na opinião de Rowland, o jovem fez um favor ao Twitter. “Ele ainda precisa amadurecer bastante, mas é um bom garoto e adora o que faz”, disse. “Espero conseguir levá-lo para o bom caminho”³.

Os dois exemplos descritos acima, que poderiam se somar a muitos outros, nos levam a refletir sobre como a transgressão tem sido absorvida pelo sistema econômico atual. Em uma extensa obra na qual se debruçam sobre a nova ordem do capitalismo mundial, os sociólogos Luc Boltanski e Eve Chiapello tecem interessantes considerações sobre o que denominam de o “novo espírito do capitalismo”. Em resposta à crise econômica e de credibilidade decorrente do movimento de Maio de 68, o capitalismo, segundo a tese dos autores, passou a incorporar ao sistema parte do que seriam “os ingredientes vindos do caldo contestatório ideológico, político, filosófico e existencial dos anos 60”, como observa Pelbart (2003: 96), autor de uma contundente resenha do livro. Demandas por autonomia, criatividade, liberdade, bem como as críticas à rigidez, à burocracia e à alienação, antes alçadas contra o sistema capitalista, passaram a ser parte constitutiva de uma nova normatividade, cujos principais mandamentos constam dos inúmeros manuais de *management* dispostos nas prateleiras das livrarias. Para citar apenas um exemplo, o texto de apresentação da obra *Recursos Humanos: o capital humano das organizações*, de Idalberto Chiavenato, destaca a importância da “qualidade dos funcionários de uma organização, seus conhecimentos e habilidades, seu entusiasmo e satisfação e seu senso de iniciativa”. De acordo com o texto, “tudo isso tem um forte impacto na produtividade da organização, no nível de serviços prestados ao cliente, na reputação e na competitividade. É que as *pessoas* fazem a diferença em um ambiente competitivo de negócios” (grifo nosso).

Esta descrição, que apela à *pessoa* capaz de ser revelada por trás do papel social de “funcionário de uma empresa”, valoriza a sensibilidade, as habilidades, as iniciativas e o entusiasmo do sujeito. Tal descrição em muito se distancia da imagem associada ao trabalhador autômato, massificado e maquinizado que predominava no passado, pelo menos até as décadas de 1960 e 70. Mas se a rejeição ao cumprimento de tarefas estritamente mecânicas e repetitivas – tais quais desempenhadas pelo personagem do filme *Tempos modernos*, de Charles Chaplin – partiu inicialmente dos trabalhadores, estas aos poucos passaram a ser incorporadas e rechaçadas pelo próprio sistema, que adotou como suas as críticas que antes lhes eram atribuídas. E, vale destacar, não apenas adotou, como as converteu em elemento indispensável na nova configuração produtiva.

“Ao satisfazer em parte as reivindicações libertárias, autonomistas, hedonistas, existenciais, imaginativas, o capitalismo pôde ao mesmo tempo mobilizar nos seus trabalhadores esferas antes inatingíveis”, destaca Pelbart (2003: 96).

Nesse processo, demandas e comportamentos que antes, de alguma maneira, desqualificavam o trabalhador, então tratado como um desviante, passaram a ser vistos como algo a se valorizar. A mudança nesse tipo de avaliação se reflete, por exemplo, na outrora impensável decisão das empresas de contratarem hackers⁴ para seus quadros, como anteriormente exemplificado. Jovens criativos, que buscam desafios e se colocam diante deles com uma atitude ousada e até mesmo subversiva, são avaliados positivamente por um mercado ávido por vitalidade, inventividade e capacidade de lidar com situações imprevistas. Diferentemente do que ocorria antes, a subversão torna-se a regra e o sujeito perde sua função na medida em que deixe de lado essa espécie de “perversão malandra” (Zizek, 2006: 112). “A história do capitalismo não será a longa história da maneira através da qual a estrutura ideológico-política dominante se revelou capaz de conciliar (e de atenuar o caráter subversivo) dos movimentos e das exigências que pareciam ameaçar a sua própria sobrevivência?” (Zizek, 2006: 87).

Outro aspecto apontado pelo autor e que nos parece pertinente tratar neste artigo diz respeito ao fato de que os hackers são recrutados pelas empresas justamente para “serem o que são”. Dessa forma, observa Zizek, esses jovens parecem “realizar uma espécie de utopia protossocialista que consiste em anular a oposição entre a atividade comercial alienada, mediante a qual se ganha dinheiro, e o passatempo privado, que se leva a cabo por prazer, durante os fins-de-semana. De certa maneira, o seu trabalho é o seu passatempo” (2006: 111).

Em maio de 2008, em uma lista de discussão do Yahoo⁵, foi realizado o 1º Seminário de Iniciação Hacker⁶. O evento contou com mais de 7 mil participantes – entre os quais iniciantes, usuários avançados, estudantes de sistemas de informação e profissionais de informática (técnicos, analistas, consultores, administradores de rede, etc.) – e foi organizado pela Escola de Hackers (www.escoladehackers.com.br), sobre a qual nos deteremos mais detalhadamente adiante. O que nos interessa nesse momento é justamente trazer à tona alguns depoimentos dos participantes sobre essa questão:

Ser inteligente não é fazer o que gosta e ainda ser recompensado por isso?
(Mediador do grupo).

A minha visão de um hacker é a de uma pessoa que gosta do que faz e sente prazer naquilo que é feito, o principal motivo na vida de um hacker é superação. Devemos ser o que somos, o que nascemos para fazer. (João)

Com efeito, Pais (2005) destaca que atualmente novas concepções de trabalho e lazer estão se desenvolvendo. Se a palavra trabalho advém etimologicamente do termo em latim *tripalium*, que também designava um instrumento de tortura, as ideias a ela associadas hoje são, aparentemente, bem diferentes. Nesse sentido, a compatibilidade do trabalho com o lúdico vem se tornando uma realidade para muitos cibernautas, observa o autor. A realização pessoal e os prazeres proporcionados por uma atividade profissional são uma aspiração cada vez mais frequente entre os jovens, que “rejeitam a instrumentalidade do trabalho e valorizam as satisfações intrínsecas que dele possam retirar. A tal ponto que o trabalho já invade a esfera dos lazeres, sendo vivido como uma aventura”⁷ (Pais, 2005: 19). Nesse sentido, seria possível falar de uma contaminação, em vez de tratar da questão em termos estanques e dicotômicos, ou mesmo sob a ótica da anulação⁸.

É também Pais (2005: 21), referindo-se à obra clássica de William Thomas e Florian Znaniecki, *The Polish Peasant in Europe and America*, quem afirma que possivelmente haverá uma tendência à diluição das fronteiras entre a ética tradicional do trabalho – cuja marca principal é o desejo de segurança e de correspondência – e a de aventura – pautada pelo desejo de novas experiências e de reconhecimento.

A esse respeito, faremos novamente referência a um dos comentários feito pelo hacker Mikeyy na tentativa de justificar o ataque realizado ao site de microblogs Twitter, qual seja, o de “promover seu nome”. De fato, a espetacularidade e visibilidade do ato transgressor, tanto no caso de Mikeyy como no de Owen, renderam frutos. Ambos tornaram-se reconhecidos pela capacidade de burlar normas e encontrar falhas nos programas, o que, nesse contexto, representa um conceituado cartão de visitas. Isto porque, quanto mais grandioso – e, por que não, destrutivo? – for o ataque, maior será o reconhecimento quanto ao desempenho do hacker.

De acordo com Ball (2005), na sociedade atual o desempenho, cuja “eficácia só existe quando é medida e demonstrada”, serve de parâmetro de produtividade, como forma de o sujeito demonstrar suas “qualidades”. Nesse sentido, o valor do indivíduo passa a ser medido pela capacidade que este possui de demonstrar resultados. Isso significa que se o conhecimento não for exteriorizado e julgado, de nada adianta detê-lo. Em termos gerais, o que estaria ocorrendo, segundo Lyotard (2004), seria a conversão do conhecimento em mercadoria.

Com efeito, é nessa lógica que, pouco a pouco, parecem estar se inserindo os hackers: o que antes era uma atividade marcada centralmente pelo anonimato – ainda o é em muitos casos, como indicam as várias imagens de sujeitos vendados ou com óculos escuros em sites de comunidades hacker – atualmente começa a ser introduzida a idéia de autoria, e não apenas restrita a um pequeno grupo. Isso parece ser resultado do processo de institucionalização dos hackers, antes altamente estigmatizados. Hoje, por exemplo, é

possível localizar na internet várias escolas e cursos de formação na área. Para escrever este artigo, nos detivemos principalmente no trabalho desenvolvido pelo Curso de Hackers (www.cursodehacker.com.br), que acabou sendo desativado no final do mês de junho de 2009. A partir de agora, quando se digita o endereço do Curso de Hackers o internauta é imediatamente direcionado à página da Escola de Hackers (www.escoladehackers.com.br), que seria, segundo informa o site, uma “evolução” do Curso de Hackers, porém totalmente desvinculada dele.

De fato, há algumas diferenças entre os dois sites e que se revelam interessantes para a análise. Um exemplo pode ser observado no layout da página inicial. No Curso de Hackers, a imagem que constava na abertura do site era a de um homem sentado sozinho em um escritório repleto de computadores, utilizando uma cartola preta e uma venda nos olhos⁹, acessórios um tanto quanto enigmáticos e que, portanto, remetem ao anonimato¹⁰. Já na Escola de Hackers a imagem que consta na página inicial é a de um jovem, cujo rosto não é possível identificar devido ao excesso de luminosidade no tratamento da foto, mas ele está sem vendas ou qualquer outro acessório. O jovem, que parece um estudante, usa uma camisa social e utiliza um laptop. Nessa mesma página também consta, logo abaixo da imagem, o seguinte slogan: “Hacker se aprende é na escola”.

É interessante observar que, contraditoriamente, no discurso dos participantes do 1º Seminário de Iniciação Hacker, a ideia de que este conhecimento possa advir de um aprendizado adquirido, isto é, de uma formação, é de certa maneira questionada. Isso ocorre porque, para muitos deles, a atuação como hacker pressupõe uma espécie de “dom”, de aptidão inata, como veremos nos depoimentos a seguir:

Acho que hackers são gênios, no sentido de que são uma das poucas classes de pessoas hoje em dia que não têm preguiça de raciocinar, de não se submeter ao sistema como a maioria das massas. Que questiona, tenta entender os porquês por trás das coisas. (Whelynton)

O hacker é um fuçador por natureza. (Rafaela)

[O hacker é] Aquele cara que é autodidata e aprende sozinho qualquer assunto através de livros ou pesquisas. (Nilo)

Para mim hacker é aquela pessoa que possui um olhar diferenciado para as coisas, percebe o que ninguém percebeu, enxerga o que ninguém enxergou (...). É aquela pessoa que possui um conhecimento próprio sobre as coisas, digo sem um estudo profissional, uma formação, mas resolve e faz tudo o que um profissional formado não consegue. (André Luiz)

[Fazer hacks] Depende de um algo mais que não é ensinado em lugar nenhum. Já vem (ou não) com a pessoa. O que podemos fazer é despertar ou expandir a percepção. Mas não sejamos ingênuos pensando que todos se tornarão grandes mestres. (Mediador do grupo).

[Os hackers] São as pessoas mais inteligentes na terra, então eles possuem algo “diferencial” em relação às outras pessoas. (Rodrigo).

Uma das questões abordadas no seminário diz respeito a uma espécie de hierarquia existente entre os hackers. Assim, os mais valorizados são aqueles capazes de criar hacks¹¹ originais, mesmo que sejam fórmulas simples. Tais fórmulas seriam uma espécie de concretização do dom. Noutro patamar encontram-se os que fazem adaptações de hacks e os que apenas reproduzem os que foram criados por outros.

Os que fazem hacks é que fazem a diferença. (id_mit_nit)

Num mundo onde nada se cria e tudo se copia, quem é criativo e consegue gerar algo realmente novo tem que ser valorizado. (Rafaela)

Qual a pessoa que mostra maior capacidade: aquela que cria ou a que copia? Os exploradores que pegam uma nova área que já é explorada, sempre será menos valorizado do que o pioneiro, aquele que desbravou, percorreu o caminho sozinho e, onde muitos achavam que não havia nada, encontrou algo de valor. (Luiz)

É interessante notar a associação feita pelo participante Luiz entre hackers e desbravadores, exploradores, o que nos leva a pensar como ambos estão em busca de conquistar novos territórios, sejam eles reais ou virtuais. Em entrevista concedida ao autor Frederico Casalegno (2006), a pesquisadora Sherry Turkle aponta como, de fato, as fronteiras entre essas duas dimensões estão cada vez mais porosas. “Como as pessoas passam cada vez mais tempo em lugares virtuais, há um impulso, um tipo de expressão do desejo humano, de fazer com que as fronteiras entre o físico e o virtual sejam mais permeáveis”, ressalta Turkle (Casalegno, 2006: 289). É também a autora quem observa que, em meio às pressões e ameaças cotidianas que incidem desde a infância, os jovens hoje já não encaram a adolescência como um período de experimentação sem consequências, isto é, como um tempo de moratória, em que haveria uma espécie de “pausa”. Nesse sentido, o ciberespaço estaria despontando como uma zona livre para ser explorada, algo que estaria frequentemente ausente no “Resto da Vida”. Esta expressão a autora utiliza em substituição ao termo “vir-

tual” que, segundo seu ponto de vista, representaria uma ruptura, com a qual não concorda, com o que seria o real.

Retomando a análise dos depoimentos colhidos durante o seminário, outro aspecto que merece ser destacado é o fato de que não poucas vezes os participantes manifestaram a importância do que se poderia chamar de uma “função social” do hacker. As invasões e ataques a sites deveriam ser vistas com bons olhos, segundo este ponto de vista, na medida em que permitiriam aos fabricantes de software aprimorar a qualidade de seus produtos. Nesse sentido, o hackerismo – termo utilizado pelos próprios usuários – seria de interesse público. O depoimento do hacker Mikeyy, citado no início desse artigo, sugere que ele compartilha dessa visão, tendo em vista que um dos motivos pelo qual realizou o ataque teria sido avisar o Twitter sobre suas falhas de segurança. Abaixo, estão reproduzidos alguns depoimentos que constam do documento que resultou do seminário:

Quem vende um produto com falhas é que deveria ser mal visto pela mídia. Qualquer outro produto que compramos se identificamos uma falha nós vamos ao Procon. Como é muito difícil alguém ir ao Procon por causa de um software, cabe a nós mostrarmos para que sejam corrigidos e tenhamos um produto mais seguro. (id_mit_nit).

Na minha opinião os hackers ajudam muito a sociedade e as empresas de software avisando sobre os erros existentes. (Marcelo)

É enorme a contribuição dos hackers para a melhoria dos sistemas e serviços existentes e, o melhor de tudo, É UMA PRESTAÇÃO DE SERVIÇO GRATUITA (sic). (Adriano)

Vale destacar que o processo de institucionalização dos hackers vem acompanhado de uma tentativa de dissociar o imaginário negativo comumente vinculado a este vocábulo. Nesse sentido, foi possível observar em diversos sites e mesmo em livros publicados sobre o tema uma busca por diferenciar o significado do termo hacker, que agora seria positivado, do conceito de cracker, que assumiria toda a carga negativa antes referida a hacker¹². De acordo com Assunção (2002), autor do livro *O guia do hacker brasileiro*, os hackers possuem os mesmos “poderes” que os crackers, mas os utilizam para promover a proteção. Em suas palavras, o hacker “é um curioso por natureza¹³, uma pessoa que tem o objetivo de aprender e desenvolver seus conhecimentos com um hobby, assim como ajudar os ‘menos prevalecidos’” (Assunção, 2002: 6). Já os crackers são definidos como pessoas que possuem “um alto grau de conhecimento e nenhum respeito, [que] invadem sistemas e podem apenas deixar a sua ‘marca’ ou destruí-los completamente” (Assunção, 2002: 6).

O autor informa ainda que “hackers e crackers costumam entrar muito em conflito. Guerras entre grupos são comuns, e isso pode ser visto em muitos fóruns de discussão e em grandes empresas, as quais contratam hackers para proteger seus sistemas”¹⁴ (Assunção, 2002: 6-7).

Ainda que diferenciados a partir de critérios bem claros e definidos, na prática foi possível observar que a linha que supostamente separa as ações hackers e crackers é um tanto quanto tênue. No próprio discurso dos participantes do seminário anteriormente referido isto fica explícito, como sugerem os depoimentos abaixo:

Usar esse poder para o mal ou para o bem é indiferente. Uma faca você pode usar para cortar um pão ou para matar alguém. Continua sendo uma faca. (Whelynton)

Os hackers são feras da informática que adoram aprender como os sistemas funcionam externa e principalmente internamente. Eles sabem que nada os pode impedir de fazer o que querem, a não ser eles mesmos. (Danúbio)

Ética não é se comportar como um anjo sem asas. (Mediador do grupo)

Somos éticos até que nosso desejo fale mais alto do que nossa razão. (Id_mit_nit)

É interessante chamar atenção para o comentário feito pelo internauta Danúbio, no sentido de que atribui exclusivamente ao indivíduo o papel de regulador. Essa observação é bastante reveladora do sujeito de nosso tempo, pois na medida em que certas atividades passam a ser menos estruturadas por instituições heteronormativas (escola, igreja, família, etc.), cabe ao indivíduo, na mesma proporção, assumir parte desses domínios, aumentando a exigência de tomada de decisão (Giddens, 2003: 56). O mesmo autor se refere ao surgimento de um “sujeito hiper-reflexivo” como resposta ao fim das instituições balizadoras da vida cotidiana. O que significa que o sujeito fica “exposto a uma pressão do supereu incomparavelmente mais forte” (Zizek, 2006: 112), na medida em que cabe apenas a ele determinar qual trajeto deverá ser percorrido.

A noção de “trajetórias yô-yô”, proposta por Pais (2005), parece útil para pensar a realidade experimentada pelos jovens na sociedade contemporânea. De acordo com o autor, “perante estruturas sociais cada vez mais fluidas e modeladas em função dos indivíduos e seus desejos, os jovens sentem a sua vida marcada por crescentes inconstâncias, flutuações, descontinuidades, reversibilidades, movimentos autênticos de vaivém”, os quais a metáfora do yô-yô pretende traduzir. E, acrescenta, “nos labirintos da vida alguns jovens acham-se depois de se perderem”.

Para além da fluidez presente nos constantes movimentos de idas e vindas (do emprego, da casa dos pais, dos relacionamentos), como sugere Pais, não nos parece descabido pensar que as inconsistências que permeiam a vida desses jovens talvez se reflitam também em seus julgamentos sobre o que é certo e errado, lícito e ilícito, ético e anti-ético, havendo uma linha tênue entre esses pólos.

Nesse sentido, pelo que foi possível observar no site do Curso de Hackers, o julgamento acerca do uso ético do conhecimento pode ganhar interpretações e contornos distintos caso as situações se refiram à esfera privada ou à pública. Assim, ainda que o site recomende que não se empregue o conhecimento adquirido para cometer atos ilícitos, como desviar dinheiro de contas bancárias e fazer uso de senhas de cartões de crédito, por outro lado informa que após o curso o aluno “achará divertido abrir e-mails de parentes e amigos”. Além disso, a página vende, entre outros DVDs, um intitulado “Love Hacker: Hackeando no Dia dos Namorados”, que contém “vídeo-aulas para quem tem dúvidas sobre a idoneidade do relacionamento. Voltado ao público leigo, o material ensina formas simples de investigar o(a) companheiro(a)”. Na página são divulgados os temas abordados no DVD, que incluem técnicas de *wetware* para perceber mentiras; técnicas para descobrir senhas de e-mail, Orkut e MSN, além de ensinamentos sobre como usar a webcam com propósitos de vigilância. Um último item trataria das implicações legais dessas práticas.

Durante o seminário, no módulo sobre ética, comentou-se inclusive sobre a importância daqueles que pretendem se tornar hackers de conhecerem a fundo a legislação, de modo a “procurar formas de fazer a mesma coisa que você queria, mas de forma legal”, explica o mediador. Ele também esclarece como pequenos detalhes determinam a diferença entre o que seria ou não crime:

Saber a senha de acesso da conta [bancária] de alguém não é crime. Usar a senha para visualizar as informações, como o saldo, por exemplo, caracteriza a quebra de sigilo bancário sem autorização judicial. Da mesma forma, a senha do e-mail: saber a senha não é invadir a privacidade. Visualizar o e-mail sim. Uma diferença mínima, mas que no tribunal vai livrar a cara do invasor (p. 89).

O mediador ainda compara a atuação do “bom hacker” a de um “bom advogado”, que consegue descobrir brechas na lei e fazer com que seus clientes sejam “absolvidos, recebam condenação mínima, respondam em liberdade ou tenha as provas de acusação recusadas, porque não foram produzidas em conformidade com a lei”.

Assim, é interessante observar como a discussão sobre ética acaba se convertendo em uma discussão sobre leis e formas de nelas encontrar brechas. Parece que os hackers estão sempre no limiar entre o que seria o ético e o antiético, o crime e a legalidade, como que caminhando em uma corda-bamba¹⁵. E assim, se equili-

brando sobre o fio que separa esses dois pólos, esses jovens são orientados a usar o mesmo espírito que os leva a serem exímios exploradores do universo cibernético para explorar a fundo a legislação e dela tirar partido.

O objetivo final? Que possam continuar “sendo o que são”.

Olivia Hirsch
Professora da PUC-Rio
olivianh@gmail.com

Notas

1. Fonte: Portal G1. A matéria encontra-se disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL1057527-6174,00-OPERADORA+CONTRATA+HACKER+QUE+CAUSOU+PREJUIZO+DE+US+MILHOES.html>. Último acesso em 23/06/09.

2. Um worm (verme), assim como um vírus, cria cópias de si mesmo de um computador para outro, mas faz isso automaticamente. Primeiro, ele controla recursos no computador que permitem o transporte de arquivos ou informações. Depois que o worm contamina o sistema, ele se desloca sozinho. O grande perigo dos worms é sua capacidade de se replicar em grande volume. Por exemplo, um worm pode enviar cópias de si mesmo a todas as pessoas que constam no catálogo de endereços de e-mail, e os computadores dessas pessoas passam a fazer o mesmo, causando um efeito dominó de alto tráfego de rede que pode tornar mais lentas as redes corporativas e a internet como um todo. Quando novos worms são lançados, eles se alastram muito rapidamente, obstruem redes e fazem com que se leve mais tempo para abrir páginas na internet. Fonte: Site da Microsoft. <http://www.microsoft.com/brasil/athome/security/viruses/virus101.msp> Último acesso em 25/06/09.

3. Fonte: Site Terra. A matéria encontra-se disponível em: <http://tecnologia.terra.com.br/interna/0,,OI3717160-EI4805,00-Hacker+que+invadiu+o+Twitter+ganha+emprego+e+volta+a+atacar.html>. Último acesso em 23/06/09.

4. Mais adiante problematizaremos o uso desse termo, apresentando o conceito de “cracker”, aparentemente criado para absorver a conotação negativa antes associada ao hacker.

5. O endereço é: <http://tech.groups.yahoo.com/group/grupodocursodehacker/>

6. O documento de 175 páginas que resultou do seminário encontra-se disponível em: http://www.escoladehackers.com.br/I_Seminario_de_Iniciacao_Hacker.pdf. Último acesso em 25/06/09.

7. É interessante observar como a oposição entre trabalho e aventura, que por ora parece não dever ser tratada em termos polarizados, havia sido tratada por Sérgio Buarque de Holanda no clássico livro *Raízes do Brasil*. Na obra, o autor dedica um capítulo ao tema, no qual destaca a existência de dois princípios que se contrapõem e regulam de maneira distinta as atividades dos homens: o da aventura e o do trabalho.

Sobre aqueles que são adeptos do primeiro, Buarque afirma que o objetivo final se revela tão importante que acaba por dispensar todos os processos intermediários. Por outro lado, aqueles que encarnam o princípio do trabalho, colocam como meta ultrapassar o obstáculo e não alcançar o objetivo final, o qual será apenas uma consequência. Cabe questionar se esses dois princípios encontram-se hoje distanciadas de maneira tão estanque.

8. As observações feitas por Rodrigues (1989) acerca do trabalho em sociedades ditas “tradicionais” nos indicam como esta ideia de contaminação talvez não seja tão nova assim. Nesse sentido, o autor destaca como nessas sociedades a labuta não se opõe ao lazer, dele não se separando nem espacial nem cronologicamente. Além disso, não há uma desvinculação entre o trabalho e as demais atividades sociais. A título de exemplo, Rodrigues cita a experiência da caça entre os bosquímanos !Kung, que vivem no Sul da África e são obrigados a realizar longas expedições para caçar. Como a atividade desempenhada é percebida como altamente prazerosa, as jornadas por eles empreendidas estão longe de representarem tarefa árdua. “A caça é a maior paixão que têm na vida”, afirma Rodrigues (1989: 101).

9. Uma imagem que, confesso, me deixou um tanto quanto insegura no momento em que tive que fazer *download* de alguns documentos: Quem está por trás desse site? Será que é confiável? Será que estará transmitindo um vírus ao meu computador? Cheguei inclusive a evitar acessar esses documentos de meu computador pessoal, privilegiando o uso de laboratórios.

10. A cartola, por exemplo, pode ser associada à mágica e, portanto, à surpresa e à imprevisibilidade.

11. O hack é a fórmula ou o caminho encontrado pelo hacker para ultrapassar um obstáculo, o que lhe permite fazer coisas para as quais o sistema não foi programado. Um exemplo, bastante simples, citado pelo mediador do grupo foi o seguinte: o Windows não permite que sejam criadas pastas com nomes tais como PRN, COM1, LPT1. Para alcançar esse objetivo, o sujeito deverá fazer o seguinte percurso: Ir em “Iniciar”, clicar em “Executar”, digitar “CMD” e clicar em OK. Por fim, na janela do prompt de comando deverá digitar: `mkdir \\.\c:\prn`. Dessa forma, será possível criar a pasta que antes o sistema não permitia. A fórmula criada para alcançar esse objetivo é chamada de hack.

12. Mesmo que haja essa tentativa, ainda é grande o preconceito que paira sobre os hackers. Acerca dessa questão o internauta Nilo, que participou do seminário, fez a seguinte comparação: “Acho que o termo hacker assumiu a mesma conotação que o comunismo na política, que foi deturpado e vilipendiado para que não crescesse como deveria, ou seja, só exploraram o lado ruim do comunismo e estão fazendo a mesma coisa com as pessoas que são adeptas do hackerismo” (Nilo).

13. Mais uma vez, deve-se destacar a importância atribuída a algo que seria decorrência de uma “natureza” curiosa e aventureira do hacker, por oposição à ideia de formação.

14. Sobre esse aspecto, de fato chamou a atenção o uso recorrente pelos participantes do seminário, e mesmo por autores que escrevem sobre o tema, de terminologias que

fazem referência a uma lógica belicista. Assim, fazem parte do universo vocabular dessas pessoas termos como “invasão”, “ataque”, “proteção”, “destruição”, “guerra”, etc. No próprio seminário, o moderador buscou fazer uma diferenciação entre o profissional de segurança da informação e o hacker, que se revela bastante elucidativa do que queremos apontar. De acordo com ele, o primeiro “é treinado para tempos de paz, recorrendo a técnicas de defesa apenas para ataques conhecidos”. Já o segundo “é treinado para a guerra e a guerrilha, treinado nas técnicas de ataque conhecidas e incentivado a desenvolver e buscar novas técnicas”.

15. Há inclusive um filme sobre hackers, cujo título não poderia ser mais sugestivo: *Hackers: anjos ou criminosos?*

Referências bibliográficas

- ASSUNÇÃO, Marcos Flávio. *Guia do hacker brasileiro*. Florianópolis: Visual Books, 2002.
- BALL, Stephen. Profissionalismo, gerencialismo e performatividade. *Cadernos de Pesquisa*, v.35, n.126, p. 539-564, set./dez. 2005.
- BARBERO, Jesús Martín. A mudança na percepção da juventude: sociabilidades, tecnicidades e subjetividades entre os jovens. In: BORELLI, Silvia e FILHO, João Freire. *Culturas juvenis no século XXI*. São Paulo: Educ, 2008.
- CASALEGNO, Frederico. Diálogo com Sherry Turkle: a memória na tela. In: CASALEGNO, Frederico. *Memória cotidiana: comunidades e comunicação na era das redes*. Porto Alegre: Sulina, 2006.
- GIDDENS, Anthony. *Mundo em descontrole*. Rio de Janeiro: Editora Record, 2003.
- HOLANDA, Sérgio Buarque. *Raízes do Brasil*. São Paulo: Companhia das Letras, 26ª edição, 1995.
- LEVY, Steven. *Hackers: heroes of the computer revolution*. New York: Penguin Books, 1994.
- LYOTARD, Jean François. *A condição pós-moderna*. Rio de Janeiro: José Olympio, 2004.
- PAIS, José Machado. *Ganchos, tachos e biscates: jovens, trabalho e futuro*. Porto: Âmbar, 2005.
- PELBART, Peter Pál. *Vida capital: ensaios de biopolítica*. São Paulo: Iluminuras, 2003.
- RODRIGUES, José Carlos. *Antropologia e Comunicação: princípios radicais*. Rio de Janeiro: Espaço e Tempo, 1989.
- ZIZEK, Slavoj. *Elogio da intolerância*. Lisboa: Relógio D'água Editores, 2006.

Resumo

O artigo busca refletir sobre como a transgressão tem sido absorvida pelo sistema econômico atual. Demandas por autonomia, criatividade, liberdade, bem como críticas à rigidez, à burocracia e à alienação, antes alçadas contra o sistema capitalista, passaram a ser parte constitutiva de uma nova normatividade. É nesse cenário que jovens hackers são, pouco a pouco, recrutados por empresas de segurança da informação para “serem o que são”, borrando as fronteiras entre trabalho e lazer. A análise se baseia em depoimentos colhidos durante o 1º Seminário de Iniciação Hacker, realizado em um fórum na internet por um curso de formação hacker. Do evento, realizado em 2008, participaram mais de 7 mil pessoas.

Palavras-chave

Hackers; Institucionalização; Trabalho; Lazer; Capitalismo.

Abstract

The article looks to reflect how transgression has been absorbed by the current economic system. The demands for autonomy, creativity, freedom, as well as criticisms to rigid ways, to bureaucracy and to alienation, before went against the capitalist system, now have become constitutive part of a new normativity. It's in this scenario that hackers are, little by little, recruited by security information companies to “be what they are”, blurring the borders between work and leisure. The analysis bases itself in the reports done in the first seminar of Hacker Initiation, which happened in an Internet forum by a course for hacker formation. In the event, that took place in 2008, there were 7 thousand people participating.

Keywords

Hackers; Institutionalization; Work; Leisure; Capitalism.