

O uso do terror simbólico como estratégia discursiva na questão da segurança no ciberespaço¹

Paulo Alves de Lima²

Resumo

A despeito de todos os recursos tecnológicos já disponíveis, e ainda em desenvolvimento, parte importante das estratégias de combate ao cibercrime e ao SPAM centram-se em práticas discursivas baseadas no terror simbólico e no medo, voltando o foco do problema contra as alteridades e imputando ao outro e ao desconhecido a razão de todas as mazelas que afligem a existência nas redes.

Institui-se uma corrente onde os elos mais fortes representados pelos fabricantes de infraestrutura lógica, desenvolvedores da indústria de segurança, provedores de acesso, grandes portais geradores de conteúdos, agências de publicidade e organizações não governamentais em uníssono clamam contra o estranho os invés de formar um usuário médio autônomo e capaz de discernir as ameaças. Essa abordagem além de manter o volume circulante de dados na rede, conservando a pressão pela necessidade de expansão da infra-estrutura preserva o atual modelo comercial protegendo o Status Quo, centralizado, vigente.

Inevitavelmente o uso dessas estratégias discursivas contribui para a construção de uma subjetividade fragilizada e propensa a aderir, como se inevitável fosse, aos modelos de navegação tutelada proposto por diversos setores privados e estatais.

Palavras-chave: Anti-vírus, Cibercrime, hacker, SPAM, segurança, cybersecurity, alteridade.

Introdução

Dioturnamente fluxos randômicos de bites vagam pelo ciberespaço, fragmentos de palavras, imagens e sons embaralham-se em caótico mosaico. Internautas, avatares e múltiplas alteridades interagem intensa e fugazmente. Em sua marcha de rumo incerto a cibercultura –vetor tecnológico da pós-modernidade – segue seu tropel sob a lógica da

¹ Artigo científico apresentado ao eixo temático 3. “Vigilância, ciberativismo e poder”, do III Simpósio Nacional da ABCiber.

² Graduado em Design de Multimídia pelo Centro Universitário Senac-SP (2005), cumpriu bolsa de iniciação científica com o tema "Conceitualização da *Web Semântica*". Mestrando, bolsista CAPES, do Programa de Comunicação e Semiótica - COS - da PUC/SP onde desenvolve projeto de pesquisa sobre interfaces *WEB* e processos de percepção e produção de sentido no ciberespaço. É membro do CENCIB e atua profissionalmente como designer de interfaces para internet e multimídia. E-mail para contato: paulo@garagedigital.com.br

velocidade, convertendo a civilização humana à sua empiria. Paradoxalmente essa onda avassaladora de tendência homogeneizante, ao menos no tempo presente, segue produzindo um cenário fragmentado, assíncrono e híbrido, uma combinação especial de singular e plural.

Estranhamente a despeito dessa realidade caleidoscópica ao menos um tema já começa a produzir um rápido consenso entre empresas, profissionais e usuários, a segurança no ciberespaço. Invariavelmente um emaranhado de argumentos, raramente tecnológicos ou éticos, embaralhando as esferas psicológicas públicas e pessoais, interesses privados, comerciais e estatais, criando uma confusão notoriamente conveniente aos mercados da segurança. Consolida-se um discurso referenciado nas sombras e medos ancestrais do homem, ergue-se um histórico e apressado uníssono acerca da necessidade, aparentemente inevitável, de mecanismos terceirizados de vigiar e tutelar a presença no ciberespaço.

A “questão segurança” no ciberespaço

O questão da segurança no ciberespaço trata primordialmente de uma relação dinâmica e complexa, que opõe indivíduos, grupos e instituições interessados em usufruir dos mais diferentes modos da grande rede mundial de computadores – além de outras redes conexas a essa como as *Intranets*, as redes de telefonia fixa, móvel e agora as redes elétricas – dentro dos parâmetros legais, éticos, tecnológicos e comerciais estabelecidos. De outro lado, indivíduos e grupos que valendo-se de práticas transgressoras objetivam invadir redes, sistemas e computadores em busca de violar dados e a privacidade alheios, usualmente com a intenção de roubar, fraudar ou lesar uma pessoa ou instituição e seus patrimônios simbólicos, informacionais ou materiais.

Outros tantos arriscam-se a essas práticas ilícitas pelo simples desafio que a intrusão de sistemas alheios representa, ou até, pelo prestígio que esse feito confere perante seus pares, dentro e fora da rede, um reconhecimento que pode, de modo bastante heterodoxo, para se dizer o mínimo, resultar em cooptação pela indústria de segurança ou por organismos estatais de vigilância e controle, sempre em troca de ótima remuneração, sob a justificativa de tratarem-se de trabalhadores de alta especialização técnica!

Nenhum panorama ou reflexão sobre o tema segurança no ciberespaço se completa sem que se dê o devido destaque à prática conhecida como *SPAM*, o envio massivo de mensagens eletrônicas sem a solicitação do destinatário. Ainda que o envio não solicitado de mensagens a

princípio não seja crime, tal prática têm provocado uma onda histórica de repulsa entre os usuários que a percebem como delituosa, confusão despudoradamente insuflada pelas empresas de segurança, provedores de acesso, geradores de conteúdo, a quem juristas, parlamentares e governantes fazem impensado cômico, usualmente incluindo sua prática na categoria dos *cibercrimes*, independentemente inclusive dessas mensagens intentarem ou não a prática de fraude ou de estarem de acordo com as chamadas “*Boas Práticas do Mercado*”, que no caso do Brasil utilizam como referência mais comum o código da ABEMD³.

Esse cenário pouco amistoso para com essa forma de publicidade pulverizada, barata e massiva, em nada se assemelha ao humor do *sketch* da série “*Flying Circus*” do grupo inglês *Monty Python*, de onde o termo foi tirado por alguns de programadores nos anos setenta. Passado em um restaurante onde todas as preparações eram variações de um mesmo ingrediente, o *SPAM* (um tipo de presunto enlatado cujo nome supõe-se seja um acrônimo de *spiced ham*) de modos que qualquer que fosse pedido o cliente receberia, quisesse ou não, *SPAM*.

Alguns poucos números talvez ajudem a jogar um pouco de luz sobre essa fronteira cinza de interesses chamada *SPAM*, e os personagens que por ela transitam. O primeiro aspecto diz respeito ao volume total de *e-mails* enviados, embora os valores oscilem significativamente, as estimativas apontam que algo entre 63% e 90% do total das mensagens de *e-mails* que trafegam na rede sejam *SPAM*. O *engine* alemão *SPAM-O-METER*⁴ que faz avaliações dinâmicas diariamente indica no mês de outubro de 2009 o percentual foi de 88,9%, segundo os irlandeses da *IEInternet*⁵, empresa especializada em monitoramento de segurança na *WEB*, aproximadamente 4% das mensagens não solicitadas continham algum tipo de *agente infectante*. Habitualmente o Brasil aparece entre os dez maiores emissores nos *rankings* globais, onde invariavelmente a liderança cabe aos EUA.

É inegável que embora vilipendiado o *SPAM* é hoje responsável direto por parcela significativa do tráfego de dados na rede, e pelo sustento das demandas de expansão da infraestrutura lógica e física, e caso fosse eventualmente eliminado é certo que provocaria níveis devastadores de ociosidade em toda a infra-estrutura da *WEB*. Curiosamente vários serviços

³ ABEMD - Associação Brasileira de Marketing direto, possui um código de ética para o e-mail marketing que pode ser consultado em:

<http://www.abemd.org.br/autoregulamentacao/CodigoEtica.aspx>

⁴ <http://www.spam-o-meter.com>

⁵ <http://www.ieinternet.com/>

públicos e não governamentais, de aferição do tráfego e de sua tipologia, quando não possuem vínculos diretos ou indiretos com empresas de infra-estrutura lógica, recorrem ao menos a suas estatísticas como fundamento, assim o faz por exemplo o *Comitê Gestor da Internet no Brasil* (CGI.BR) responsável pelo REGISTRO.BR, e mantenedor do ANTI-SPAM.BR, que publica um ideário a cerca de como tratar esse assunto.

Há que se frizar que o temor pelas fraudes *online* possui justificativas evidentes, e não se poderia afirmar que as preocupações com seu progresso sejam descabidas, porém é importante notar que o *SPAM* gera receitas bilionárias aos que o promovem e aos que o combatem. Os números de apenas uma modalidade de fraude realizada com mensagens de falsos softwares anti-virus, entre julho de 2008 e junho de 2009 podem dar uma idéia de qual o faturamento ao redor desse assunto, nesse período cerca de 40 milhões de internautas compraram um falso *up-grade* para seus programas anti-virus, calcula-se que cada fraudador possa ter arrecadado cerca de US\$ 2 milhões com o golpe, estima-se que 250 fraudadores no mundo aderiram a essa modalidade de fraude, isso significa que arrecadaram apenas nessa rodada cerca US\$ 500 milhões, valor que certamente estava previsto nas estimativas de vendas das empresas de segurança.

Considerando que apenas 4% do *SPAM* possui conteúdo malicioso, não necessariamente criminoso, manter a confusão que coloca o manto da falta de ética crime e do crime sobre toda e qualquer mensagem não solicitada é bastante conveniente aos grandes e influentes atores da rede.

Naturalmente ao contrario dos que ganham com *SPAM* outros perdem, receita e prestígio, com essa modalidade fragmentada, quase caótica, de publicidade, de lógica semelhante aos bombardeios de saturação da segunda grande guerra. Sabe-se que a eficiência média do *SPAM* como recurso publicitário e de marketing é sabidamente baixa – cerca de 0,02 a 0,04 das mensagens são abertas e recebem clicks – o que é compensado pelo gigantismo do número total de usuários da rede – fazendo com que em termos absolutos continue sendo um grande negócio o envio de mensagens não solicitadas. Para piorar, raramente grandes agências ou empresas são contratadas para planejar, criar e enviar *SPAM*, afinal outra atraente característica dessa modalidade é sua simplicidade e baixo custo de produção e disparo.

Não é portanto difícil perceber porque o *SPAM* atenta contra o modelo de negócio dos provedores de acesso e conteúdo, das grandes agências de publicidade e as empresas de marketing direto, que por seu turno alinham-se com aqueles cujo discurso criminaliza todo e

qualquer tipo de mensagem não solicitada, pois não só desqualificam os concorrentes como valorizam um dos mais cobiçados recursos da *WEB*, os cadastros dos internautas, em particular seus e-mails, os já populares maillings – tecnicamente conhecidos como bases de dados – o mais cobiçado *Eldorado* do comércio eletrônico, da política e da vigilância na rede, já que permitem acesso privilegiado aos internautas, essa é grande jóia do tesouro dos provedores de acesso e dos portais geradores de acesso, cuja nuvem do *SPAM* ameaça ocultar o brilho.

Experimente um mundo sem ameaças⁶

Embora aos olhos do senso comum, os míticos poderes dos *ciberfraudadores* supostamente emanem do domínio que esses possuem dos códigos computacionais capazes de transpor as fortalezas lógicas – atributo que muitos efetivamente possuem – essa é uma visão romântica e tecnicamente ultrapassada do cotidiano dos logros no ciberespaço. Qualquer *hacker* minimamente experiente sabe que o caminho do desmonte de senhas é, na ampla maioria das vezes, o mais difícil pois além de exigir mais tempo, fator de risco crucial nessas empreitadas, demanda a posse de *hardware* com incomum capacidade de processamento, equipamentos desse porte invariavelmente estão inacessíveis aos *ciberfraudadores*, embora essa dificuldade possa ser eventualmente contornada com o partilhamento do processamento entre várias máquinas, o que por seu turno incrementaria, em muito, o risco de detecção e vazamento da atividade ilícita. O caminho mais eficaz, e curto, é outro, passa pela cognição e pela produção de sentido, pelo logro emocional do usuário e das instituições. Aos que duvidam dessa afirmação não é preciso ir além da primeira página, do primeiro capítulo de “*The Art of Deception: Controlling the Human Element of Security*”⁷ escrito por um dos mais conhecidos, senão o mais lendário *hacker* que se têm notícias, Kevin Mitnick⁸, norte-

⁶ Frase grafada em folheto promocional da Dell Computadores acerca do software *McAfee* Antivirus fornecido de modo pré-instalado em seus computadores. Impresso encartado no jornal *O Estado de S.Paulo*, edição de 16 de agosto de 2009.

⁷ MITNICK, Kevin David, SIMON, William L. *The Art of Deception: Controlling the Human Element of Security*, Indianapolis, Wiley, 2002.

⁸ Kevin David Mitnick, nascido em 6 de agosto de 1963, iniciou suas atividades ilegais aos 12

americano que durante 15 anos burlou com sucesso a perseguição do *FBI* contra si, Mitnick é claro ao advertir: "...*the human factor is truly security's weakest link*".

Embora profundo conhecedor dos códigos computacionais Kevim recorria ao que comumente se denomina de “engenharia social”, realizava um conjunto de estratégias por vias não computacionais organizados para obter informações que o conduzissem às senhas ou aos dados pretendidos. Suas táticas podiam variar de buscas em sacos de lixo a telefonemas promocionais de uma *petshop* inesistente, afinal Mitnik sabia que obter o nome de um cão de estimação – utilizado como senha – é muito mais rápido e simples do que quebrar uma chave criptográfica de 128 bits. Desde criança não foi difícil para ele perceber onde se encontravam as maiores fraquezas na questão da segurança no ciberespaço, certamente não eram, ou são, tecnológicas, normativas ou jurídico-policiais, o alvo de Kevim, era, e continua sendo, o mesmo de seus seguidores, uma antiga e convencional peça dos sistemas sociais, o homem e seu imaginário.

Certamente as lições de Mitnick foram aprendidas pelos departamentos das grandes corporações, não é sem razão que o discurso desses agentes do mercado de segurança no ciberespaço não se restringem a alardear o poder tecnicológico de seus produtos, pouco importa informar aos usuários sobre os sofisticados mecanismos eurísticos de apartação de termos, os algoritmos evolutivos, os modelos de propensão, as blacklists, as séries de IPs, zonas de domínio e servidores bloqueados. As estratégias das empresas apontam para os medos que habitam o homem.

Invariavelmente os textos promocionais iniciam-se pelas célebres advertências: “Contra nós – eles!”, os vocábulos da psicanálise crivam os discursos com expressões como: “*estranho*”, “*oculto*”, “*malicioso*” e “*furtivo*”, revivem despididamente o imaginário da *Guerra-Fria* (a mãe oclusa da *Internet*) sem dubiedades, contra o nós (o *Bem*) eles (o *Mal*). O

anos de idade adulterando cartões de acesso aos ônibus de Los Angeles, posteriormente burlou o sistema telefônico realizando gratuitamente chamadas de longa distância. Como rádio amador obtinha refeições gratuitas nas redes de comunicação das cadeias de FastFood. Na Internet invadiu computadores das empresas Motorola, NEC, Nokia, Sun Microsystems, Fujitsu Siemens, SCO, PackardBell, Novell e ainda as redes do FBI, Pentágono, Los Angeles Unified School District, Universidade do Sul da Califórnia entre outras. Preso em 1996 cumpriu 5 dos 25 anos de prisão a que foi condenado, hoje possui uma empresa de segurança de sistemas computacionais. Irônicamente em 20 de agosto de 2006 teve seu site invadido por um grupo de hackers paquistaneses chamado *FBH* e pelo ciberativista francês *DkD*.

desconhecido, o outro, agora em versão espectral, mutante e fugidia, insurge ameaçador contra o pacato *cibercidadão*.

O ciberespaço que até a pouco era seara utópica, de liberdades inauditas, torna-se já em sua aurora um local perigoso, habitado por *hackers*, *crackers*, *spammers* e *warez*. Os vírus e suas variantes os *sniffers*, *malwarers* e *scarewares* abandonam o mundo digital e passam à categoria de seres míticos da cibercultura, entidades que assombram a existência na era das redes. Neste contexto como não lembrar do estranho Freudiano?

*“O tema do “estranho” é um ramo desse tipo. Relaciona-se indubitavelmente com o que é assustador - com o que provoca medo e horror; certamente também, a palavra nem sempre é usada num sentido claramente definível, de modo que tende a coincidir com aquilo que desperta o medo em geral...”*⁹

Os perigos da internet, reais ou não, dominam a agenda midiática, pautam a imprensa, norteiam projetos políticos, clamam por normatização dos juristas, mobilizam os vigilantes, moldam os negócios, permeiam o imaginário e o cotidiano do homem médio. Nas filas do comércio contam-se casos de logros, de furtos e de *phishing*. Quantos de nós já não se deteve, por um instante ao menos, a olhar os alertas ameaçadores que povoam as telas e as embalagens dos *softwares* de segurança comuns em qualquer vitrine de bairro ou estante de supermercado?

O espectro de setores e especialistas que discursam e aconselham sobre o tema é de uma amplitude incomum, suas falas estão comumente pontuadas por expressões onde “o outro” é o problema, basta ver o que diz uma das mais destacadas advogadas especializadas no tema, ou mesmo o órgão gestor da Internet brasileira, o REGISTRO.BR:

*“...É inegável que o avanço tecnológico trazido pela internet melhorou a qualidade de vida de boa parte da população mundial... Da mesma forma que facilitou a vida do cidadão de bem, a rede também contribuiu para a disseminação de práticas ilícitas, os chamados cibercrimes...”*¹⁰

⁹ FREUD Sigmund. *Além do Princípio de Prazer*, Edição Standart Brasileira, Vol. XVIII, pág13, São Paulo, Imago, 1976.

¹⁰ Texto extraído de artigo do site institucional da Patrícia Peck Pinheiro Advogados, especializado em Direito Digital (sic) em:
<http://www.patriciapeck.com.br/cconhecimento.asp?Passo=Exibir&Materia=452>

“...Cuidado com comunidades online. Sem querer, você pode se envolver com algum conteúdo que possa gerar problemas legais, tanto no âmbito civil como no criminal... Evite abrir e-mail de estranhos...”¹¹

“...Não iniciar o primeiro contato com o cliente por e-mail, ou seja, o envio do primeiro e-mail, sem prévia autorização do cliente, caracteriza a prática de spam...”¹²

Certas proposições variam do razoável às raias da paranóia, quando não da comédia, imaginar que na recomendação do REGISTRO.BR há a sugestão aos internautas que façam um primeiro contato através de outra modalidade de comunicação previamente ao envio de uma mensagem por e-mail, ou no caso da Revista VEJA em sua edição de 28 de maio de 2008 onde alerta para os riscos decorrentes dos endereços (*URLs*) com “excessos de consoantes” ou site onde os textos sejam exibidos “com erros de grafia”. Em novembro de 2007, estarrecido e enfático o deputado Inocêncio de Oliveira¹³ informava haverem 15 projetos em tramitação na Câmara Federal tratando do assunto, entre eles o projeto do senador Eduardo Azeredo que prevê entre tantas restrições a gravação de todos os logins de acesso dos provedores por durante 3 anos para que possam ser encaminhados as autoridades judiciais.

A defesa contra as fraudes e abusos na Internet é um negócio crescente, cobiçado e bilionário¹⁴, a despeito dos investimentos vultuosos das empresas em pesquisa e em equipes multidisciplinares de *tecno-especialistas* para o desenvolvimento de intrincadas fortalezas lógicas, que ampliem a eficiência de seus produtos. A despeito desses investimentos manter a utilização dos recursos simbólicos ortodoxos como os discursos contra o “mal”, circunstanciado como o estranho, permanecem como estratégia valiosa não só por turbinar as

¹¹ Texto extraído de artigo do site institucional da Patrícia Peck Pinheiro Advogados, especializado em Direito Digital (sic) em:

http://www.patriciapeck.com.br/paginas_unicas.asp?PaginaUnicaTipoID=7

¹² Texto extraído de orientações do Grupo AntiSpam no NIC/Registro-BR entidade responsável pelo registro e gerência dos domínios na *WEB* brasileira (zona de domínio BR) em: <http://www.antispam.br/boaspraticas/>

¹³ Entrevista concedida à Seção “Pinga Fogo” do Jornal da Câmara Federal, edição nº 1945, ano 8, publicada em 13 de novembro de 2007.

¹⁴ Consultorias especializadas na área de segurança na *WEB* como a *DarkReading* (EUA) e a *SecurityPark* (Inglaterra) projetam faturamento de mais de 6 bilhões de dólares americanos para os próximos 12 meses. (http://www.darkreading.com/document.asp?doc_id=96672)

vendas, mas também, e principalmente, por promoverem o desenvolvimento de uma subjetividade centrada no medo. A começar pelas falhas e brechas nos próprios sistemas de proteção, que não são designadas como tal, mas como “vulnerabilidades”, em tal cenário não ansiar por tutela e proteção é quase uma imprudência.

Desse modo os discursos que evidenciam a fragilidade em que se encontram o indivíduo e seus dispositivos, e a necessidade dos usuários clamarem por proteção, é uma estratégia recorrente e comum, por sinal longe de ser nova. Há muito o “outro” é vitimado por estratégias *antropoêmicas*, como as relatadas por Claude Lévi-Strauss em “*Tristes Trópicos*” e tão bem descritas por Zygmunt Bauman em *Modernidade Líquida*:

“...As formas elevadas, “refinadas” (modernizadas) da estratégia “êmica” são a separação espacial, os guetos urbanos, o acesso seletivo a espaços e o impedimento seletivo a seu uso”¹⁵.

É mais do que evidente, por exemplo, que a forja do termo *Firewall* compartilha dessa visão e a supor pelo discurso da indústria o horizonte não será outro, basta ver o que dizem algumas delas em seus sites institucionais:

Symantec¹⁶ empresa americana criadora do Norton Anti-Virus e uma das pioneiras desse segmento:

“Online threats today are more sophisticated, damaging, and potentially dangerous than ever before. Symantec plays an important role in educating consumers about protecting themselves from online fraud, theft of personal information, and other cybercrimes. We participate in public-policy initiatives and law-enforcement efforts geared towards detecting and deterring cybercrimes. We also support the development of the next generation of cybersecurity talent through our internship and scholarship programs.”¹⁷

Os russos do Kaspersky Lab seguem na mesma rota:

“Os vírus, ataques de hackers e outras ameaças virtuais fazem parte de nossa vida diária. A disseminação de malware por toda a Internet, o roubo de dados confidenciais por hackers e as caixas de correios repletas de spam são o preço que pagamos pela facilidade que os computadores nos proporcionam. Qualquer computador ou rede desprotegida está vulnerável.”

¹⁵ BAUMAN, Zygmunt, *Modernidade Líquida*, Rio de Janeiro, Zahar, 2001, Tradução de Plínio Dentzien, pag. 118.

¹⁶ Symantec Corporation, empresa norte-americana sediada em Cupertino no estado da Califórnia, EUA, líder mundial do mercado de softwares de segurança de uso pessoal e corporativo. (<http://www.symantec.com/pt/br/index.jsp>)

¹⁷ <http://www.symantec.com/about/profile/responsibility/cyberawareness.jsp>

A McAfee, desenvolvedora com duas décadas de mercado:

“...Roubo de identidade pode custar a você muito tempo e dinheiro destruindo seu crédito e arruinando seu nome. É um crime sério.... Você precisa de proteção de identidade on-line porque os ladrões de identidade e criminosos cibernéticos podem roubar suas informações pessoais a fim de cometerem fraude em seu nome ou abusar de suas informações financeiras pessoais...”

É justo constar que esse não é um fenômeno exclusivo da cibercultura. Nesse tema o ciberespaço parece funcionar a um só tempo como caixa de ressonância e ampliador, não só refletindo mas também potencializando fenômenos já existentes na vida humana.

A *Web* comparece como uma versão imaterial e frenética de tema ancestral da socialidade humana, seara onde mais uma vez podemos recorrer a Zygmunt Bauman:

“...a crença na conspiração dos outros contra nós não é novidade; seguramente atormentou certos homens em todos os tempos e em todos os cantos do mundo. Nunca e em nenhum lugar faltaram pessoas prontas a encontrar uma lógica para sua infelicidade, frustrações e derrotas humilhantes atribuindo a culpa a intenções malévolas e mal-intencionados planos alheios...”¹⁸

Ainda que possua um corpo específico determinado por suas características tecnológicas e de época particulares, o tópico da segurança no ciberespaço anda às voltas com um objeto que não é absolutamente novo, o outro como fonte de risco, aquele que simultaneamente familiar é desconhecido e como tal potencialmente ameaçador.

Embora não se trate de tema ou de desafio inéditos ao convívio social, a questão da segurança no ciberespaço está diretamente vinculada ao tema das alteridades, ocorre que na era da cibercultura toda estabilidade e rigidez estão em derrocada, a espectralização do eu agora mais fugaz que nunca, é preciso tratar com individualidades múltiplas e refratadas, como claramente alerta Lúcia Santaella, lembrando que a cibercultura só faz acrescentar vivacidade e drama ao tema,

“...a novidade do ciberespaço não está na transformação de identidades previamente unas em identidades múltiplas, pois a identidade humana é, por natureza, múltipla. A novidade está, isso sim, em tornar essa verdade evidente e na possibilidade de encenar e brincar com essa verdade, jogar com ela até o limite último da transmutação, da metamorfose; enfim, da “mutamorfose” identitária.”¹⁹

Talvez por essa razão o debate da segurança no ciberespaço siga tomando rumos quase históricos e não nos falem apóstolos da vigilância total, cuja suposta eficiência protegeria a

¹⁸ BAUMAN, Zygmunt, *Modernidade Líquida*, Rio de Janeiro, Zahar, 2001, Tradução de Plínio Dentzien, pag. 109.

¹⁹ SANTAELLA, Lúcia, *Linguagens líquidas na era da mobilidade*, São Paulo, Paulus, 2007.

todos do mal. Mas do que nunca vale a lembrança de que a fonte do perigo está tanto fora, quanto dentro das *ciberfortalezas*, está isso sim, fincada no cerne do homem, e embora trate-se de desafio antigo, complexo e ainda sem solução, adquire nos tempos atuais novos e intrincados desdobramentos que trazem mais uma vez a questão da possibilidade da autonomia e a coragem de optar pelo dissennimento como alternativa à tutela.

Aqui as reflexões de Levinas são um convite ao rompimento com a trajetória humana de dissimulação e hostilidade denunciadas pelo filósofo, como partir em direção ao trato franco e aberto com o outro? a possibilidade de uma atitude hospitaleira em resposta ao “apelo silencioso da face do Outro”. Como repensar outro final para o trato com as alteridades no contexto do ciberespaço?

BIBLIOGRAFIA

- BAUMAN, Zygmunt. *Modernidade Líquida*, 1º ed. Rio de Janeiro, Jorge Zahar, 2001.
_____. *Vida para consumo, a transformação das pessoas em mercadoria*, 1º ed. Rio de Janeiro, Jorge Zahar, 2007.
- FREUD, Sigmund. *Além do Princípio de Prazer*, Edição Standart Brasileira, Vol. XVIII, pág13, São Paulo, Imago, 1976.
- HARVEY, David. *Condição pós-moderna*, 16. ed. São Paulo, Loyola, 2007.
- LÉVY, Pierre. *Cibercultura*, São Paulo, 34, 1999.
- MITNICK, Kevin David, SIMON. William L. *The Art of Deception: Controlling the Human Element of Security*, Indianapolis, Wiley, 2002.
- NASCIMENTO, Evandro. (org). *Jacques Derrida - Pensar a desconstrução*, 1º ed. São Paulo, Estação Liberdade, 2005.
- POSTMAN, Neil. *Tecnopólio, A rendição da cultura à tecnologia*, Nobel, São Paulo, 1992.
- SANTAELLA, Lúcia, *Linguagens líquidas na era da mobilidade*, 1º ed. São Paulo, Paulus, 2007.
- TRIVINHO, Eugênio. *A dromocracia cibercultural, lógica da vida humana na civilização mediática avançada*, São Paulo, Paulus, 2007.