Os Impactos sobre o Panorama Educacional diante das Ofertas Gratuitas da Internet, Armadilhas e Vigilância, que Ameaçam a Segurança e Privacidade na Web.

Rogerio Roth, Ph.D.
Università Ca' Foscari Venezia
Departamento de Ciências Ambientais, Informática e Estatística
Veneza, Italia
Fundação CAPES, Ministério da Educação
posdoctor at gmail.com
rogerio.roth at unive.it

Resumo
O horizonte da educação contemporânea – pedagógica e tecnologicamente correta – vem sofrendo diversas transformações, principalmente no que diz respeito ao bom senso na exposição pessoal e institucional, compartilhamento de conteúdos e arquivos. A falta de conhecimentos sobre segurança e privacidade além de caminhos diversos dos ambientes virtuais de aprendizagem não é garantia de uma nova abordagem ou inovação. Por outro lado, a adoção e a efetiva utilização de modismos sem um contexto prévio de experimentação, testagem, proteção e lógica de utilização podem trazer resultados diversos dos esperados impactando negativamente o uso das tecnologias para apoiar a educação.
Palavras-chave: e-recursos, privacidade, segurança, redesenho, oversharing, releitura.

1. Olhando para o futuro: Quebrando os laços com o passado recente.

Não se trata de um clichê, ou mesmo da trilogia De Volta para o Futuro de filmes de aventura e ficção científica escrita por Bob Gale e Robert Zemeckis, mas repensar a educação em termos e possibilidades tecnológicas atuais e futuras envolve experimentação, prática e pressentimento. Para onde ir?
Diante da diversidade de cenários e opções – gratuitas ou pagas, abertas ou proprietárias, locais ou remotas, nacionais ou estrangeiras – o processo de tomada de decisão deveria levar em conta algo mais do que apenas os custos onipresentes. Itens como segurança e privacidade das informações deveriam ser considerados essenciais.

Muitas pessoas de destaque são reconhecidas mais por seus eventuais erros e tropeços do que por suas grandes conquistas. Não é fácil prever o futuro com 100% de certeza. O que dizer então quando as apostas estão relacionadas ao futuro da área da educação, tão resiliente, resistente, conservadora e avessa às mudanças...

O passado recente nos trouxe uma massificação virtual da academia, muitas vezes sem nenhuma qualidade ou mesmo interação que deveria ser imperativa em tempos de Web 2.0. Com relação ao comportamento na Internet de pessoas e instituições – inclusive educacionais, assistimos ao renascimento dos modernosos, dos deslumbrados, dos chatos e dos invasivos.

“Mas eu tenho tudo no meu Plex. Meu diário, minhas tarefas, minhas músicas, meus livros – minha vida inteira!” (Marshall & Gaviola, 2011).

Este artigo é parte dos resultados da pesquisa “Construindo uma Experiência Imersiva de Aprendizagem a Distância além dos Cursos Online Abertos e Massivos com Webconferência, Método Socrático, Aprendizagem Baseada em Problemas e as Redes Sociais” financiado pela CAPES.

Segurança, privacidade e responsabilidade são temas que insistentemente e de forma recorrente são trazidos à tona – relacionados aqui aos diferentes usos que se conferem à

Internet.
Várias universidades e estudantes não enxergam limites, para se expor (oversharing) nas redes sociais. Da mesma forma parece faltar bom senso na adoção dos diferentes modelos de serviços oferecidos em nuvem (cloud computing), bem como soluções Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e Software como Serviço (SaaS), como o Google Apps. Alguns serviços aparentemente são gratuitos, mas há um preço a pagar por tudo.

Há décadas a Microsoft tem sido criticada por suas práticas monopolistas predatórias. O Google está atualmente sob os holofotes também.
No dia 1º de abril de 2014 o serviço de emails Gmail (Google Mail) completou 10 anos ("Gmail," 2004), ("Gmail," 2014). A data sempre remete à comemoração do dia da mentira, dos bobos ou tolos – principalmente na Austrália, Brasil, Canadá, Estados Unidos e Europa ("April Fools' Day," 2013).

Para os brasileiros o 1º de abril tem diversas interpretações, pois lembra também a revolução militar que ocorreu neste dia, em 1964 – e os difíceis anos que se seguiram.
Intervenções como esta tipificam a técnica do golpe de Estado, que a CIA desenvolveu e aplicou no Brasil, radicalizando artificialmente as lutas sociais até ao ponto de provocar o desequilíbrio político e desestabilizar governos (spooling actions), que não se submetiam às diretrizes estratégicas dos Estados Unidos – que negam a responsabilidade e a cumplicidade com o golpe de estado (plausible denial), norma pela qual os governos americanos pautaram muitas vezes suas políticas de intervenção em outros países (Bandeira, 2004).

"Friday, April 3, 1964 – 12:06 p.m. Thomas Mann: I hope you're as happy about Brazil as I am. Lyndon B. Johnson: I am. I think that's the most important thing that's happened in the hemisphere in three years. Lyndon B. Johnson: I hope they give us some credit, instead of hell." (Beschloss, 1997).

Interpretações e eventos históricos à parte, todos nós (usuários do Gmail) podemos ser vítimas deste estigma.
Somos tolos ao usar o Gmail e as ferramentas associadas do Google?
Qual o preço que pagamos por utilizar estas ofertas "gratuitas"?

Ribble (2014) declara que, "...o Gmail, não foi o primeiro de seu tipo. Na verdade, foi um retardatário relativo à festa do webmail. O objetivo do Gmail não era criar uma maneira totalmente nova de se comunicar, mas fazer melhorias radicais no modelo de webmail existente. E os últimos dez anos deixam pouca dúvida de que eles conseguiram."

Realmente, eles conseguiram fazer "melhorias radicais", indo do absurdo ao inacreditável, verificável em uma documentação judicial de 30 páginas, quando o Google reconheceu que os usuários do Gmail não deveriam ter "expectativas razoáveis" que suas comunicações fossem confidenciais. Seus usuários não têm privacidade total (Rushe, 2013).
Esse processo, aberto em maio (2013), afirma: "Sem que milhões de pessoas o saibam, e há anos, o Google vem sistemática e intencionalmente cruzando a linha do inadmissível e lendo mensagens de email privadas de todos os seus usuários para adquirir o conteúdo, coletar e minerar informações valiosas."
Para John Simpson (Rushe, 2013), diretor do privacy project da organização Consumer Watchdog, o "Google admitiu finalmente que não respeita a privacidade", ressaltando que, aqueles que querem alguma segurança ou intimidade, não deveriam usar o Gmail.

O documento veio à luz em um momento no qual o Google e outras empresas de tecnologia (AOL, Apple, Facebook, Microsoft, Paltalk, Skype, Yahoo e YouTube) tentam explicar o papel que desempenham na vigilância em massa praticada pela Agência Nacional de Segurança (NSA) sobre os cidadãos dos Estados Unidos e estrangeiros (governos, autoridades e cidadãos) de vários países amigos, incluindo a França, Alemanha, Espanha e o Brasil.

As denúncias de Snowden (2013), ex-técnico da Agência Central de Inteligência (CIA), ocorreram através dos jornais The Guardian (Greenwald, 2013) e The Washington Post (Gellman & Poitra, 2013), dando detalhes do tráfego de informações executada através de vários programas de vigilância, entre eles o PRISM (2013) e o XKeyscore (2013). Segundo as informações publicadas, é possível (XKeyscore) ler os conteúdos de emails de qualquer pessoa em todo o mundo, basta saber o endereço eletrônico. Qualquer website pode ser verificado (tráfego de entrada e saída). Qualquer computador que uma pessoa utilize na Internet é possível de ser monitorado. Qualquer notebook é possível de ser rastreado – ao acessar a Internet – enquanto o usuário viaja, por qualquer parte do mundo.

Snowden (2014) disse (00:03:46,445 – 00:03:59,131): “Toda vez que você pegar o telefone, discar um número, escrever um email, fazer uma compra, viajar num ônibus carregando um telefone celular, passar um cartão de crédito em algum lugar, você deixa um rastro. E o governo decidiu que é uma boa idéia recolher toda esta informação, tudo. Mesmo se você nunca foi suspeito de qualquer crime.” (“Snowden Interview,” 2014).

Nenhuma informação nova. Snowden apenas provou o que todos nós, de certa forma, já sabíamos – de que o controle e a manipulação da informação têm sido utilizados (por todas as partes) não apenas em tempos de guerra declarada para mudar a opinião pública, para apoiar determinadas ações dos governantes ou mesmo para conter os resistentes e politicamente incorretos aos olhos do poder dominante.

Se alguém viaja para um país diferente (dos seus deslocamentos habituais – que são monitorados) e tenta acessar o Gmail através de uma forma diversa do webmail imediatamente tem o acesso bloqueado, obrigando a utilização de um celular para receber um código de desbloqueio via SMS ou mensagem de voz. O Google mantém um histórico de dados dos endereços IP utilizados e desconfia sempre que alguém saia de sua zona de conforto “controlada”. Algum usuário solicitou este tipo de “proteção” ou é possível desativar? Não... (“Basics,” 2015), (“SMS from Google,” 2015).

Este tipo de controle – que não apenas o Google faz – parece ser insignificante para quem já transformou a sua vida (pessoal/institucional) em um livro aberto, atualizado e exposto 24 horas por dia (Twitter/Facebook) numa espécie de Big Brother (reality show). Provavelmente, em busca dos seus “quinze minutos de fama” (Warhol, 1967)...

O Google ou qualquer outro provedor de serviços pagos ou “gratuitos” não pode ser o nosso PlexPad, não agora; muito menos no futuro (2149), (Terra Nova – Marshall & Gaviola, 2011).

O ano de 2014 foi pródigo em exemplos de falta de privacidade e segurança tanto para usuários como para instituições, incluindo a falta de uma cultura digital. O incidente de agosto – o maior escândalo de vazamentos de fotos de celebridades já ocorrido – expôs uma brecha de segurança do serviço iCloud, da Apple (“2014 celebrity,” 2014).

Nossas vidas não podem ficar totalmente expostas e/ou dependentes de um único fornecedor. Dessa forma estaremos possibilitando ligações entre os diversos serviços e fornecendo mais informações do que o necessário – tanto para quem hospeda quanto para nossos contatos pessoais e profissionais. Além disso, vamos ficar reféns de uma determinada empresa – sob um determinado governo ou país – e de suas políticas, interesses econômicos e falhas tecnológicas.

Eventualmente tudo o que vai para a nuvem poderá ser perdido ou mesmo acessado por outras pessoas. Se determinadas informações são sensíveis, secretas ou mesmo íntimas, a Internet e a imensa maioria dos seus serviços gratuitos ou pagos com certeza não é o melhor lugar para armazená-los. Afinal nada é para sempre. O Google também nos ensinou isso. Na terça-feira, 30 de setembro de 2014, a crônica de uma morte anunciada finalmente se tornou realidade: o Orkut acabou (Orkut, 2014), (“Orkut Archive,” 2014).

Para Assange (2014), “Ao contrário de agências de inteligência, que espionam linhas de telecomunicações internacionais, o complexo de vigilância comercial atrai bilhões de seres humanos com a promessa de 'serviços gratuitos'. Seu modelo de negócio é a destruição industrial da privacidade. E mesmo os maiores críticos da vigilância da NSA não parecem estar pedindo o fim do Google e do Facebook.”

Este “modelo de negócio” busca não apenas a destruição da privacidade como também o fim do anonimato e o fim da liberdade de opinião sem represálias.
Quem não deve não teme? Quem não deve, deveria temer sim, e com razão...

O fundador do WikiLeaks, Julian Assange, é ele próprio vítima do sistema, da mesma forma como todos aqueles que tentam desafiar as verdades construídas e manipuladas, que se tornaram posteriormente evidências definitivas e inquestionáveis (“WikiLeaks,” 2011).

Mas quais são as opções disponíveis? Fance (2013) reconhece que o Gmail pode ser um dos serviços mais populares, mas há muitas pessoas que sentem que ele está longe de ser o melhor. Ela cita alguns problemas e aponta como a justificativa mais importante o fato do Google escanear cada mensagem de email que é enviada e recebida. Isto é feito para que os anunciantes possam segmentar melhor os usuários e exibir anúncios que sejam mais relevantes para eles – embora do ponto de vista de um usuário do Gmail, isso é considerado uma invasão de privacidade.

Se, por estas razões – ou quaisquer outras – alguém deseja ficar longe do Gmail/Google ou simplesmente queira experimentar algo novo, ela relaciona dez grandes alternativas: Hushmail, Zoho, Mail.com, Outlook.com (substituiu o Hotmail), GMX, Facebook, Inbox.com, Yandex, Shortmail e Yahoo Mail.
Existem muitas outras opções em quase todos os países – a Internet é um mar de possibilidades – e, os maiores players, parecem ter servidores localizados nos Estados Unidos, China e Rússia. Na Wikipédia, por exemplo, existe uma extensa compilação e comparação de provedores (“webmail providers,” 2014).

Algumas pessoas ou instituições podem querer não depender de serviços russos ou chineses por diversas razões. Mas qual a diferença entre ficar sob a vigilância de um Big Brother (Orwelliano) americano, chinês, russo ou qualquer outro controlador?

Este texto não tem a intenção ou mesmo pretensão de se mostrar antirrusso, antiamericano ou anti qualquer outro país. Nada contra ou a favor de qualquer das partes. Apenas reflete os absurdos a que todos fomos jogados, implícita ou explicitamente, após a Segunda Guerra Mundial, durante a Guerra Fria e à bipolarização político-ideológica.
O que pensávamos que tinha ficado no passado se mostra mais vivo do que nunca.

Impossível não relacionar as atuais práticas onipresentes e pervasivas à novela distópica 1984 (“Nineteen Eighty-Four,” 2010) escrita em 1949 por Eric Arthur Blair, ou melhor, através do seu pseudônimo “George Orwell”. O pseudônimo sempre foi uma das formas de anonimato.

Wilde (1891) através de um ensaio e utilizando um diálogo Socrático, afirmou que: “A vida imita a arte muito mais do que a arte imita a vida.” O pesadelo Orwelliano tornou-se realidade.

“Às vezes demora. Às vezes é rápido. Mas a gente sempre tem que acordar” (Cameron, 2009).

O anonimato hoje em dia é algo perseguido por todos os meios e formas. Na Internet, devido à ilusão que muitos têm de estarem anônimos, se verifica a prática inclusive em fóruns de discussão e/ou opinião que, de forma ubíqua, obrigam a utilização de um email de identificação ou filiação a uma rede social – como se as duas possibilidades não fossem possíveis de serem falsas e, dessa forma, ser possível postar um comentário “anônimo”.

Como podemos distinguir as práticas atuais às verificadas na idade média?
De certa forma, vivemos em uma nova “santa” inquisição e caça às bruxas... Alguma diferença mesmo entre as práticas contemporâneas da Gestapo, Kempeitai, NKVD, Stasi, SAVAK, KGB, MSE, FSB, OSS, DOPS, CIA, Mossad e similares?

Em nome de uma paranóia antiterror sistematicamente alimentada, o “Ato Patriótico” (“Patriot Act,” 2008), uma lei fascista que invade a privacidade de qualquer cidadão americano (com reflexos em todo o mundo – nos aeroportos, por exemplo), não podemos criar um estado de exceção, atropelar liberdades fundamentais e direitos constitucionais em alegado combate contra a um imaginado – ou criado intencionalmente – “terrorismo”...

Os novos hereges – acusados de heresia, pirataria ou mesmo terrorismo – permanecem sendo todos os que são contrários aos dogmas estabelecidos, aqueles que questionam certas verdades, consideradas como incontestáveis – criadas sem provas, lógica ou moral de utilização – ou mesmo os que se opõe às opiniões determinadas por certos grupos dominantes. Ninguém é discordante em si mesmo, e qualquer fundador ou participante de alguma prática ou comportamento que venha a ser considerada divergente – em um determinado período histórico e realidade social – nada mais é do que alguém que, do seu próprio ponto de vista, julgava estar ele mesmo percorrendo o caminho correto. O heterodoxo é classificado desta forma apenas porque alguém, investido com algum tipo de poder institucional, classificou a sua prática ou as suas ideias como destoantes e contrárias a uma ortodoxia oficial que se autoconsidera como o caminho correto (Barros, 2008, p. 125).

Não há fatos eternos, como não há verdades absolutas (Nietzsche, 1908, p. 22).
Tanto a ciência como o direito e a própria história são feitos de verdades transitórias. Não existem verdades cabais em áreas do conhecimento humano, em constante evolução, muito menos em nossa “história oficial”, a versão manipulada dos fatos que passa aos livros.
Afinal o papel aceita tudo e quem escreve, define, governa ou mesmo julga o faz de acordo com o seu viés de vida, o que inclui os seus preconceitos bem como a manutenção e o comprometimento com a situação vigente.

Todo homem tem direito à liberdade de opinião e expressão?
Cientistas, juristas, governantes e historiadores sérios, isentos, descomprometidos e sem receio de enfrentar o status-quo e as verdades impostas?
Galileu Galilei (2007) teria, com certeza, opinião divergente sobre tribunais inquisitórios. A realidade que impera corrompe e marginaliza os que se opõem à verdade estabelecida, através do medo da rejeição ou do ridículo, o que faz com que muitos pensadores permaneçam ocultos.

Muitas ações de determinados grupos que, sem opções, tentam sobreviver ao extermínio que lhes é imposto e à ocupação de seus territórios – reais ou virtuais – são erroneamente classificadas como “terroristas”. Isso nunca pode ser comparado com os bombardeios aéreos generalizados contra populações civis que começaram na Segunda Guerra Mundial e culminaram com o ataque de bombas nucleares em Hiroshima e Nagasaki (6 e 9 de agosto de 1945). Perdemos a moral.

O verdadeiro terror permanece sendo as ações de estados poderosos, imperialismos primitivos, bélicos e pré-históricos; que não aprenderam lições com os erros do passado e insistem – através de um caminho unilateralmente imaginado – em negar o direito à autodeterminação dos povos, bem como em impor a sua visão de mundo a outras culturas, na maioria das vezes ignorando as diversidades culturais e minorias étnicas.

Na Internet verificamos que os ataques não se limitam a alvos “estratégicos”. No caso das ações do Google, elas são generalizadas. Além do controle do conteúdo dos emails podemos perceber uma insistente e resiliente forma de induzir e/ou obrigar a identificação corresponde completamente às políticas praticadas por esta empresa que, frequentemente, não se furta de

solicitar meios adicionais – outro email, celular – para ligar os pontos. Em conseqüência, virou prática usual, inclusive em bancos, o envio de códigos via SMS para confirmar operações, como se celulares não pudessem ser roubados. Ao contrário, celulares podem identificar o exato local onde está o usuário – ou quem usa o seu telefone.

Remoaldo (1998) recorda que o anonimato sempre foi uma característica importante da sociedade. A necessidade da sua existência tem sido demonstrada ao longo dos anos. Tem sido de grande valor para dissidentes em países com pouca ou nenhuma liberdade de expressão, para as vítimas de violação e para pessoas que podem querer compartilhar suas experiências sem revelar sua verdadeira identidade. Sem o anonimato, estas ações poderiam resultar no silenciamento dessas pessoas através da censura, agressão física, perda de emprego, processos legais ou mesmo através de assassinato.

Muitos países permitem aos cidadãos ocultar a sua identidade como parte do direito à privacidade, desde que os atos não sejam considerados ilegais. Mas até mesmo este conceito de legalidade é variável em função de uma determinada época ou conjuntura social ("Anonymity," 2011).
A Wikipédia, por exemplo, é escrita colaborativamente principalmente por autores que, ou usam pseudônimos não identificáveis ou usam apenas seus endereços IP, embora alguns usem pseudônimos identificáveis ou seu verdadeiro nome ("Wikipedia: Anonymity," 2014).

As ações do Big Brother (Orwelliano) podem atingir a todos e a atual desconfiança dos provedores de soluções na Internet provoca ainda mais o desejo de permanecer anônimo. O anonimato total na Internet é possível, mas nem sempre garantido, já que os endereços IP podem ser rastreados e associados a um determinado computador através do qual uma mensagem tenha sido enviada ou através do qual o conteúdo de um website tenha sido alterado – sem identificar diretamente um usuário.

Serviços de ocultação de identidade como a Deep Web (Tor, Freenet, I2P e outros como Morphmix/Tarzan, Mixminion/Mixmaster, JAP, MUTE/AntsP2P e Haystack) dificultam o rastreamento, utilizando tecnologias de computação distribuída e encriptação ("Deep Web," 2008), ("Tor Project," 2002), ("Freenet Project," 2000), ("I2P," 2003).
Outra possibilidade é a utilização de uma Rede Privada Virtual ("VPN," 2013).

Hoffman (2012) diz que: "Todos os principais motores de busca rastreiam seu histórico de pesquisa e criam um perfil sobre você, mostrando resultados diferentes baseados no seu histórico de pesquisa." Ele sugere cinco motores de busca alternativos para quem está cansado de ser rastreado: DuckDuckGo, Ixquick's Startpage, Ixquick, Blekko e Ask.com/AskEraser. Também nos recorda que, para navegar anonimamente em toda parte – com velocidade de navegação mais lenta – a melhor opção é o navegador Tor.

O SlashGeek ("Anonymous," 2012) recomenda que não seja usada apenas a Tor (anteriormente um acrônimo para The Onion Router). Indica como melhor opção associar Tor com VPN: Você-Tor-VPN ou mesmo Você-VPN-Tor. Dá dicas sobre VPNs, aponta que o buscador Google não deve ser utilizado e indica o Firefox como o melhor navegador (com as extensões Ghostery, NoScript e Adblock Plus).

Um dispositivo que promete total anonimato online de forma simples, não técnica e de forma barata (US$ 51) é o Anonabox (2012), ("Anonabox," 2015), e há também uma solução gratuita e chave na mão para a privacidade on-line de todos os aplicativos. Ela é chamada de Tails ("Tails," 2009) e trata-se de um sistema operacional "live", desenvolvido a partir do Debian (Linux) e otimizado para a privacidade, onde todos os dados da rede são encaminhados através da rede Tor.

Servidores proxy também podem ser utilizados ("Proxy," 2010). Existem diferentes níveis de proxy (web, cache, revertido, transparente, etc.) com diferentes níveis de proteção e anonimato – suficientes para burlar as restrições de websites até mesmo em países onde a Internet é censurada ou ocorrem guerras, para denunciar os últimos acontecimentos.

Essas tecnologias permitem que o tráfego passe por outro computador antes de se comunicar com o destinatário, revelando um endereço IP diferente do usuário.

O Lizard Squad, grupo que se apresentou como responsável pelos ataques de Natal (2014) à PlayStation Network e Xbox Live acima de tudo fizeram-no para demonstrar a incompetência da Sony e da Microsoft em evitar estes ataques (Pilkington, 2014).
Com o ataque ao Tor, serviço anônimo de Internet, o Lizard Squad (@LizardMafia) atraiu até mesmo a ira do Anonymous (@YourAnonNews) cuja única preocupação é a privacidade possibilitada pelo Tor, que é usado por pessoas ao redor do mundo para navegar e se comunicar sem ter qualquer outra pessoa espreitando suas atividades privadas (Smith, 2014), (Arce, 2014).

O Projeto Tor é um dos sites mais eficazes para comunicação criptografada, tornando-se um dos mais importantes serviços da Internet no mundo.
Denunciantes como Edward Snowden tem utilizado o serviço bem como muitos movimentos dissidentes e usuários – que estejam sob controle das informações – de países como China, Coréia do Norte, Cuba, Egito, Irã, Rússia e Venezuela. Sem querer criar um eixo do mal, onde estamos livres?
Os norte-americanos – e não apenas eles – deveriam considerar seriamente sua utilização.

2. Cavalo de Troia

Em Outubro de 2006 o Google permitiu que instituições educacionais utilizassem o serviço Google Apps, que passou a ser chamado de Google Apps for Education (“Google for Education,” 2015), anteriormente Google Apps Education Edition. O Google Apps for Education (“Apps for Education,” 2015) é gratuito e oferece o mesmo espaço de armazenamento que o Google Apps for Work (“Apps for Work,” 2006), anteriormente Google Apps for Business. Parece ser uma proposta irrecusável. Mas, ainda que as histórias de sucesso se multipliquem; não tem sido uma unanimidade entre as universidades, nem mesmo entre as americanas (Whittaker, 2010).

Na União Européia (atualmente, 2015) são verificadas várias demandas relativas à privacidade dos usuários e o direito a ser esquecido – processo que iniciou na Espanha em 2010 – ou mesmo a divisão de negócios do Google. Tudo para tentar frear o domínio da empresa no mercado de buscas na Internet (Fioretti, 2014), (European Commission, 2014). Problemas recorrentes de (falta de) privacidade vem em um momento em que a empresa Google também está lutando há quatro anos contra uma investigação antitruste (European Commission, 2010).

A partir do ano letivo 2008/09 a Ca' Foscari (UNIVE) começou a utilizar os serviços do Google, iniciando pelo Gmail através da transferência do registro MX do domínio unive.it:

IP address: 157.138.7.88 – Host name: unive.it
MX aspmx.l.google.com
MX alt1.aspmx.l.google.com
MX alt2.aspmx.l.google.com
MX aspmx2.googlemail.com
MX aspmx3.googlemail.com
source: http://network-tools.com/default.asp?prog=express&host=unive.it

Esta iniciativa é verificada inicialmente em Ca' Foscari (2008, 26): “E-mail @stud.unive.it – A partire dall'a.a. 2008/09 a tutti gli studenti è stata predisposta una casella di posta elettronica identificata da numero.di.matricola@stud.unive.it. Le caselle di posta, ospitate presso l'operatore Google, dispongono di oltre 7 GByte di spazio disco. L'iniziativa intende migliorare la qualità delle comunicazioni verso gli studenti e da questi all'Ateneo.” Posteriormente em Ca'

Foscari (2012, 55) há a referência “Si prevede inoltre che la migrazione a Google Apps for Education possa incontrare qualche problema (di non grave entità) relativo ad aspetti tecnici e/o organizzativi” e percebe-se que, mesmo sendo uma oferta “gratuita” do Google (sem custos diretos de aquisição), a UNIVE pagou (indiretamente) por serviços de consultoria: “Investimenti relativi alle consulenze per il passaggio ai sistemi Google Apps for Education, Moodle e iTunes U.”
Tanto o Google, como o Moodle e a Apple não cobram (diretamente) pela utilização de suas plataformas por universidades. Mas um dia a fatura chega.

Atualmente (ano letivo 2014/15), todos os serviços do Google Apps for Education estão disponíveis para professores, funcionários, investigadores (username@unive.it) e para os estudantes (matricola@stud.unive.it). Il sistema di autenticazione di Ateneo: “Per i docenti, dipendenti, ricercatori l'email username@unive.it e i servizi Google Apps for Education associati; per gli studenti l'email matricola@stud.unive.it e i servizi Google Apps for Education associati;” (“autenticazione di Ateneo,” 2015): “Avvertenza: sebbene la nuova casella di posta sia ospitata presso l'operatore Google vi si accede esclusivamente dall'indirizzo web http://mail.stud.unive.it e non via www.gmail.com”, (“account di posta studenti,” 2015).

Contudo os emails estão explicitamente expostos no website da UNIVE, ignorando os riscos envolvidos e se abstendo de utilizar, por exemplo, JavaScript ou imagens.

Piotto (2014) disse: “Use image instead text email is forbidden by Italian law (legge Stanca 17/01/2004 about public administration sites accessibility). Use text like [dot] [it] or _AT_ help spammers (see http://techie-buzz.com/featured/tips-to-tackle-email-harvesting-spam.html). Use complex system like captcha, JavaScript, etc... help us to prevent spam but block Google indexing and reduce site's usability. We are a public service, @unive.it isn't a personal email (if you want a personal email use @gmail.com), our first goal is help student and users to find us (Google indexing is necessity, not a problem), no matter if we receive spam.”

Este posicionamento é simplesmente absurdo, e o mesmo pode se dizer com relação a todos os argumentos oferecidos como razão para não proteger os emails. Atualmente todas as contas @unive.it recebem uma razoável quantidade de spams, maior do que o verificado em contas “normais” do Gmail já incluídas em listas de spammers. Isso se deve, principalmente, à comercialização das listas de email para as pessoas da instituição acadêmica (“clientes” internos e externos) que são feitas através de ofertas enviadas para todos os detentores de contas. E não me refiro às absurdas mailing lists (CIdE) que são criadas internamente e, como sempre, atiram primeiro para perguntar depois (“Mailing List CIdE,” 2015).

Por que necessitamos de um email institucional? Para “provar” algum vínculo?
Este tipo de conta é aquela sobre a qual não temos completo controle, que está sujeita ao recebimento de mensagens não solicitadas – institucionais ou não – com origem na própria instituição e que, na maioria das vezes, perdemos o acesso a todo o conteúdo e contatos quando nos desligamos, ou somos desligados.

A UNIVE, por outro lado, disponibiliza um servidor proxy (“Proxy Settings,” 2015), proxy.unive.it (157.138.1.34: 3128) que permite acessar os serviços internos – como se estivéssemos dentro da rede interna, o que inclui email – e desta forma omitir a localização.

A questão da segurança passa também pela correta atenção e informação dos professores aos estudantes – de todos os níveis – em expor e demonstrar os riscos bem como sugerir alternativas – não apenas com relação à exposição excessiva. Diversificando as opções estaremos colaborando para criar uma sociedade digitalmente um pouco mais segura e justa.

O chanceler russo, Sergei Lavrov, disse na ONU que “...ninguém tem o monopólio da verdade e ninguém é agora capaz de adaptar processos globais e regionais para as suas próprias necessidades.” (Lavrov, 2014). Trata-se de uma afirmação correta e coerente – ainda que absurda, vindo da Rússia, que pratica o oposto do discurso, e de forma recorrente, nos casos

da Ucrânia, Geórgia e Moldávia.

Tal declaração deveria inclusive ser aplicada à versão Stalinista da história – principalmente relacionada à Segunda Guerra Mundial, cujos eventos insistentemente têm sido alterados e utilizados de forma equivocada (por todas as partes) e “Hollywood” que, na falta de novas “vitórias” militares e diante do repetitivo insucesso verificado posteriormente (Coreia, Vietnam, Afeganistão, Iraque e Síria) não se furta de distorcer os fatos e explorar o evento, pelo visto, até a última gota: Fury, um filme da Sony (Block & Ayer, 2014).

Não se trata de assuntos estanques ou problemas alheios à realidade encastelada em que vivem muitas universidades. Vivemos em estado de guerra, mesmo quando não declarada, inclusive na Internet e com todos os contornos admitidos, o que inclui todas as formas de vigilância, ataques eletrônicos, ciberataques e ciberterrorismo; patrocinados muitas vezes por governos e estados soberanos – democráticos ou não – ou por grupos independentes.

Angela Merkel (Alemanha) e Dilma Rousseff (Brasil) teriam sido apenas duas, dos 35 lideres mundiais vigiados pela NSA (Rawlinson, 2013), (“Global surveillance,” 2013). Segundo Aymone (2014), desde que as denúncias foram comprovadas muitas universidades públicas federais brasileiras adotaram diversas novas normas de segurança, dentre elas a utilização de servidores próprios de emails, algo que a maioria delas já fazia.

De forma geral, existe a recomendação (DOU de 17/10/2014) para que seja adotado o “Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação”, da Secretaria de Fiscalização de Tecnologia da Informação do TCU (SEFTI), para diminuir os riscos a que a área de TI está sujeita, especialmente no que se refere à criação de acordos de nível de serviço com as áreas demandantes e à realização de documentação dos produtos desenvolvidos pelas empresas terceirizadas, para que não fiquem reféns das empresas contratadas, detentoras do conhecimento dos produtos desenvolvidos, (“Guia,” 2012).

O vazamento de informações não é algo inerente à Internet ou ao uso de computadores. Sempre existiu. E não foram apenas espiões do “inimigo” a fotografar documentos secretos. Na maioria das vezes é fogo amigo e o problema está em casa – os vazamentos se originam principalmente de dentro das instituições. Dormimos com o “inimigo” ou com heróis, dependendo do ponto de vista do observador...
A digitalização apenas tornou as coisas mais fáceis e rápidas. E a Internet permitiu uma maior divulgação, ou seja, mais pessoas tem acesso à informação.
O WikiLeaks (2006) é uma organização que publica, em seu website, postagens de fontes anônimas, documentos, fotos e informações confidenciais, vazadas de governos ou empresas, sobre assuntos sensíveis.

Na Rússia, o Kremlin retornou às máquinas de escrever – para evitar vazamentos. Já teriam sido gastos quase US$ 15 mil na compra destes equipamentos “modernos” (“Kremlin,” 2013). A piada parece estar prestes a se tornar literal também na Alemanha (Farivar, 2014).

Informações secretas deveriam, como diz o nome, serem mantidas em segredo. No caso dos emails, o maior problema é o que nós escrevemos e para quem. Ao contrário de palavras faladas (que podem ser gravadas) emails são escritos e identificam (digitalmente) a origem e o destino. Podem e são usados como meio de prova, inclusive depois de nossa própria morte (e.g. Steve Jobs), (Ames, 2014).

Determinadas palavras ou expressões podem classificar uma mensagem qualquer como interessante ou potencialmente perigosa aos olhos dos softwares espiões que monitoram os computadores (local ou remotamente). Isso é válido também para websites de todos os tipos, o que inclui blogs e redes sociais. A McAfee tem relacionado as palavras-chave de busca mais perigosas aos scammers (Keats & Koshy, 2008).

Uma mesma mensagem estará armazenada, no mínimo, em dois lugares: no emissor e no

receptor. Caso os dois lados mantenham cópias das mensagens enviadas e recebidas em seus equipamentos de uso pessoal bem como em seus servidores (nuvem) a mesma mensagem estará, no mínimo, em quatro lugares. Ou seja, bastará invadir ou ter acesso a apenas uma das opções para se apropriar de todo o conteúdo, algo que não apenas a NSA faz com perfeição.

Existem diversas tecnologias para melhorar o nível de segurança das mensagens enviadas como a encriptação e o uso de certificados. Mas nada é perfeito. Basta uma senha fácil de ser quebrada para que estes dados sejam acessados por qualquer um. O principal é ter bom senso nos conteúdos e, mesmo com relação às mensagens privadas, ter em mente que, eventualmente o texto será acessado por outras pessoas, mesmo não autorizadas, que poderão fazer uso diverso das informações, inclusive contra nós.

A questão da segurança, para as universidades, não deveria ficar restrita aos emails e servidores próprios. Para Roth (2014), deveriam ser avaliadas quais as opções são disponíveis gratuitamente neste momento – e seriam tecnicamente e pedagogicamente utilizáveis. O enfoque não seria cair na discussão pago vs. gratuito, mas se posicionar sobre questões como segurança e privacidade. Levando em conta a qualidade atual das opções gratuitas (como o pacote do Google), trata-se de um apelo irresistível para as instituições, públicas e/ou privadas, em tempos de vacas magras.

Mas não deveríamos cometer o mesmo erro dos troianos.

O fim do anonimato, por exemplo, não significa qualquer garantia do fim da publicação de conteúdo impróprio (Blum, 2014).

O Marco Civil da Internet brasileira – oficialmente chamado de Lei nº 12.965, de 23 de abril de 2014 – também garante a liberdade de expressão, mas registra possibilidade de indenização quando houver violação à intimidade e à vida privada (“Civil Rights Framework,” 2014). Moody (2011) descreveu o Marco Civil como um uma lei “anti-ACTA”, em referência ao Acordo Comercial Anticontrafação, muito criticado por restringir a liberdade na Internet e que acabou rejeitado pela União Europeia. Tim Berners-Lee, inventor da World Wide Web, afirmou ser um “fantástico exemplo de como os governos podem desempenhar um papel positivo na promoção dos direitos da web e mantê-la aberta”, além de pedir para outros países seguirem o exemplo do Brasil (McCarthy, 2014).

A Internet é um reflexo do mundo imperfeito em que vivemos e, de uma forma ou de outra, permanecerá com bons e maus aspectos. Podemos observar práticas que podem ser, ao mesmo tempo, consideradas certas ou erradas, dependendo de quem as julga (status-quo). Países como a China, Coréia do Norte e Cuba, dentre outros, são criticados pela segunda maior "democracia" do mundo (EUA) com relação ao controle que fazem sobre o acesso à Internet.
Qual país não faz o mesmo (e não apenas na Internet)?

3. Remando contra a maré

Com relação ao compartilhamento de conteúdos existem diferenças conceituais – e distorcidas – bem como interpretações diversas sobre o droit d'auteur (direito do autor) francês (“Authors' rights,” 2014) e o copyright (direito de cópia) anglo-saxão (“Copyright,” 2009).

Wong (2013) relaciona a apropriação chinesa da cultura ocidental e a construção no imaginário do ocidente de uma China que representa o mimetismo por excelência. E revela que, a cópia como método de aprendizagem, comum nas academias de artes no mundo todo, faz parte da cultura chinesa e de sua pedagogia, ligada ao pensamento de Confúcio, para quem copiar é um exercício de humildade. Em 2004, em resposta a alegações de violações

de direitos autorais, o governo da China alegou que, graças às habilidades de imitação dos artistas de Dafen (Shenzhen) consumidores de todo o planeta podiam ter acesso ao mundo da grande arte.

Este ponto de vista pode ser extrapolado para as músicas e os livros. Mas por que não aplicar também à educação, para que mais pessoas tenham acesso?
O processo de replicação enquanto instrumento facilitador de acesso à informação e de mudança social esbarra sempre nas mesmas questões.

Alguns governos insistem no caminho da criminalização. Projetos como o PROTECT IP Act (Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act), ("PIPA," 2011) e o Stop Online Piracy Act ("SOPA," 2011) não seguiram adiante. E as perseguições, o encerramento de alguns serviços de hospedagem bem como o controle dos mecanismos de busca ("Chilling effect," 2011) não têm atingido os resultados esperados, como era previsto.
Afinal existem diversos outros meios de compartilhar os conteúdos, com maior ou menor exposição bem como comprometimento de quem o pretende fazer.
Os casos do Napster, Megaupload e The Pirate Bay são exemplares. Após estes serviços terem sido retirados do ar, as opções – clones ou similares – se multiplicaram de forma exponencial. Em tempos de economia compartilhada a solução para o "problema" não passa por este caminho: proibir, perseguir e punir...

A história nos tem demonstrado que determinadas ações e/ou posicionamentos tem diferentes interpretações ao longo do tempo. Nós deveríamos aprender mais com nossos erros do que com nossos sucessos acidentais. Há exemplos notórios provando o inverso, repletos de discriminações dos mais variados tipos: classe social, convicção, cor da pele, credo, deficiência, etnia, idade, instrução, nacionalidade, opção sexual, opinião política, origem, raça, religião, sexo ou qualquer outro tipo. No passado e ocasionalmente hoje em dia, a discriminação era algo explícito. Em tempos politicamente corretos a discriminação segue outros moldes. Muitas pessoas já foram barradas ou mesmo perderam empregos por se exporem em redes sociais: suas opiniões, suas preferências, seus "amigos", seus seguidores.

As novas gerações nasceram com a ilusão de que existia liberdade – pelo menos na Internet – e não existe nelas o sentimento dominante, de se fazer algo errado, com relação ao compartilhamento de informações e dados, sejam simples fotos pessoais bem como de músicas, filmes e livros de terceiros. Considerando que eles são o futuro e quem controla o mundo é sempre uma questão datada – todos nós temos um limite de vida – esta dificuldade em breve estará ultrapassada.

O caminho da cópia como como método de aprendizagem não pode ficar restrito às escolas de arte (de todo o mundo) nem ser visto de forma discriminatória como acontece atualmente contra os chineses, da mesma forma como ocorreu com os japoneses após a Segunda Guerra Mundial. Ambos nos deram lições que o processo de cópia sempre tem um custo e que sempre ocorre alguma apropriação de conteúdo por quem a realiza...

Não cabe aqui discutir direitos de autor ou de cópia, mas se uma determinada obra é exibida ao público, ou seja, foi exposta, publicada, alugada ou mesmo vendida não há como impedir, na prática, que as pessoas façam registros (fotos, áudio, vídeo, cópias em papel, etc.) e depois as exibam e/ou compartilhem. É impossível e não há Big Brother (Orwelliano) que consiga conter este tsunami devido à onipresença das câmeras de foto e vídeo nos telefones celulares.
Pode-se apenas tentar, mas é e será sempre uma batalha perdida.

4. Efeito Streisand

Em 24/11/2014 um grupo autointitulado "Guardians of Peace" ou "GOP" teria invadido os

servidores da Sony Pictures, bloqueando todos os computadores, tirando do ar o website da empresa, além de roubar arquivos e vazar filmes inéditos (“Sony hack,” 2014).
Como uma empresa tão poderosa como a Sony – tecnologicamente falando – se mostra tão vulnerável a diferentes ataques (Guardians of Peace, Lizard Squad) em tão pouco tempo?

A origem dos “Guardians of Peace” ainda é incerta. Segundo o canal de televisão americano NBC, fontes do FBI “investigam” se Coreia do Norte “estaria” por trás do ataque (Williams, 2014), (“North Korea,” 2014). O país asiático possui sua própria divisão de hackers dentro das forças armadas, conhecida como Unidade 121, que é “suspeita” de ataques aos Estados Unidos e à Coreia do Sul.

Poderiam ter sido os norte coreanos? Sim, da mesma forma que, poderiam ser os chineses, russos, iranianos, japoneses, europeus, americanos (do norte, do centro ou do sul) ou o próprio pessoal da Sony. Os pseudo defensores da liberdade de expressão e privacidade estão em todas as partes.

O “indício” mais forte da autoria do ataque seria o fato da Coreia do Norte ter um “motivo” para atacar a Sony Pictures: o filme “The Interview”, uma comédia de mau gosto da Sony sobre o assassinato fictício do líder supremo norte-coreano Kim Jong-um (Roger & Goldberg, 2014).

Se a Sony foi novamente vítima do inimigo oculto (ou declarado) talvez nunca tenhamos todas as respostas. Poderia ter sido uma ação de marketing (interna) ou obra de fogo amigo (Lena), afinal os repetidos ataques à estrutura da Sony tem obtido um aparentemente fácil sucesso.

Tudo o que os “Guardians of Peace” obtiveram com relação às ameaças para suspender o lançamento do filme foi tornar o mesmo muito mais comentado do que normalmente seria, ou seja, o Efeito Streisand. Trata-se de um fenômeno da Internet onde uma tentativa de censurar ou remover algum tipo de informação se volta contra o censor, resultando na vasta replicação (“Streisand effect,” 2007).

É bem provável que o filme A Entrevista passasse batido, não fosse toda a polêmica que o envolveu. Segundo Chedin (2014) e Spargo (2014), há motivos para suspeitar dessa história – que aponta o envolvimento da Coréia do Norte, ou mesmo a isenção da Sony.

Através do ocorrido a Sony recebeu uma atenção desproporcional e o filme ganhou um absurdo marketing gratuito. Em nome da “liberdade de expressão” e como um ato de protesto e apoio, muitas pessoas recorreram a websites sobre cinema, notadamente o IMDb, e deram nota 10 ao filme, antes mesmo de assisti-lo (IMDb, 2014), (Savov, 2014).

Chegaram ao cúmulo (Barack Obama) para sugerir o filme ser nomeado para um Oscar! (Maddocks, 2014).

O mesmo filme que é destaque na corrida pela Framboesa de Ouro (Kreps, 2015), que “homenageia” as piores produções do ano (2014) do cinema americano.

Se o filme é bom ou não, depende do gosto pessoal de cada um.
Com muita boa vontade, protesto e tudo mais, Chedin (2014) afirma que o filme não merece nem metade disso. Pode ser, mas melhor não confiar em críticos da mesma forma que não devemos confiar em políticos, pesquisadores e historiadores isentos.

Os lucros da Sony provavelmente estão sendo maiores do que “normalmente” teriam sido sob condições normais de “temperatura e pressão”. Apenas no fim de semana de estréia foram cerca de US$ 18 milhões, sendo que US$ 15 milhões seriam de vendas on-line (Baker & Milliken, 2014) – o filme foi lançado simultaneamente em diversos serviços de streaming, como YouTube, Google Play, Xbox Videos e Kernel.

Segundo a Sony, apenas neste período o filme foi comprado ou alugado online mais de 2

milhões de vezes (Baker, 2014), tornando-se o maior filme online da Sony Pictures de todos os tempos.

Entre 24 de dezembro e 4 de janeiro este número subiu para mais de 4,3 milhões de vezes, tendo arrecadado mais de US$ 31 milhões com exibições on-line, na TV a cabo e em vendas de telecomunicações. Além disso, mais US$ 5 milhões nas bilheterias de cinemas, com 580 salas independentes exibindo o filme na América do Norte (Sinha-Roy, 2015).

Até que ponto a Sony aprendeu com os erros do passado e pode ser considerada isenta de responsabilidade no processo? Ou seja, colocar informações sensíveis em um servidor – possível de ser acessado via Internet – não remete à releitura de uma cilada antecedente, ao estilo Pearl Harbour ("Japan Questions," 2008) – quando todos os porta-aviões americanos da frota do Pacífico já haviam abandonado o porto, restando apenas os navios encouraçados, quase todos velhos e ultrapassados – para alcançarmos nossos verdadeiros propósitos?

Os resultados, posteriores ao lançamento do filme, tem sido tão expressivos que, provavelmente, as portas dos servidores da Sony estarão abertas à futuras "invasões". Custa bem menos para promover os novos lançamentos e os lucros on-line são imediatos.

Alguma "confirmação" da autoria do ataque apresentada até o momento?
O governo da China afirmou que não há provas de que a Coreia do Norte seja responsável por atacar a Sony Pictures, como disseram os Estados Unidos (Rajagopalan & Holland, 2014). No passado os EUA também acusaram a China de fazer espionagem eletrônica, sem provas, e uma autoridade norte-americana disse que o ataque contra a Sony "pode ter usado" servidores chineses para mascarar suas origens (Wroughton & Rajagopalan, 2014).

"Pode ter usado" é uma afirmação imprecisa, parcial e tendenciosa. Suspeitar e investigar indícios é algo normal. Divulgar estas informações antes de provar algo é irresponsável. Dar nome aos bois, com isenção e sem comprometimento, é outra história.

A insistente e oportunista atitude de tentar incriminar – sem provas – todos os que se opõem às idéias dominantes de um determinado país não nos confere o direito de expô-los e ridicularizá-los (bascos, comunistas, cubanos, nacionalistas, nacional-socialistas, norte-coreanos, palestinos, iranianos, ucranianos, venezuelanos, etc.).

Este modus-operandi recorrente sempre remete ao argumento utilizado, por exemplo, com relação às alegadas grandes reservas ocultas de armas de destruição em massa do Iraque...
As agências de "inteligência" americanas CIA (Iraque) e FBI (Sony) andam tão desacreditadas que suas informações deveriam ser sempre interpretadas ao contrário.
Algo como a previsão do tempo: erraríamos menos...

Trata-se de estratégia adotada por diversas nações, ao longo da história, para distorcer os fatos, criar falsas verdades, obter o apoio da maioria de outros países – e, às vezes, nem isso.

Desde os primeiros anos do século XX assistimos a adulteração, negação, criação ou mesmo imposição de versões consideradas "históricas" de episódios como Holodomor, massacre de Katyn, ataque a Pearl Harbor, Holocausto, assassinato de John F. Kennedy, ataques de 11 de Setembro, armas de destruição em massa de Saddam Hussein, Campo de Detenção da Baía de Guantánamo, etc. A lista não pretende ser exaustiva e nem exclusiva de algum país.

Teorias da conspiração? Até poderiam ser, mas isso não significa que a enorme lista de evidências e provas das versões extra-oficiais sejam mentiras ("American False Flag Operations," 2015), (Sutton, 2001), (Sutton, 2000).

Hoje em dia pensamos que sabemos o que realmente aconteceu na Ucrânia (1932-1933), na Polônia (1940), no Brasil (1964-1985) e no Iraque (2003). A história foi parcialmente reescrita – nestes casos. Mas, muitas outras revisões (releituras) são necessárias ("Holodomor," 2010),

(“Katyn,” 2004), (“Iraq,” 2003).

A história oficial dificilmente reflete a história real – o que realmente aconteceu – pois sempre é distorcida pelo viés de quem a conta – ou é obrigado a contar.
Não podemos mudar o passado, mas deveríamos ao menos tentar corrigir nossos erros – inclusive das versões “oficiais” da história – e, na medida do possível, não repeti-los.

Diversos episódios permanecem sendo vítimas da manipulação dos fatos hoje em dia. Deveríamos ter evoluído – como raça humana – mas permanecemos utilizando campos de concentração, realizando a deportação forçada de pessoas e o extermínio, praticando os mais diversos tipos de discriminações, forçando diversas formas de escravatura – de todas as cores – e explorando o trabalho de crianças.

Se o ano de 2014 trouxe esperança à Cuba, também nos provou que este país – e não apenas – permanece limitando e perseguindo a liberdade de opinião.

Diante de uma Organização das Nações Unidas inerte frente às limitações de poder e diante de um “conselho de segurança” que não permite o posicionamento da maioria, verificamos o recrudescimento de conflitos em todos os continentes e assistimos ao renascimento de uma nova guerra-fria em plena Europa.

Este conselho de “segurança” cujos cinco membros permanentes (que possuem direito a veto) são os mesmos que, atualmente, praticam as maiores atrocidades e crimes contra a humanidade – sem nenhuma punição, pois se consideram acima da lei que eles mesmos criaram para os outros: China (Tibet), França (Libia), Rússia (Ucrânia), Reino Unido (Argentina) e Estados Unidos (Iraque).
Além disso, assistimos paralisados, a eterna vítima da Segunda Guerra Mundial (Israel) não se furtar de aplicar nos dias de hoje (com provas) os mesmos crimes e perseguições que alegaram terem sido vitimas no passado (sem provas).

O combate de informações – ou melhor, desinformações – hoje em dia acontece principalmente através da Internet. Muitas pessoas que ocupam cargos importantes – o que inclui presidentes e primeiros ministros – optam por divulgar informações relevantes através do Twitter do que através de comunicados oficiais. Nada como criar um ruído...

As verdades criadas (mentiras) contra a Ucrânia e os seus heróis (1942-1956) se repetem nos dias de hoje (2013-2015), (Stopfake, 2014), distorcendo o papel histórico de nacionalistas como Stepan Andriyovych Bandera (“Stepan Bandera,” 2010) e seus seguidores atuais, assim como o Exército Insurgente da Ucrânia (“UPA,” 2007) e todos os trágicos acontecimentos que se seguiram a Euromaidan (“Euromaidan,” 2013), que começou na noite de 21 de Novembro de 2013, com protestos públicos na Maidan Nezalezhnosti (Praça da Independência) em Kiev, exigindo uma maior integração europeia. Tudo na esperança de criar um estado independente ucraniano, e agora totalmente integrado na União Europeia.

E como em qualquer conflito bélico, dá origem à guerra de propaganda. Diante da manipulação das notícias por agencias russas ou pró-russas – muitas invertendo totalmente o sentido do que acontece – merece destaque o blog “Ucrânia em África” (“Ucrânia em África,” 2015), uma das mais isentas fontes de informações sobre os absurdos que acontecem neste país europeu.

Os episódios citados trazem lições em todos os sentidos de interpretação.

O ano de 2015 será apenas mais um em que as potências mundiais mostrarão sua inabilidade para resolver as crises internacionais. O próximo presidente dos Estados Unidos terá que descobrir se há um meio-termo entre as imprudências de George W. Bush e a retração de Barack Obama. A União Europeia terá que decidir vai se manter nas fronteiras atuais ou se vai permitir o ingresso da Ucrânia e Turquia. Recrudescimentos das tensões na Ucrânia serão

considerados pelo Ocidente como culpa da Rússia. Vladimir Putin, por sua vez, culpará o Ocidente, ao mesmo tempo em que estimulará os russos a se fortalecer internamente contra a maligna dominação estrangeira. A China deve usar sua influência para pressionar quanto a mais poder na governança global da internet. O Big Brother (Orwelliano) poderá se tornar mundial (Ahmed, Doucet, Gracie, Kendall & Mardell, 2015).

O atentado ocorrido na França (Charlie Hebdo) em 7 de janeiro 2015 – na hipótese de se confirmarem indícios de que os assassinos sejam terroristas muçulmanos – indiretamente poderá introduzir mais dificuldades para a Turquia, além de favorecer a atual ofensiva racista na Europa (Schofield, 2015). Provavelmente no dia em que todas as liberdades apregoadas (expressão, opinião, religião e manifestação) guardem distancias e limites éticos entre si – politicamente corretas e contemporâneas – seja possível obter uma solução adequada para todas as questões que envolvem não apenas o complexo mundo religioso, sem correr o risco de mexer com as paixões existentes quando se trata da fé, seja ela qual for.

A história da Europa foi um longo drama sanguinário repleto de guerras, conflitos, revoluções, pragas, discriminações, migrações forçadas, golpes e catástrofes – a maioria destes eventos relacionados à religião ou a diferentes visões e opções religiosas. Em nome de “deus” permanecemos assistindo a maioria dos resilientes e lamentáveis episódios.
“Não é momento de repetir a história. É tempo de fazer história” (#McLaren Honda).

Da mesma forma que estúdios de cinema podem obter melhores resultados financeiros através de operações on-line seguras – de menor custo e valor ao consumidor final – do que em salas de cinema, deveriam as universidades se questionarem sobre o modelo de venda de conhecimentos dominante e apostar em soluções inovadoras on-line (diferentes deste modelo de e-learning de baixa qualidade que se massificou) e com um novo modelo de sustentabilidade, sem cobrar diretamente dos clientes.

Os OpenCourseWare evoluíram para os Massive Open Online Course e a tendência irreversível é seguir em frente em direção a cursos universitários completos, via internet, em ambientes seguros e com privacidade garantida, com certificação e totalmente gratuitos. Não seria enfim um caminho às avessas de todos os outros – um redesenho – para se atingir a bela norma revolucionária, democrática e constitucional da “educação universal, obrigatória e gratuita” a todos os níveis, para todos e sem nenhuma distinção ou discriminação? (Neves, 2003).

A utilização de recursos gratuitos disponíveis na Internet é uma mais valia para todas as universidades, sejam elas públicas ou privadas, pois teoricamente e provavelmente sua utilização demanda menos recursos financeiros do que seriam necessários para desenvolver e/ou manter serviços e estrutura própria. Contudo, é preciso moderar o entusiasmo dos primeiros adeptos e amortecer o ceticismo em relação às novidades, bem como repassar esses benefícios – de alguma forma – aos usuários e garantir que os mesmos terão segurança e privacidade preservadas.
A destruição da privacidade amplia o desequilíbrio de poder existente entre quem decide e o povo, deixando os povos subjugados e as classes oprimidas, como Orwell escreveu, ainda mais sem esperança (Assange, 2014).

No filme Homem de Ferro 3 (Feige & Black, 2013), Tony Stark (Robert Downey Jr.) cita uma frase no inicio e no final do filme: “Nós criamos nossos próprios demônios”...

O contexto é diverso do presente artigo e muito mais próximo da relação estratégica da Europa com a Rússia após o fim da Guerra fria, mas pode ser aplicado e generalizado, na medida em que, quando apostamos todas as nossas fichas em uma determinada solução de mercado – produto e/ou serviço, tecnologia proprietária e/ou disponibilizada por um único fornecedor; e hospedada em um único país – nos tornamos reféns de nossas próprias opções, ou pior ainda, das opções de terceiros a quem confiamos as nossas informações na Internet.

Referencias

2014 celebrity photo hack (2014, September 1). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/2014_celebrity_photo_leaks

Ahmed, K., Doucet, L., Gracie, C., Kendall, B. & Mardell, M. (2015, January 2). What will the big stories be in 2015? BBC News. Retrieved Jan 3, 2015, from http://www.bbc.com/news/world-30648444

Ames, M. (2014, March 25). Newly unsealed documents show Steve Jobs' brutal response after getting a Google employee fired. PandoDaily. Retrieved Jan 22, 2015, from http://pando.com/2014/03/25/newly-unsealed-documents-show-steve-jobs-brutally-callous-response-after-getting-a-google-employee-fired/

Anonabox (2012, January). Retrieved Jan 22, 2015, from https://anonabox.com/

Anonabox: the Tor hardware router (2015, January 7). Retrieved Jan 22, 2015, from https://www.indiegogo.com/projects/anonabox-the-tor-hardware-router

Anonymity (2011, March 24). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Anonymity

April Fools' Day. (2013, April 4). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/April_Fools%27_Day

Arce, N. (2014, December 27). Anonymous to Lizard Squad: Keep Your Hands off Tor. Tech Times. Retrieved Jan 22, 2015, from http://www.techtimes.com/articles/23248/20141227/anonymous-to-lizard-squad-keep-your-hands-off-tor.htm

Assange, J. (2014, December 4). Who Should Own the Internet? Julian Assange on Living in a Surveillance Society. The New York Times. Retrieved Dec 16, 2014, from http://www.nytimes.com/2014/12/04/opinion/julian-assange-on-living-in-a-surveillance-society.html?_r=0

Aymone, D. (2014). Internet publication [personal communication]. Message received from <domingos.filho@unipampa.edu.br> in October 17.

Baker L. B. & Milliken, M. (2014, December 28). Sony's 'The Interview' makes $18 million in opening weekend. Reuters. Retrieved Jan 22, 2015, from http://www.reuters.com/article/2014/12/29/northkorea-cyberattack-sony-idUSL1N0UC0JO20141229

Baker L. B. (2014, December 28). 'The Interview' Becomes Sony's No. 1 Online Movie Of All Time. HuffPost. Retrieved Jan 22, 2015, from http://www.huffingtonpost.com/2014/12/28/the-interview-online_n_6388086.html

Bandeira, L. (2004). 1964: A CIA e a técnica do golpe de Estado. Revista Espaço Acadêmico, 64, ISSN 1519.6168. Retrieved Jan 22, 2015, from http://www.espacoacademico.com.br/034/34ebandeira.htm#_ftn4

Barros, A. (2008). Heresias entre os séculos XI e XV: uma revisitação das fontes e da discussão historiográfica – notas de leitura. In Arquipélago, 2 (11-12), 125-162. ISSN 0871-7664. Retrieved Dec 20, 2014, from http://hdl.handle.net/10400.3/626

Basics: Recover your account via text message (2015). Retrieved Jan 22, 2015, from https://support.google.com/accounts/answer/152124?hl=en

Beschloss, M. (1997). Taking Charge: the Johnson White House Tapes, 1963-1964. New York: Simon & Schuster, p. 306.

Block, B. (Producer), & Ayer, D. (Director). (2014). Fury [Motion Picture]. Culver City, CA, United States: Columbia Pictures

Blum, R. (2014, October 19). Proibir anonimato não impede publicação de conteúdo impróprio na Internet. Universo Online. Retrieved Dec 29, 2014, from http://noticias.uol.com.br/opiniao/coluna/2014/10/19/proibir-anonimato-nao-impede-publicacao-de-conteudo-improprio-na-Internet.htm

Brazilian Civil Rights Framework for the Internet (2014, April 23). Retrieved Jan 22, 2015, from

http://en.wikipedia.org/wiki/Brazilian_Civil_Rights_Framework_for_the_Internet

Ca' Foscari (2008). Inaugurazione 141° Anno Accademico 2008/09 Università Ca' Foscari Venezia. Retrieved Dec 10, 2014, from http://www.unive.it/nqcontent.cfm?a_id=61185

Ca' Foscari (2012, May 18). Rapporti dei Delegati del Rettore 2011. Retrieved Dec 10, 2014, from http://blogs.unive.it/users/blogrettore/weblog/09d3a/Il_lavoro_dei_delegati.html

Cameron, J. & Landau, J. (Producers), Cameron, J. (Director). (2009). Avatar [Motion Picture]. Santa Monica, CA, United States: Lightstorm Entertainment

Chedin, R. (2014, December 26). Eu vi “A Entrevista” para que você não precise. Retrieved Dec 30, 2014, from http://www.manualdousuario.net/a-entrevista-critica/

Chilling effect (2011, October 19). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Chilling_effect

Comparison of webmail providers (2014, December 6). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Comparison_of_webmail_providers

Deep Web (2008, December 27). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Deep_Web

Edward Snowden (2013, June 10). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Edward_Snowden

Euromaidan (2013, November 27). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Euromaidan

European Commission (2010, November 30). Antitrust: Commission probes allegations of antitrust violations by Google. Press release IP/10/1624. Retrieved Dec 10, 2014, from http://europa.eu/rapid/press-release_IP-10-1624_en.htm

European Commission (2014, July 3). Factsheet on the “Right to be Forgotten” rulling (C-131/12). Retrieved Dec 10, 2014, from http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

Fance, C. (2013, August 31). 10 Google Gmail Alternatives. Retrieved Dec 23, 2014, from http://www.hongkiat.com/blog/gmail-alternatives/

Farivar, C. (2014, July 14). In the name of security, German NSA committee may turn to typewriters. Ars Technica. Retrieved Jan 22, 2015, from http://arstechnica.com/tech-policy/2014/07/in-the-name-of-security-german-nsa-committee-may-turn-to-typewriters/

FBI: North Korea responsible for Sony hack (2014, December 19). NBC2 News. Retrieved Jan 22, 2015, from http://www.nbc-2.com/story/27671344/fbi-north-korea-responsible-for-sony-hack#.VKGrZsBA

Feige, K. (Producer), & Black, S. (Director). (2013). Iron Man 3 [Motion Picture]. Burbank, CA, United States: Marvel Studios & DMG Entertainment

Fioretti, J. (2014, July 24). Google under fire from regulators on EU privacy ruling. Reuters. Retrieved Dec 10, 2014, from http://www.reuters.com/article/2014/07/24/us-google-eu-privacy-idUSKBN0FT1AZ20140724

Galileo Galilei (2007, August 9). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Galileo_Galilei

Gellman, B. & Poitra, L. (2013, June 7). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. The Washington Post. Retrieved Dec 21, 2014, from http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-Internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

Get started with Google Apps for Education (2015). Retrieved Jan 22, 2015, from https://support.google.com/a/answer/2856827

Global surveillance disclosures (2013–present) (2013, August 16). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013%E2%80%93present)

Google Apps for Work (2006, March 6). Retrieved Jan 22, 2015, from

http://en.wikipedia.org/wiki/Google_Apps_for_Work

Google for Education: Save time and stay connected (2015). Retrieved Jan 22, 2015, from https://www.google.com/edu/products/productivity-tools/

Google Launches Gmail, Free Email Service. (2004, March 30). Retrieved Jan 22, 2015, from http://searchenginewatch.com/sew/news/2065293/google-launches-gmail-free-email-service

Greenwald, G. (2013, June 6). NSA collecting phone records of millions of Verizon customers daily. The Guardian. Retrieved Dec 21, 2014, from http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Guia de boas práticas em contratação de soluções de tecnologia da informação (2012). Retrieved Jan 22, 2015, from http://portal2.tcu.gov.br/portal/pls/portal/docs/2511467.PDF

History of American False Flag Operations (2015). 9-11 Review. Retrieved Jan 22, 2015, from http://www.911review.com/articles/anon/false_flag_perations.html

History of Gmail. (2014, December 3). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/History_of_Gmail

Hoffman, C. (2012, May 9). 5 Alternative Search Engines That Respect Your Privacy. How-To Geek. Retrieved Jan 4, 2015, from http://www.howtogeek.com/113513/5-alternative-search-engines-that-respect-your-privacy/

Holodomor (2010, November 6). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Holodomor

How to be completely Anonymous online (2012, June 15). Retrieved Jan 22, 2015, from http://www.slashgeek.net/2012/06/15/how-to-be-completely-anonymous-online

I2P Anonymous Network (2003). Retrieved Jan 22, 2015, from https://geti2p.net/en/

Il sistema di autenticazione di Ateneo (2015). Retrieved Jan 22, 2015, from http://www.unive.it/nqcontent.cfm?a_id=156283

Informazioni account di posta studenti (2015). Retrieved Jan 22, 2015, from http://www.unive.it/nqcontent.cfm?a_id=55452

Iraq War (2003, March 20). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Iraq_War

Japan Questions 9/11 and the Global War on Terror (2008, February 2). The Straight Dope - Fighting Ignorance Since 1973. Retrieved Jan 22, 2015, from http://boards.straightdope.com/sdmb/showthread.php?t=490675

Katyn massacre (2004, December 16). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Katyn_massacre

Keats, S. & Koshy, E. (2008). The Web’s Most Dangerous Search Terms. McAfee, Inc. Retrieved Jan 22, 2015, from http://promos.mcafee.com/en-US/PDF/most_dangerous_searchterm_us.pdf

Kremlin security agency to buy typewriters 'to avoid leaks' (2013, July 12). BBC News. Retrieved Jan 22, 2015, from http://www.bbc.com/news/world-europe-23282308

Kreps, D. (2015, January 5). 'The Interview,' 'Sex Tape' Lead Razzies' Worst Film Shortlist. Rolling Stone. Retrieved Jan 22, 2015, from http://www.rollingstone.com/movies/news/interview-sex-tape-razzies-worst-film-shortlist-20150105

Lavrov, S. (2014, October 15). No One Has A Monopoly On Truth. Sergey Lavrov’s U.N. Address. Retrieved Jan 22, 2015, from http://www.informationclearinghouse.info/article39972.htm

Maddocks, P. (2014, December 26). Obama says 'The Interview' should be in Oscar conversation. Seacoast Online. Retrieved Jan 22, 2015, from http://www.seacoastonline.com/article/20141226/News/141229425

Mailing List CIdE (2015). Retrieved Jan 22, 2015, from http://virgo.unive.it/cide/?page_id=1728

Marshall, B. (Writer), & Gaviola, K. (Director). (2011, December 12). Within [Television series episode]. In Spielberg, S., Braga, B., & Ovitz, M. (Producers), Terra Nova. Los Angeles, CA: 20th Century Fox Television. Retrieved Oct 20, 2014, from

http://www.springfieldspringfield.co.uk/view_episode_scripts.php?tv-show=terra-nova&episode=s01e11

McCarthy, K. (2014, April 23). Brazilian president signs Internet civil rights law. The Register. Retrieved Dec 30, 2014, from http://www.theregister.co.uk/2014/04/23/new_bill_signed_in_brazil_guaranteeing_civil_rights_on_internet/

McDougall, P. (2010). Exclusive: Gmail Ditched By Major University. Dark Reading: Connecting the Information Security Community, May 5. Retrieved Oct 17, 2014, from http://www.darkreading.com/risk-management/exclusive-gmail-ditched-by-major-university/d/d-id/1088833?

Moody, G. (2011, October 4). Brazil Drafts An 'Anti-ACTA': A Civil Rights-Based Framework For The Internet. Techdirt. Retrieved Dec 30, 2014, from https://www.techdirt.com/articles/20111004/04402516196/brazil-drafts-anti-acta-civil-rights-based-framework-Internet.shtml

Neves, F. S. (2003, November 29). Propinas, ensino superior público, a razão dos estudantes e a falta dela. Retrieved Nov 30, 2011, from http://a_verdade_da_mentira.weblog.com.pt/arquivo/040197.html

Nietzsche, F. (1908). Human, all too human; a book for free spirits. Chicago: C. H. Kerr. Retrieved Dec 20, 2014, from http://hdl.handle.net/2027/mdp.39015003747733

Nineteen Eighty-Four (2010, March 25). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Nineteen_Eighty-Four

Orkut (2014, september 30). Retrieved Sep 30, 2014, from https://www.orkut.com/

Orkut Community Archive (2014, October 1). Retrieved Jan 22, 2015, from http://orkut.google.com/

Pilkington, E. (2014, December 25). PlayStation and Xbox facing issues after Christmas Day attack. The Guardian. Retrieved Jan 22, 2015, from http://www.theguardian.com/technology/2014/dec/25/playstation-xbox-down-lizard-squad-hack-christmas

Piotto, A. (2014). Internet publication [personal communication]. Message received from <piotto@unive.it> in April 23.

PRISM (2013, July 4). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/PRISM_%28surveillance_program%29

PROTECT IP Act (2011, May 12). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/PROTECT_IP_Act

Proxy server (2010, August 14). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Proxy_server

Proxy Settings Instructions (2015). Retrieved Jan 22, 2015, from http://www.unive.it/nqcontent.cfm?a_id=164714

Rajagopalan, M. & Holland, S. (2014, December 22). China condemns cyberattacks, but says no proof North Korea hacked Sony. Reuters. Retrieved Dec 30, 2014, from http://www.reuters.com/article/2014/12/22/us-sony-cybersecurity-idUSKBN0K006U20141222

Rawlinson, K. (2013, October 26). NSA surveillance: Merkel's phone may have been monitored 'for over 10 years'. The Guardian. Retrieved Jan 22, 2015, from http://www.theguardian.com/world/2013/oct/26/nsa-surveillance-brazil-germany-un-resolution

Receiving an SMS from Google (2015). Retrieved Jan 22, 2015, from https://support.google.com/accounts/answer/3367674?hl=en

Remoaldo, L. (1998). O anonimato na Internet: um direito ou uma ameaça? UP. Retrieved Dec 23, 2014, from http://paginas.fe.up.pt/~mgi97018/is/anoni.html

Ribble, J. (2014, March 31). Happy 10th Birthday, Gmail! Marketing Cloud. Retrieved Dec 20, 2014, from http://www.exacttarget.com/blog/happy-10th-birthday-gmail/

Rogen, S. (Producer), & Goldberg, E. (Director). (2014). The Interview [Motion Picture]. Culver

City, CA, United States: Columbia Pictures

Roth, R. (2014). Technology Integration at a Crossroads: Dead End Street or New Horizons? TOJDEL, 2 (4), 112-140. ISSN 2147-6454. Retrieved Oct 17, 2014, from http://www.tojdel.net/volume.php?volume=2&issue=4

Rushe, D. (2013, August 15). Google: don't expect privacy when sending to Gmail. The Guardian. Retrieved Dec 19, 2014, from http://www.theguardian.com/technology/2013/aug/14/google-gmail-users-privacy-email-lawsuit

Savov, V. (2014, December 22). The internet decides that The Interview is a perfect movie. The Verge. Retrieved Jan 22, 2015, from http://www.theverge.com/2014/12/22/7433229/the-internet-decides-that-the-interview-is-a-perfect-movie

Schofield, H. (2015, January 7). Charlie Hebdo: Gun attack on French magazine kills 12. BBC News. Retrieved Jan 22, 2015, from http://www.bbc.com/news/world-europe-30710883

Sinha-Roy, P. (2015, January 6). Sony's 'The Interview' earns $31 million online, $5 million at theaters. Reuters. Retrieved Jan 22, 2015, from http://www.reuters.com/article/2015/01/06/us-northkorea-cyberattack-sony-idUSKBN0KF23L20150106

Smith, D. (2014, December 26). Anonymous To 'Lizard Squad': Stop Attacking Tor. Business Insider. Retrieved Jan 22, 2015, from http://www.businessinsider.com/anonymous-to-lizard-squad-stop-attacking-tor-2014-12

Snowden Interview NDR English (2014, January 26). Retrieved Jan 22, 2015, from https://archive.org/details/SnowdenInterviewNDREnglish

Snowden, E. (2014, January 26). Interview by H. Seipel. Edward Snowden exklusiv – Das Interview [Television broadcast]. Moscow: Norddeutscher Rundfunk. Retrieved Dec 21, 2014, from http://www.liveleak.com/view?i=f1d_1390839693

Sony Pictures Entertainment hack (2014, November 21). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Sony_Pictures_Entertainment_hack

Spargo, C. (2014, December 25). North Korea was NOT behind the Sony hack according to multiple security experts who discredit FBI findings and reveal that a studio insider named 'Lena' may be responsible. Daily Mail. Retrieved Dec 30, 2014, from http://www.dailymail.co.uk/news/article-2887081/North-Korea-NOT-Sony-hack-according-multiple-security-experts-discredit-FBI-findings-reveal-insider-named-Lena-responsible.html

Stepan Andriyovych Bandera (2010, January 22). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Stepan_Bandera

Stop Online Piracy Act (2011, October 26). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Stop_Online_Piracy_Act

Stopfake.org (2014, March 2). Retrieved Jan 22, 2015, from http://www.stopfake.org/en/news

Streisand effect (2007, June 15). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Streisand_effect

Sutton, A. C. (2000). Wall Street and the Rise of Hitler. Studies in Reformed Theology. Retrieved Jan 22, 2015, from http://reformed-theology.org/html/books/wall_street/index.html

Sutton, A. C. (2001). Wall Street and the Bolshevik Revolution. Studies in Reformed Theology. Retrieved Jan 22, 2015, from http://reformed-theology.org/html/books/bolshevik_revolution/index.html

The Freenet Project (2000, March). Retrieved Jan 22, 2015, from https://freenetproject.org/

The Interview (2014). The Internet Movie Database (IMDb). Retrieved Jan 22, 2015, from http://www.imdb.com/title/tt2788710/

Tor Project: Anonymity Online (2002, September 20). Retrieved Jan 22, 2015, from https://www.torproject.org/

Ucrânia em África (2015). Retrieved Jan 22, 2015, from http://ucrania-mozambique.blogspot.com/

Ukrainian Insurgent Army (2007, December 18). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Ukrainian_Insurgent_Army

Virtual private network (2013, February 2). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Virtual_private_network

Warhol, A. (1967, October 13). Sculpture: Master of the Monumentalists. Time, 90, 80-86. Retrieved Dec 24, 2014, from http://content.time.com/time/magazine/article/0,9171,837402,00.html

Whittaker, Z. (2010, May 7). UC Davis scraps Gmail pilot: Privacy levels “unacceptable”. ZDNet, iGeneration. ZDNet. Retrieved Dec 23, 2014, from http://www.zdnet.com/article/uc-davis-scraps-gmail-pilot-privacy-levels-unacceptable/

WikiLeaks (2006, December). Retrieved Jan 22, 2015, from https://wikileaks.org/

WikiLeaks: Secrets and Lies. (2011, November 30). Retrieved Jan 22, 2015, from https://wikileaks.org/Guardian-s-WikiLeaks-Secrets-and.html

Wikipedia: Anonymity (2014, December 11). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Wikipedia:Anonymity

Wilde, O. (1891). The Decay of Lying: An Observation. London: Oneworld Classics. Retrieved Dec 20, 2014, from http://www.online-literature.com/wilde/1307/

Williams, P. (2014, December 18). North Korea Behind Sony Hack: U.S. Officials. NBC News. Retrieved Jan 22, 2015, from http://www.nbcnews.com/storyline/sony-hack/north-korea-behind-sony-hack-u-s-officials-n270451

Wong W. (2013). Van Gogh on Demand: China and the Readymade. Chicago: University of Chicago Press. 320 p. ISBN: 0-226-02489-X

Wroughton, L. & Rajagopalan M. (2014, December 23). Internet outage seen in N. Korea amid U.S. hacking dispute. Reuters. Retrieved Jan 22, 2015, from http://in.reuters.com/article/2014/12/22/china-usa-cybersecurity-idINKBN0K004G20141222

XKeyscore (2013, July 31). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/XKeyscore