DIREITO A PROPRIEDADE CONTRA O DIREITO A PRIVACIDADE: DESAFIOS PARA A REDE[1]

Emilio C. Viano
Mestre em Sociologia e Antropologia e Ph.D. em Sociologia do Direito na New York University. É professor e pesquisador na American University, Washington DC, tendo sido professor da Universidade de Paris, Bari, Bologna (Italia), Córdoba (Argentina), Panteion (Atenas, Grécia), Universidade China de Ciência Política e Direito (Beijing), e na Xangai Universidade de Estudos Internacionais (SISU). É Presidente da Comissão Científica e membro também do Conselho de Administração da Sociedade Internacional de Criminologia (Paris), Membro do Conselho de Administração (suplente) da Associação Internacional de Direito Penal, Membro Votante da Fundação Internacional Penal e Penitenciária, Membro do Grupo de Trabalho Anti-Corrupção da Organização para Cooperação e Desenvolvimento Econômico (OCDE).

ÁREA DE DIREITO
Penal; Internacional.

RESUMO
Este artigo analisa a Internet como instrumento, não só sob o prisma do veículo de comunicação global, mas também como um mundo novo, um mundo que existe de forma paralela e simultânea ao mundo físico e que funciona de forma independente deste. É neste mundo novo virtual que se estabelece uma nova realidade de relações jurídicas, mercantis, enfim relações sociais como um todo. Dentro desse contexto eis que surge uma nova realidade econômica. Nesse novo mundo, mais especificamente nessa nova realidade econômica onde são travadas relações interpessoais entre os usuários da internet (também consumidores dos produtos disponíveis na rede) e os criadores dos produtos, (autores das obras literárias, artísticas) surge um conflito travado na seara dos direitos reais de propriedade e direitos autorais. A sociedade, em geral, valoriza e sobreleva os direitos autorais em detrimento do direito de uso (direito real de propriedade) e dos direitos humanos. Isto tem conseqüências importantes, principalmente, quando se trata da aplicação dos direitos de propriedade no mundo eletrônico. O ponto principal desse artigo é abordar esta área de crescimento da atividade econômica global, em que bilhões de dólares estão em jogo e onde a disputa pelo poder econômico e o controle de informações disponíveis na rede têm implicações importantes não só financeiramente, mas também, na mesma proporção, em relação ao conteúdo, às notícias, ao entretenimento e à expressão artística. Assim, a liberdade de expressão, os direitos à privacidade, a expressão artística são confrontados com o direito à propriedade e os direitos econômicos, que parecem estar a ganhar quando se trata de legislação correlata e decisões judiciais, favorecendo, mais uma vez, o poderio econômico em prejuízo do cidadão.

PALAVRAS-CHAVE
Relações Jurídicas; Internet; Direitos reais; Direitos autorais; Legislação.

RESUMEN
Este artículo analiza la Internet como una herramienta, no sólo a través del prisma de vehículo de comunicación global, sino también como un mundo nuevo, un mundo que existe en forma paralela y simultáneo al mundo físico y que funciona de forma independiente de este. Es en ese mundo nuevo virtual que se establece una nueva realidad de las relaciones jurídicas, mercantis, finalmente sociales como un todo. En ese contexto, aquí viene una nueva realidad económica. En este nuevo mundo, más específicamente en esta nueva realidad económica en la que las relaciones interpersonales entre los usuarios

[1] O autor reconhece com gratidão a ajuda e colaboração de Vanessa Fiúsa Moura, que traduziu o texto original para o Português.

de Internet (también los consumidores de los productos disponibles en la red) y los creadores de los productos, (autores de obras literarias, artísticas) surge un conflicto en los gustos de los Derechos Reales de Propriedad y los Derechos de Autor. La sociedad, en general, valora y pesa más los Derechos de Autor, en detrimento del Derecho de Uso (Derecho Real de la Propiedad) y los Derechos Humanos. Esto tiene consecuencias importantes, especialmente cuando se trata de la aplicación de los Derechos de Propiedad en el mundo electrónico. El punto principal de este artículo es abordar esta área de crecimiento de la actividad económica global, en que billones de dólares están en juego y donde la lucha por el poder económico y control de las informaciones disponibles en la red tienen implicaciones importantes no sólo financieramente, sino también, pero también, en la misma proporción, en relación a los contenidos, noticias, entretenimiento y expresión artística. Luego, la Libertad de Expresión, los Derechos a la Privacidad, la expresión artística se enfrentan con el Derecho de Propiedad y los Derechos Económicos, que parecen ganar cuando se trata de la legislación relacionada con las decisiones judiciales, favoreciendo, una vez más, el poder económico en perjuicio de lo ciudadano.

PALABRAS CLAVE
Relaciones jurídicas. Internet. Derechos Reales. Derechos de Autors. Legislación.

ABSTRACT
This paper examines the Internet not only as a tool, a means for global communication, but also as a new world in parallel to the physical world, working independently. It is in that virtual new world that a new reality is established, filled with legal, commercial, social networks. In this context of a new reality for economy, interpersonal relationships are formed between Internet users (as well as consumers of the products available on the net) and creators of the products (or literary authors, artists). Along with that, conflicts arise in the field of property rights and copyright. Society, generally, outweighs royalties over the rights of use (real estate law) and human rights. It brings important consequences, mainly when it comes to the enforcement of property rights in the cybernetic world. The article focuses on addressing this increase in global economic activity, in which billions of dollars are at stake. Additionally, the battle for economic power and for control over information available on the network has important implications not only financially; the same occurs in relation to content, news, entertainment and artistic expression. Thus, freedom of expression, privacy and artistic expression rights are confronted with property and economic rights. The latter two appear to win when it comes to pertinent legislation and judicial decisions, which favors the power economic at the expense of the individual once more.

KEYWORDS
Legal Relations. Internet. Property Rights. Copyright. Legislation.

Sumário

1. Internet: a promessa e as contradições; 2. Internet: potencialidades e problemas; 3. Internet como um mundo intangível, mas real; 4. Internet como Instrumento de Vigilância; 5. Falsa impressão de privacidade; 6. A Internet como um Mundo Novo; 7. O direito à propriedade prevalece: O caso do Napster; 8. Vigilância privada e a sua execução: desafios contra o devido processo; 9. SOPA e PIPA: Supremacia dos Direitos a Propriedade?; 10. Privatização Internacional da Aplicação da Lei; 11. O ACTA: Protecção da Propriedade e do Monopólio; 12. Os Frutos da Árvore Envenenada; 13. Pesquisa Eletrônica: Parceria entre a Polícia e as Entidades Privadas; 14. O Vazio Legal e a Necessidade de um Remédio; 15. Preocupações Constitucionais e Liberdades Civis; 16. Conclusão.

.

1. A internet: a promessa e as contradições

Um tema e um desafio fundamental para a criminologia é o quê é definido como crime e como se chegou à definição dele, e a consequente formulação de leis relacionadas a cada definição de tipo penal. Este artigo tratará do crime no meio virtual. Por isso, o artigo aborda a Internet como a melhor ferramenta, dentro da nova realidade da globalização nas comunicações, de compartilhamento de informações, mídia e entretenimento.

Enquanto a maioria das pessoas limitam a sua conta de internet a uma tecnologia que lhes dá acesso aos meios de comunicação social, o artigo sublinha que a internet é uma verdadeira realidade nova e coexistente, onde impérios: políticos, financeiros, militares e de comunicação estão sendo construídos para um enorme ganho através de: uma concorrência feroz, espionagem, sabotagem e até mesmo a ciberguerra.

Dentro deste contexto, o artigo analisa como os poderosos e influentes estão moldando a lei para afirmar seu controle e exploração completa da internet para os seus próprios ganhos maciços, e para o controle do conteúdo veiculado (censura) e até mesmo o controle da mente.

Desse modo, o modelo da internet como o prenúncio de comunicação livre e liberdade de expressão é contrastado com o de internet como ferramenta de monitorização, vigilância e controle de conteúdo, uso e, em última análise, do usuário.

Além disso, a tensão entre os direitos de privacidade e direitos de propriedade é analisada. A este respeito, o artigo analisa o apoio que a lei e os tribunais muitas vezes dão a mega-empresas com a intenção de monopolizar a internet através de várias práticas e leis. Então de forma explícita, mais uma vez, a definição do que é legal ou ilegal, crime ou não, está nas mãos dos poderosos e das classes superiores, o "1% versus os 99%".

O artigo também discute questões processuais, especialmente aquelas relacionadas à busca e apreensão que podem ser realizadas ilegalmente por particulares (por exemplo, por hacking) e, e de outro lado, legalmente quando os mesmos instrumentos forem utilizados pelo ordenamento jurídico dentro do contexto processual em qualquer esfera, seja cível penal, administrativa, tributária etc.

As violações dos direitos humanos por intrusões, vigilância e buscas privadas e por leis para proteger os direitos de propriedade intelectual da grandes mídia, notícias e empresas de entretenimento em detrimento da liberdade de expressão, como o SOPA / PIPA propostas nos EUA, a Directiva da União Europeia e leis relacionadas pelos Estados-Membros, a ACTA e outras convenções, são destaques neste artigo.

Assim, o mundo cibernético é analisado como o novo teatro onde a luta pela definição do que é ou não é crime e para a proteção dos direitos humanos, civis e constitucionais está sendo jogado de forma invisível, silenciosamente, imperceptivelmente, mas mesmo assim realmente.

2. Internet: potencialidades e problemas

A Internet tem sido considerada até a presente data, na maior parte do mundo, uma inovação maravilhosa que permite uma possibilidade ilimitada de larga interação humana: sem fronteiras e barreiras e em qualquer momento, a

qualquer hora do dia. Um verdadeiro e genuíno mercado aberto virtual de ideias e informações que podem ser compartilhadas instantaneamente em todo o globo.

Diante do atual cenário da política mundial, com a chamada "Primavera Árabe", a internet tem se mostrado um instrumento de alta capacidade e confiabilidade para fornecer e formar uma plataforma mundial de redes, compartilhar informações sobre acontecimentos históricos e políticos de várias áreas do planeta em velocidade quase que simultânea com a realidade e por meio desse poderoso canal de comunicação se opera: a organização, a cooperação, o compartilhamento de informações e planos para criar de forma bem coordenada eventos de massa capazes de desafiar e, até mesmo, de derrotar o regime posto.

Durante esses tempos agitados, a internet é vista como um mecanismo quase irrefreável para a mudança radical. Esse mecanismo é uma força poderosa para forjar o propósito, idéias e ações, um meio confiável para comunicações instantâneas, organização e mobilização social nunca antes vista ou testada.

Ressalta-se, especialmente, a importância da ligação entre a internet (como veículo transportador) e as notícias, muitas vezes ao vivo, que estão sendo compartilhadas em todo o mundo, trouxe à tona a visualização de situações de: abuso, exploração, tirania e escravidão. Graças à velocidade e ao alcance da internet, foi proporcionado à comunidade mundial o impulso para a mudança e a reforma política e social ou, pelo menos, condenação e repulsa a nível mundial, e, às vezes, intervenção de organizações transnacionais, a exemplo da ONU, da OTAN, e da OEA.

Os meios de comunicação social, já perceberam o potencial e a realidade que é a internet como o grande instrumento conector de todo o mundo para atingir as massas sociais em todos os lugares onde há acesso.

Milhões de pessoas são membros de Facebook ou outras redes sociais similares, se envolver em bate-papo instantâneo com pessoas que podem estar a metade do mundo de distância, compartilhar instantaneamente fotos e comentários ou vídeos retratando uma situação específica, e disseminar pelo mundo seus: pensamentos, desejos, felicidade, conquistas e derrotas.

O próprio modo com que as pessoas: se comunicam, aprendem, recebem as notícias, vêem a realidade, se relacionam entre si; encontram: amizade, amor, companhia, obtém conselhos e informações mudou drasticamente desde a geração anterior e até agora e continua em constante mutação, com inovações tecnológicas que introduzem incessantemente modelos novos e melhorados de produtos eletrônicos, como iPhones (palms), iPads (tablets) e outros dispositivos intrigantes.

A influência da Internet está se tornando mais e mais profunda e ela está intimamente entrelaçada com nossa vida diária.

A interface dinâmica, em constante avanço, entre os dispositivos eletrônicos necessários para acessar a rede mundial e a versatilidade dessa rede em nos ajudar a enfrentar e resolver desafios diários e mais ainda a viabilização da administração de tudo o quanto se engloba na nossa vida diária, está a crescer exponencialmente e vem desmistificando a lei da física clássica de que um corpo não pode estar em mais de um lugar ao mesmo tempo, haja vista que, mesmo que virtualmente, é possível se fazer presente quase que fisicamente em vários lugares ao mesmo tempo e praticamente: ser, ver, agir e exercer o controle além de desenvolver atividades em várias zonas espaciais e temporais, ao mesmo tempo.

Na Exposição Eletrônica para o Consumidor de Las Vegas em 2012 uma miríade de deslumbrantes novos produtos foi introduzida desde maiores, mais

brilhantes televisores mais finos a Ultra Violet, o novo formato "Play Anywhere" na frente de entretenimento doméstico, a Ultrabook, um tipo especial, muito fino de laptop, a muitos produtos de computação móvel, como telefones inteligentes e computadores tablet.

Estes não são apenas dispositivos para jogar e divertir-se. Esses dispositivos impactam cada vez mais profundamente e intimamente nossas vidas como: seres humanos, pais, filhos, professores, viajantes e pessoas do mundo dos negócios.

A conexão direta entre todos os aspectos da vida, como por exemplo: afazeres, lugares, atividades (lúdicas ou relacionadas ao labor) e comunicações é surpreendente. Inclusive quando observamos muitas máquinas, robôs e ferramentas computadorizadas que já estão encaixadas em cada espectro de nossas vidas diárias, vejamos como exemplo as lavadoras e secadoras inteligentes que se ajustam ao tipo e carga de roupas e até mesmo enviam uma mensagem para o dispositivo móvel do proprietário, quando as roupas estão prontas, ou seja, lavadas e secas, as geladeiras inteligentes, que conseguem mensurar o tempo de consumo, a quantidade e a qualidade do que é consumido pelo proprietário e tão logo seja percebida uma redução ou ausência de algum produto a máquina elabora uma lista de compras e envia para o proprietário da geladeira ou pessoa responsável pelas compras da casa ou a loja em que as compras costumam ser feitas.

A tecnologia eletrônica, robôtica e ótica está começando a realmente revolucionar a forma de conduzir veículos, para constatar isso basta notar que cada vez mais carros são e serão capazes de se comunicar uns com os outros e tomar decisões em relação: a velocidade, direção e distância em relação a outros carros e há sistemas de segurança e controle computadorizados que são capazes de substituir os comandos do motorista pelos comandos do computador.

3. A Internet como um mundo intangível, mas real

O que muitos de nós não vemos ou pensamos é no mundo cibernético como um: vasto; etéreo; invisível, mas real, espaço de propriedade intelectual expressa e que desempenha sua função através da criatividade, da inovação e dos avanços da tecnologia, a exemplo do software e dos componentes eletrônicos que usamos todos os dia. Num mundo dominado por itens tangíveis que podemos ver, tocar, cheirar, ouvir e usar, há um outro mundo, invisível, mas impactante, onde bilhões de dólares estão em jogo para o ganho econômico, o predomínio político, o poder militar, a definição de valores e dominação cultural.

Assim como titãs da indústria, do transporte, da agricultura, da pecuária ou da moda que se chocam e se degladiam no mundo "real", assim fazem os magnatas da música, mídia, notícias e entretenimento no "ciber" mundo. Países participam, assim, controlando o acesso, a filtragem de material, publicando materiais de propaganda, praticando espionagem industrial, e até mesmo fazendo a guerra cibernética.

A intensidade da batalha é sentida por suas manifestações mais óbvias como os altos e baixos das fortunas de diversas empresas relacionadas à Internet, pelo sigilo com que operam, mesmo internamente, como, por exemplo: a Apple é conhecida por ingressar com ações judiciais objetivando a reivindicação de patentes e direitos autorais ou práticas monopolistas; a Microsoft é muitas vezes acusada de fazer as mesmas coisas e muito mais. Alguns vêem as grandes empresas como a tentativa de se apossar do mundo virtual e cada aspecto lucrativo

ou estrategicamente importante dele, monopolizá-lo e usá-lo para enormes ganhos financeiros e sistematicamente eliminar a concorrência e qualquer "startup" inovador que seja um desafio à sua posição dominante.

Da mesma forma, alguns países, especialmente os EUA e a China, estão investindo pesadamente para usar a internet para afirmar seu domínio, sua capacidade de monitorar e influenciar os acontecimentos e fatos mundiais e a interpretação deles, realizando, para atingir esse objetivo, operações de monitoramento e espionagem, e travando guerra cibernética contra seus inimigos.

4. A Internet como Instrumento de Vigilância

Não há dúvida de que a internet pode ser usada como uma ferramenta muito eficiente dando às mais variadas entidades, instituições, governos e pessoas a capacidade de realizar 24 horas por dia, sete dias por semana a vigilância de: pessoas, lugares, movimentos, comunicações e trocas (Assange, 2011; Sonne, 2011; York, 2011; Eaves, 2012).

Ela pode ajudar um regime autoritário a vigiar continuamente para identificar e neutralizar os dissidentes e reformadores; que pode identificar e levar as forças de repressão ao local onde as vozes da mudança estão, para que aquelas pessoas, que representam uma ameaça ao regime totalitarista, sejam: presas, torturadas, silenciadas ou mesmo mortas.

A ferramenta do onisciente, onipresente, "omni-visualizante" "Big Brother"[2] pode se transformar num instrumento de terror. A internet pode rastrear as compras de milhões de consumidores em todo o mundo, produzindo vasta informação sobre estilos de vida, hábitos alimentares, higiene pessoal e comportamentos sexuais. Essas informações obtidas pelo rastreamento de dados pessoais podem, então, ser usadas contra o cidadão quando se tratar de: contratação para uma vaga de emprego, promoção, seguros, investigações de acidentes, processos criminais e, às vezes, extorsão e sequestros.

O banco de dados que é criado com essas informações rastreadas é usado como um marketing, publicidade, filtragem de notícias e máquina de propaganda para difundir certas mensagens aprovadas, doutrinar e controlar a mente de um povo e muito mais.

O Panóptico, idealizado e concebido pelo filósofo do século XVIII, Jeremy Bentham, deveria permitir a um funcionário do governo, um guarda da prisão, observar (-Opticon) a todos (Pan-) os reclusos numa instituição sem que eles sejam capazes de dizer se estavam ou não sendo observados.

Este sistema foi concebido para criar o medo, a insegurança, a dúvida, mal-estar, e para controlar as massas simplesmente com a ideia de ter potencialmente um tirano espionando-os a tempo integral, enquanto vivem suas vidas diárias. Assim como o sistema serve para criar a ideia no subconsciente da população da intervenção punitiva para acabar com qualquer desvio de conduta percebido pelo monitoramento constante.

[2] Julian Assange, Internet has Become a Surveillance Machine, Agence France Presse, November 28, 2011; Paul Sonne, (U.S. Secretary of State Hillary) Clinton Criticizes Sale of Surveillance Tools to Some Countries, Wall Street Journal, December 8, 2011, ; Jillian York, Government Internet Surveillance Starts with Eyes Built in the West, Electronic Frontier Foundation, September 2. 2011, https://www.eff.org/deeplinks/2011/09/government-internet-surveillance-starts-eyes-built ; David Eaves, The Internet as Surveillance Tool, http://eaves.ca/2010/01/20/the-internet-as-surveillance-tool/, 20 January 2010.

A internet pode ser descrita como um Panóptico crescente de hoje, especialmente, quando combinado com outras tecnologias eletrônicas que podem capturar nosso paradeiro, atividades e localização ao redor do relógio, se necessário ou desejado, e gravar e armazenar permanentemente a sequência de nossas atividades quotidianas (Katyal, 2004) .
Este contraste entre a natureza e funcionamento da internet, muitas vezes passa despercebido ou desconhecido (Crook, 2008).

5. Falsa impressão de privacidade

A maioria das pessoas agem e se comunicam através de dispositivos eletrônicos como se estivessem em seu próprio mundo privado, um mundo totalmente isolado do mundo real circundante cheio de: vigilância, marketing, monitoramento por meio de cookies, polícia fazendo escutas telefônicas por agências e/ou setores de inteligência e monitoramento e por parte dos seus empregadores (os governos e instituições privadas).

Especialmente, em se tratando do uso de meios de comunicação social, as pessoas agem como se tivessem total anonimato, como se pudessem viver, interagir e se comunicar em sua própria bolha hermética do seu mundo particular, isolado e diminuto. Contudo, essas pessoas esquecem ou não percebem que na realidade existe um constante, persistente e agressivo monitoramento 24h por dia, 7 dias por semana (Lessig, 1999).

6. A Internet como um Mundo Novo

Assim, enquanto a maioria das pessoas pensa na Internet e nos dispositivos eletrônicos conectados a seu uso, sobretudo, como um meio para melhorar a comunicação social, obter informações para ajudar a rotina diária, encontrar um caminho para um destino, receber atualizações sobre a família e o paradeiro dos amigos, e comprar vários bens sem sair de casa ou do escritório, a rede mundial é e representa realmente muito mais que isso.

É uma nova realidade, um mundo novo onde existem batalhas que alcançam bilhões de dólares pelo domínio eletrônico e os lucros de empresas virtuais, sites, blogs, navegadores, portais eletrônicos, redes sociais, dentre outros, onde o poder dos governos e corporações para: assistir, espionar, coletar informações, montar arquivos sobre milhões de pessoas, investigar e julgar as infrações, e saber, se desejado, o paradeiro de todos, cresce exponencialmente com o crescente: uso, poder e sofisticação da tecnologia.

Esta é uma área com forte potencial para a violação dos direitos humanos e também para um grande conflito pelo controle do ciberespaço e seu conteúdo. Isso pode levar a uma redefinição do que é ou não criminoso, do conceito de crime e daquilo que é digno de punição visivelmente facilitará a ação do governo e das empresas privadas a criar e afirmar mais intensamente as políticas de controle, o conteúdo do que é acessível ou não na internet e para instituir um regime de monitoramento e espionagem no uso da rede por parte dos cidadãos comuns, transformando-o em sua cabeça quando se trata de liberdade de expressão, comunicação e partilha.

Além disso, há também a questão de "censura prévia", ou a censura antes da publicação do material ou de uma mensagem. Por exemplo, o Twitter anunciou no final de janeiro de 2012, que estaria pronto a interceptar e interromper a

transmissão ou excluir mensagens consideradas impróprias, insultantes ou politicamente incorretas em certos países. Recentemente, certos países, como Arabia Saudita, ameaçaram eliminar o acesso ao Twitter em seu território nacional. Entre os vários exemplos são mensagens que são ou pró-nazismo ou simpáticos ao nazismo na Alemanha, contêm críticas ou questionamentos sobre a monarquia na Tailândia, ou citam material de "Versos Satânicos" de Salman Rushdie em muitos países muçulmanos.

O Brasil está processando o Twitter por divulgar os pontos nas estradas onde há um posto da policial rodoviária, que é responsável pelas blitz de veículos em trânsito e que dentre entras coisas deve garantir que motoristas alcoolizados não conduzam veículos automotores.

Por causa disso, às vezes, o Twitter impõe censura, eliminando material ofensivo em um determinado país ou grupo de países ao mesmo tempo permitindo a sua difusão em outras partes do mundo. A pessoa que envia o "tweet" eliminado será informada da ação, se possível.

Como conseqüência, no final de Janeiro de 2012, a hashtag "Twitter Censored" saltou para primeiro lugar na lista dos tópicos da moda. Muitos usuários do Twitter na Europa estão ameaçando passar para o site gêmeo idêntico e/ou organizar greves cibernéticas. Suspeita-se que está ação do Twitter é calculada para tranquilizar os governos de alguns países com censura, de forma que o Twitter se compromete a cooperar com eles para impedir a entrada de material considerado censurável nesses países.

Em troca, o Twitter poderá ser autorizado a entrar nesses mercados muito lucrativos. A China é o principal exemplo desses países. Não há dúvida de que a decisão do Twitter de respeitar o direito nacional local, mesmo quando este viola direitos humanos, limita a liberdade de expressão, especialmente, quando se trata de criticar o governo ou expor a corrupção.

7. O direito à propriedade prevalece: O caso do Napster

Uma das lutas mais importantes no mundo cibernético é entre o direito à propriedade e o direito à privacidade. Um bom exemplo desta disputa entre o direito à propriedade e o direito à privacidade foi o caso do Napster, originalmente criado em 1999 como uma rede pioneira peer-to-peer de serviço de compartilhamento de arquivos pela Internet.

Este serviço é especializado em compartilhamento de arquivos de audio, geralmente de música, codificados no formato MP3, através de uma interface amigável (Wikipedia, 2012). Napster tornou bastante simples o acesso a arquivos, no formato MP3, para os entusiastas da música por conta do "download" de arquivos ou descarregamento de cópias de músicas que, não fosse esse sistema, seria muito difícil encontrar como, por exemplo, músicas mais antigas, cujas gravações ainda não foram liberadas para entrar no domínio público, e músicas de gravações realizadas em concertos de forma amadora e não autorizada (Warren, 2000).

Esse hábito tornou-se extremamente popular entre os jovens, especialmente entre os estudantes universitários, a tal ponto que muitas universidades tiveram que bloquear o seu uso em redes intranet nos seus campus, inicialmente por causa da sobrecarga dos seus sistemas operacionais e, em seguida, também por causa de violação de direitos autorais. A empresa enfrentou

em dificuldades e obstáculos legais, no que diz respeito à violação de direitos autorais, e teve de cessar as operações por ordem judicial em 2001[3].

Tudo isto foi acompanhado por um intenso debate sobre as questões: por um lado, a Recording Industry Association of America afirmou que o Napster estava prejudicando as vendas das gravações (Gillen, 2007) e privando artistas e outras pessoas envolvidas no processo criativo e técnico/industrial, de seus ganhos legítimos (Macavinta, 1999); de outro lado ao invés disso, há uma corrente que afirma, comprovadamente, que o contrário é verdade, mostrando que o comércio de arquivos, na internet, estimulava as vendas, especialmente em relação a músicas de artistas e bandas menos conhecidas e que o Napster realmente enriqueceu a música e entretenimento do mundo, dando uma chance e proporcionando uma notoriedade a grupos que não faziam parte do cenário mundial de famosos.

Em certo sentido, Napster representou o que se tornou cada vez mais uma das conseqüências mais poderosas do desenvolvimento universal e uso da internet: a mudança revolucionária e a abertura da estrutura de poder e financeira de: notícias, música, entretenimento e cultura, até recentemente rigidamente controlada por costumes estabelecidos e arranjos, muitas vezes apoiados por leis promulgadas, não surpreendentemente, a pedido daqueles beneficiando mais de monopólios.

A transição tecnológica da cultura musical é incrível. Música como ouvíamos desapareceu. Agora, nós a ouvimos em nosso desktop, laptop, iPod, etc. As vendas de CDs despencaram, desde que a música se tornou disponível para os ouvintes no formato digital seja em sites que disponibilizam downloads, iTunes ou a tecnologia ora já defasada do MP3. Ninguém viu a revolução que viria quando os arquivos MP3 surgiram em meados dos anos noventa.

A indústria fonográfica, especialmente, não tinha antecipado ou não estava tão bem preparada para o que estava a bater-lhes à porta, especialmente a natureza peer-to-peer de troca, ignorando a arquitetura cliente-servidor do Web, servido e controlado por Provedores do Serviço de Internet (ISPs) (Nair, 2009; Katyal, 2004).

Hoje, rígidas linhas profissionais e papéis foram bastante suavizados e, em muitos casos, podendo até mesmo desaparecer. Desse modo, nos dias atuais, com a tecnologia disponível, qualquer um pode ser um repórter, um jornalista, um músico, um artista, um especialista etc. diretamente: publicando, executando e buscando seguidores na internet, sem necessariamente ter que passar e ser ungido por um poder e uma estrutura financeira que se engaja em práticas monopolistas de um "clube fechado" ou ter que pagar caro para obter um diploma universitário para apenas pegar um emprego de entrada no mercado de trabalho do jornalismo.

O Napster, por exemplo, foi fundamental no lançamento da, então totalmente desconhecida, banda inglesa de rock-Radiohead e apresentou uma de suas músicas no número da Billboard 2000, algo inédito na época. Foi um passo revolucionário desafiar a hierarquia dos mundos da mídia e do entretenimento e os seus arranjos (Woefel, 2001). Os tribunais dos EUA, no entanto, apoiaram os direitos de propriedade.

Não há dúvida de que a decisão Napster pelo Tribunal de Apelações para o Nono Circuito [A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9 Cir. 2001)] foi

[3] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (2001)

um grande golpe para o compartilhamento de arquivos e à liberdade de expressão e inovação no mundo do entretenimento (Brenner, 2001; Katyal, 2004).

8. Vigilância privada e a sua execução: desafios contra o devido processo

Napster foi o início de uma tendência que tem profundas implicações para o devido processo legal e a repartição na sociedade de quem tem o direito de investigar, processar e punir, e até mesmo de quem tem o poder de definir o que é crime, dependendo de quais interesses prevalecem. A decisão do tribunal dos EUA no caso Napster deu, ao detentor dos direitos autorais, o direito de exercer a vigilância vigorosa e monitoramento de comunicações eletrônicas, independentemente, dos direitos de privacidade de outras pessoas.

A vigilância é extra-legal, como a que é realizada por uma empresa privada ou por qualquer órgão não governamental e, muitas vezes, leva a uma conclusão extrajudicial de violação de direitos autorais, criando assim um sistema paralelo de aplicação da justiça e do Direito.

O monitoramento é feito normalmente com os chamados "agentes inteligentes" automáticos (Chopra, 2008) que detectam violações de direitos autorais e permitem que os detentores de direitos autorais rapidamente identifiquem e entrem em contato com o infrator (Wikipedia, 2011b; Katyal, 2004). É essencial lembrar que, neste momento no sistema jurídico dos EUA, não há proteção constitucional se ambas as partes são privadas, entidades não estatais (Navetta, 2010).

Conseqüentemente, diferentes conceitos fundamentais como a propriedade, privacidade, personalidade e autonomia [sob o Digital Millennium Copyright Act de 1998 (DMCA)] estão claramente em conflito.

Vigilância pirata como é praticada hoje levanta desafios consideráveis para o devido processo legal: não há fiscalização, tem vigilância privada, indesejada e não autorizada, e uma determinação extra-judicial do conceito da infração e da tipificação penal.

Como Sônia Katyal (2004) escreveu com habilidade, estamos agora publicando em um sistema de "publicação panóptica", isto é, para todos verem imediatamente, sem estarmos conscientes disso, e somos, portanto, passíveis de sermos encontrados extrajudicialmente em violação de direitos autorais.

O proprietário dos direitos autorais tem capacidade, quase que completa, de monitorar o uso do seu trabalho por outros, fugindo considerações de uso justo e livre expressão (primeira emenda) e, além disso, sob o Digital Millennium Copyright Act (DMCA)[4], de atuar contra qualquer autor na internet mesmo com apenas um mínimo de acusação de violação (Katyal, 2004).

Ainda mais complicados e ameaçadores são leis e tratados internacionais que estão sendo propostos ou decretados para expandir o poder de desligar provedores de serviços de internet (ISPs), sites e mídias sociais tomando como base uma acusação.

Não há dúvida de que existe uma necessidade de mais veículos de proteção legal aqui. Uma das conseqüências do clima legal pós-Napster é que há menos criatividade e expressão legítimas que são inovadoras. Prevalecem, ao contrário, as que são analisadas e canalizadas através dos corredores usados pelo poder, controle e, às vezes, a corrupção, estabelecidos mais para proteger os interesses

[4] Pub.L. 105-304, 112 Stat. 2860 (1998)

financeiros de magnatas da mídia e dos grandes estúdios, que para promover a expressão literária, artística e criativa.

Assim, há um impacto significativo sobre a privacidade, liberdade de expressão e os direitos do autor em si. Uma relação com razão inversa está operando aqui e está continuamente se expandindo: quanto mais poder os titulares dos direitos autorais têm para proteger a sua propriedade, tanto menos haverá liberdade de informação e privacidade (Katyal, 2004).

Basicamente, o que está ocorrendo com o apoio de leis favoráveis intermediadas pelos maiores interesses das empresas do entretenimento e da mídia é um acordo entre os tribunais com o objetivo de instituir um regime "stand-alone", auto-contido, onde as questões de direitos autorais são resolvidas sem serem confrontadas ou analisadas sobre o prisma de outras leis ou valores constitucionais como: o devido processo legal, a liberdade de expressão, ou privacidade (Katyal, 2004).

Não há dúvida de que essas abordagens e decisões jurídicas representam um reordenamento do poder, controle e ganhos financeiros sobre os mundos da mídia, notícias, entretenimento, simultaneamente dando a gente particular capacidade de monitorar, controlar e acusar outros, especialmente os concorrentes, com conseqüências devastadoras. Mais uma vez, quem tem poder e dinheiro, e está aliado a outros em situação semelhante, pode definir o que é crime e o qual é a penalidade imputada a ele.

9. SOPA e PIPA: Supremacia dos Direitos a Propriedade?

Esta abordagem que dá supremacia aos direitos de propriedade em detrimento da privacidade e da liberdade de expressão, continua a gerar controvérsia considerável, especialmente, nos Estados Unidos com a proposta de leis "SOPA" e "PIPA".

A Lei para Parar Pirataria Online (SOPA)[5] é um projeto de lei que foi introduzido na Câmara dos Deputados dos Estados Unidos em 26 de outubro de 2011.

A lei pela Prevenção de Ameaças Reais a la Actividad Economica e Roubo de Propriedade Intelectual ou Protect Intellectual Property Act (PIPA)[6] é o projeto de lei companheiro de SOPA no Senado dos EUA. A Lei PIPA é um aproveitamento do projeto de lei anterior com algumas modificações, de modo a ser um re-escrever dela lei Combate à Violação Online e Falsificação (COICA), que não foi aprovado em 2010.

A SOPA propõe capacitar o Departamento de Justiça dos EUA e os detentores privados de direitos autorais para buscar ordens judiciais contra sites suspeitos ou acusados de permitir, facilitar ou apoiar a violação de direitos autorais. As ordens judiciais podem incluir proibir redes de publicidade online e serviços de pagamento, como PayPal, de fazer negócios com o site que supostamente infringir, impedindo os motores de busca de fornecer links para tais sites, e ordenando que provedores do serviço internet bloqueiem o acesso a tais sites.

O resultado mais imediato seria que uma simples acusação, ainda a ser provada, sem sentença transitada em julgado, colocaria um site fora do negócio. O

[5] HR 3261
[6] S 968

projeto de lei exigiria de fornecedores de serviços na Internet que bloqueassem o acesso a certos sites estrangeiros considerados "sites desonestos" (Tribe, 2011).

SOPA criminaliza a transmissão não autorizada de conteúdo que seja protegido pelos direitos autorais. Mais importante, o projeto também prevê a imunidade para os serviços de Internet que, por conta própria, tomam iniciativas privadas não judicialmente sancionadas, contra sites acusados de infração. O potencial para agir mal contra um concorrente real ou percebido aqui é claro, para ver.

Aqueles que apóiam e defendem a lei dizem que ela protege o mercado da propriedade intelectual e das indústrias correlatas, numerosos postos de trabalho e ganhos consideráveis. Eles também alegam que a lei é necessária para reforçar a aplicação das leis de direitos autorais, especialmente contra sites estrangeiros fora do alcance das leis dos EUA.

O cartão emocional de sites estrangeiros roubando com impunidade ideias americanas e, portanto, emprego e renda também é utilizado visivelmente (Marlowe, 2011). Os adversários da lei, ao revés, afirmam que a proposta de lei viola a Primeira Emenda (Tribe, 2011), e significa basicamente a censura na internet (Albanesius, 2011), vai trazer uma série de prejuízos e engendrar paralisia na internet, e irá desencorajar, e até mesmo punir, a inovação por parte das empresas (grandes e pequenas), a delação da corrupção e outras formas de liberdade de expressão, ao mesmo tempo protegendo o "status quo" e os monopólios de fato existentes (Timm, 2011).

O encerramento de uma conta é um grande evento, potencialmente embaraçoso, danoso e dramático, o equivalente moderno a ser socialmente excluído, excomungado, que significa ser ejetado, sem proteção, ainda mais do grupo social, tendo bens confiscados.

Ela pode realmente significar, às vezes sem aviso, a perda de todos os ativos virtuais que uma pessoa tem armazenados na conta. Isto é realmente prejudicial, quando no mundo virtual de hoje pode ter obtido ativos substanciais. Além disso, há sempre a perda de tempo, dinheiro investido, e reputação. Exemplos disso são os cancelamentos de contas de e-mail de rede social e de hospedagem na web (Goldman, 2011).

10. Privatização Internacional da Aplicação da Lei

Deve ser notado que este tipo de legislação, SOPA e PIPA, não é exclusiva para os Estados Unidos.

Na França, por exemplo, legislação semelhante dirigida ao usuário pirata entrou em vigor em 01 de janeiro de 2010. A lei estabeleceu a Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet (Alta Autoridade para a Difusão de Obras e a Protecção dos Direitos na Internet), geralmente conhecido por sua abreviação, "Hadopi" (Krug, 2011).

Esse termo francês significa fazer cumprir a lei anti-pirataria, que foi concebida como um tipo de lei: "Terceiro erro consecutivo e você está fora". Os detentores de direitos autorais dependem de uma empresa privada, Trident Media Guard localizada em Nantes, para monitorar a internet e identificar o endereço IP (Intellectual Property) dos violadores.

Para pegar os infratores, a indústria da música tem preparado um banco de dados de 10.000 trechos das músicas mais populares que muitas vezes são baixadas ilegalmente. Os endereços IP dos violadores são então enviados para

Hadopi, que por sua vez, exige nomes e endereços dos provedores. Sobre a violação detectada pela primeira vez, Hadopi envia um email exigindo o cumprimento da lei pelo infrator.

Na segunda, uma carta registrada também é enviada. Quando do registro da terceira violação, Hadopi pode iniciar um processo criminal que implica uma multa de 1.500 euros. No caso de uma aparição na frente de um juiz, uma audiência, o direito de contestação do réu foi abolido por essa lei e o réu fica absolutamente impedido de fazer sua defesa.

Dependendo das circunstâncias e da gravidade da infração, um violador, que está incorrendo no erro pela terceira vez, também pode ser privado de estabelecer conexão com a Internet e ser proibido de adquirir uma outra conexão com um servidor diferente ou de um provedor diferente, ao mesmo tempo que é obrigado a continuar a pagando as taxas do serviço da internet bloqueada.

Um toque legal sutil de Hadopi é que o infrator não é acusado de ser um pirata, mas de não ter impedido a pirataria de acontecer. A infração é tratada como uma omissão, como negligência, como um crime de responsabilidade estrita, vale a dizer que o ato criminoso em si mesmo é suficiente, não há necessidade de ter uma intenção criminosa.

Conseqüentemente, o dispositivo eletrônico do ofensor será equipado com um monitor para impedir futuras transgressões. Empresas de software estão ocupadas na incumbência de criar programas que realizem esta missão.

Por outro lado, Hadopi tem a responsabilidade de identificar os "downloads" realizados nos padrões legais e determiná-los como tais, para que as pessoas possam ser orientadas a respeitar os direitos de propriedade e baixar músicas e outros materiais legalmente.

O potencial da Hadopi é que muitos, se não a maioria, dos "laptops" e outros dispositivos eletrônicos, na França, podem ser monitorados num futuro próximo. Essa situação nos remete a pensar instintivamente no "Big Brother", constantemente observando o que os internautas franceses estão fazendo eletronicamente.

É realmente irônico que a internet, saudada como o veículo mundial da liberdade de expressão pode, em sentido antagônico e verticalmente oposto, venha se tornar um projeto de âmbito nacional de "escuta" por parte do governo da França e em outros países (Eaves, 2010). Grã-Bretanha tem uma lei similar à Hadopi, a Lei de Economia Digital 2010 (c 24).

11. O ACTA: Protecção da Propriedade e do Monopólio

Alega-se que uma provisão similar, "Terceiro erro consecutivo e você está fora da jogada", estava sendo considerada para inclusão no Acordo de Comércio Anti-Contrafacção (ACTA) (Wikipedia, 2012, a).

O objetivo do Acordo é estabelecer padrões internacionais para a aplicação dos direitos de propriedade intelectual e, assim, confirmar a atual ordem existente, que protege o direito de propriedade e mantém o monopólio, em detrimento da liberdade de expressão e da livre circulação de informações. Este acordo foi proposto pela primeira vez pelos Estados Unidos e Japão, e negociado em segredo entre os vários países: os Estados Unidos, a União Européia, Suíça, Japão, Austrália, República da Coréia, Nova Zelândia, México, Jordânia, Marrocos, Singapura, os Emirados Árabes Unidos e Canadá.

A sociedade civil e os países em desenvolvimento foram excluídos das negociações. Vale ressaltar que em matéria de contrafacção ACTA inclui a "distribuição de internet e tecnologia da informação". O texto final foi lançado, ainda em condições de sigilo, em 15 de novembro de 2010. A cerimônia de assinatura foi realizada em 10. de outubro de 2011 em Tóquio, com os Estados Unidos, Austrália, Canadá, Japão, Marrocos, Nova Zelândia, Singapura e Coréia do Sul assinando o tratado.

O acordo tem sido amplamente contestado e criticado por conta do sigilo das negociações, para a imposição de políticas públicas, sem uma discussão aberta e supervisão judicial, e pela ameaça que representa aos direitos humanos e à liberdade de expresso (EFF, 2008).

O potencial do acordo se transformar numa censura promovida pelos governos internacionais e signatários desse tratado é muito forte. Uma conferência sobre o ACTA foi realizada no Washington College of Law, em Washington DC, entre os dias 16 e 18 de junho de 2010.

A conferência foi assistida por mais de 90 pessoas entre: acadêmicos, profissionais e ONGs de interesse público que expressaram profunda preocupação em muitos aspectos da ACTA como uma ameaça para muitos interesses públicos. Concluiu que, "ACTA é hostil ao interesse público em pelo menos sete áreas críticas da política pública global: direitos e liberdades fundamentais; controle da Internet, acesso aos medicamentos; âmbito e natureza do direito de propriedade intelectual; comércio internacional, direito e instituições internacionais; e o processo democrático."

Outras leis semelhantes à SOPA e à ACTA têm sido propostas e/ou introduzidas em outros lugares. A União Européia (UE) adotou uma linha de ação que permite cortar o acesso, à internet, sem uma ordem judicial, dos violadores de direitos autorais.

Essas leis ainda prevêem que os detentores de direitos autorais podem obter uma ordem judicial obrigando os provedores de serviços de internet (ISPs) a fornecer os endereços IP para identificar os computadores que estão compartilhando, fora dos padrões da lei, material que estão sob a tutela dos direitos autorais. Cada membro da UE deverá adotar a sua própria legislação de execução, quer dizer que o processo que irá instrumentalizar essa lei pode ser diferente em cada um dos países signatários da lei.

O acusado, cujo serviço foi suspenso, tem o direito de solicitar uma revisão judicial. A Espanha tem a lei para uma Economia Sustentável ou lei Sinde aprovada em 31 de dezembro de 2011. Wikileaks publicou um grande número de comunicações e documentos mostrando que ela foi proposta em março de 2010 e, em seguida, aprovada sob considerável pressão dos Estados Unidos e um forte "lobby" pela grande mídia dos Estados Unidos e a indústria do entretenimento. Tem um componente, a Lei sobre os Serviços da Sociedade da Informação, que abrange a aplicação de direitos autorais e é semelhante a Hadopi.

No México, houve uma proposta de revisão da principal lei federal sobre Direitos Autorais e Propriedade Industrial, basicamente, para transformá-la numa versão mexicana da SOPA nos EUA.

12. Os Frutos da Árvore Envenenada

A maneira pela qual as pessoas se comunicam e armazenam suas comunicações hoje mudou drasticamente. Toda essa mudança provém de apenas alguns anos atrás.

A caixa de sapatos debaixo da cama, guardando cartas amareladas recebidas ao longo dos anos, está muito distante das pessoas do mundo contemporâneo. As pessoas se conectam usando dispositivos eletrônicos que estão sempre "online" e cujos modelos mudam a uma velocidade vertiginosa.

O compartilhamento de arquivos, seja de: música, vídeo, texto, imagem é uma atividade muito comum e constantemente em curso. Ao mesmo tempo, muitas redes de computadores estão inseguras e até mesmo aquelas supostamente seguras têm pontos de vulnerabilidade que podem ser violados por hackers inteligentes e que têm conhecimento técnico necessário para se infiltrarem na rede justamente através dos pontos de debilidade apresentados pelo sistema. A qualidade, os conhecimentos técnicos e as habilidades dos hackers também têm crescido exponencialmente. Bancos de dados contendo coleções de documentos e informações são relativamente de fácil acesso e podem ser pesquisados com uma variedade de propósitos, incluindo uma investigação criminal.

Wikileaks demonstrou isso mais de uma vez para todo o mundo, desafiando a classificação "Top Secret" do Governo dos Estados Unidos. Assim, a busca de informação e acesso aos bancos de dados, informações confidenciais, números de cartões de crédito, informações médicas e outros dados por particulares são bastante frequentes (Wikipedia, 2011d).

Essas atividades estão em constante andamento e muitas vezes são bem sucedidas. O perigo se dá em que acessa essas informações que deveriam ser bem protegidas.

Ocorre que, às vezes, essas informações que deveriam ser confidenciais ou acessadas apenas por agentes do governo, podem ser acessadas por particulares, pessoas não juridicamente autorizadas (Cluley, 2011).

Muito novo, perturbador e preocupante, especialmente para os libertários civis e ativistas de direitos humanos, é a parceria entre a polícia ou outros órgãos oficiais de investigação e os hackers, com os últimos fornecendo evidência substancial para os primeiros, muitas vezes por sua própria vontade e, em seguida, possivelmente, continuando a colaborar para encontrar mais uma prova do delito (Folkenflik, 2012; Lyall, 2011; Lyall, 2012).

Às vezes as coisas ficam ainda mais complicadas quando há conluio entre a mídia e os hackers ou em várias combinações, entre a mídia, a polícia, os hackers e os políticos.

Assim, ao contrário da crença popular, não é apenas o Estado ou a polícia que fazem espionagem e vigilância da conduta dos cidadãos, acessando seus aparelhos eletrônicos, mas também os particulares ou as empresas privadas, que muitas vezes o fazem extensivamente e de forma ilegal, usando fortes capacidades técnicas e armadilhas engenhosas para coletar provas incriminatórias que, então, oferecem para a utilização do Estado para prender, processar e condenar.

Assim, um dos menos notadas, mas mais controversas questões da Quarta Emenda no ciber espaço é admitir no tribunal busca e apreensão privadas, dos computadores ou outros dispositivos eletrônicos das pessoas, mesmo antes de se tornarem suspeitos formais de crimes, ou seja, sem causa provável.

13. Pesquisa Eletrônica: Parceria entre a Polícia e as Entidades Privadas

A parceria entre a polícia e as entidades privadas não é nova. Muitas vezes essa parceria é feita com o propósito de evitar as restrições e controles dos

preceitos constitucionais (nos EUA, a Quarta Emenda e sua regra de exclusão). As parcerias podem ser abertas, escancaradas ou tácitas e secretas.

Professores na escola podem inspecionar as mochilas ou armários escolares individuais dos estudantes ou ainda interrogar os alunos sobre a venda de drogas na escola ou participar de outras atividades ilegais e depois passar as informações para a polícia, sem ter que se preocupar com as limitações constitucionais do poder de invasão da privacidade e liberdade individual.

O mesmo pode ser feito por um vigia de uma loja privada, quando ele apanha um ladrão e obtém uma confissão sem a necessidade de dar ao suspeito os "avisos Miranda" [Miranda v. Arizona, 384 EE.UU. 436 (1966)], quando o policial faz a leitura dos direitos constitucionais do preso. E, claro, informantes existiram por milênios (Brenner, 2001).

No entanto, quando essas buscas eletrônicas, sem limitações constitucionais acontecem no ciber espaço, é mais preocupante e perigoso, porque uma parte privada, com as ferramentas adequadas, pode pesquisar uma vasta quantidade de informações facilmente, de forma eficiente, silenciosa e anônima. Isso pode ser feito em todo o mundo na segurança e conforto de um estúdio ou sala de estar, sem ninguém saber, ouvir, ver ou sequer suspeitar.

Pode ser uma busca rápida e descontinuada ou uma vigilância constante e por longo prazo. De acordo com a legislação constitucional dos EUA, para a polícia realizar uma pesquisa, eles precisam de uma causa provável (indícios de materialidade) e, dependendo do caso, um mandado judicial. Entidades privadas pesquisando, mesmo no sentido de uma "expedição de pesca", não precisam nem de causa provável nem tampouco de um mandado, e as informações que obtêm são utilizáveis dentro do processo criminal.

Conseqüentemente, dados e informações guardadas em computadores pessoais, que podem ser fisicamente seguros, estão potencialmente sujeitos a buscas eletrônicas por entidades privadas que podem, no final das contas, estar fazendo o trabalho da polícia.

Tudo que esses agentes particulares têm que fazer é entrar e obter acesso ao material armazenado no dispositivo eletrônico; e depois podem fazer o que quiserem com a informação obtida de forma extrajudicial e mais agressiva que o de abuso de poder por uma autoridade (Shah, 2005).

Não há dúvida de que a Quarta Emenda não vislumbrou operações conjuntas realizadas pelos policiais e particulares para conduzir investigações sobre delitos cibernéticos. Esta ideia foi alheia à compreensão da função e operação de aplicação da lei no momento de escrever a Constituição, especialmente porque naquela época esses dispositivos eletrônicos ainda não existiam.

Diante de tudo que foi anteriormente, pode-se afirmar que a Quarta Emenda, tradicionalmente, só se aplica a entidades e pessoal governamentais, não a particulares. Os particulares podem realizar buscas em computadores pessoais ou outros dispositivos eletrônicos conectados à internet.

Para eles não existem limitações constitucionais ou restrições legais infra-constitucionais (Katyal, 2004).

14. O Vazio Legal e a Necessidade de um Remédio

Não há dúvida de que existe um vazio legal que deve ser eliminado através de um estatuto que forneça um remédio para a supressão da busca e apreensão

por entidades privadas como meio de obtenção de provas e/ou a supressão, o descarte do uso dessas provas obtidas fora dos parâmetros legais do devido processo legal nos autos do processo.

Como por exemplo, as provas obtidas por hackers que passariam a não mais poder integrar o processo. A principal justificativa para criação da lei de reparação da lacuna legal existente no momento é o anonimato, o alcance e a eficiência das buscas feitas por hackers juntamente com a ilegalidade da pirataria em si. Isto definitivamente justifica um remédio como a supressão (Shah, 2005).

Não há dúvida que, quando as entidades privadas podem fazer uso da tecnologia de vigilância eletrônica utilizando para isso uma ferramenta ilegal, fazendo "hacking", para depois enviar as informações obtidas para serem usadas pelo o sistema de justiça para processar e condenar, isso pode legitimamente ser considerado bastante: anti-ético, injusto, incentivando a prática do crime de pirataria, sem repercussões legais para os particulares envolvidos e, às vezes, com recompensas para eles.

O ponto de discórdia é o aspecto de porta dos fundos ("backdoor") de tudo isso: o acesso de terceiros a informações privadas armazenadas num computador abrindo a porta para uma intromissão legalmente suportada pelo governo na vida privada. Pode-se dizer que quanto mais privacidade entregamos a particulares, como condição para utilizar os serviços eletrônicos, menos privacidade temos perante o governo, traídos pela tecnologia, sem a qual não podemos existir e gerenciar nossas rotinas de vida no mundo de hoje (Isom, 2010).

O banco de dados digital que contém arquivos relacionados a cada um de nós tem, goste ou não, um mix de informações: algumas obtidas por entidades privadas, muitas vezes ilegalmente, sem consequência jurídica para eles, e outras geradas pela polícia, que é mais limitada por normas legais no que pode e não pode fazer.

Um exemplo de um grupo que procura por uma prova de comportamento criminoso, como o descrito acima, são os Anjos do Cyber que são treinados para navegar na internet à procura de pornografia infantil (Shah, 2005: 261-62).

Alguns destes grupos usam cavalos de Tróia e vírus para quebrar barreiras e abrir caminho dentro das contas privadas em busca de possíveis evidências incriminatórias. Estes grupos fazem a vigilância de salas de chat públicas e privadas e cruzam o conteúdo das conversas com informações pessoais disponíveis na rede, especialmente através da mídia social, como é o caso do Facebook.

Não é necessário ter indícios de materialidade do crime para justificar a invasão da privacidade de alguém. Querem se envolver numa pura "expedição de pesca" e o sistema usará legalmente os frutos dessas pesquisas a seu favor.

Assim, pode-se dizer que o que pode ser descrito como policiamento cibernético de base comunitária é uma licença para interferir significativamente na vida privada dos vizinhos, amigos e desconhecidos (Awsumb, 2009).

Assim, no sistema jurídico dos EUA, réus que respondem a processos criminais não são necessariamente protegidos contra o uso das provas obtidas a partir da captura de informações em seus equipamentos eletrônicos por entidades privadas, ainda que o "hacking" em si mesmo seja considerado ilegal, como o é. Tribunais dos EUA afirmam que as pesquisas não são uma "interceptação". Alegam que o acesso a conteúdos que já existem armazenados num computador privado não é uma interceptação [U.S. v. Steiger 318 F. 3d 1039 (11 Cir 2003)].

O princípio básico legal nos EUA é o seguinte: Uma vez que uma pesquisa

privada é realizada, a expectativa original de privacidade é frustrada, quebrada, anulada e, como tal, a Quarta Emenda não proíbe a utilização governamental da informação obtida, que agora não é mais privada [United States v. Jacobsen, 466 U.S. 109, 117 (1984)].

Uma ilustração interessante de tudo isto é o caso de um informante turco, que decidiu investigar e descobrir a pornografia infantil nos "laptops" praticamente em todo o mundo e reportar os proprietários à polícia para serem processados.

O primeiro caso em que a evidência descoberta pelas buscas do hacker "Unknownuser", como ele(a) foi chamado(a) pelo FBI, foi utilizado com sucesso para a acusação e condenação é o caso Steiger [United States v. Steiger, 318 F.3d 1039, 1044 (11 Cir. 2003)].

O mesmo informante turco que trouxe Steiger à atenção das autoridades, conduziu outras investigações privadas invadindo o histórico de navegação na internet registrado pelo computador e os dados armazenados na memória da máquina, que contém informações acerca dos usuários desta.

A metodologia de "Unknownuser" foi a seguinte: ele anexou um programa "Cavalo de Tróia" a uma foto que ele postou num grupo de notícias frequentados por entusiastas da pornografia (Wikipedia, 2012d). Quando alguém baixou a foto, eles também baixaram o programa "Cavalo de Tróia", que forneceu a Unknownuser acesso a seus computadores.

Unknownuser na Turquia, eventualmente, descobriu e denunciou Jarrett William, nos Estados Unidos, acusando-o de ter pornografia infantil no seu computador. Desta vez, houve uma relação mais estreita entre o informante e o FBI, seguindo a linha de trabalho do o bem sucedido caso Steiger.

O estreitamento da relação foi tão grande que, por exemplo, os agentes do FBI ligaram para o informante para que este os ajudasse a obter acesso ao computador de Jarrett, que era protegido por senha.

O Tribunal Distrital esteve do lado de Jarrett e suprimiu a evidência, sustentando que o hacker agiu como um agente do governo e, conseqüentemente, violou a Quarta Emenda, quando ele forneceu à polícia o material pornográfico que obteve a partir de arquivos de Jarrett.

No entanto, na decisão em grau de recurso, a Corte de Apelações não concordou em caracterizar as ações do informante como ações que se enquadrassem na definição do padrão de atribuições da "agente do governo", que se fossem realmente realizadas por um agente público teriam sido fornecidas mais proteções constitucionais para Jarrett [United States v. Jarrett, 338 F.3d 339 (4tth Cir. 2003)].

A decisão do Tribunal Distrital foi revertida e Jarrett foi condenado. Assim, é muito difícil satisfazer as condições de enquadramento da conduta investigativa privada para entrar na padrão de conduta do agente público, o que ofereceria garantias constitucionais de defesa do réu dentro do processo.

Mesmo que seja admitida a parceria entre o agente privado e o agente público por meio da polícia comum ou do FBI. A Quarta Emenda só é aplicada a condutas investigativas privadas, quando é possível encaixar comportamento do particular na determinação legal da conduta a ser adotada pelo agente público.

15. Preocupações Constitucionais e Liberdades Civis

Há preocupações sobre liberdades civis e proteções constitucionais em ambos os casos, Jarrett e Steiger, e outros similares já que este tipo de pesquisa

investigativa é muito diferente de outras pesquisas (por exemplo, espionar casa de uma pessoa) que podem ser realizadas por uma entidade privada.

Além disso, outras características, que diferenciam essas pesquisas são: o anonimato e também a eficiência, exponencialmente maior, na caçada de diversos computadores conectados à internet simultaneamente.

Além disso, essas pesquisas privadas exigem uma boa capacidade técnica e por isso mesmo não fornecem informações sobre quem realizou a investigação ou deixam quaisquer vestígios, e oferecem a possibilidade de pesquisar muitos dispositivos eletrônicos, ao mesmo tempo, e sem que para isso haja qualquer indício que requeira uma investigação mais apurada sobre o assunto.

O "Cavalo de Tróia" é a estratégia usada frequentemente, como nos casos Jarrett e Steiger.

O "Cavalo de Tróia" é um software que está destinado a desempenhar, simultaneamente, um efeito desejável (esperado) e um efeito encoberto (inesperado).

Por exemplo, "Cavalos de Tróia" podem se multiplicar, roubar informações e prejudicar ou assumir o controle de um sistema de computador.

Uma vez que um Cavalo de Tróia é instalado num sistema do computador destinatário, um hacker pode ter acesso remoto ao computador e realizar várias operações, como: download ou upload de arquivos no computador do usuário; modificar ou apagar arquivos; registrar as teclas digitadas, observando a tela em uso; pesquisar os arquivos que contenham algum tipo de informação confidencial e/ou pessoal para furtar contas bancárias, e muito mias (Wikipedia, 2012d).

Adicionalmente, também há claramente um elemento de captura e assenhoramento de informações pessoais: os hackers utilizam um dispositivo eletrônico de outras pessoas para seu uso particular.

É também problemático e deficitário o sistema legal, que implicitamente aprova este tipo de pesquisa, que é de fato ilegal, permitindo seu uso em processos judiciais. Estes processos podem ser verdadeiras "expedições de pesca" (Wikipedia, 2011b).

Isto representa muito mais uma invasão do direito à privacidade, dentre outros, do que, por exemplo: "neighborhood watch" (o vizinho que está sempre de olho e disposto a denunciar atitudes suspeitas); linhas diretas de denúncia e delação, que dão pistas à polícia; ou um informante. Essas pesquisas eletrônicas são sistemáticas e podem atingir um grande número de pessoas em todo o mundo, silenciosamente, sem deixar impressões.

Além disso, diferentemente de uma invasão de domicílio ou da entrada indevida e desautorizada nas instalações de outra pessoa, não há qualquer vestígio ou sinal, como por exemplo: a violação do sistema de segurança ou o arrombamento de portas.

As próprias vítimas podem ser um grupo muito maior de pessoas, totalmente alheias ao que está ocorrendo (Katyal, 2004).

Tribunais, no mundo inteiro, ainda se sentem mais confortáveis com o manuseio físico de processos e crimes físicos, que ocorrem no mundo real do que com crimes eletrônicos, que acontecem no mundo virtual. Eles também acham mais difícil reconhecer a existência de um interesse na privacidade eletrônica. De certa forma, as opiniões dos tribunais parecem transmitir a ideia de que a violação da privacidade no espaço cibernético é muito mais aceitável do que no espaço físico (Shah, 2005).

Outro elemento perigoso é a aparente aprovação pelos tribunais do uso de

um vírus para penetrar no armazenamento eletrônico privado. Um vírus pode afetar muitas pessoas, talvez milhares, internacionalmente, e causar danos econômicos com perdas consideráveis.

Os mesmos tribunais que rejeitam uma prova derivada de um meio ilícito e/ou criminoso (os frutos de uma árvore envenenada, contaminada, podre) no mundo real, são muito mais inclinados a aceitá-la no mundo virtual. Pode-se dizer que os tribunais apoiam e incentivam "com uma piscadela e um aceno de cabeça" a aliança entre a polícia e os hackers ou pessoas envolvidas em atividades ilegais.

Ironicamente e talvez vergonhosamente, essa confiança do FBI ou da polícia nos hackers privados revela uma incapacidade deles ou uma falta de treinamento do seu pessoal para esta categoria de investigação.

Isto poderia ser um ponto importante. Tradicionalmente, a tolerância do tribunal e a vontade de facilmente permitir a vigilância e investigação de outros por parte de uma pessoa privada é baseada na visão de que não se espera que o cidadão, não sendo um "profissional", seja tão bom e, portanto, não pode fazer muito dano.

São os "profissionais", especialmente a polícia, que realmente sabem o que estão fazendo, são treinados para fazê-lo de forma rápida e eficaz, e podem causar uma série de prejuízos, que devem ser monitorados e controlados.

Na verdade, o inverso pode ser a realidade no ambiente eletrônico de hoje com os hackers, muito mais versados e experimentados, quando o assunto é se infiltrar num dispositivo eletrônico e fazendo a pesquisa e captura do seu conteúdo, do que a polícia ou o FBI. Por isso mesmo os hackers são utilizados para fazer esse trabalho de espionagem e, em seguida, apresentam as provas recolhidas às autoridades competentes (Shah, 2005:206).

A evidência mais contundente de que isso possa ser verdade, pode ser encontrada nos casos citados Garrett [338 F. 3d 339(4th Cir. 2003)] e Steiger [318 F. 3d 1039, 1044 (11th Cir 2003)], nos quais os agentes do FBI souberam reconhecer a superioridade do conhecimento técnico e capacidade do informante e, definitivamente, revelaram que quem produziu as provas foi o Unknownuser (Adams, 2008).

Se os juízes continuarem a manter esta atitude, devido ao uso cada vez maior e onipresente da internet e eletrônicos no cotidiano de todos, a proteção fornecida no Estados Unidos pela Quarta Emenda e os estatutos aplicáveis (por exemplo as leis anti-hacking) será cada vez mais seriamente enfraquecida e diluída.

É hora de introduzir um remédio eficaz, que deve incluir especialmente a capacidade de suprimir: as evidências obtidas ilegalmente e os "frutos da árvore envenenada". Uma lei que expressamente tratasse do tema, suprimindo a lacuna legal e a conseqüente deficiência do sistema existente hoje, seria muito útil (Shah, 2005: 276).

Existem técnicas de interpretação clássicas da Quarta Emenda que fazem com ela seja compreendida e aplicada para: assegurar a integridade do sistema judiciário, dissuadir comportamentos ilícitos na coleta de provas e prover os remédios principais previstos pela Regra de Exclusão.

Esse entendimento é reforçado pela legítima necessidade de garantir a segurança da Internet e desencorajar a pirataria.

16. Conclusão

A Internet tem sido universalmente considerada como intrinsecamente livre de regulamentação. A rede mundial é percebida como um lugar onde valores como: a liberdade de expressão e liberdade de criação; o compartilhamento de informações, que se tornam acessíveis a todos; a possibilidade de inspiração diante da exposição dos mais variados conteúdos, estariam assegurados pela própria natureza e arquitetura do ambiente da rede.

Contra esse sonho de liberdade crescente e irrestrita, existe a realidade de interesses poderosos, que estão cada vez mais dominando o mundo da propriedade intelectual, visando monopolizá-la ainda mais.

O regulamento dessa matéria é inevitável (Murray, 2003). A esperança é que isso pode ser feito de forma equilibrada, tendo em conta a natureza única, a essência e qualidades do mundo cibernético, dentro de uma forte tradição constitucional de respeito: à privacidade, à singularidade de cada ser humano e sua expressão, e aos aspectos maravilhosos da criatividade que atravessa o espaço e o tempo.

Equilibrar liberdade, criatividade e privacidade com os interesses de propriedade, tendências monopolistas, aspirações capitalistas e a justificação de segurança onipresente é um grande desafio, uma luta de Davi contra Golias, uma competição feroz entre os diferentes blocos e nações.

O resultado é incerto e imprevisível. Será uma prova do compromisso da comunidade internacional com os direitos humanos universais, dentre os quais: a privacidade, a liberdade de expressão e, em última instância, o florescimento e a prosperidade da humanidade num mundo interconectado.

LISTA DE ABREVIATURAS

ACTA - Anti-Counterfeiting Trade Agreement (Tratado contra a Falsificação no Comércio)

CAFA - Computer Abuse and Fraud Act (Lei contra Fraude e Abuso realizados por Computadores)

DCMA - Digital Copyright Millenium Act (Lei do Milênio Digital sobre os Direitos do Autor)

ECPA - Electronic Communications Protection Acr (Lei de Proteção às Comunicações Eletrônicas)

HADOPI - Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet. (Lei francesa que estabeleceu a Autoridade Máxima para a Difusão dos Trabalhos e Proteção dos Direitos do Autor na Internet).

IP - Intellectual Property (Propriedade Intelectual)

ISP - Internet Service Providers (Provedores de serviços de Internet)

PIPA - Protect Intellectual Property Act (Lei para proteger a propriedade intelectual)

SINDE - Lei da Economia Sustentável (na Espanha)

SCA - Stored Communications Act (Lei sobre as Comunicações Ameaçadas)

SOPA - Stop Online Piracy Act (Lei para deter a pirataria virtual ou online)

BIBLIOGRAFIA

Ackermann, T. (2009). Consent and Discovery Under the Stored Communications Act. Retrieved from http://www.pattersonsheridan.com/images/uploads/SCA_Control_article_PUBLISHED-crop.pdf

Adams, P. (2008). Fourth Amendment Applicability: Private Searches, National Center for Justice and the Rule of Law. Retrieved from http://www.olemiss.edu/depts/ncjrl/pdf/PrivateSearchDoctrine.pdf

Albanesius, C. (2011). Will Online Piracy Bill Combat "Rogue" Web Sites or Cripple the Internet? Retrieved from http://www.pcmag.com/article2/0,2817,2395653,00 asp # fbid = 6r9KNM2HX7x

Angarola, R. (2011). Exclusionary Rule. Enotes. Retrieved from http://www.enotes.com/exclusionary-rule-reference/exclusionary-rule

Argenpress. (2012). La SOPA y la doble cara de la "propiedad intelectual.". Retrieved from http://www.argenpress.info/2012/01/la-sopa-y-la-doble-cara-de-la-propiedad.html

Assange, J. (2011). Internet Has Become a Surveillance Machine. Agence France Presse.

ASIL. (2008). The Emergence of Cyber-Security as a Policy Driver. The American Journal of International Law.

Awsumb, S. (2009). Social Networking Sites: The Next E-Discovery Frontier, 66 Bench & Bar of Minn. Bench and Bar. Retrieved from http://www.mnbar.org/benchandbar/2009/nov09/networking.html

BBC. (2011). Entenda o escandalo dos grampus envolvendo o news of the world.

Bellia, P. (2007). Cyberlaw: Problems of Policy and Jurisprudence in the Information Age. West Academic Publishing.

Bennett, Brian. (2011) Police employ Predator drone spy planes on home front. Los Angeles Times Articles. Retrieved from http://articles.latimes.com/2011/dec/10/nation/la-na-drone-arrest-20111211

Brenner, J. (2001). Napster Fallout: Privacy Loses? Wired. Retrieved from 03/06/01,http://www.wired.com/politics/law/news/2001/03/42203;Sonia

Brenner, S. (2011). Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement Citizens Media Law Project. Retrieved from http://www.citmedialaw.org/threats/popular?

Chopra, S. (2008). Is Google Reading My Email? Retrieved from http://www.sci.brooklyn.cuny.edu/~schopra/choprawhite497.pdf

Cluley, G. (2011). "We could hack the Queen"s medical records if we wanted. Naked Security. Retrieved from http://nakedsecurity.sophos.com/2011/12/16/ournalists-under-the-spotlight/

Courtney, M. (1999). Recording Industry Sues Music Start-up, Cites Black Market. CNET News.

Crook, J. (2008). US Views on Norms and Structures for Internet Governance. The American Journal of International Law, 648.

DiBianca, M. (n.d.). Romano v. Steelcase: Defendant Granted Discovery of Plaintiff's Facebook Profile, Delaware Employment Law Blo. Retrieved from http://www.delawareemploymentlawblog.com/

DCMA. (1998). Derechos de Autor. Retrieved from http://www.derechos de autor.gov/legislation/dmca.pdf

Doernber, D. (2006). "Can You Hear Me Now?": Expectations of Privacy, False Friends, and the Perils of Speaking Under the Supreme Court's Fourth Amendment Jurisprudence. Retrieved from http://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1263&context=lawfaculty

Eaves, D. (2010). The Internet as Surveillance Tool. Retrieved from http://eaves.ca/2010/01/20/the-internet-as-surveillance-tool/

EFF. (2011). Cierra el News of the World por escándalo de escuchas ilegales. Electronic Frontier Foundation.

EFF. (2008) Anti-Counterfeiting Trade Agreement. Electronic Frontier Cooperation. Retrieved from https://www.eff.org/issues/acta

EFF. (2011) US vs Jones. Retrieved from https://www.eff.org/cases/us-v-maynard
Entenda o escândalo dos grampos envolvendo o "News of the World." (n.d.).UOL Naticias.

Epstein, R. (1978). Privacy, Property Rights and Misrepresentation, GA. L. Rev.

Folkenflik, D. (2012). U.K. Hacking Scandal Exposes Media-Police Ties. NPR.

Gallo, M. (2009). E-mail Privacy – Whether Court Order Disclosure of E-mail Content, per the Stored Communications Act, Violates the Fourth Amendment. Retrieved from http://www.michbar.org/computer/pdfs/vol26_1.pdf

Gillen, A. (2007). Study: Napster Eroding Retail. Billboard.

Goldman, E. (2011). Online User Account Termination and 47 U.S.C. §230(c)(2). Faculty Publications. Retrieved fromhttp://digitalcommons.law.scu.edu/facpubs/124

Goldman, E. (2010). Deleted Facebook and MySpace Posts Are Discoverable – Romano v. Steelcase, Technology & Marketing Law Blog. Retrieved from http://blog.ericgoldman.org/archives/2010/09/deleted_faceboo.htm?

Huffington Post. (2012) SOPA/PIPA Discussion: Internet Censorship & the Attack on Tech Innovators .Huffington Post. Retrieved fromhttp://www.huffingtonpost.com/2012/01/17/sopa-pipa-internet-censorship_n_1210614. html

Isom, D. (2010). Romano and Facebook: Muddling Toward the Law of Privacy on Social Networks, Information Law Group. Retrieved fromhttp://www.infolawgroup.com/2010/10/articles/social-networking/romano-and-facebook-muddling-toward-the-law-of-privacy-on-social-networks/

Jeffrey, D. (2000). The Evolution of E-Music and Its Consumers. Billboard.

Kanter, S. (2006). The Griswold Diagram; Toward a Unified Theory of Constitutional Rights,, 2006.

Katyal, N. K. (2004) Criminal Law in Cyberspace. SSRN eLibrary. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=249030

Kerr, O. S. (2009). The Case for the Third-Party Doctrine. SSRN eLibrary. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1138128

Kerr, O. S. (2004). A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It. SSRN eLibrary. Retrieved fromhttp://papers.ssrn.com/sol3/papers.cfm?abstract_id=421860

Krug, Francois. (2011). L'Hadopi expliquée aux nuls et à ceux qui piratent sans le savoir. Rue 89. Retrieved fromhttp://www.rue89.com/2010/10/08/lhadopi-expliquee-aux-nuls-et-a-ceux-qui-piratent-sans-le-savoir-169745

Laurence, T. (2012). SOPA Violates the First Amendment, Tribe Legis Memo. Retrieved from http://www.scribd.com/doc/75153093/Tribe-Legis-Memo-on-SOPA-12-6-11-1

Legal Information Institute. (2010). Fruit of the Poisonous Tree, Cornell.

Lessig, L. (1996). Reading the Constitution in Cyberspace, 45. Emory LJ.

Lessig, L. (1999). The Architecture of Privacy: Remaking Privacy in Cyberspace, 56-61.

Liptak, A. (2011). Court Case Asks If "Big Brother" is Spelled "GPS". The New York Times.

Litan, R. (2002). A Complicated Intersection: Public Action to Protect Private Property,. Brookings Review,.

Long, G. (2010). New York Trial Judge Orders Access to Private Facebook® and MySpace® Postings, Lexology. (2010) Retrieved fromhttp://www.lexology.com/library/detail.aspx?g=

Lyall, S. (2011, November 30). British Inquiry Is Told Hacking Is Worthy Tool. The New York Times. Retrieved fromhttp://www.nytimes.com/2011/12/01/world/europe/british-inquiry-is-told-hacking-is-worthy-tool.html

Lyall, S. (2012, January 4). Tip for London Police Officers: Booze and Secrets Don't Mix. The New York Times. Retrieved fromhttp://www.nytimes.com/2012/01/05/world/europe/report-tells-of-cozy-relationship-between-british-news-media-and-london-police-surrounding-phone-hacking-scandal.html

Macavints, C. (1999) Recording Industry sues Music Start-Up, Cites Black Market. CNET News.

Marlowe, Bet. (2011) SOPA (Stop Online Piracy Act) debate: Why are Google and Facebook against it? The Washington Post. Retrieved fromhttp://www.washingtonpost.com/business/sopa-stop-online-piracy-act-debate-why-are-google-and-facebook-against-it/2011/11/17/gIQAvLubVN_story.html?tid=pm_business_pop

Murray, A. D. (2003). Regulation and Rights in Networked Space. Journal of Law and Society, 30(2), 187-216.

Nair, Manoj. (2009). Cry Freedom is Sound Music, 19. India Times.

Navetta, D. (2010). The Law of Privacy on Social Networks, InfoSec Island. Retrieved from https://www.infosecisland.com/blogview/8917-The-Law-of-

Noorani. (1997). Cyberspace and citizens' Rights. Economic and Political Weekly.
Noorani. (2011). Intellectual Property Rights on the Internet: A Survey of the Issues. Economic and Political Weekly. Retrieved fromhttp://www.wipo.int/copyright/en/ecommerce/ip_survey/

Patrick, L. (2011)Right to privacy on the internet, internet and intellectual property justice clinic. (). Retrieved from http://internetjustice.blogspot.com/2010/06/right-to-privacy-on-internet.html

Payne, A. (2010). Twitigation: Old Rules in a New World. Washburn LJ. Retrieved from http;//www.washburnlaw.edu/wjl/49-3/articles/paynes-andrew.pdf

Penumbra. (n.d.).The Free Dictionary.

Podesta, J. (2005). Lost in Cyberspace? Finding American Liberties in a Dangerous Digital World. Yale Law & Policy Review.

Rodan, G. (1998) The Internet and Political Control in Singapore, Political Science Quarterly 113, 1 (Spring), 63-89

RPP Noticias (2011) The News of the World closes because if the illegal eavesdropping scandal. .

Schaufenbuel, B, (2011). Social Networking: Open Discovery Versus privacy and the Battle Between the coasts. Thomas Shaw.

Scolnik, A. (2009). Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment,.

Sembok,, T. (2003). Ethics of Information Communication Technology (ICT).

Serwin, A. (2010) ECPA Reform - Inconsistent Holdings on Social Media | Privacy & Security Source. Retrieved May 4, 2012, from http://www.privacysecuritysource.com/2010/10/02/ecpa-reform-inconsistent-holdings-on-social-media/

Shah, M. R. (2005). The Case for a Statutory Suppression Remedy to Regulate Illegal Private Party Searches in Cyberspace. Columbia Law Review,105(1), 250-278.

Sonia. (2004). The New Surveillance, 54. Case Western LR.

Sonne, P. (2011). U.S. (Secretary of State, Hillary) Clinton Criticizes Sale of surveillance Tools to Some countries. Wall Street Journal.

Stephens, O and Scheb, John. (2008). American Constitutional Law. New York, NY: Harcourt, Brace, Jovanovich.

Teitelbaum, J. (2002) Dueling for Da'wa: State v. Society on the Saudi Internet, Middle East Journal 56, 2 (Spring, 222-230

TIC Beat. (2012) Lo que traerá la recién aprobada Ley Sinde. Retrieved May 3, 2012, from http://www.ticbeat.com/tecnologias/aprobada-ley-sinde/

Timm, T. (2011) Proposed Copyright Bill Threatens Whistle blowing and human rights. Electronic Frontier Foundation.

Tribe, L. (2011) Is Congress Pushing Web Censorship? PC Magazine. Retrieved from http://www.scribd.com/doc/75153093/Tribe-Legis-Memo-on-SOPA-12-6 -11-1

Tully, S. (2000). Is It Sharing or Stealing? U.S. News & World Report, 38-40.

Tully, S. (2011). US Drones helping Local Police Agencies. U.S. News.

Walder, N. (2010). J Judge Grants Discovery of Postings on Social Media. Law.Com. Retrieved from http://www.law.com/jsp/law/article.jsp?id=1202472483935.

Warren, C. (2000). Napster is Rocking the Music Industry. U.S. News & World Report, 41-54.

Wikipedia contributors. (2011, April 18). Panopticon. Wikipedia, the free encyclopedia. Wikimedia Foundation, Inc. Retrieved fromhttp://en.wikipedia.org/w/index.php?title=Panopticon&oldid=487598351

Wikipedia Contributor. (2011a). Exclusionary Rule. Wikipedia the free encyclopedia. Wikimedia Foundation, Inc. Retrieved fromhttp://en.wikipedia.org/wiki/Exclusionary_rule

Wikipedia. (2011b). Fishing Expedition. Wikipedia. Retrieved from http://en.wiktionary.org/wiki/fishing_expedition

Wikipedia. (2011c) Stop Online Privacy Act/PIPA. Retrieved from http://en.wikipedia.org/wiki/Stop_Online_Piracy_Act

Wikipedia contributors. (2011d, May 4). WikiLeaks. Wikipedia, the free encyclopedia. Wikimedia Foundation, Inc. Retrieved fromhttp://en.wikipedia.org/w/index.php?title=WikiLeaks&oldid=490670353

Wikipedia contributors (2012). Napster. Wikipedia the free encyclopedia.Wikimedia Foundation, Inc. Retrieved from http://en.wikipedia.org/wiki/Napster

Wikipedia contributors. (2012a, May 3). Anti-Counterfeiting Trade Agreement. Wikipedia, the free encyclopedia. Wikimedia Foundation, Inc. Retrieved from http://en.wikipedia.org/w/index.php?title=Anti-Counterfeiting_Trade_Agreement&oldid=490456593

Wikipedia contributors. (2012b, April 13). Stored Communications Act. Wikipedia, the free encyclopedia. Wikimedia Foundation, Inc. Retrieved from http://en.wikipedia.org/w/index.php?title=Stored_Communications_Act&oldid=487159871

Wikipedia contributors. (2012c, April 14). Electronic Communications Privacy Act. Wikipedia, the free encyclopedia. Wikimedia Foundation, Inc. Retrieved from http://en.wikipedia.org/w/index.php?title=Electronic_Communications_Privacy_Act&oldid=487260975

Wikipedia contributors. (2012d, May 4). Trojan Horse. Wikipedia, the free encyclopedia. Wikimedia Foundation, Inc. Retrieved fromhttp://en.wikipedia.org/w/index.php?title=Trojan_Horse&oldid=489254985

Woefel, A. (2001). The Napster Phenomenon: Turning the Music Industry Upside Down. Retrieved from murphylibrary.uwlax.edu/digital/jur/2001/woelfel.pdf

York, J. (2011). Government Internet Surveillance Starts with Eyes Built in the West. Electronic Frontier Education.