Análise Econômica e Social dos Crimes Informáticos

Coriolano Almeida Camargo*

Renato Leite Monteiro**

***Resumo*:** O presente artigo expõe análise feita sobre os incentivos econômicos e sociais levados em consideração pelos perpetradores de crimes informáticos, concluindo pela necessidade de uma cooperação entre os diferentes setores da sociedade para diminuir tais estímulos.

Palavras - chave: *Crime informática, Análise Econômica, Fiscalização.*

I. INTRODUÇÃO

Para que possamos planejar adequadamente o nível de recursos necessários para combater os crimes informáticos é necessário um melhor entendimento dos custos que estes causam. Ao mesmo tempo, para podemos entender os incentivos vislumbrados pelos cibercriminosos, é igualmente importante investigar os procedimentos de ataque virtual.

II. A ECONOMIA DA CRIMINALIDADE: ANÁLISE *LATO SENSU*

O panorama básico da economia aplicada aos estudos de atos ilícitos parte do pressuposto que os perpetradores desses atos respondem a incentivos. O crime é considerado uma escolha social, apesar dos aspectos éticos e morais, ou até desvio de comportamento dos indivíduos responsáveis. Sobre esse pressuposto, Gary Becker [1] desenvolveu um modelo que considera os custos e ganhos que motivam o crime, e as opções para controle da criminalidade, o seu custo social. Becker modela a opção do ofensor como uma função dos ganhos com o ato ilícito, a probabilidade de apreensão e a severidade e o tipo da punição. Seu objetivo é minimizar o custo social líquido produzido pelos crimes, visto que os custos imputados às vitimas e ao judiciário superam qualquer benefício auferido pelos criminosos, gerando um desequilíbrio na economia. Becker demonstra que para maximizar o rendimento social agregado, as sanções ótimas opostas a criminosas devem ser na forma de multas. Ele argumenta que multas pecuniárias têm mais eficiência na repressão do que penas de restrição de liberdade, visto que essa ainda inclui um custo para o Estado.

O modelo de Becker foi expandido para uma miríade de cenários. Uma das extensões fundamentais é o mercado de ofensas e o análise do seu equilíbrio associado. O modelo de mercado consiste no (i) suprimento de ofensas (taxa de crimes, por exemplo); (ii) demanda – provisão de bens ilegais e serviços como drogas, desvio de produtos furtados etc; e (iii) demanda negativa – vítimas em potencial de ações penais que demandem intervenção pública, como aplicação correta dos provimentos legais e administração da justiça, ou de proteção privada.

O suprimento de ofensas consiste no estudo dos benefícios e custos aos ofensores, como oportunidades de ganhos, aversão pessoal a crimes e percepção individual sobre a probabilidade de apreensão. Interações sociais também são consideradas uma parte fundamental, pois influenciam as taxas de crimes na sociedade [2]. Uma das conclusões dos estudos de Becker é que os gastos em atividades com o

objetivo de redução de crimes devem ser consideradas a longo prazo, visto que taxas de criminalidade são influenciadas por taxas anteriores [3], então qualquer estratégia para combater crimes pode levar gerações para obter qualquer resultado observável. Outro ponto importante é a expectativa de aumento das taxas de crimes em medida proporcional ao desequilíbrio social de uma comunidade por duas razões: (i) aqueles nas camadas inferiores têm poucos custos para cometer crimes; (ii) a presença de indivíduos que auferem altas rendas promove alvos altamente lucrativos.

O estudo de demandas públicas para a aplicação da lei lida diretamente com a distribuição ótima de recursos para o sistema jurídico. As medidas utilizadas para a otimização dos problemas são normalmente baseadas nas rendas sociais agregadas. Todavia, alguns incluem conceitos de justiça. A maioria dos modelos parte de um plano social que tem a opção de influenciar a probabilidade de apreensão e condenação de um indivíduo, a severidade de uma punição e as sanções imputadas aos ofensores. Na prática, entretanto, não existe nenhum plano social e os responsáveis pela correta aplicação da lei estão apenas preocupados com o seu bem-estar social, o que pode levar a corrupção [4].

Vitimas em potencial também têm incentivos para se protegerem, para assim reduzirem o risco de vitimização, e adquirirem seguros, para então reduzirem as perdas caso venham a ser vitimadas [5]. Uma das questões principais nesse âmbito é se a proteção privada reduz os níveis de crimes, ou apenas desvia os riscos para vitimas menos protegidas. O estudo do mercado de ofensas assume que a freqüência com que cada tipo de crime acontece reflete em um equilíbrio implícito entre o fornecimento e a demanda desses atos [6]: o fornecimento agregado de atos ilícitos, taxa de criminalidade, por exemplo, é proporcional ao retorno esperado por ofensa, o que por sua vez decresce com a proteção privada utilizada por vitimas em potencial, e pelas sanções legais esperadas.

Modelos de mercado também têm sido utilizados para estimar o custo social da criminalidade [7]. Mercados marginais podem levar a um alto nível de crimes. Visto que as trocas são ilegais, é impossível celebrar contratos explícitos e que possam ser resolvidos pelo judiciário, levando a disputas que terminam em violência. Outra análise de mercado considera o público como provedores de oportunidades para os criminosos, e vitimas em potencial [8]. Uma das conclusões é que estes respondem às oportunidades e a provisão destas oferecidas pelo público determina as taxas de criminalidade. Enquanto que a maioria dos modelos de mercado leva em consideração grupos desorganizados, lidar com a criminalidade organizada requer modelos diferentes, em face desta representar uma entidade que tenta funcionar como um monopólio, e restringe o fluxo de transações ilegais. Em adição, participam na elevação artificial de preços e na depreciação dos esforços para aplicação da lei [9].

III. O CUSTO SOCIAL DOS CRIMES INFORMÁTICOS

Existe uma falta de entendimento sobre a precisa magnitude do cibercrime e os seus impactos devido ao fato que estes nem sempre são detectados ou reportados. Razão para que estes não sejam denunciados incluem impacto financeiro no mercado, reputação ou danos a marca, preocupação com possíveis processos judiciais, o fato que reportar uma falha envia um sinal verde para novos ataques, inabilidade em fornecer informações, receios com relação à perda de emprego por parte dos profissionais responsáveis pela segurança da empresa, e uma perceptível falta de imposição da lei por parte do Estado.

Dados relativos aos custos dos crimes informáticos são fáceis de obter em alguns dos casos de falha de segurança mais notórios. Por exemplo, a falha de segurança da empresa TJX custou aproximadamente 200 milhões de dólares [10]. A companhia

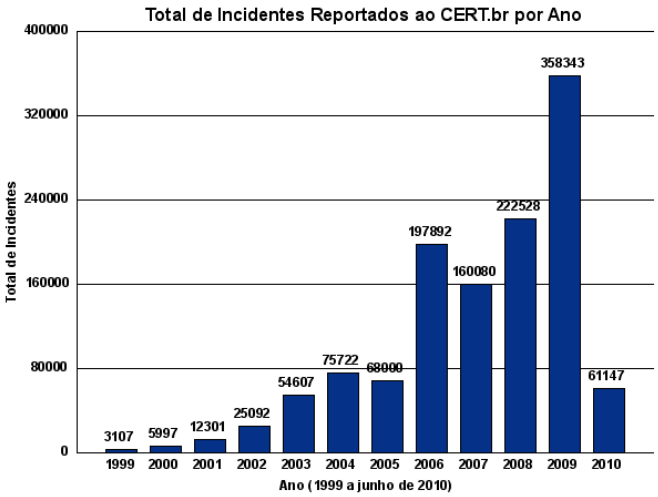
Heartland teve um prejuízo total de quase 40 milhões de dólares devido a sua falha que expôs milhares de históricos médicos. Todavia, muitos desses custos vieram de forma indireta, quando a empresa se deparou com processos judiciais e potenciais pedidos de responsabilidade civil [11].

Além de dados oriundos de grandes falhas de segurança, é muito difícil obter registros confiáveis de casos menores. Em particular, a metodologia utilizada pelos cibercriminosos tem por alvo usuários de uma grande variedade de cenários, com acesso a diferentes serviços financeiros. No entanto, enquanto cada caso individual pode aparentar singelo e menos significante, o montante acumulado de fraudes informáticas pode se espalhar por diversas entidades e não serão identificados por nenhuma instituição isoladamente. Várias são as estimativas feitas por diferentes entidades nas mais diversas jurisdições [12]. Todavia, estudos indicam que perdas podem superar a cifra de 01 trilhão de dólares anuais [13]. Enquanto que essas estimativas são valiosas, elas não são de inteira confiança, pois detém grandes diferenças sem explicação aparente e alguns institutos não informam suas fontes ou a metodologia utilizada para realizarem suas estimativas [14]. Além disso, várias empresas de segurança recebem incentivos para inflarem artificialmente essas estimativas [15].

Atualmente, umas das estatísticas mais confiáveis internacionalmente são as catalogadas e coletadas pelo Inter Crime Complaint Center (IC3). O relatório anual de 2009 revelou que o número de denúncias online atingiu um recorde, recebendo um total de 336.665 reclamações, um aumento de 23% se comparado ao ano anterior. O valor total das fraudes virtuais superou os 559 milhões de dólares [16]. A média individual foi de 931 dólares. Apesar de servirem como demonstração da gravidade dos crimes informáticos, essas estimativas são apenas uma pequena fração das reais perdas por diversas razões: muitas empresas preferem não reportar os ataques, pelos motivos acima expostos; vitimas podem não ser conhecidas e o IC3 compila dados apenas dos Estados Unidos da América – EUA.

O Reino Unido estimou perdas no montante a 610 milhões de libras com relação a prejuízos oriundos de fraudes de cartão de crédito, que incluem práticas onde o ilícito se deu sem a presença física dos cartões. Estes números representam um crescimento contínuo desde que começaram a ser medidos, em 2004. Enquanto que neste ano as fraudes realizadas com a presença de cartões físicos eram similares a de quando estes eram inexistentes, agora fraudes virtuais são a fonte primária dessas modalidades de delitos, sofrendo um aumento de 243%. No mesmo período, o total de transações de comércio eletrônico sozinhas aumentou 524%.

No Brasil, o instituto responsável pela coleta de dados e por receber denúncias de falhas de segurança e crimes informáticos é o CERT.br [17] (Computer Incident Response Team do Brasil). O ano de 2009 recebeu um total de 358.343 denúncias, número superior ao recebido por organizações americanas. O crescimento voluptuoso da economia brasileira e fragilidade dos sistemas informáticos que a sustenta foi um dos motivos ao crescimento massivo da criminalidade informática em território nacional.



Enquanto que os relatórios dessas instituições podem fornecer dados sólidos para podermos estimar as perdas oriundas dos crimes informáticos, muito precisa ser feito para que prospecções confiáveis sejam feitas. Atualmente, não temos identificar de forma precisa o real cenário do problema. Podemos apenas afirmar categoricamente que este existe, mas sem estimativas reais não podemos mensuras se as ações tomadas pelas iniciativas públicas e privadas estão surtindo efeito.

Uma maneira possível para melhorar o conhecimento sobre os custos reais dos cibercrimes é compelir, através de leis e fiscalização freqüente (*enforcement*), bancos, instituições financeiras, provedores de serviços de internet e demais empresas a revelarem os registros e os custos associados com ataques a seus sistemas, incluindo o volume de dinheiro envolvido nos delitos. Alguns estados americanos já dispõem de legislação que determina que qualquer falha de segurança deve ser reportada, sob pena de responsabilidade civil no montante das perdas caso seja descoberta posteriormente que a instituição não informou o incidente [18]. Reportar irá facilitar a elucidação das falhas e as tendências, assim como criar um mercado para a prevenção de fraudes, onde as instituições podem encontrar meios para proteger seus usuários [19].

IV. POTENCIAL DE ARRECADAÇÃO DOS CRIMES INFORMÁTICOS

Para que seja possível desenvolver um modelo econômico dos crimes informáticos também é necessário estimar os benefícios em potencial. Isso irá ajudar a entender os incentivos vislumbrados por criminosos em potencial e o perda social total: em quanto a margem de lucro sobre as vítimas supera os perigos oriundos de um sistema legal e de segurança.

Enquanto que alguns casos podem fornecer um material basal sobre diferentes atividades, ainda é nebuloso o quão representativo esses são com relação a essa economia marginal, visto que apenas uma fração dos incidentes são reportados, investigados e processados. Para obter um melhor panorama do real valor que adentra essa economia é necessário mais transparência por parte das instituições, tanto públicas quanto privadas, ao reportar suas perdas decorrentes de crimes informáticos. Estimar os ganhos dos cibercrimes é diferente do que trabalhar os danos pecuniários, visto que estes se estendem não só as informações perdidas, mas também estão distribuídas entre recuperação destas, processos judiciais, depreciação de valor de marcas e outros efeitos colaterais. Caso as instituições sejam obrigadas a informar essas perdas diretas talvez possamos estimar o real fluxo de dinheiro que sustenta a economia marginal dos crimes informáticos.

V. PROTEÇÃO PÚBLICA

A proteção pública pode influenciar o suprimento de ofensas ao reduzir os incentivos para atos de cibercriminosos. As principais variáveis que a aplicação da lei e legislação podem influenciar são: (i) a probabilidade de apreensão de cibercriminosos; (ii) e as penalidades associadas aos cibercrimes. Com relação à probabilidade de apreensão, diversos fatores contribuem para natureza pouco arriscada do cibercrimes. Por exemplo, é altamente improvável que os aplicadores da lei se envolvam com casos que envolvem o furto de identidade, visto que a maioria das vitimas não reporta esses ilícitos para as autoridades [20]. Esse também pode ser caso o caso de furto de contas bancárias, porque a vitima normalmente resolve o problema através de um contato com o banco sem qualquer continuação de procedimentos para com o incidente. Até quando um consumidor tenta contatar a polícia, algumas autoridades ainda são relutantes em receber as denúncias. Algumas entendem que a vitima seria a instituição financeira. Ou em caso que o furto se deu em jurisdição diversa, elas podem requerer que o ofendido protocole a reclamação em outro lugar. Por outro lado, entidades privadas não recebem nenhum incentivo para reportarem incidentes de segurança.

O cenário é mais complicado para as prioridades das autoridades e *expertise*. Em um nível local, a polícia normalmente não tem recursos ou conhecimento para de forma efetiva identificar responsáveis por crimes informáticos. Isso leva um problema de interação entre as entidades públicas e privadas, quando estas, em muitos casos, realizam funções eminentemente públicas para que casos sejam resolvidos. Na esfera federal, apenas casos de grande monta são investigados, e os demais arquivados por falta de justa causa. Em 2003 foi estimado que cibercriminosos têm uma chance em setecentos de serem pegos por autoridades policiais [21], enquanto que em delitos comuns mais graves a probabilidade aumenta de um para cinco [22]. Essa falta de resposta das autoridades leva ainda mais as vitimas a não reportarem seus incidentes.

Mesmo que as autoridades decidam investigar e iniciar um procedimento judicial, a natureza sem fronteiras desses tipos de crimes aumentam as ambigüidades de jurisdição e as dificuldades associadas ao processo. A maioria das penalidades no Brasil atribuídas a crimes informáticos são brandas e não levam a penas alternativas. Como referenciado anteriormente, as penas mais eficientes são as monetárias, modalidade que encontra pouco respaldo na jurisdição brasileira. Nos casos em o responsável recebe uma pena de restrição de liberdade, afora o fato de essa pena ser mais cara para o Estado, o aprisionamento pode contribuir para o comportamento malicioso ao agregar uma comunidade de pessoas que podem compartilhar técnicas e criar redes criminosas. Dois casos clássicos podem servir de ilustração. John Draper, um dos mais famosos *phreakers*, *crackers* que utilizam seus conhecimentos para acessos sistemas telefônicos, foi preso nos EUA em 1972 devido a fraudes tarifárias. Ao sair da prisão, informou que adentrando no sistema prisional teve que ensinar a todos no estabelecimento como ele praticava as suas fraudes. O método se espalhou e as companhias telefônicas registrarem perdas ainda maiores [23]. Da mesma maneira, Max Butler iniciou suas atividades como um hacker recreativo. No entanto, quando invadiu computadores do Pentágono, ele foi apreendido e preso. Na prisão ele conheceu um fraudador profissional que o introduziu ao mundo do *carding.* Ao cumprir sua pena, ele começou a atacar sistemas de bancos, mercados e outros *crackers* pra furtar números de cartões de créditos, que eram então vendidos para *carders*[24].

VI. PROTEÇÃO PRIVADA

No molde de cooperação entre entidades públicas e privadas, a indústria de segurança computacional pode contribuir para a redução nas ofensas virtuais ao aumentar o custo para o início e a manutenção de ataques cibernéticos. Enquanto que a

indústria de segurança computacional tem tradicionalmente focado em tecnologias de prevenção, firewall, antivírus, encriptação, autenticação etc, existe um mercado emergente para a detecção de ataques e a recuperação destes. Entidades privadas já foram responsáveis por muitos casos de desbaratamento de organizações criminosas cibernéticas. Do mesmo jeito, várias empresas estão utilizando monitoramento de marcas e soluções antifraude, que incluem sistemas de desligamento, que consistem em rastrear servidores maliciosos e entrar em contato com os provedores responsáveis para que o conteúdo ofensivo seja retirado. Uma das questões principais é se proteção privada diminui os níveis de crimes ou apenas desviam para vitimas menos protegidas.

VII. MOLDANDO OS INCENTIVOS DOS TOMADORES DE DECISÕES

Provedores de serviços de internet têm abordagens diferentes ao gerenciarem o nível de segurança dos seus usuários, o que é diretamente relacionado à sua hierarquia e princípio de interconexão. A Internet atual consiste em múltiplas semi-autônomas redes que compartilham um número IP [25] em comum e uma estrutura global de roteamento do tráfego que provê diretamente ou indiretamente conectividade a essas redes. Essas redes são classificadas em três tipos de acordo com a natureza de suas conexões com outras redes.

Provedores de acesso a internet motivados podem aplicar um grande número de medidas para melhorar a segurança de suas redes, por exemplo: (i) atuar preventivamente, ao proteger clientes de ataques ao oferecerem softwares de segurança de forma mais acessível; (ii) resposta ativa, aplicando quarentena automática e conserto de falhas ao serem detectadas; (iii) defesa da rede, através de um monitoramente local e tráfego de rede interconectado; (iv) e colaboração, implementado defesas de rede compartilhadas e criar grupos de combate conjuntos.

Todavia, é importante notar que até mesmo os provedores de internet mais vigilantes não têm sempre condições de proverem segurança a seus usuários sem iniciativas colaborativas. Primeiro, muitas ameaças não se manifestam na camada de conexão, mas sim na camada de aplicativo, a exemplo do que acontece no furto de credenciais através de *phishing*. Segundo, muitos países, como o Brasil, têm leis de privacidade estritas que proíbem provedores de acesso à internet monitorarem as ações de seus usuários, de forma que estes somente podem atuar após o recebimento de notificações de abuso. Tecnologias que identificam automaticamente essas ameaças podem reduzir a logística das denúncias.

Com relação a empresas e usuário domésticos, é necessário avaliar os possíveis papeis que estes podem exercer no combate a crimes informáticos. É importante mencionar que diferentes classes de usuários têm diferentes níveis de incentivos para investir em segurança.

O sucesso de esquemas de cibercrimes depende frequentemente da falta de investimentos em segurança entre usuários residenciais e pequenos negócios. Àqueles raramente estão cientes dos riscos e falham em se adequar as medidas de segurança necessárias em face da complexidade de medidas efetivas [26]. Por exemplo, eles podem abrir arquivos maliciosos anexados a e-mails ou não instalarem atualizações das assinaturas de vírus, mesmo tendo consciência que tais atos podem levar em perdas financeiras e infortúnios. Ainda, a grande maioria de usuários a quem são oferecidos serviços diferenciados de segurança escolhem manter os planos básicos por questões financeiras. Outro motivo é a falta de responsabilização quando usuários e negócios são atingidos negativamente por máquinas comprometidas [27]. Infelizmente, usuários residenciais combinados com a falta de ações preventivas podem resultar em um aumento substancial no dano coletivo [28].

Usuários também podem agir de forma passiva por estarem protegidos dos danos que podem originar de cibercrimes. Por exemplo, a legislação consumeirista protege a responsabilização dos consumidores pelo furto de suas contas bancárias. Decisões em sentido contrário ainda são raras, mesmo quando provado a culpa da vitima. Todavia, existem sim alguns incentivos para que estes apliquem medidas de segurança em suas redes, de forma que evitem os inconvenientes e as eventuais perdas monetárias.

Grandes empresas, incluindo instituições financeiras e de comércio eletrônico normalmente investem em segurança para protegerem seus procedimentos operacionais e segredos industriais. Elas podem contar com a cooperação dos provedores de acesso a Internet para se defenderem de ataques de larga escala. Também estão interessadas em manter políticas de segurança bem estritas, que normalmente incluem operarem em redes separadas.

Em contraste, empresas também têm incentivos para obscurecer os cibercrimes como furto de identidade e de credenciais, com receio que o valor de suas marcas seja atingido. Em adição, a exposição de perdas severas devido a incidentes de segurança pode levar a ensejos regulatórios indesejados pelo mercado. Altos níveis de fraude podem diminuir a credibilidade de instituições financeiras, iniciando um movimento em cadeia que pode levar a uma instabilidade em todo mercado.

Ainda, usuários maliciosos pagam por serviços diferenciados a provedores de internet fraudulentos, recebendo em retorno a possibilidade de conduzirem suas atividades por mais tempo sem que seus conteúdos sejam retirados ou atingidos.

A indústria de *software* é um caso interessante na análise dos cibercrimes. Enquanto que a maioria das empresas é responsabilizada pela segurança de seus produtos, a prática atual na indústria de software é a não imputação de responsabilidade pela qualidade do *software* através do contrato de utilização de licença (*user license agreement*). São raras as decisões judiciais em sentido contrario.

VIII. CONCLUSÃO

Podemos concluir que os crimes informáticos ainda são muito vantajosos sob a análise dos incentivos econômicos e sociais que levam a sua prática. A falta de fiscalização adequada, a alta lucratividade, a grande possibilidade dos criminosos não serem encontrados, o hábito das vítimas de não reportarem os incidentes e as penas pequenas são incentivos para a ocorrência desses crimes. Somente através da cooperação entre as diferentes esferas é possível diminuir estes incentivos.

REFERÊNCIAS

[1] BECKER, Gary S. Crime and punishment: An economic approach. Journal of Political Economy, vol. 1968, p. 169.

[2] GLAESER, Edward; SACERDOTE, Bruce; SCHEINKMAN, Jose. **Crime and social interactions**. Quarterly Journal of Economics, 2:507–548, 1996.

[3] SAH, Raaj K. **Social osmosis and patterns of crime**. Journal of Political Economy, vol. 99. 1991, p.1272–1295.

[4] FRIEDMAN, David. **Why not hang them all: the virtues of inefficient punishment**. Journal of Political Economy, vol.107. 1999, p. 259–269.

[5] LAKDAWALLA, Darius; ZANJANI, George. Insurance, self-protection, and the economics of terrorism. Journal of Public Economics, vol. 89. 2005, p. 1891–1905.

[6] EHRLICH, Isaac. On the usefulness of controlling individuals: an economic analysis of rehabilitation, incapacitation, and deterrence. American Economic Review; vol. 71. 1981, p. 307–322.

[7] ANDERSON, David.**The aggregate burden of crime**. Journal of Law and Economics, vol. XLII. 1999, p. 611–642.

[8] COOK, Philippe. **The demand and supply of criminal opportunities**. Crime and Justice. vol.7. 1986, p. 1–27.

[9] GAROUPA, Nuno. **The economics of organized crime and optimal law enforcement**. Economic Inquiry. vol.38. 2000, p. 278–288.

[10] TJX hacker was awash in cash; his penniless coder faces prison. Disponível em: <http://www.wired.com/threatlevel/2009/06/watt>. Acesso em: 15 jul 2011.
[11] Payment Processor Breach May Be Largest Ever. Disponível em:<http://voices.washingtonpost.com/securityfix/2009/01/payment_processor_breach_may_b.html>. Acesso em: 15 jul 2011.
[12] ITU Study on the Financial Aspects of Net- work Security: Malware and Spam. Disponível em:<http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ itu-study-financial-aspects-of-malware-and-spam.pdf>.Acesso em: 15 jul 2011.
[13] Unsecured Economies - Protecting Vital Information. Disponível em:< http://resources.mcafee.com/content/NAUnsecuredEconomiesReport>. Acesso em: 08 set 2009.
[14] A ONG Safernet (www.safernet.org.br) detém valiosos dados com relação à segurança eletrônica no Brasil, mas não divulga suas fontes e a metodologia aplicada.
[15] ITU Study on the Financial Aspects of Net- work Security: Malware and Spam. Disponível em:<http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ itu-study-financial-aspects-of-malware-and-spam.pdf>.Acesso em: 15 jul 2011.
[16] IC3 2009 Annual Report on Internet Crime Released. Disponível em:<http://www.ic3.gov/media/2010/100312.aspx>. Acesso em: 10 jul 2011.
[17] http://www.cert.br/stats/incidentes/
[18] Disponível em: http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html
[19] HOOFNAGLE, Chris Jay. **Identity theft: Making the known unknowns known**. Journal of Law and Technology, vol. 21, 2007.
[20] Identity theft survey report. Disponível em:<http://www.ftc.gov/os/2003/09/synovatereport.pdf>.Acesso em: 15 jul 2011.
[21] Underreporting of identity theft rewards the thieves. Gartner Group Research ID: M-20-3244, 2003.
[22] Porque a Lei Não Deve Almejar a Justiça, mas sim o Bem Estar. Disponível em:<http://www.redel.com.br/~dennisww/lei1.htm>. Acesso em: 15 jul 2011.
[23] Interview with John Draper. First episode of stop H*Commerce. Disponível em:<http://www.stophcommerce. com>. Acesso em: 15 jul 2011.
[24] Kevin Poulsen. Superhacker max butler pleads guilty. Disnponível em:<http://www.wired.com/threatlevel/2009/06/butler_court/>. Acesso em: 15 jul 2011.
[25] Internet address - IP: número atribuído a cada conexão de internet, permitindo sua individualização.
[26] ACQUISTI, Alessandro; GROSSKLAGS, Jens. **Privacy and rationality in individual decision making**. IEEE Security & Privacy. vol. 3. 2005, p. 26–33.
[27] Managing online security risks. Disponível em: <http://www.nytimes.com/library/financial/columns/060100econ-scene.html>. Acesso em: 28 jul 2010.
[28] GROSSKLAGS, Jens; CHRISTIN, Nicolas; CHUANG, John. **Secure or insure? A game-theoretic analysis of information security games.** World Wide Web Conference (WWW'08). China. 2008, p. 209–218.

* Advogado, CEO do Almeida Camargo Advogados, Coordenador do Programa de Pós Graduação em Direito Eletrônico e Inteligência Cibernética da FADISP.

** Advogado do Opice Blum Advogados Associados, Mestre em Direito Constitucional, Professor do Programa de Pós Graduação em Direito Eletrônico e Inteligência Cibernética da FADISP.