UM ESTUDO SOBRE A FRAUDE DE CLIQUE: CASOS CONHECIDOS E IMPACTO NO DIREITO BRASILEIRO

A STUDY ON CLICK FRAUD: KNOWN CASES AND THEIR IMPACT ON THE BRAZILIAN LAW

UN ESTUDIO SOBRE EL FRAUDE DEL CLICK: CASOS CONOCIDOS E IMPACTO EN EL DERECHO BRASILEÑO

Ruy J. G. B. de Queiroz[1]

Rodrigo Alves Costa[2]

RESUMO

O crescimento da indústria de anúncios *on-line* tem criado novas oportunidades em termos de negócios na Internet. Neste ambiente, métricas como cliques em anúncios originam transações financeiras entre anunciantes, redes de anúncios e publicadores de anúncios. Uma vez que estes cliques possuem impacto financeiro, criminosos têm buscado obter vantagens e gerar divisas de maneira ilícita por meio destas novas oportunidades. Este trabalho analisa a sistemática da chamada fraude de clique, expondo as suas implicações legais em casos recentes. Também analisa a sua relação com o direito brasileiro em função da teoria geral dos contratos e do projeto de lei sobre crimes cibernéticos. Finalmente, entende a fraude de clique como ameaça concreta para o futuro da publicidade na Internet.

PALAVRAS-CHAVE: Anúncios na Internet. Redes de anúncio. Fraude de clique. Crimes cibernéticos. Teoria dos contratos.

ABSTRACT

The growth of the online advertising industry has created new business opportunities on the Internet. In this environment, actions such as clicking an ad result in financial transactions amongst advertisers, advertising networks and publishers. Since these new opportunities have financial impact, criminals have been trying to gain illegal advantages and profit through them. This paper analyzes the click fraud mechanism, focusing on its legal implications in recent cases. It also evaluates the relationship between click fraud and the Brazilian legislation, considering both general contract theory and the bill on cybercrime. Finally, we understand click fraud as a genuine threat to the future of Internet advertising.

KEYWORDS: Internet advertising. Advertising networks. Click fraud. Cybercrime. Contract theory.

1 Doutor em Informática pelo Imperial College Univerisity of London e Mestre em Informática pela Universidade Federal de Pernambuco (UFPE). Editor-in-Chief de revista científica - Logic Journal of the IGPL (Oxford Univ Press), membro do corpo editorial do International Directory of Logicians. Professor Associado do curso de Ciências da Computação da Universidade Federal de Pernambuco (UFPE). De 2006 a 2008 foi membro eleito do Council da Association for Symbolic Logic. Criou em 1994 a série internacional WoLLIC de encontros científicos em lógica. Em 2006, foi premiado com uma cátedra de Edward Larocque Tinker Visiting Professor - Dept Philosophy, Stanford Univ, por indicação de Solomon Feferman e Grigori Mints. Integrou o advisory group do Nominating Committee para o Rolf Schock Prize in Logic and Philosophy for 2011 concedido pela Royal Swedish Academy of Sciences, tal qual ocorreu em 2008. Recife, Pernambuco, Brasil. *E-mail*: ruy@cin.ufpe.br

2 Doutorando em Ciência da Computação e Mestre em Ciência da Computação pela Universidade Federal de Pernambuco (UFPE). Graduando em Direito pela Universidade Federal da Paraíba (UFPB). Professor Assistente do curso de Ciências da Computação da Universidade Estadual da Paraíba (UEPB), *campus* VII. Campina Grande, Paraíba, Brasil. *E-mail*: rodrigo.costa@gmail.com

ISSN Eletrônico 2175-0491

RESUMEN

El crecimiento de la industria de anuncios *on-line* ha creado nuevas oportunidades en términos de negocios en la Internet. En este ambiente, métricas como clicks en anuncios originan transacciones financieras entre anunciantes, redes de anuncios y publicadores de anuncios. Considerando que estos clicks poseen impacto financiero, los delincuentes han buscado obtener ventajas y generar divisas de manera ilícita por medio de estas nuevas oportunidades. Este trabajo analiza la sistemática del llamado fraude del click, exponiendo sus implicaciones legales en casos recientes. También analiza su relación con el derecho brasileño en función de la teoría general de los contratos y del proyecto de ley sobre crímenes cibernéticos. Finalmente, entiende el fraude del click como amenaza concreta para el futuro de la publicidad en la Internet.

PALABRAS CLAVE: Anuncios en la Internet. Redes de anuncio. Fraude del click. Crímenes cibernéticos. Teoría de los contratos.

INTRODUÇÃO

Os mercados e a economia global, os quais operam e competem os negócios, têm sido alvos de constantes mudanças na última década. O desenvolvimento de *sites* de Internet comerciais acompanhou a popularização da própria Internet, desde meados dos anos 1990. Hoje em dia, anunciar pela Internet é uma das formas mais rentáveis de realizar campanhas de *marketing* com o objetivo de atingir diversos tipos de clientes, tanto para pequenas quanto para grandes empresas. Um dos grandes benefícios de anunciar na Internet é a possibilidade de publicar informação e conteúdo sem fronteiras geográficas ou de fuso horário.

Outro benefício é a eficiência do investimento. Anunciar *on-line* permite a personalização de anúncios, incluindo o conteúdo dos mesmos e os lugares onde serão exibidos. O *AdWords*, o *AdSense*[3] e o *Yahoo! Search Marketing*[4], por exemplo, permitem que anúncios sejam mostrados tanto em páginas Web relevantes quanto em resultados de pesquisas de palavras-chave relacionadas.

Em um ambiente no qual se verifica uma ebulição de negócios tão significativa quanto a Internet, com um número crescente de relações (e interesses) sociais entre empresas e pessoas, é inevitável o surgimento de disputas e contestações de natureza jurídica. São diversos os exemplos disponíveis de casos legais que têm aparecido desde que a Internet começou a ser efetivamente utilizada para fins comerciais, especialmente no direito estadunidense.

Concomitantemente, ao falar de direito digital e sua relação com o ordenamento jurídico brasileiro, é inevitável não realizar uma análise mais fundamental acerca da própria função do direito para uma sociedade. Esta necessidade é consequência das indiossincrasias e particularidades do direito nacional, que decorrem de um processo histórico de formulação e caracterização de conceitos[5]. Exemplo disso é o Código Penal Brasileiro, que data de 1940. É impossível ignorar o fato óbvio de que, após 70 anos, importantes mudanças sociais motivarão a necessidade de ajustes na norma, a exemplo do surgimento de um mercado de anúncios na Internet.

Tal mercado se fundamenta em modelos de negócio, ou seja, em métodos por meio dos quais as empresas participantes se organizam para obter receitas. Os modelos de negócio de anúncios na Internet mais comuns são o pagamento por clique, o pagamento por exibição e o pagamento por ação[6]. Em cada um desses, há diferentes brechas para que usuários maliciosos busquem

3 GOODMAN, Andrew. **Winning Results with Google AdWords**. New York: McGraw-Hill, 2008, p. 33.

4 O'REILLY, T. What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. **Communications & Strategies**, v.1, n.65, jan./mar. 2007, p. 21. Disponível em: <http://papers.ssrn. com/sol3/papers.cfm?abstract_id=1008839>. Acesso em: 23 out. 2011.

5 JUSTO, Antonio Santos. O direito brasileiro: raízes históricas. **Revista Brasileira de Direito Comparado**, Rio de Janeiro, v.20, n.1, pp. 1-14, jan. 2011, pp. 9-13. Disponível em: <http://www.estig.ipbeja.pt/~ac _direito/dir_bras_raiz_hist.pdf>. Acesso em 04 dez. 2011.

6 MANN, C. How Click Fraud Could Swallow the Internet. **Wired Magazine**. São Francisco, v.14, n.1, pp. 17-20, 2006, p.17.

obter vantagens de maneira ilícita por meio de fraude. Uma das fraudes associadas ao método de pagamento por clique (PPC) é a chamada fraude de clique, que será abordada em detalhe mais à frente. Este artigo visa estudar essa fraude sob uma ótica jurídica, fazendo, para isso, referência a alguns casos legais da fraude, apresentando, inclusive, os prejuízos financeiros em cada um dos casos. Pretende-se, ainda, analisar o impacto da fraude no direito brasileiro, levando em consideração a teoria geral dos contratos e o projeto de lei sobre crimes cibernéticos, substitutivo do Senado aos projetos de lei n. 76/2000 e 89/2003.

A RELEVÂNCIA DE SE ANUNCIAR NA INTERNET

Quando a Internet começou a ser utilizada efetivamente para fins comerciais, em meados dos anos 1990, milhares de novos *sites* nasceram e bilhões de dólares em capital de ventura fluíram por meio deles[7]. Nesse período, anunciar na Internet significava elaborar anúncios em *banner*, que são imagens de 728x90 *pixels* exibidas em quase todas as páginas na Internet de hoje. No fim dos anos 1990, esta forma de anunciar na Internet era extremamente lucrativa, e *sites* populares como o *Yahoo*! cobravam entre 30 e 100 dólares a cada mil exibições dos anúncios em *banners* em suas páginas[8]. Essas taxas de anúncio representavam boa parte do capital disponível na Internet, uma vez que a mesma já apresentava uma natural disposição para *marketing*: milhares de *sites* com milhões de acessos por mês. Desta forma, empresas como a *DoubleClick*[9] começaram a armazenar esses anúncios em repositórios de *banner*. O princípio econômico da "oferta e procura" começou a ser aplicado na Internet, de maneira que as taxas pagas por anúncios em *banners* começaram a flutuar. Surgiram as redes de anúncios *on-line*.

REDES DE ANÚNCIOS

Uma rede de anúncios *on-line* (ou, simplesmente, rede de anúncios) é uma empresa que conecta anunciantes a *sites* de Internet que querem publicar anúncios em suas páginas. O principal negócio das redes de anúncios é vender espaço para que um subconjunto do seu inventário total de anúncios apareça. Esse subconjunto pode ser visualizado de formas diferentes, incluindo espaços sublocados em *websites* de terceiros (publicadores de anúncio), em RSS *feeds*[10], em *blogs*, em aplicações de mensagens instantâneas, em *adwares*, em *e-mails* e em quaisquer outras fontes de comunicação na Internet. A forma dominante de exibição de anúncios ainda são *websites* de terceiros, que trabalham com redes de anúncios por uma taxa, ou recebem uma porcentagem das receitas obtidas pelo anúncio. Grandes *sites* de Internet que publicam anúncios vendem apenas parte do seu inventário de anúncios por meio dessas redes. Já *sites* menores normalmente associam todo o seu inventário por meio delas.

O mercado das redes de anúncios cresce de maneira exponencial. De acordo com Khan et al.[11], as 20 principais empresas deste mercado lucraram nada menos que 2 bilhões de dólares em 2007. Isto representa aproximadamente 13% do mercado total de anúncios, cuja previsão de crescimento beirava 18% em 2010. Tal crescimento levou a grandes investimentos na área por parte de diversas empresas. Em 2007, por exemplo, o Google comprou a *DoubleClick* por 3,1 bilhões de dólares.

7 SAGAR, C. **SEO: A Quick Primer on the Difference Between Ecommerce and Content Sites.** Disponível em: <https://www.openforum.com/idea-hub/topics/innovation/article/seo-a-quick-primer-on-the-difference-between-ecommerce-and-content-sites-chaitanya-sagar>. Acesso em: 04 dez. 2011.

8 O'REILLY, T. What is Web 2.0: **Design Patterns and Business Models for the Next Generation of Software**. p. 22.

9 O'REILLY, T. What is Web 2.0: **Design Patterns and Business Models for the Next Generation of Software**. p. 21.

10 LIU, Hongzhou; RAMASUBRAMANIAN, Venugopalan; SIRER, Emin Gün. Client Behavior and Feed Characteristics of RSS, A PublishSubscribe System for Web Micronews. In: **Internet Measurement Conference 5**. IMC´05, 5, Berkeley, California, Estados Unidos. Proceedings… Berkeley: UNENIX Association, 2005, p. 2.

11 KHAN, I. et al. **The Rise of Ad Networks:** An In-Depth Look at Ad Networks. Disponível em: <http://www.itsupplierindex.com/uploads/5_1277452962_JPMorgan.pdf>. Acesso em: 20 nov. 2011.

ISSN Eletrônico 2175-0491

PAGAMENTO POR CLIQUE

Também conhecido como *PPC advertising*, o pagamento por clique é, em síntese, um acordo entre empresas. O primeiro grupo de empresas, os publicadores, exibe em seus *sites links* contendo anúncios do segundo grupo, os anunciantes. Em troca, há uma cobrança por cada clique. Com o crescimento desta indústria, desenvolveu-se uma terceira entidade, a rede de anúncios, que passou a agir como mediadora entre publicadores e anunciantes. Neste novo modelo, quando um usuário comum da Internet visita a página de um publicador, é associado a um dos servidores da rede de anúncios por meio do seguinte esquema:

i) O usuário acessa o portal de um publicador de anúncios;

ii) O publicador possui na página a ser exibida uma requisição por anúncios, que é feita à rede de anúncios devida;

iii) A rede de anúncios retorna o conjunto de anúncios para o publicador;

iv) O publicador exibe o conteúdo de seu *site* contendo o conjunto de anúncios retornado pela rede;

v) O usuário clica em um desses anúncios;

vi) O *banner* contém *links* que redirecionam o usuário ao *site* de um dos anúnciantes;

vii) Ao verificar o clique, a rede de anúncios registra a cobrança junto ao anunciante;

viii) Parte da verba arrecadada junto ao anunciante é repassada para o publicador.

O sistema de divisão de lucros entre a rede de anúncios e os publicadores é, naturalmente, visto como um incentivo para a fraude de clique, pois a rede de anúncios ganha dinheiro ao realizar as cobranças originárias de cliques fraudulentos junto ao anunciante, e parte desse lucro ilícito é repassado ao publicador.

FRAUDE DE CLIQUE

Uma rede de anúncios *on-line* pode sofrer abusos de diferentes formas. Cada um dos modelos de receita descritos anteriormente (pagamento por clique, por exibição e por ação) está sujeito a fraudes correspondentes. Estas fraudes têm como principal consequência a redução do lucro dos anunciantes. Alguns exemplos dessas fraudes seriam[12]: a) fraude de exibição, quando requisições para *sites* anunciantes são realizadas sem a exibição efetiva dos anúncios; b) fraude de conversão, quando publicadores fraudulentos tentam obter receita a partir de ações produzidas artificialmente; e c) fraude de clique.

A fraude de clique ocorre quando requisições pelos endereços de Internet dos anúncios em exibição são realizadas sem intenção legítima. Quando detectados, esses cliques são classificados como inválidos. No entanto, como a intenção por trás de um clique em um anúncio na Internet é algo pessoal e subjetivo, que só pode ser explicada pelo usuário, nos sistemas de redes de anúncios atuais é impossível ter certeza absoluta de que um dado clique é fraudulento ou não[13]. Desta forma, os sistemas de redes de anúncios buscam armazenar sinais e evidências que serão posteriormente avaliadas caso haja suspeita de uma ação maliciosa. Assim, cliques suspeitos podem acabar sendo marcados como inválidos após esta análise, mas não há uma garantia acerca da totalidade do número de cliques fraudulentos que serão detectados e classificados como inválidos.

Quando cliques suspeitos são marcados como inválidos, o usuário que executou o clique ainda é redirecionado ao *site* do anunciante. Esta abordagem oferece dois benefícios:

i) O fraudador não recebe indício de que foi detectado como tal;

12 JAKOBSSON, Markus; RAZMAN, Zulfikar. **Crimeware:** Understanding New Attacks and Defenses. Londres: Addison-Wesley Professional, 2008, pp. 292-307.

13 TUZHILIN, Alexander. **The Lane's Gifts v. Google Report.** p. 16. Disponível em: <http:// googleblog. blogspot.com.br/pdf/Tuzhilin_Report.pdf >. Acesso em: 20 nov. 2011.

ii) Se um clique suspeito na verdade for legítimo (ou seja, a avaliação retornou um falso positivo), então a experiência do usuário com a rede de anúncios e com o anúncio em si não é impactada negativamente.

Como se pode imaginar, um alto número de falsos positivos é danoso para o publicador, que deixa de receber pelo anúncio que exibiu. Portanto, é fundamental que a rede de anúncios realize todos os esforços possíveis para minimizar o número de falsos positivos e, assim, balancear o aumento do lucro dos anunciantes com a prospecção de novos publicadores, de modo a desenvolver um relacionamento de qualidade com ambos.

É importante notar que nem todos os cliques marcados como inválidos são necessariamente fraudulentos. Cliques podem ser marcados como inválidos pelo simples interesse legítimo de uma rede de anúncios em aumentar o lucro de seus anunciantes. É o caso, por exemplo, de cliques repetidos ocasionados por um usuário que clicou duas vezes no mesmo anúncio.

Dois tipos de cliques inválidos que ocorrem por intenção maliciosa e, portanto, estão associados à prática da fraude de clique: são aqueles originados por concorrentes dos anunciantes e também os cliques de publicadores desonestos. Uma vez que os publicadores lucram com os eventos de clique nos anúncios exibidos em seus *sites*, é possível observar uma brecha para que publicadores gerem receita aumentando o número de cliques que seus *sites* geram[14]. No caso dos concorrentes dos anunciantes, existe a possibilidade de "simular" cliques nos anúncios destes, com o objetivo de onerar seu orçamento de *marketing*[15].

Os números envolvidos em fraude de clique são difíceis de quantificar. Existem diversas formas de se estimar a proporção de cliques falsos, que variam de 10% a 50%. Um estudo largamente citado da MarketingExperiments.com[16], ferramenta de pesquisa sobre *marketing on-line*, relatou que 29,5% dos cliques em três campanhas experimentais do Google em 2005 eram fraudulentos. Mesmo com números tão expressivos, as empresas de busca e muitos dos seus clientes argumentam que o problema em suas redes está sob controle. Entretanto, alguns observadores do mercado de anúncios na Internet, como a Holcomb, acreditam que a fraude de clique traz prejuízos da ordem de bilhões de dólares e tem potencial para destruir a indústria inteira[17].

Independentemente do número exato, a fraude de clique, hoje, está impregnada no negócio de anúncios pela Internet. Embora as ferramentas de busca procurem se defender de diferentes maneiras, os fraudadores tornam-se cada vez mais sofisticados, por meio da utilização de programas para automatização da fraude complexos, capazes de disfarçar, inclusive, a origem dos cliques.

SISTEMÁTICA DA FRAUDE DE CLIQUE

A forma mais simples da fraude de clique ocorre quando um usuário, ao iniciar um pequeno empreendimento na Internet, torna-se um publicador de anúncios e passa a clicar os endereços que aparecem em seu próprio *site* para gerar receita. Normalmente, o número de cliques e o seu valor são tão pequenos que a fraude não é detectada. O grande problema é, realmente, quando a fraude acontece em larga escala. Os envolvidos nesse tipo de esquema normalmente rodam *scripts* para simular que um usuário humano está clicando nos anúncios[18].

Obviamente, uma quantidade enorme de cliques originados de um único computador, de um pequeno grupo de computadores ou, ainda, de uma única região geográfica, parecerá suspeito para a rede de anúncios e para os anunciantes, bem como cliques originários de computador que reconhecidamente pertence ao publicador. Desta forma, uma pessoa que tenta realizar fraude em larga escala sozinha, em casa, certamente corre grande risco de ser descoberta.

14 ANUPAM, V. et al. On the Security of Pay-Per-Click and Other Web Advertising Schemes. In: **8th WWW International Conference on World Wide Web, 8**. 8th International Conference on World Wide Web. Toronto, Canadá, 1999. Proceedings… Amsterdam: Elsevier Science, 1999, pp. 3-5.

15 MANN, C. How Click Fraud Could Swallow the Internet. p.17.

16 ALT, Brian et al. **Click Fraud – Our Research**. Disponível em: <http://www.marketing experiments.com/ppc-seo-optimization/click-fraud.html>. Acesso em: 04 dez. 2011

17 ALT, Brian et al, **Click Fraud** – Our Research.

18 JAKOBSSON, Markus; RAZMAN, Zulfikar. **Crimeware**: Understanding New Attacks and Defenses. p. 363.

ISSN Eletrônico 2175-0491

Existe outro tipo de fraude, que transforma o tráfego de usuários reais em cliques inválidos e dificilmente é detectada, mesmo quando aplicados métodos de filtragem de padrões repetidos de endereços IP[19]. Tal ataque pode ser escondido dos usuários e camuflado de anunciantes e portais. Esta e outras técnicas que usam visitantes reais podem ser combinadas com o chamado tráfego incentivado, em que colaboradores de determinados *sites*, conhecidos como *paid to read* (ou PTR), recebem pequenas quantidades de dinheiro para, centenas de vezes por dia, visitar um *site*, clicar em palavras-chave ou, ainda, em resultados de pesquisa[20]. Alguns donos de *sites* PTR também são membros de ferramentas PPC, e enviam anúncios para seus usuários.

O crime organizado também pode fazer uso de fraude de clique usando códigos maliciosos em cavalos de troia (*trojans)*[21]. Esse artifício transforma o computador de usuários comuns, espalhados em diversas localidades geográficas, em uma espécie de "computador zumbi" que, esporadicamente, realiza ações indevidas. Lidar com casos envolvendo redes de pessoas espalhadas em diferentes países torna dificultosa a identificação de fraude para anunciantes, redes de anúncios e autoridades.

Existe ainda outra forma de fraude, chamada de *Impression Fraud*[22]. Trata-se de uma forma de manipular o sistema de busca de modo a aumentar a relevância de um determinado anúncio. A fraude consiste em realizar inúmeras pesquisas sobre uma mesma palavra-chave, sem nunca clicar no anúncio, fazendo com que seu índice de aceitação diminua. Isso faz com que anúncios mais caros, que deveriam aparecer nas primeiras páginas da pesquisa, deixem de ser exibidos em detrimento do anúncio mais barato, do fraudador.

IMPLICAÇÕES LEGAIS DA FRAUDE DE CLIQUE

Os problemas legais em torno da fraude de clique têm se proliferado desde os primórdios do PPC. Normalmente, quando algum fraudador é descoberto, a sua conta de PPC é desabilitada junto à rede de anúncio e, como um resultado, ele perde os pagamentos pendentes e potenciais. Entretanto, dependendo dos valores envolvidos, o caso pode acabar sendo direcionado para a justiça.

Quando alguém concorda com os termos de utilização de serviço de uma empresa de PPC, esta pessoa está assinando um contrato. Por meio desse acordo, as partes são obrigadas a cumprir as regras e as condições estabelecidas, e evitar quaisquer comportamentos proibidos. Se uma das partes comete uma fraude, abre-se uma brecha no contrato e, consequentemente, um precedente para disputa legal. Além disso, dependendo de certas circunstâncias, a violação consciente do contrato pode implicar penalidades criminais, como no caso de flagrante de delito no exercício da fraude de clique. Este seria o caso da detecção da fraude por meio da utilização, por parte da autoridade policial, de programas que exponham a perpetração[23]. Os resultados dessa ação podem ser usados como evidências contra o perpetrador.

Em algumas jurisdições internacionais, como a do Estado da Califórnia, cometer fraude de clique é considerado um ato criminoso[24]. Isto significa que qualquer pessoa que seja flagrada no ato de realizar a fraude de clique pode ser processada e condenada a uma pena de prisão. A duração da pena vai variar com a soma obtida ilegalmente: quanto mais dinheiro o fraudador consiguir, maior será a sentença. Normalmente, as possibilidades de sucesso em um caso de fraude de clique estão associadas ao uso de *scripts* de computador para automatizar o clique nos anúncios. Assim, quando apresentadas evidências geradas por programas de rastreamento, as cortes americanas dificilmente olharão de maneira favorável ao réu. Tais evidências são consideradas indicações fortíssimas de que o réu cometeu a fraude premeditadamente.

19 ANUPAM, V. et al. **On the Security of Pay-Per-Click and Other Web Advertising Schemes**. p. 6.

20 MANN, C. **How Click Fraud Could Swallow the Internet**. p. 18.

21 JAKOBSSON, Markus; RAZMAN, Zulfikar. **Crimeware**: Understanding New Attacks and Defenses. p. 23.

22 JAKOBSSON, Markus; RAZMAN, Zulfikar. **Crimeware**: Understanding New Attacks and Defenses. pp. 355-356.

23 JAKOBSSON, Markus; RAZMAN, Zulfikar. **Crimeware**: Understanding New Attacks and Defenses. p.363.

24 URBACH, R. R.; KIBEL, G. A. **Adware/Spyware**: An Update Regarding Pending Litigation and Legislation. Intelectual Property & Technology Law Journal. Chapel Hill, p. 12, 15 jun. 2004, p. 14.

Semelhantemente, quando se descobre que a obtenção de grandes lucros decorrentes de uma campanha de PPC deve-se ao uso de fraude, a rede de anúncio provavelmente iniciará um processo civil para recuperar os pagamentos impróprios. O caso pode resultar em um julgamento extenso, especialmente se a rede de anúncios também buscar sanções punitivas de caráter criminal.

Existe, ainda, a perspectiva do anunciante na fraude de clique, que muitas vezes é ignorada na literatura sobre o assunto. O anunciante pode processar a empresa de PPC para recuperar os pagamentos realizados como resultado de uma fraude de clique por parte de terceiros. Foi o que aconteceu no caso do acordo de 90 milhões de dólares entre o Google e a Lane's Gifts & Collectibles[25], depois que esta provou ter pagado ao *site* milhões de dólares por cliques de origem fraudulenta. Uma empresa como o Google certamente tem uma motivação em perseguir agressivamente na justiça aqueles que cometem a fraude de clique no seu ambiente de anúncios, já que pode acabar sendo ré em processo que tenha como vítima seus clientes, os anunciantes. Infelizmente, na prática, o Google tem se mostrado relutante em disponibilizar informações específicas sobre o tráfego de dados associado aos cliques[26]. Isto certamente deve ser uma preocupação para os anunciantes, que podem estar sendo cobrados arbitrariamente sem receber informações devidamente acerca do detalhamento da cobrança nem sobre como proteger suas campanhas no futuro. Normalmente, a cobrança envolve grandes quantias de dinheiro e é realizada junto à fatura de cartões de crédito dos anunciantes, com uma simples linha de identificação.

CASOS LEGAIS

Há diversas disputas sobre a fraude de clique que resultaram em um grande número de processos legais. Em um caso notório, descrito por Davis[27], o Google (que agia como rede de anúncios) venceu um processo contra uma empresa do Texas chamada de Auction Experts (que agia como publicador). O Google acusava a Auction Experts de pagar pessoas para clicar nos anúncios que apareciam no seu *site*, causando um prejuízo de 50 mil dólares aos anunciantes.

Em julho de 2005, o *Yahoo*! entrou em acordo em um processo no qual era acusado de não ter prevenido a fraude de clique adequadamente. O *site* teve que desembolsar 4,5 milhões de dólares em taxas legais para os queixosos. Este caso é mais bem explicado por Ryan[28].

Em 2004, um morador da Califórnia criou o chamado Google Clique[29], um programa que, de acordo com o criador, tornaria possível que o Google fosse fraudado em milhões de dólares. O autor foi preso e declarado culpado por chantagem, condenado a pagar 150 mil dólares e forçado a entregar o programa à empresa. Acredita-se que esta foi a primeira prisão por fraude de clique. No entanto, as acusações foram retiradas, sem explicação, em 22 de novembro de 2006[30]. Tanto o Google quanto o escritório de procuradores dos Estados Unidos se recusaram a comentar o caso. De acordo com Elgin[31], o Google não quis cooperar com o processo, já que seria obrigado a: i) expor publicamente suas técnicas de detecção de fraude de clique; ii) admitir publicamente que lucra (por meio dessas técnicas ou não) com cliques fraudulentos.

O relatório de Alexander Tuzhilin[32], produzido como parte do acordo entre a Google e a The Lane's Gifts & Collectibles, possui uma discussão detalhada sobre os métodos de detecção de fraude de clique. Em particular, o relatório define que o "problema fundamental de cliques inválidos (fraudulentos)" é que:

25 TUZHILIN, Alexander. **The Lane's Gifts** v. Google Report. p. 15.

26 DAVIS, W. **Google Wins $75,00 in Click Fraud Case**. Disponível em: <http://www.mediapost.com/publications/index.cfm?fuseaction=Articles.san&s=31772>. Acesso em: 04 set. 2011.

27 DAVIS, W. Google Wins $75,00 in Click Fraud Case.

28 RYAN, K. M. **Big Yahoo Click Fraud Settlement**. Disponível em: <http://www.imediaconnection.com/content/10294.asp>. Acesso em: 04 set. 2011.

29 NARAINE, R. **Feds Arrest Google Extortionist**. Disponível em: <http://www.internetnews.com/bus-news/article.php/3329281>. Acesso em: 11 ago. 2010, p. 1.

30 ELGIN, B. **The Vanishing Click Fraud Case**. p.1. Disponível em: <http://www.businessweek.com/technology/content/dec2006/tc20061204_923336.htm?campaign_id=bier_tcc.g3a.rssd1204f>. Acesso em: 08 nov. 2011.

31 ELGIN, B. **The Vanishing Click Fraud Case**. pp.1-2.

32 TUZHILIN, Alexander. **The Lane's Gifts** v. Google Report. pp. 15-47.

ISSN Eletrônico 2175-0491

i) Não há uma definição conceitual de cliques inválidos que possa ser operacionalizada (com a exceção de casos óbvios);

ii) Uma definição operacional não pode ser totalmente revelada ao público em geral, uma vez que possibilitará que usuários maliciosos utilizem a informação para realizar a fraude de clique. Como já se falou, se as técnicas de detecção dos cliques inválidos não são reveladas, anunciantes não terão como se opor à cobrança de determinados cliques.

Existe atualmente, nos Estados Unidos, um considerável *lobby* da indústria de PPC para que leis mais rígidas sejam definidas para lidar com esse problema. Espera-se que essas leis venham a descrever casos que não podem ser especificados em contratos. Um grande número de empresas está desenvolvendo soluções viáveis para a identificação da fraude de clique por meio de relações intermediárias com redes de anúncio. Tais soluções subdividem-se em duas categorias[33]:

i) Análise judicial dos arquivos de histórico, originados nos servidores dos anunciantes: essa análise de dados requer uma investigação profunda da fonte do tráfego de dados e do seu comportamento. A ideia é desenvolver padrões para análise e compará-los com os dados disponíveis nos servidores da rede de anúncios. O problema com esta abordagem é que ela confia na idoneidade das ferramentas de busca, que passam a ter a responsabilidade de identificar a fraude;

ii) Confirmação de terceiros: ao visitar as páginas dos anunciantes, o visitante recebe um *cookie*, que grava suas informações como histórico em um banco de dados e disponibiliza-o para *download*[34]. Por meio desse histórico, é possível identificar um conjunto de cliques suspeitos e expor as razões para a desconfiança. Comparando-se essas informações às do histórico dos anunciantes, tem-se um conjunto de evidências mais convincente, que pode ser apresentado à rede de anúncios para verificação. O problema com esse tipo de solução está no fato de que ele pode visualizar apenas uma parte do tráfego na rede. Logo, dificilmente se identificará a amplitude total de padrões de fraude de clique, que pode afetar muitos anunciantes ao mesmo tempo.

A FRAUDE DE CLIQUE E O DIREITO BRASILEIRO

Nos casos envolvendo o direito digital, em especial aqueles relacionados às práticas de natureza criminal, a diferença entre realidade social e casos previstos no ordenamento brasileiro é flagrante. Não obstante, um dos temas mais relevantes nas atuais discussões por parte dos operadores do direito diz respeito aos crimes praticados no ambiente virtual, isto é, na Internet. Entre as questões mais comumente referenciadas está a que diz respeito à tipificação e à imputação penal daqueles que praticam delitos como a fraude de clique, ou seja, que utilizam o espaço virtual para cometer delitos de maneria intencional.

Na verdade, os casos de fraude de clique podem ser vistos como um dos melhores exemplos de como o direito tem dificuldades de acompanhar a evolução da sociedade, devido à ausência de meios que refutem condutas delituosas contra normas penais pertencentes ao ordenamento jurídico. Em casos como a fraude de clique, há uma ausência de meios reguladores, o que deve gerar uma preocupação precípua: enquanto a sociedade caminha rapidamente a uma tendência de globalização, sem fronteiras físicas, o direito ainda esbarra em uma inoficiosidade, com relação ao ordenamento jurídico atualmente vigente no Brasil.

Não se podem ignorar os crimes pela Internet no Brasil. De acordo com Lobo[35], por dia, 77 mil internautas brasileiros são vítimas de alguma variação de crime virtual. Este número seria traduzido em prejuízos financeiros da ordem de 15,3 bilhões de reais ao ano. A inexistência de

33 METWALLY, A.; AGRAWAL D.; ABBADI, E. DETECTIVES: Detecting Coalition Hit Inflation Attacks in Advertising Networks Streams. In: **International World Wide Web Conference**. 16th WWW International World Wide Web Conference. Alberta, Canada, 2007. Proceedings... Nova Iorque: ACM Digital Library, 2007, pp. 242-247.

34 DOYLE, Eric. **Not All Spyware is as Harmless as Cookies:** Block it or Your Business Could Pay Dearly. Disponível em: <http://www.computerweekly.com/Articles/2003/11/27/198884/Not-all-spyware-is-as-harmless-as-cookies. htm>. Acesso em: 23 out. 2011.

35 LOBO, Ana Paula. **Crimes cibernéticos custaram R$ 15,3 bilhões no Brasil**. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=27750&sid=18>. Acesso em: 03 dez. 2011.

uma legislação brasileira sobre os crimes virtuais propriamente ditos tem dificultado a persecução criminal de tais delitos. Além disso, a falta de normas claras sobre crimes de computador também produz controvérsias doutrinárias e jurisprudenciais.

Neste sentido, podem-se identificar diversas iniciativas para se definir uma legislação penal e processual para endereçar os problemas envolvendo bens jurídicos inerentes à sociedade de informação. Por exemplo, ao examinar a questão da cópia de senhas bancárias para a obtenção de vantagem patrimonial ilícita, o STJ entendeu que esta conduta caracteriza crime de furto qualificado pela fraude, previsto no art. 155, §4º, inciso II, do Código Penal (pena de 2 a 8 anos de reclusão e multa), afastando o enquadramento no art. 171 do Código Penal (CP), pelo delito de estelionato (pena de reclusão de 1 a 5 anos e multa). A questão foi decidida no conflito negativo de competência 67.343/GO, 3ª Seção, de 28 de março de 2007, o que por si só revela a falta de dispositivos penais. No caso concreto, divergia-se se o tipo penal incidente se tratava de furto ou estelionato e, assim, não havia consenso sobre a competência para a ação penal. Destaca-se o relato da Ministra Laurita Vaz: "Conflito negativo de competência. Penal e processo penal. Fraude eletrônica na Internet. Transferência de numerário de conta da Caixa Econômica Federal. Furto mediante fraude que não se confunde com estelionato".

Infelizmente, ainda não existem números concretos sobre a fraude de clique no Brasil. Estudo da *Click Fraud Network*[36], no entanto, cita o Brasil como um dos países que possuem alta taxa de risco para campanhas *on-line*. Essa ausência de números se reflete nas contínuas iniciativas de tipificação de crimes virtuais do legislativo brasileiro. Dentre elas se destaca a PL sobre Crimes Cibernéticos[37], substitutivo do Senado aos projetos de lei n. 76/2000 e 89/2003, que tipifica crimes informáticos.

SUBSTITUTIVO AOS PROJETOS DE LEI N. 76/2000 E 89/2003

Uma análise extensiva a respeito do Projeto de Lei sobre Crimes Cibernéticos foi realizada por Vladimir Aras[38]. Não é escopo desse artigo realizar uma análise semelhante, extensiva, de maneira que se vai limitar ao estudo de alguns dos dispositivos que influenciam diretamente a questão da fraude de clique.

Uma das versões do substitutivo ao PLS 76/2000 buscava tipificar o chamado furto eletrônico no artigo 155, §4º, inciso V do CP, com pena de reclusão de 2 a 8 anos e multa. O substitutivo aprovado no Senado em julho de 2008 abandonou inteiramente o tratamento do furto eletrônico propriamente dito. De maneira simples e direta: não se cuidará do furto eletrônico de maneira própria, por se entender que o mesmo se trata de crime impróprio, podendo ser enquadrável aos esquemas típicos das formas qualificadas de furto, seja com fraude ou mediante destreza. Vladimir Aras[39] não acredita que essa decisão por si só seja errada, especialmente se comparada com a tipificação do furto eletrônico nos códigos penais de outros países.

O *captio* do artigo 22 do substitutivo associa ao responsável pelo provimento de acesso a rede de computadores uma série de obrigações. Como já se viu, a fraude de clique em sua versão de larga escala pode ser executada por meio de programas que simulam cliques de maneira automática. A maior parte desses programas, por questão de continuidade de ação, raramente será executada em um computador pessoal. Na verdade, o fraudador de larga escala fará uso de um serviço de hospedagem de conexão e utilizará tal serviço para rodar o programa, remotamente. O artigo 22 não fala de obrigações legais dos provedores de hospedagem, de modo que o objetivo da lei pode acabar sendo frustrado, no caso em que os dados requeridos para iniciar a ação penal não

36 IDG NOW. **Fraude de clique atinge 15,8% das campanhas online no 2o trimestre**. Disponível em: <http://idgnow.uol.com.br/internet/2007/07/19/idgnoticia.2007-07-19.4914743477>. Acesso em 20 nov. 2011.

37 ARAS, V. O projeto de lei dos cibercrimes (PLS 76/2000): crítica ao substitutivo aprovado no Senado. **Revista ANPR Online**, Brasília, v.1, n.8, jan./jun. 2009, p. 1. Disponível em: <http://www.anpr.org.br/portal /components/com_anpronline/media/Artigo_Projeto de lei dos cibercrimes - PLS 76 de 2000.doc>. Acesso em: 17 out. 2011.

38 ARAS, V. **O projeto de lei dos cibercrimes** (PLS 76/2000): crítica ao substitutivo aprovado no Senado. pp. 7-15.

39 ARAS, V. **O projeto de lei dos cibercrimes** (PLS 76/2000): crítica ao substitutivo aprovado no Senado. p. 5.

ISSN Eletrônico 2175-0491

se encontrem disponíveis no provedor de acesso. Este será o caso típico de um perpetrador que faça uso de um cibercafé, ou de uma *lan house*, para enviar o *script* para execução remota em um serviço de hospedagem virtual, que é onde de fato se consuma a conduta criminosa.

A análise de tráfego e histórico de ações é uma das formas mais utilizadas para a detecção da fraude de clique. No inciso I do mesmo artigo, observa-se o prazo de 3 anos para a guarda de histórico de tráfego de conexão. Nas suas versões primitivas, o projeto previa a guarda por 5 anos. Essa redução se deu provavelmente devido a pressões por parte das entidades representativas dos provedores de acesso, já que os históricos de tráfego geram uma quantidade enorme de dados e um grande gasto de recursos por parte dos provedores e das empresas de telecomunicações. Na verdade, embora a manutenção dos dados de tráfego possa ser prorrogada mediante ordem judicial, em regra, o prazo de 3 anos deve ser suficiente para a cópia de dados e perícia de computação forense. No entanto, alguns dos crimes objetos do substitutivo, ou até mesmo os crimes previstos em outros diplomas (como seria o caso do furto eletrônico), têm penas superiores a 4 anos de reclusão. É o caso do art. 171, §2º, VI; do art. 163-A, §§1º e 2º; do art. 265; do art. 297 e do art. 298, do CP. Em todas essas situações, a prescrição da pretensão punitiva em abstrato ocorrerá em 12 anos, pela regra do art. 109, inciso III, do CP. Como é de se imaginar, pode ocorrer o caso de que uma investigação acerca de crime ainda não prescrito tenha dificuldades para acessar dados de conexão que tenham sido excluídos por ocasião da expiração do prazo de três anos, dificultando a identificação do autor da fraude.

No inciso II do artigo 22, observa-se outra obrigação aos provedores, a de preservar imediatamente todos os dados úteis à persecução penal. O provedor, nesse caso, apenas mediante requisição judicial, deve preservar informações, tais como os dados cadastrais e outros elementos probatórios por um prazo a ser estabelecido pela autoridade judicial requisitante. Neste caso, recai-se em situações nas quais a guarda dos dados de conexão não permite rastrear o autor do ilícito. Mais uma vez, no caso de fraude de clique decorrente da utilização de Internet em cibercafés, ou por meio de redes sem fio públicas (como zonas de *wi-fi* em *shopping centers*), a identificação do fraudador dependerá de outros instrumentos de investigação (como câmeras de segurança ou dados de cartão de crédito).

Outro problema em potencial diz respeito a mais uma especificidade da fraude de clique. O inciso I do artigo 22 utiliza expressões como "objetivo de provimento de investigação pública formalizada" e "cujo fornecimento será feito exclusivamente à autoridade investigatória". Pela análise realizada anteriormente neste mesmo trabalho, destacam-se os papéis envolvidos na fraude de clique, que dificilmente envolverá uma autoridade pública. Assim, a redação exclui o querelante do rol do substitutivo, que é possível autor da ação penal privada, e não "autoridade investigatória". Entende-se que esta redação simplesmente impede o acesso aos dados de tráfego em causas cíveis não públicas, exatamente o caso da maioria esmagadora das fraudes de clique.

Para finalizar esta breve análise, é interessante destacar um notório silêncio do projeto em definir o que venham a ser "dados cadastrais". O conceito de dados cadastrais não pode se confundir com o de dados de tráfego nem com os dados de empacotamento de informação, que são transmitidos durante a seção de conexão. Normalmente, tais dados deveriam dizer respeito ao nome, ao CPF ou à identidade, endereço, telefone, *e-mail*, profissão e filiação, no mínimo. O substitutivo, nesse caso, apresenta certo atraso em relação aos outros projetos de lei que o antecederam – o PLS 209/2003, por exemplo, que trata da lei de lavagem de dinheiro, permite à autoridade policial e ao Ministério Público acesso aos dados cadastrais do investigado que sejam oriundos da "Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de Internet e administradores de cartão de crédito".

A TEORIA DOS CONTRATOS E A FRAUDE DE CLIQUE

De acordo com Maria Helena Diniz[40], pode-se definir contrato como o "acordo de duas ou mais vontades, na conformidade da ordem jurídica, destinado a estabelecer uma regulamentação de interesses entre as partes". Juridicamente falando, pode-se dizer que um contrato é um negócio jurídico que gera obrigações para as partes. Na fraude de clique envolvendo participantes de uma

40 DINIZ, Maria Helena. **Curso de direito civil brasileiro**. São Paulo: Saraiva, 2008, p. 30.

rede de anúncios, a teoria dos contratos desempenha papel fundamental quanto à definição de mecanismos de reembolso e de cursos de ação cíveis, no caso de condutas fraudulentas.

Os contratos para utilização de serviços de PPC são de natureza virtual, firmados por meio da aceitação de termos exibidos em uma página de Internet e por meio da interação com o potencial usuário do serviço, seja ele o publicador de anúncios, o anunciante, e a rede de anúncios. No Brasil, ainda não há legislação específica para os contratos virtuais, de maneira que é necessário utilizar as leis constantes no nosso ordenamento jurídico e as adaptar para o universo dos anúncios na Internet, procurando identificar possíveis lacunas. É interessante também analisar a identificação das partes no universo virtual, tanto no momento da efetivação do contrato como em uma eventual lide.

O momento da efetivação de um contrato virtual depende de alguns fatores comuns aos contratos regulares[41]: vontade das partes de modificar deveres e obrigações; terem as partes pressupostos jurídicos para exercer o contrato; o proponente, após a proposição, deve receber a aceitação do aceitante; as partes devem se guiar sobre os princípios de boa-fé e probidade, respeitando a função social do contrato. Os contratos virtuais podem ser considerados contratos nos quais as partes estão presentes por ocasião de comércio na Internet, já que trocam informações em tempo real. Reforçando este entendimento, pode-se afirmar que o código do consumidor se aplica aos contratos virtuais de maneira análoga, de maneira que ele é válido desde que não seja contrário ao direito[42].

Uma das questões principais para se aferir a veracidade, legitimidade e regularidade do vínculo obrigacional em um contrato virtual, consiste na identificação das partes envolvidas na operação remota[43]. Em geral, as redes de anúncios são empresas de grande porte que normalmente possuem escritórios fixos, sendo, portanto, de fácil localização para uma eventual lide. No entanto, existem *sites* que não possuem lojas ou escritórios fixos, sendo somente virtuais. Neste caso, o interessado em realizar qualquer tipo de negociação na rede precisa tomar cuidados para garantir que suas informações chegarão efetivamente aos proprietários da loja virtual, por meio da utilização de um certificado digital[44].

A grande implicação da teoria dos contratos na fraude de clique relaciona-se com a possibilidade de se encerrar e de se executar um contrato por ocasião que o torne anulável. Um contrato anulável é aquele que foi celebrado por incapaz, ou que tenha sido viciado por um erro, dolo, coação, estado de perigo, lesão ou fraude contra credores[45]. Neste sentido, chama-se atenção para o dolo e para fraude contra credores, verificáveis em casos de fraude de clique. O dolo significa o uso de astúcia com o objetivo de enganar. Assenta-se na má-fé e na indução ao erro. As ações dolosas têm por objetivo o não cumprimento da promessa. O agente visa obter o resultado ilícito, que seja contrário ao direito firmado por acordo. Ou seja, o objetivo seria conduzir a outra parte ao erro. Verifica-se a possibilidade de dolo na fraude de clique com posterior execução e anulação do contrato quando houver, por exemplo, má-fé por parte da rede de anúncios na definição dos termos do contrato, possivelmente induzindo os anunciantes ou publicadores à fraude.

No entanto, a forma mais natural de anulação e execução de contratos decorrente de fraude de clique estaria associada à categoria de fraude contra credores. Esta ocorreria no ato de falseamento ou de ocultação da verdade com intenção de prejudicar ou enganar a outra parte. Trataria-se da manobra realizada com o objetivo de fraudar terceiros, com o intuito de fugir à incidência da lei e aos seus efeitos. A fraude contra credores é o artifício malicioso empregado para prejudicar terceiros despidos de garantias reais. Para caracterizar uma fraude, basta que o devedor tenha consciência de que seu ato irá prejudicar ou trazer prejuízos a um terceiro. Os atos viciados por fraude são anuláveis por meio da Ação Pauliana[46], pela qual os bens transferidos de maneira fraudulenta retornam ao patrimônio do credor. Os casos mais comuns da fraude de clique envolvendo contratantes se encaixam nessa categoria.

41 VENOSA, Silvio de Salvo. **Direito Civil**: Teoria Geral das Obrigações e Teoria Geral dos Contratos. São Paulo: Atlas, 2007, p. 549.

42 BRASIL, Angela Bittencourt. **Contratos Virtuais**. Disponível em: <http://www.jurisdoctor.adv.br/artigos/contvirt.htm>. Acesso em: 04 dez. 2011.

43 DIAS, Jean Carlos. **O direito contratual no ambiente virtual**. Curitiba: Juruá, 2004, p. 82.

44 PEREIRA, Maria Neuma. **Processo Digital** – A Tecnologia Aplicada na Solução de Conflitos. São Paulo: Biblioteca 24horas, 2011, p. 41.

45 MIRANDA, M. B. Teoria Geral dos Contratos. **Revista Virtual Direito Brasil**, São Paulo, v.2, n.2, jul./dez, p. 8. 2009. Disponível em: <http://www.direitobrasil.adv.br/artigos/cont.pdf>. Acesso em: 03 dez. 2011.

46 MIRANDA, M. B. Teoria Geral dos Contratos. p. 10.

ISSN Eletrônico 2175-0491

Ressalta-se que a fraude de clique não se configura apenas quando há contrato entre o fraudador e o fraudado. É possível, por exemplo, que o concorrente de determinada organização que participe de um esquema de PPC realize a fraude de clique contra uma rede da qual ele não faça parte para gerar prejuízos para o seu concorrente, conforme se detalhou anteriormente.

CONSIDERAÇÕES FINAIS

Em um mundo ideal, o direito evoluiria ao lado da sociedade e em uma frequência sincronizada, de ajuste contínuo. Na prática, até mesmo devido ao processo legal em si, o direito sempre se encontra alguns passos atrás da realidade social, sempre em mora na relação com a sociedade. Isto se deve, em parte, ao modelo legislativo que se possui, por vezes intencionalmente oneroso, que acaba elevando à categoria de legais normas que por vezes são promulgadas já sem eficácia prática. Além disso, o advento da chamada sociedade da informação[47], na qual o progresso técnico-científico acontece em ritmo extremamente acelerado nos diversos ramos da ciência moderna, torna ainda mais difícil ao direito o acompanhamento da evolução dessa mesma sociedade.

Não se pode mais fechar os olhos para a realidade da sociedade da informação, nem se pode deixar de enxergar as potencialidades da Internet para aqueles que a utilizam. Ao mesmo tempo, relações virtuais geram negócios jurídicos, tais como contratos, e o direito precisará se apressar para regular transações eletrônicas e crimes cometidos no ambiente virtual. Na maioria das vezes as normas constantes no ordenamento jurídico nacional podem, de forma analógica, ser utilizadas no universo digital, mas não há uma garantia que tal interpretação analógica se aplicará à totalidade dos fenômenos eletrônicos. Na verdade, considerando especificamente a questão dos contratos, pode-se dizer que os mesmos só terão sua plenitude quando forem feitos com total segurança, utilizando mecanismos como certificação digital[48]. Assim, sua sobrevivência dependerá não só do desenvolvimento tecnológico, mas também da atuação legislativa necessária para levar o país à nova dimensão que se aproxima no âmbito mundial.

Neste contexto, um dos negócios mais rentáveis atualmente na Internet é o de anúncios *on-line*. Esta área, embora bastante recente, têm atraído o foco de inúmeras pesquisas acadêmicas, sinalizando grandes perspectivas de crescimento. Destaca-se neste trabalho o foco dado à necessidade de se combater o problema da fraude de clique como requisito fundamental para a continuidade da publicidade na Internet, que, por sua vez, torna-se cada vez mais relevante para o mundo dos negócios. Esse trabalho busca contribuir com o detalhamento da sistemática da fraude de clique, ainda pouco pesquisada na literatura acadêmica, embora tão presente no dia a dia das organizações brasileiras.

Como trabalhos futuros, pode-se destacar a possibilidade de duas vertentes básicas de trabalho:

i) Uma discussão futura acerca da possibilidade de utilização de metodologias que auxiliem na prevenção da fraude de clique, em vez da simples detecção após a ocorrência. Este seria um trabalho que necessitaria de uma colaboração multidisciplinar para explorar as potencialidades dos sistemas de informação envolvidos na sistemática das redes de anúncio. O aumento do sentimento de segurança para anunciantes é importantíssimo para a consolidação deste mercado;

ii) Uma proposta de modificação da redação do substitutivo do Senado para a PLS 76/2000 e 89/2003 para tipificar particularidades dos contratos virtuais firmados pelos participantes de uma rede de anúncios. Acredita-se ser necessário caracterizar criminalmente a fraude de clique, se não como tipo próprio, no mínimo como variação do crime de furto, e mapear suas implicações nas diversas áreas do direito, tais como civil, penal e empresarial. O fundamento para essa caracterização encontra-se na complexidade por trás deste modelo de negócios, que se buscou explicitar anteriormente neste artigo.

Com o grande avanço tecnlógico e a necessidade cada vez maior de utilização da grande rede, é mister que os legisladores discutam, elaborem e votem os projetos de lei, de maneira a tornar o

47 DUPAS, Gilberto. **Ética e poder na sociedade da informação**: de como a autonomia das novas tecnologias obriga a rever o mito de progresso. São Paulo: UNESP, 2000, p. 33.

48 DIAS, Jean Carlos. **O direito contratual no ambiente virtual**. p. 86.

universo da Internet um espaço seguro para os contratos e, consequentemente, para o comércio mundial, com normas específicas e a tipificação de crimes próprios. Esta é a única maneira de dirimir litígios decorrentes dos negócios jurídicos virtuais. São muitos os que acreditam que podem cometer a fraude de clique sem serem descobertos. Entretanto, caso sejam, as implicações legais podem ser significativamente severas. A esperança é que a mera possibilidade de tais implicações seja suficiente para dissuadir um grande número pessoas da realização de fraude, reduzindo, assim, os casos de fraude de clique ao longo do tempo.

REFERÊNCIAS

ALT, Brian et al. **Click Fraud – Our Research**. Disponível em: <http://www.marketingexperiments .com/ppc-seo-optimization/click-fraud.html>. Acesso em: 04 dez. 2011.

ANUPAM, V. et al. On the Security of Pay-Per-Click and Other Web Advertising Schemes. In: **8th WWW International Conference on World Wide Web, 8***.* 8th International Conference on World Wide Web. Toronto, Canada, 1999. Proceedings… Amsterdã: Elsevier Science, 1999.

ARAS, V. O projeto de lei dos cibercrimes (PLS 76/2000): crítica ao substitutivo aprovado no Senado. **Revista ANPR Online**, Brasília, v.1, n.8, jan./jun. 2009. Disponível em: <http://www.anpr.org.br/portal/components/com_anpronline/ media/Artigo_Projeto de lei dos cibercrimes - PLS 76 de 2000.doc>. Acesso em: 17 out. 2011.

BRASIL, Angela Bittencourt. **Contratos Virtuais**. Disponível em: <http://www.jurisdoctor.adv.br/ artigos/contvirt.htm>. Acesso em: 04 dez. 2011.

DAVIS, W. **Google Wins $75,00 in Click Fraud Case**. Disponível em: <http:// www.mediapost.com/publications/index.cfm?fuseaction=Articles.san&s=31772>. Acesso em: 04 set. 2011.

DIAS, Jean Carlos. **O direito contratual no ambiente virtual**. Curitiba: Juruá, 2004.

DINIZ, Maria Helena. **Curso de direito civil brasileiro**. São Paulo: Saraiva, 2008.

DOYLE, Eric. **Not All Spyware is as Harmless as Cookies**: Block it or Your Business Could Pay Dearly. Disponível em: <http://www.computerweekly.com/ Articles/2003/11/27/198884/Not-all-spyware-is-as-harmless-as-cookies.htm>. Acesso em: 23 out. 2011.

DUPAS, Gilberto. **Ética e poder na sociedade da informação**: de como a autonomia das novas tecnologias obriga a rever o mito de progresso. São Paulo: UNESP, 2000.

ELGIN, B. **The Vanishing Click Fraud Case**. Disponível em: <http://www. businessweek.com/technology/content/dec2006/tc20061204_923336.htm?campaign_id=bier_tcc.g3a.rssd1204f>. Acesso em: 08 nov. 2011.

GOODMAN, Andrew. **Winning Results with Google AdWords**. New York: McGraw-Hill, 2008.

IDG NOW. **Fraude de clique atinge 15,8% das campanhas online no 2o trimestre**. Disponível em: <http://idgnow.uol.com.br/internet/2007/07/19/idg noticia.2007-07-19.4914743477>. Acesso em 20 nov. 2011.

JAKOBSSON, Markus; RAZMAN, Zulfikar. **Crimeware: Understanding New Attacks and Defenses**. Londres: Addison-Wesley Professional, 2008.

JUSTO, Antonio Santos. O direito brasileiro: raízes históricas. **Revista Brasileira de Direito Comparado**, Rio de Janeiro, v.20, n.1, jan 2011. Disponível em: <http://www.estig.ipbeja.pt/~ac_direito/dir_bras_raiz_hist.pdf>. Acesso em: 04 dez. 2011.

KHAN, I. et al. **The Rise of Ad Networks:** An In-Depth Look at Ad Networks. Disponível em: <http://www.itsupplierindex.com/uploads/5_1277452962_JP Morgan.pdf>. Acesso em: 20 nov. 2011.

LIU, Hongzhou; RAMASUBRAMANIAN, Venugopalan; SIRER, Emin Gün. Client Behavior and Feed Characteristics of RSS, A PublishSubscribe System for Web Micronews. In: **Internet Measurement Conference 5**. IMC´05, 5, Berkeley, California, Estados Unidos. **Proceedings...** Berkeley: UNENIX Association, 2005.

LOBO, Ana Paula. **Crimes cibernéticos custaram R$ 15,3 bilhões no Brasil**. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start. htm?infoid=27750&sid=18>. Acesso em: 03 dez. 2011.

ISSN Eletrônico 2175-0491

MANN, C. How Click Fraud Could Swallow the Internet. **Wired Magazine**. São Francisco, v.14, n.1, pp 17-20, 2006.

METWALLY, A.; AGRAWAL D.; ABBADI, E. DETECTIVES: Detecting Coalition Hit Inflation Attacks in Advertising Networks Streams. In: **International World Wide Web Conference**. 16th WWW International World Wide Web Conference. Alberta, Canada, 2007. **Proceedings....** Nova Iorque: ACM Digital Library, 2007.

MIRANDA, M. B. Teoria Geral dos Contratos. **Revista Virtual Direito Brasil**, São Paulo, v.2, n.2, jul./dez. 2009. Disponível em: <http://www.direitobrasil.adv. br/artigos/cont.pdf>. Acesso em: 03 dez. 2011.

NARAINE, R. **Feds Arrest Google Extortionist**. Disponível em: <http://www. internetnews.com/bus-news/article.php/3329281>. Acesso em: 11 ago. 2010.

O'REILLY, T. What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. **Communications & Strategies**, v.1, n.65, jan./mar. 2007. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm? abstract_id=1008839>. Acesso em: 23 out. 2011.

PEREIRA, Maria Neuma. **Processo Digital** – A Tecnologia Aplicada na Solução de Conflitos. São Paulo: Biblioteca 24horas, 2011.

RYAN, K. M. **Big Yahoo Click Fraud Settlement**. Disponível em: <http://www. imediaconnection.com/content/10294.asp>. Acesso em: 04 set. 2011.

SAGAR, C. **SEO:** A Quick Primer on the Difference Between Ecommerce and Content Sites. Disponível em: <https://www.openforum.com/idea-hub/ topics/innovation/article/seo-a-quick-primer-on-the-difference-between-ecommerce-and-content-sites-chaitanya-sagar>. Acesso em: 04 dez. 2011.

TUZHILIN, Alexander. **The Lane's Gifts v. Google Report.** p. 16. Disponível em: <http://googleblog.blogspot.com.br/pdf/Tuzhilin_Report.pdf >. Acesso em: 20 nov. 2011.

URBACH, R. R.; KIBEL, G. A. **Adware/Spyware**: An Update Regarding Pending Litigation and Legislation. Intelectual Property & Technology Law Journal. Chapel Hill, p. 12, 15 jun. 2004.

VENOSA, Silvio de Salvo. **Direito Civil:** Teoria Geral das Obrigações e Teoria Geral dos Contratos. São Paulo: Atlas, 2007.