A Ação dos *Hackers* -
Repercussões para o Mercado Segurador*:*

Sumário: (i). Introdução; (ii). *Hacker* – conceito e classificações; (iii) Problemática decorrente da inexistência de legislação específica, que tipifique como crime as condutas ilícitas praticadas no âmbito da *Internet; (iv)* Comércio eletrônico; *(v)* Repercussões sobre o mercado segurador – dados do mercado norte-americano; (vi) Conclusão.

(i) Introdução:

"A Consciência de um Hacker

Prenderam outro hoje, está em todos os jornais. "Adolescente preso no Escândalo do Crime Informático", "Hacker preso após invadir banco"... Malditos garotos. São todos iguais.

Mas você, em sua psicologia de cabeça-de-lata da década de 50 alguma vez indagou-se sobre o que o move, que forças o formaram, o que teria o moldado? Eu sou um hacker, entre em meu mundo... Meu mundo é um mundo que começa na escola... Eu sou mais esperto que a maioria das outras crianças, (...) Malditos fracassados. São todos iguais.

Fiz uma descoberta hoje. Eu descobri o computador. Espere um segundo, isto é legal. Ele faz o que eu mando. Se comete um erro, é porque eu o obriguei a isso. Não porque não goste de mim ... Ou se sinta ameaçado por mim... (...) Ou não goste de ensinar e não devesse estar aqui... Maldito garoto. Tudo o que ele faz é jogar. São todos iguais...

(...)

Este é nosso mundo agora... o mundo do elétron e do switch, a beleza do baud. Usamos um serviço já existente sem pagar por aquilo que poderia ser baratíssimo e não fosse explorado por especuladores insaciáveis, e vocês nos chamam de

> *criminosos. Nos exploram e ... nos chamam de criminosos. Somos sem cor, sem nação, sem preconceitos religiosos... e nos chamam de criminosos. Vocês constroem bombas atômicas, declaram guerras, assassinam, trapaceiam e mentem para nós e tentam nos fazer crer que é para nosso próprio bem, e ainda assim os criminosos somos nós.*
>
> *Sim, sou um criminoso. Meu crime é a curiosidade. Meu crime é julgar as pessoas pelo que dizem e pensam, não pelo que aparentam ser. Meu crime é ser mais inteligente que você, algo porque você jamais irá me perdoar.*
>
> *Eu sou um hacker, e este é meu manifesto. Você pode parar este indivíduo, mas não poderá parar todos nós... apesar de tudo, somos todos iguais".*[1]

Há aproximadamente vinte anos atrás, o número de usuários de microcomputadores no mundo era pequeno. Os custos elevados à aquisição das máquinas, as então complexas formas de ensinamento da tecnologia apropriada, entre outros elementos, tornavam os benefícios inerentes à informática acessíveis a um número bastante limitado de pessoas ao redor do mundo.

Com o passar dos anos, numa progressão geométrica, de razão elevadíssima, milhares de pessoas passaram a ter acesso aos microcomputadores, que, sem dúvidas, trouxeram muitos benefícios à sociedade, sobretudo com o surgimento e aprimoramento da *Internet*.

Poder-se-ia escrever páginas e mais páginas acerca das vantagens decorrentes da maior utilização da informática como ferramenta de

[1] O texto em referência foi objeto de transcrição de artigo redigido por Túlio Lima Viana, entitulado "HACKERS: um estudo criminólogico da subcultura *cyberpunk*", Belo Horizonte, Faculdade de Direito da UFMG. O texto se trata de conhecido 'manifesto Hacker', por demais divulgado na comunidade *cyberpunk*, escrito em Janeiro de 1.986, por *hacker* preso nos Estados Unidos da América – o original do texto encontra-se redigido na língua inglesa, cuja íntegra pode ser encontrada no site (www.attrition.org/~modify/texts/ethics/hackers manifesto.html).

trabalho, como forma de evolução da ciência, mas este não é o objetivo deste trabalho.

Há décadas atrás, precisamente no final dos anos 60 e início dos anos 70, fez considerável fortuna nos Estados Unidos da América o Sr. Frank Abagnale[2], cujo "ofício", se é que o que este Sr. desenvolvia poderia ser classificado como ofício, consistiu em por alguns anos passar-se pelos mais diversos personagens, desde co-piloto de Cias. Aéreas (Pan American Air Ways), advogado com aprovação em exame de Ordem em tradicional Universidade Norte-Americana, professor de Sociologia, médico, tendo se apropriado, no decorrer desses anos, o equivalente a três milhões de dólares por intermédio de cheques falsificados e desprovidos de fundos.

Atualmente, tem-se conhecimento de crimes, tais como os praticados pelo Sr. Abagnale, proliferando-se no âmbito da *Internet*. Os *hackers*, com conhecimentos incríveis em matérias relacionadas à informática, rompem poderosos sistemas de segurança das mais diversas empresas (instituições financeiras por exemplo), alteram dados, operam transferências de recursos à ordem de milhões de dólares, sem que para isto precisem sacar uma arma, ou, ao menos, sair detrás de um simples microcomputador.

Vive-se, atualmente, numa era em que, ao lado do crime organizado, representado pelo narcotráfico e pelo tráfico de armas, apresentam-se perigosos *hackers*, que em frações de segundos, são capazes de provocar adulterações em sistemas das mais diversas empresas, causando acintosos prejuízos, cujas conseqüências, naturalmente, deságuam no mercado segurador.

(ii) *Hacker* – Conceito e Classificações:

[2] A história verídica de Frank W. Abagnale foi publicada no Brasil na obra "Prenda-me se for capaz", ed. Record, tendo dado origem ao longa metragem de mesmo título, estrelado por Tom Hanks e Leonardo DiCaprio, dirigido por Steven Spielberg.

Diversas são as classificações que se podem encontrar sobre os *hackers*, aqui entendidos como gênero dentre o qual se destacam diversas espécies.

Partindo da classificação de Túlio Lima Vianna[3], molda-se o seguinte quadro:

> *"Optamos por uma classificação de ordem objetiva dos hackers que leva tão somente em conta o seu* ***modus operandi****. Em rigor, somente as três primeiras categorias são de hackers, pois as demais não exigem conhecimento técnico avançado para agirem, mas resolvem os constá-las para que possamos ter uma classificação geral dos criminosos informáticos:*
>
> 1) *CRACKERS DE SERVIDORES – hackers que invadem computadores ligados em rede;*
> 2) *CRACKERS DE PROGRAMAS – hackers que quebram proteções de software cedidos a título de demonstração para usá-los por tempo indeterminado;*
> 3) *PHREAKERS – hackers especializados em telefonia móvel ou fixa.*
> 4) *DESENVOLVEDORES DE VÍRUS, WORMS E TROJANS – programadores que criam pequenos softwares que causam algum dano ao usuário.*
> 5) *PIRATAS – indivíduos que clonam programas, fraudando direitos autorais.*
> 6) *DISTRIBUIDORES DE WAREZ – webmasters que disponibilizam em suas páginas softwares sem autorização dos detentores dos direito autorais".*

No que se refere ao conceito, Aurélio Buarque de Holanda[4] assim define o verbete *hacker:*

> ***"hacker*** *. [Ingl., substantivo de agente do v.* to hack*, 'dar golpes cortantes (para abrir caminho)', anteriormente aplicado a*

[3] Ob. Cit., 13.
[4] Definiação constante do site http://www.uol.com.br/aurelio/index_result.html?stype=k&verbete=hacker

> *programadores que trabalhavam por tentativa e erro.] S. 2 g. Inform. 1. Indivíduo hábil em enganar os mecanismos de segurança de sistemas de computação e conseguir acesso não autorizado aos recursos destes, ger. a partir de uma conexão remota em uma rede de computadores; violador de um sistema de computação".*

Fazendo uma comparação entre as habilidades dos espertos bandidos que atuavam no passado recente – anos 60 e 70 – com os bandidos atuais, não restam dúvidas de que a inteligência dos mesmos, nos tempos atuais, é capaz de produzir resultados infinitamente superiores, já que, consoante afirmado, numa fração de segundos, sem riscos consideráveis, é tarefa tranqüila alcançar complexos empresariais em pólos absolutamente opostos do país e, mais ainda, do mundo.

(iii) Problemática decorrente da inexistência de legislação específica, que tipifique como crime as condutas ilícitas praticadas no âmbito da *Internet:*

No que se refere aos danos propriamente ditos, incontroverso é que as ações praticadas por um *hacker* podem gerar seríssimos problemas (danos) às mais variadas pessoas, sejam empresas propriamente ditas, sejam os diretores destas companhias – responsabilidade civil sob o enfoque D & O - seja um simples usuário individual de uma máquina que tenha seu disco rígido completamente violado, destruindo-se todos os arquivos anteriormente salvos.

Nestas condições, sob a égide do direito das obrigações (foco civil), consegue-se notar uma opção para os lesados, de modo que, identificados os lesantes, torne-se possível tomar medidas judiciais contra os mesmos, a fim de reaver as perdas e danos sofridos, sem que com isto se pretenda afirmar que seria tarefa fácil encontrá-los.

Todavia, neste item do trabalho, pretende-se trazer à tona problemática que vem ganhando campo no âmbito doutrinário, relacionada, no Brasil, à inexistência de legislação federal específica que tipifique como crime as condutas criminosas praticadas no âmbito da *Internet*.

Como argumentos favoráveis aos lesantes, sustenta-se que, simplesmente, não teria sido publicada legislação específica acerca da matéria, de maneira que, praticadas as condutas ilícitas no âmbito da *Internet*, estariam as mesmas, em matéria criminal, configuradas como fatos atípicos, restando, dessarte, beneficiados os lesantes.

Todavia, esta não soa ser a corrente mais razoável e, além disto, justa, já que, independentemente do local no qual esteja sendo praticada determinada conduta ilegal, caso se deflagre, de forma intencional, a destruição de um arquivo salvo no disco rígido de um microcomputador, ou outras condutas do gênero, estar-se-á praticando crime de dano, ocorrendo, apenas, a mudança do campo no qual estaria ocorrendo a sua consumação.

Bem dissertando sobre esta corrente, leia-se o trecho abaixo, extraído do artigo *Furto, Supressão de Dados Sigilosos Consignados em Sites na Internet de Acesso Restrito e o Estelionato Virtual*, de Flávio Augusto Maretti Siqueira, p. 06:

> *"Em que pese às idéias de que os crimes virtuais são atípicos, ressaltamos o que diz o advogado Alexandre Jean Daoun: "Em que pese a latente necessidade da legislação penal específica para os crimes praticados pela Internet, o nosso Código Penal de 1.940 e as leis penais posteriores, possuem plenas condições de serem aplicadas, uma vez que a Internet é apenas um novo meio, um novo veículo para crimes virtuais, não existe diferença para os crimes da vida real, o que muda é o modus operandi do criminoso, ou seja o modo de execução do crime. Por exemplo, é a substituição da arma de fogo pelo clique do mouse. A ausência de uma lei específica não pode avalizar o "anarquismo virtual". Apesar de a maior bandeira da globalização e do avanço tecnológico estar fincada na internet, é nela*

> *que se vislumbra um terreno convidativo para a prática de delitos e fraudes. Controlar a internet passou a ser uma necessidade social e é no Direito e na Justiça que podemos encontrar senão a perfeita, a melhor forma de controle do mundo virtual que aflora e cresce em ritmo galopante[5].”*

(iv) Comércio eletrônico:

Diante de um número cada vez maior de usuários da *Internet*, crescendo dia após dia no mundo todo, o comércio eletrônico ou *e-commerce* passou a ser adotado como ferramenta de distribuição de toda espécie de bens e serviços, desde eletrodomésticos, passando por automóveis, medicamentos, alimentos, entretenimento, enfim, atualmente é perfeitamente possível consumir bens e serviços dos gêneros mais diversos através da internet, sem maiores entraves.

Ao lado destes benefícios, não restam dúvidas quanto ao surgimento de problemas decorrentes da má utilização da grande rede de computadores, sendo de conhecimento público problemas relacionados à pornografia infantil, violação da propriedade intelectual, fomento de racismo, anti-semitismo, violência e difamação[6].

Nestas condições, ao lado de todo o desenvolvimento e benefícios, encontra-se também terreno fértil à prática de condutas ilegais, cujas conseqüências, sem dúvidas, podem repercutir sobre o mercado segurador.

(v) Repercussões sobre o mercado segurador – dados do mercado norte-americano:

---

[5] Daoun, Alexandre Jean; *O Controle dos crimes praticados pela Internet in* Security Modelo; www.modelo.com.br; 06.11.2.000.

[6] Leia-se a obra “Arbitragem e Seguro – Comércio Eletrônico e Seguro”, publicada pelo IBDS – Instituto Brasileiro do Direito de Seguro, ed. Max Limonad, pgs. 119/137, que se trata de palestra conferida pelo e. Jurista argentino Waldo Augusto Sobrino.

Até o presente momento, a experiência não foi capaz de demonstrar, com exatidão, dados concretos a respeito da sinistralidade que seria característica a apólices contratadas para prover cobertura a riscos decorrentes da ação de *hackers*.

Em âmbito mundial, por ser a sua contratação algo essencialmente novo, não é possível comentar com facilidade a respeito dos valores dos prêmios que deverão ser praticados em apólices desta natureza, cumprindo apenas ressaltar-se que sua contratação vem crescendo em proporções bastante consideráveis.

Na palestra acima comentada[7], o Professor Waldo Augusto Sobrinho assim se manifesta quanto à contratação destas apólices:

> *"[M]as temos seguros de responsabilidade civil para a Internet?*
>
> *A resposta é afirmativa. São muito numerosos, mas na realidade, não temos ainda uma experiência sinistral, o que torna muito difícil o cálculo do prêmio. Os seguros de Internet, cobrem principalmente, "First Party Insurance" (danos próprios) e "Third Party Insurance" (danos a terceiros). Dentro destas coberturas estão amparados os danos ocasionados através da Internet, intranet, "e-mails", "web-sites", etc. Também cobrem, por exemplo, questões sobre violação da propriedade intelectual.*
>
> *(...)*
>
> *Outros riscos que também estão cobertos são os danos produzidos em conseqüência dos vírus que você pode transmitir. Recentemente tivemos um caso original, em que uma pessoa recebeu um "e-mail" com um vírus e ingressou com uma ação judicial contra o "Internet Service Provider",*

[7] "Arbitragem e Seguro – Comércio Eletrônico e Seguro", pg. 131 e ss.

> *argumentando que o ISP deveria ter um filtro para detectar vírus.*
>
> *(...)*
>
> *Dentro das exclusões gerais, temos: i) a pornografia, ii) a evasão de impostos, iii) a violação da Lei de Monopólios. Em todos esses casos não há cobertura legal. (...)".*

No que diz respeito aos elementos essenciais à formação do contrato de seguro[8], quais sejam, risco, mutualidade e boa-fé, seu estudo em relação a apólices voltadas à *Internet* ainda se revela bastante embrionário.

Raciocinando-se, por exemplo, numa empresa multinacional atuante no setor de informática, que, em instantes, sofre a intervenção em seu sistema de segurança por um poderoso *hacker*.

A partir desta intervenção, suponha-se que sejam disparados milhões de *e-mails* para todos os clientes desta empresa, espalhados ao redor do mundo, constando do título desta mensagem algo didático, educacional, que motive os clientes – usuários - a promoverem a abertura destas mensagens.

Suponha-se que ao promover-se a abertura das mesmas, ocorra a destruição dos sistemas de rede de todos os computadores que até então eram geridos por esta multinacional, vítima da ação deste *hacker.*

Partindo deste cenário, partindo do pressuposto de que houvesse a pretérita contratação de apólice com cobertura para responsabilidade civil para esta empresa, como ficaria a situação da mesma perante o segurador, ante a existência de prejuízo milionário, talvez bilionário?

---

[8] "Quais são os elementos essenciais do seguro? São três: o risco, a mutualidade e a boa-fé. Esses elementos formarm o tripé do seguro, uma verdadeira trilogia, uma espécie de santíssima trindade" – Palestra conferida por Sérgio Cavalieri Filho, publicada na obra I Fórum de Direito do Seguro "José Solero Filho", ed. Max Limonad – IBDS, pgs. 85/97.

Seria dever do ente segurador arcar com o pagamento desta indenização? Deveria a empresa segurada, já que atuante no setor de informática, ter contratado melhor proteção ao seu servidor de *Internet* (*Internet Provider*)? Poderia o segurador argüir o agravamento do risco como sucedâneo à aplicação de negativa de cobertura, ao argumento de que pela empresa não teriam sido tomadas as medidas necessárias à diminuição do risco em exame?

Em síntese, o que se pode notar, diante da novidade do tema, é que muitas perguntas serão formuladas, ficando a cargo da doutrina e da jurisprudência chegar às melhores soluções.

Quanto ao questionamento acima, voltado à suposta negligência por parte da empresa multinacional, pertinente se revela a observação constante da obra acima citada, editada pelo IBDS: (pgs. 141/142)

> *"Normalmente, nos contratos se estabelece, como cláusula de adesão, que o caso fortuito exime de responsabilidade o I.S.P. Mas é um contrato muitas vezes leonino e arbitrário. Inclusive na Argentina nós decidimos a "Teoria de Exner", quando ele fala que o caso fortuito tem que ter como característica a agilidade, isto é, que não seja próprio deste negócio ou desta matéria. No caso dos "crackers" e "hackers", eu acho que não seria propriamente um caso fortuito porque não teria a agilidade, é muito conhecido. A questão do Direito do futuro é quem assume os riscos, uma grande empresa ou o consumidor?*
>
> *Então, em primeiro lugar, eu acho que os "crackers" e os "hackers" não podem ser considerados caso fortuito. Por isso, em princípio, eles têm que ser responsáveis, porque senão o único responsável seria o consumidor.*
>
> *De outra maneira, existe uma outra teoria mais sutil que fala de caso fortuito extraordinário, isto é, que sejam coisas realmente não conhecidas. Então, por exemplo, se surgir um "cracker" não via*

> *computador, mas via satélite ou algo parecido, como é uma situação absolutamente incomum e não previsível, aí sim pode ser como cláusula excludente de responsabilidade. Nos outros casos, eu acho que não. (...)".*

Desenvolvendo este raciocínio, para que seja possível avaliar-se a configuração ou não de caso fortuito (diz-se aqui fortuito externo[9]), como fator excludente do dever indenizatório por parte do ente segurador, deve-se atentar para a essência da atividade desenvolvida pelo segurado. Para o caso hipotético acima narrado, em se tratando de uma empresa cujo objeto consiste na prestação de serviços de informática, realmente deveria esta tomar maiores precauções para que não houvesse o sinistro comentado, sendo dever do segurado empregar toda a diligência necessária no sentido de evitar o infortúnio.

Sob outro prisma, se o evento em comento ocorresse, por exemplo, com um escritório de contabilidade, a aplicação do caso fortuito como excludente seria medida de Direito, já que a ação criminosa por parte do *hacker* seria totalmente imprevisível.

Ainda com relação aos elementos essenciais à formação do contrato de seguro, merece destacar-se neste momento que a cotação do risco, em matéria de apólices com cobertura para danos decorrentes da ação de *hackers* fica adstrita a elementos bastante peculiares.

As apólices com cobertura para prejuízos decorrentes da ação de *hackers* tem como característica própria a aplicação da "Teoria Indenitária[10]", sendo esta espécie do gênero "Seguro de Danos". As perdas

---

[9] Sergio Cavalieri Filho, *in* "Programa de Responsabilidade Civil", ed. Malheiros, 2ª edição, pgs. 218/219, leciona: "Entende-se por fortuito interno o fato imprevisível, e, por isso, inevitável, que se relaciona com os riscos da atividade desenvolvida (...) O fortuito externo é também fato imprevisível e inevitável, mas estranho à organização do negócio. É o fato que não guarda nenhuma ligação com a empresa, (...)".

[10] Na obra "O Contrato de Seguro", Pedro Alvim, às fls. 78/79, ensina que: 'É da maior importância a divisão de seguros de dano e de pessoas. Constituem dois grupos com estruturação técnica diferente. Não coincidem também os seus objetivos. Um tem caráter indenitário, o outro não. A peculiaridade de cada grupo reflete na sua disciplina jurídica. Os

decorrentes da ação de *hackers* trazem em si elementos tangíveis e elementos intangíveis, já que, ao sofrer o ataque, a vítima ficará sujeita a prejuízos palatáveis, quer-se dizer mensuráveis, como por exemplo a perda de discos rígidos de micro computadores, *software*, etc., avaliadas em quantias fixas, ao passo que também ficará sujeita a perdas de muito difícil mensuração, como soem ser as características à propriedade intelectual, consistentes de arquivos anteriormente armazenados, nos quais, por exemplo, poderiam ter sido despendidas horas a fio de trabalho por parte de empregados desta suposta vítima.

Logo, quando da cotação do risco, estes elementos devem ser criteriosamente examinados pelo ente segurador, desenvolvendo-se maneiras de, em momentos anteriores à contratação das apólices, fixar-se, com clareza, coberturas distintas para as perdas tangíveis e para as intangíveis, tudo em estrita observância ao princípio da boa-fé, norteador do relacionamento entre segurado e segurador.

Desenvolvendo pesquisa no mercado internacional, apurou-se que nos Estados Unidos da América, as apólices que ofertam cobertura para riscos decorrentes da ação de hackers vêm sendo amplamente comercializadas. Dentre as coberturas objeto de contratação, destacam-se as relacionadas à transmissão de vírus, ao acesso desprovido de autorização a *web sites*, a erros e omissões provocados por *hackers* quando da utilização de serviços disponibilizados na internet, etc.

---

seguros de dano são também conhecidos como seguros de coisa, denominação que tem sido abandonada pelos autores, porque se refere apenas a algumas espécies de seguros do grupo. São seguros de coisa o de incêndio, de transportes, de automóveis, etc., mas não se incluem aí os de responsabilidade civil, de garantia., de fidelidade e outros. A expressão "seguros de dano" é mais abrangente e envolve todos eles. Referem-se tanto aos prejuízos materiais como à perda de valores patrimoniais. Há um princípio que domina todos os seguros de dano, qualquer que seja sua modalidade de cobertura: ninguém pode lucrar com o evento danoso ou tirar proveito de um sinistro**.** Deverá receber em dinheiro ou espécie aquilo que perdeu. O pagamento a mais pode servir de estímulo à fraude ou à especulação, por isso a legislação de todos os povos fulmina de nulidade o seguro de valor superior ao do bem. Figura em nosso Código Civil: "não se pode segurar uma coisa por mais do que valha, nem pelo seu todo mais de uma vez" (art. 1.437). Eis porque se diz que os seguros de dano têm por objetivo uma indenização, isto é, uma reparação, compensação ou satisfação de um dano sofrido. O segurado deverá receber o que for necessário para repor a situação anterior à ocorrência. Ressarcir-se se seus prejuízos." Grifamos.

As coberturas ofertadas incluem perdas ocorridas com o *hardware* e o *software* utilizados pelo segurado, inclusive para prejuízos causados a terceiros, desde que relacionados com a origem dos danos sofridos pelo próprio segurado. (Denota-se através disto a necessidade de que se apresente bem delineado o nexo causal entre os prejuízos e eventual conduta ilícita, para que surja a obrigação de indenizar). [11]

(vi) Conclusão:

Hodiernamente, não restam dúvidas de que o progresso da sociedade na qual vivemos está intimamente relacionado com o desenvolvimento da informática.

Sob os mais diversos campos de atuação – ciências biomédicas, humanas, tecnológicas, etc -, a informática assume papel fundamental.

Lamentavelmente, com todo o desenvolvimento costumam surgir problemas carecedores de soluções e/ou, não sendo estas possíveis, formas de minimizar os prejuízos decorrentes destes problemas.

É justamente neste particular que tem atuação o mercado segurador, prestando-se para viabilizar na sociedade o seu mais amplo desenvolvimento, diminuindo, na medida do possível, possíveis perdas que possam vir a ocorrer.

À conta do que se expôs, torna-se imperiosa a necessidade de que se aprofundem os estudos sobre as coberturas que podem ser ofertadas no âmbito da responsabilidade civil decorrente da ação de *hackers.*

[11] Os dados apresentados podem ser colhidos no *site* a seguir discriminado, através do *link netadvantage* http://www.aiu.com/BusinessLine/aiuCDA_bizline_cntyprod/0,1793,99-17,00.html

Concretamente, tem-se muito pela frente a discutir quanto à comercialização das apólices desta natureza, considerando-se, sobretudo, a realidade, a iminência que este risco representa**.**

"Cadernos de Seguro, edição número 120", publicada pela Fundação Escola Nacional de Seguros (Funenseg).

* * *