

Artigo original

Hegemonia – Revista Eletrônica de Relações Internacionais do Centro  
Universitário Unieuro

ISSN: 1809-1261

UNIEURO, Brasília, número 16, 2015, pp. 4-21.

Recebido em: 2/4/2015

Avaliado em: 17/5/2015

Aprovado em: 19/6/2015

## O FENÔMENO DO CYBERCRIME SOB A PERSPECTIVA DO DIREITO A PRIVACIDADE

Pedro Rogério Melo de Lima<sup>1</sup> e Lidia de Oliveira Xavier<sup>2</sup>

RESUMO - A proteção aos Direitos Humanos deve ser prioridade constante dos governos, da sociedade civil, dos Organismos Internacionais e das pessoas de modo em geral. A sua implementação depende de grandes manifestações populares e deve envolver os Poderes Constituintes de uma Democracia: Poder Legislativo, Executivo e Judiciário. A luta por garantias sociais remonta aos primórdios. A geração de direitos aponta para uma nova conceituação de garantias individuais e sociais. O fenômeno da violência na internet por meio dos Cybercrimes, afronta os direitos humanos sendo causas inaceitáveis da condição humana. Os crimes cometidos contra as pessoas estão em espiral crescente em todo o mundo. Além desse crescimento, foi possível observar que cresceram também os métodos de ataques e agressões. Os agressores estão se valendo das inovações tecnológicas e seus avanços para praticarem crimes que se multiplicam no tempo e no espaço. Os crimes de violação dos dados pessoais na Rede levam nano segundos para se propagar, logo um número gigantesco de pessoas toma conhecimento dessa agressão aos direitos humanos.

Palavras chaves: Ciência Política. Direitos Humanos. Segurança Pública. Violência. Cybercrimes.

---

<sup>1</sup> Advogado. Mestre em Ciência Política, Centro Universitário UNIEURO Aluno dos cursos regulares do Doutorado em Direito Penal da Universidade de Buenos Aires -UBA, Pós graduado em Direito Público (Universidade Uniderp/Luís Flávio Gomes LFG) e graduado em Ciências Jurídicas pelo Centro Universitário- IESB. E-mail:

Artigo original

Hegemonia – Revista Eletrônica de Relações Internacionais do Centro  
Universitário Unieuro

ISSN: 1809-1261

UNIEURO, Brasília, número 16, 2015, pp. 4-21.

RESUME: The protection of human rights should be a constant priority to governments, civil society, international organizations and people in general. The implementation depends on a large demonstrations and must contain the Constituent Powers of Democracy: Legislative, Executive and Judiciary. The faith for social guarantees back to the dawn. The generation of rights points to a new conception of individual and social guarantees. The phenomenon of violence on the Internet through cybercrimes, affront human rights and causes unacceptable human condition. The crimes committed against people are growing in spiral around the world. Besides this growth, it was possible to notice that the methods of attacks and aggressions was growing as well. The attackers are taking advantage of innovative technologies and their advances to practice crimes that multiply in time and space. The crimes of violation of personal data on the Web lead nano seconds to propagate, then a huge number of people becomes aware of this assault to the human rights.

Key words: Political science. Human rights. Public safety. Violence. Cybercrime

## 1 - INTRODUÇÃO

O presente trabalho tem por objetivo identificar quais as formas de reação do Brasil no combate as violações de segurança no ambiente virtual de direito a intimidade no intuito de prática de crimes.

Para que o Estado possa definir quais políticas públicas aplicar a este fenômeno, fazem-se necessários responder alguns questionamentos: onde enquadrar os cybers crime? Como combater os crimes eletrônicos? Quais os desafios do cyber segurança brasileira? Como está a defesa cibernética no Brasil? Vencida esta fase de formulações, poderá ser desenhada a arquitetura de segurança.

Para tanto, buscará situar a pessoa no mundo virtual e na política de segurança pública, capitaneada pelo Estado Democrático de Direito. Neste regime, o princípio basilar é o princípio da legalidade que é identificado pela vigência da submissão de todos à lei, pela divisão de poderes e a declaração de direitos, além de ser um regime de transformação e justiça social. O Brasil adota como regime de governo o Estado Democrático de Direito.

Presumindo-se que a segurança pública e a proteção aos direitos humanos são deveres do Estado e que a Inclusão Digital é fator preponderante

Artigo original

Hegemonia – Revista Eletrônica de Relações Internacionais do Centro Universitário Unieuro

ISSN: 1809-1261

UNIEURO, Brasília, número 16, 2015, pp. 4-21.

para o crescimento da economia global, poder-se-ia inferir que os dilemas envolvendo as novas tecnologias facilitariam a vida dos chamados crimes virtuais.

Muito se tem discutido sobre a inclusão digital e a Revolução trazida pela internet, e pouco sobre o direito a proteção aos direitos humanos, em especial a intimidade e privacidade no mundo virtual no intuito de prática de crimes.

Por fim, após pesquisas e relatos sobre o tema encontra-se a importância e a abrangência de estudar o fenômeno do *Cybercrime* sob a perspectiva do direito à privacidade porque é crescente a prática de violações aos direitos humanos no mundo virtual no Brasil na última década em especial a violação dos dados pessoais.

## 2. AUSÊNCIAS DE GARANTIAS NO MUNDO VIRTUAL

A internet é um dos meios tecnológicos utilizados pelos Cybercriminosos para violarem os dados pessoais na internet utilizando de meios refinados para atacar os direitos humanos e ofender os direitos humanos por meio da injúria, calúnia e da difamação. Eles não utilizam das armas convencionais, tais como arma de fogo, agressão física, intimidação, mas sim da ausência física. O que dificulta ao Estado brasileiro decifrar esta fenomenologia, que nem sempre a vítima sofre dano verificável no momento.

Os ataques dos Cybercriminosos às suas vítimas são silenciosos, a arma utilizada geralmente é um computador, tablet, smartphone ou outro meio tecnológico de ponta. Os danos causados a imagem de uma pessoa agredida por esse tipo de criminoso são imensuráveis,

A Política de Segurança Pública no Estado Democrático de Direito deve ter mecanismos para identificar em tempo real os criminosos e suas vítimas, evitando assim que seus direitos sejam violados.

Pensando assim é que os Constituintes originários incorporaram nas Constituições Democráticas modernas garantem, dentre outros, os direitos fundamentais da pessoa humana, o livre acesso às informações e os direitos sociais de primeira geração (direitos civis e políticos), segunda geração (são os

Artigo original

Hegemonia – Revista Eletrônica de Relações Internacionais do Centro Universitário Unieuro

ISSN: 1809-1261

UNIEURO, Brasília, número 16, 2015, pp. 4-21.

direitos sociais, econômicos e culturais), terceira geração (fraternidade ou solidariedade, meio ambiente, autodeterminação dos povos e ao direito de comunicação) e quarta geração (direitos à democracia, informação e pluralismo).

Como não poderia deixar de ser, o Estado brasileiro adota como regime de governo o Estado Democrático de Direito (neste regime o princípio basilar é o princípio da legalidade), além do que ele é identificado pela vigência da submissão de todos à lei, pela divisão de poderes e a declaração de direitos, além de ser um regime de transformação e justiça social.

Na discussão sobre a violência no mundo virtual em recente seminário promovido pela Câmara dos Deputados sobre Cybersegurança vários foram os palestrantes que demonstraram suas preocupações sobre qual política pública deve ser adotada para conter o fenomenologia dos Cybercrimes. A política de segurança pública ou a política de segurança nacional. O Estado brasileiro tem que estar pronto para proteger-se e proteger as pessoas, a sociedade, os direitos humanos, seu território e o seu patrimônio.

Com relação aos temas Cybercrimes e Perícia Digital, vários foram os problemas levantados e discutidos. O principal deles é quanto à definição do local do crime, uma vez que o delito pode ocorrer aqui no Brasil, mas o criminoso está sediado em outro País. Estes crimes na sua maioria são cometidos sem violência física, sem ameaças, sem uma arma apontada para a vítima e o delinquente pode estar a milhares de quilômetros, muito bem acomodado, ou do lado da vítima.

A perícia digital é outro nó para determinar quem e quais são e onde os autores estão sediados. Os especialistas garantem que as provas são facilmente adulteradas digitalmente e os rastros apagados, dificultando assim a produção de provas. A falta de agentes estatais especializados nos órgãos de segurança pública dificulta ainda mais a obtenção de respostas em tempo real. A prova jurídica não concorre com as provas digitais.

O objetivo do presente estudo é verificar a posição do Estado brasileiro frente a fenomenologia da violência aos direitos humanos patrocinadas pelos Cybercrimes. Poder-se-ia inferir que o Cybercrimes podem ser qualificados como crimes de oportunidade, uma vez que as maiores vítimas são potenciais pessoas analfabetas digitais e/ou funcionais, além do mais o criminoso não precisa estar próximo da vítima. As fraudes eletrônicas foram bastante aprimoradas nas últimas décadas. As ferramentas digitais para o

Artigo original

Hegemonia – Revista Eletrônica de Relações Internacionais do Centro Universitário Unieuro

ISSN: 1809-1261

UNIEURO, Brasília, número 16, 2015, pp. 4-21.

cometimento de crimes digitais estão também à disposição de qualquer um do povo.

Presumindo-se que a segurança pública e a proteção aos direitos humanos são deveres do Estado e que a inclusão digital é fator preponderante para o crescimento da economia global, poder-se-ia inferir que os dilemas envolvendo as novas tecnologias facilitariam a vida dos chamados Cybercrimes.

Para que o Estado possa definir quais políticas públicas aplicar a este fenômeno, fazem-se necessários responder alguns questionamentos. O primeiro deles é, onde enquadrar os Cybercrimes? Segundo, como combater os crimes eletrônicos? A terceira, quais os desafios do cyber segurança brasileira? E a quarta, como esta a defesa cibernética no Brasil? Passada esta fase de perguntas e respostas, será desenhada a arquitetura de segurança. Neste trabalho o recorte a ser dado é com relação à violação dos Direitos humanos cometidos por meio dos Cyberscrimes e a resposta legislativa para essas atitudes.

Para realização desse trabalho adotou-se metodologia de pesquisa bibliográfica e documental, sendo desenvolvidas por meio dos Anais da Câmara dos Deputados, Senado Federal, Tribunais e revistas e jornais especializados e de grande circulação, levando em consideração o marco temporal do ano de 1999 até o ano de 2013.

### 3. A FENOMELOGIA DA VIOLAÇÃO DA PRIVACIDADE NO BRASIL

Durante a participação no Congresso Brasileiro de Internet, (CBI), 2013; dois Seminários Internacionais (O Brasil e os Órgãos Internacionais de Proteção aos Direitos Humanos, 2013, e o Seminário Internacional Terrorismo e Grandes Eventos, 2013). Seminário sobre Cyber segurança, 2013; Seminário sobre Extensão Tecnológica no País: O conhecimento a serviço da população, 2013. Seminário - Marco Civil da Internet, 2013; Seminários e audiências públicas realizadas pela Câmara dos Deputados para debater o Projeto de Lei 2126 de 2011, que dispõe sobre o Marco Civil da Internet, todos realizados em Brasília-DF; além de assistir e acompanhar os debates transmitidos via internet no ano de 2014 (Encontro Multissetorial Global Sobre o Futuro da Governança da Internet - NETmundial), foi possível observar que no âmbito das discussões governamentais, acadêmicas e legislativas, a expressão mais empregada era

Artigo original

Hegemonia – Revista Eletrônica de Relações Internacionais do Centro  
Universitário Unieuro

ISSN: 1809-1261

UNIEURO, Brasília, número 16, 2015, pp. 4-21.

“Cybercrimes”, que está sendo empregada neste trabalho, embora esta prática tenha diversos nomes e tipos.

Além desses eventos, a participação em audiência pública conjunta realizada em 22 de agosto de 2013, promovida pela Câmara dos Deputados por meio das Comissões de Relações Exteriores e Defesa Nacional e de Ciência Tecnologia e Informática, para debaterem as supostas violações da privacidade e sobre os principais aspectos relacionados à elaboração e à execução da política externa brasileira e esclarecimentos, no âmbito da esfera de atuação do Ministro das Relações Exteriores, Ministério da Justiça e o Ministério da Ciência Tecnologia e Inovação a respeito das denúncias de atividades de espionagem, ratificaram o uso do termo Cybercrime.

Nesses debates, os temas abordados foram: direitos dos usuários; liberdade de expressão e o potencial de inovação da internet; Responsabilidade civil de terceiros; neutralidade da rede e o potencial para a inovação; Neutralidade da rede e governança da internet; sendo que os mais debatidos foram neutralidade da rede e o potencial para a inovação e a Responsabilidade civil de terceiros. Após todo este debate, o Projeto de Lei foi aprovado e sancionado pela Presidenta da República em abril de 2014, no encontro sobre governança na internet.

Além disso, no Brasil o fenômeno da violência aos usuários dos sistemas informatizados é crime, segundo a Lei 12.737, de 30 de novembro de 2012. Esta Lei foi aprovada em tempo recorde pelo Congresso Nacional, depois das fotos da atriz Carolina Dickman terem sido divulgadas sem a sua autorização, ou seja, os atores externos com representação no cenário nacional pressionaram os Congressistas para que eles agissem mais rápido do que agem com a aprovação de outras matérias.

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

Artigo original

Hegemonia – Revista Eletrônica de Relações Internacionais do Centro  
Universitário Unieuro

ISSN: 1809-1261

UNIEURO, Brasília, número 16, 2015, pp. 4-21.

Dessa forma, a notícia diária sobre a exposição de fotos da intimidade da atriz pressionou os congressistas a tratar com maior rigor aqueles que invadissem ou violassem aparelho de computadores, *smartphones*, *tablets* ou qualquer dispositivo informático que não lhe pertencesse.

Assim, a falta de capacitação dos usuários para uso das ferramentas introduzidas pela modernidade tecnológica seria por consequência, mais uma condição para aumentar os ataques dos Cybercriminosos? O uso da internet por pessoas que não dominam as tecnologias digitais facilita aos criminosos o acesso não autorizado aos seus dados privados.

Quando determinadas pessoas navegam na Rede mundial de computadores as margens dos cuidados com a segurança digital e sem terem competências necessárias, acabam atraindo para si os perigos das facilidades digitais das Redes.

Conseqüentemente as pessoas que não tem domínio das novas tecnologias digitais e virtuais são levadas a fornecerem dados particulares de suas contas bancárias, cartões de crédito aos Cybercriminosos, poder-se-ia deduzir que as frequentes invasões de computadores não autorizadas terminariam sendo discutidas nos Tribunais ou os criminosos sairiam ilesos.

O que de fato acontece com as diversas pessoas que navegam sem ter o mínimo conhecimento necessário para enfrentar o mundo virtual e são alcançadas pelos Cybercrimes, muitas vezes não se tem conhecimento, perdem todos os seus dados pessoais, além de ter seu computador danificado por vírus.

A evolução dos direitos humanos fundamentais será observada tomando como parâmetro a Teoria das Gerações preconizada por Karet Vasak. Esta teoria tem como fundamento os direitos conquistados por meio da Revolução Francesa em 1789, que cunhou o tripé revolucionário Liberdade, Igualdade e Fraternidade, como garantias fundamentais da pessoa humana.

Bonavides (2009, p. 563), por sua vez, afirma que o termo gerações de direito foi cunhado por Karel Vasek “na aula inaugural de 1979 dos cursos do Instituto Internacional dos Direitos do Homem, em Estrasburgo”, onde os definia da seguinte forma: primeira geração, o direito à liberdade, segunda geração o direito a igualdade e de terceira geração a fraternidade. Do ponto de vista da proteção à privacidade este se afina com os direitos de primeira geração que consagra a dignidade humana frente ao Estado violador.

Artigo original

Hegemonia – Revista Eletrônica de Relações Internacionais do Centro  
Universitário Unieuro

ISSN: 1809-1261

UNIEURO, Brasília, número 16, 2015, pp. 4-21.

Os direitos da primeira geração ou direitos da liberdade tem por titular o indivíduo, são oponíveis ao Estado, traduzem-se como faculdades ou atributos da pessoa e ostentam uma subjetividade que é seu traço mais característico; enfim, são direitos de resistência ou de oposição perante o Estado (BONAVIDES, 2009, p.564)

Para o teórico a evolução desses direitos fundamentais segue a seguinte divisão:

“1ª Geração: Liberdade. Foco no indivíduo visando diminuir a influência do Estado na vida particular. Esta geração é representada pelo Estado Liberal.

2ª Geração: Igualdade. Após notar que o Estado obrigatoriamente precisava intervir na vida da sociedade para regulá-la da melhor forma possível, foi proposta a intervenção deste, aplicando e respeitando os Direitos Humanos, Fundamentais e Sociais. Esta geração é representada pelo Estado Social e Democrático.

3ª Geração: Fraternidade (Solidariedade). Após a Segunda Guerra Mundial houve uma forte comoção mundial a respeito da necessidade da proteção da humanidade como um todo. Foram propostos nesta geração direitos muito mais amplos, como o Direito ao Meio Ambiente, à Paz e ao Desenvolvimento.”

Neste sentido, poder-se-ia enquadrar o princípio da dignidade da pessoa humana num direito de terceira geração, ou seja, dentro do Conceito de Fraternidade. Conceito que representa para o mundo moderno uma força de ampliação efetiva da cidadania, conforme ilustra Antonio Maria Bagio.

Preliminarmente esclareceria que o direito penal deve ser chamado para socorrer o bem tutelado, a vida. Assim deveria ser no dia-a-dia da pessoa. O direito a proteção ao patrimônio pessoal, este deveria ser protegido por outro ramo do direito, que não o penal.

Para Anitua “Se dejaría en claro, con él, que lá manera en que las sociedades y sus instituciones reaccionan frente a un hecho es más



Artigo original

Hegemonia – Revista Eletrônica de Relações Internacionais do Centro Universitário Unieuro

ISSN: 1809-1261

UNIEURO, Brasília, número 16, 2015, pp. 4-21.

determinante para definirlo como delictivo o desvialo que lá própria naturaleza, dele mesmo como enseñaba el positivismo”. (ANITUA. Pg. 363. 2010).

A Revolução Francesa além de trazer mecanismos para conjugar a força popular, despontou reforçando a declaração de direitos redigida pelo Parlamento Inglês em 1689, iniciando dessa forma a jornada de reconhecimento dos direitos humanos. Os Direitos Humanos carecem também da proteção do Direito Penal, uma vez que o seu bem mais precioso está desenhando nos tabuleiros das geografias mundiais.

A Constituição Federal de 1988 confere aos acordos internacionais que versam sobre direitos humanos a mesma hierarquia das suas Emendas Constitucionais. Para Flavia Piovesan “O sistema internacional de proteção dos direitos humanos constitui o legado maior da chamada “Era dos Direitos”, que tem permitido a internacionalização dos direitos humanos e a humanização do Direito Internacional contemporâneo.”

Raul Zafaroni, ao comentar como a ciência penal deveria mirar os direitos humanos, afirma que: “Nuestra ciencia siempre está del lado de humanistas y no perdona a sus traidores”.(ZAFARONI.pg. 31.2011).

Assim sendo, o Princípio da Anterioridade não permite aplicar sanções à conduta que ainda não esteja disciplinada em Lei. Para o cometimento da violação dos direitos humanos por meio dos novos cybers crimes, este princípio é aplicado em sua plenitude.

## 5. ARRANJO LEGISLATIVO FACE A PRÁTICA DO CYBERCRIME

Os Cyberscrimes são delitos praticados utilizando como meio a internet. As redes de computadores comerciais, as redes sociais, o sistema bancário, as redes públicas e privadas são atacadas pelos Cybercriminosos, com o propósito de fraudá-las e tirar proveito financeiro, político e comercial.

Na Sociedade da Informação, o cometimento de abusos da liberdade de expressão, abuso da identidade, conteúdos nocivos, fraude, roubo de identidade, Spam, Vírus, são uma constante para Monteiro (2006, p..12).

Os analfabetos digitais e funcionais são alvos certos para estes novos golpes, planejados nas nuvens. A cada dia o número de vítimas tende a crescer.

Artigo original

Hegemonia – Revista Eletrônica de Relações Internacionais do Centro  
Universitário Unieuro

ISSN: 1809-1261

UNIEURO, Brasília, número 16, 2015, pp. 4-21.

“O fenômeno dos Cybercrimes está crescendo no mundo todo. Em 7 anos, a SaferNet Brasil recebeu e processou 3.173.061 denúncias anônimas envolvendo 472.840 URLs distintas escritas em 9 idiomas e hospedadas em 52.962 hosts diferentes, conectados à Internet através de 28.131 números IPs distintos, atribuídos para 90 países em 5 continentes. As denúncias foram registradas pela população através dos 7 hotlines brasileiros que integram a Central Nacional de Denúncias de Crimes Cibernéticos.”.

No ano de 1999, no Brasil, não havia registros de crimes cometidos pela internet, o que levou Alexandre Daounem (Daounem 1999), a concluir que no Brasil tal crime não aconteceria, pelo seu atraso tecnológico.

“Acerca da criminalidade informática, importante destacar que a maior bandeira da globalização e do avanço tecnológico está fincada na Internet, mas, pelas próprias características do meio, vislumbra-se também um terreno novo e convidativo para a prática de delitos e fraudes que, como sabido, não ocorrem só no Brasil.”

Com o advento da Globalização, a inovação tecnológica tornou-se um fator relevante para a sociedade do conhecimento. A palavra chave no século XX foi “Inovar”, como forma de manter a competitividade das empresas e dos governos. Logo, para algumas empresas, é questão de sobrevivência novos processos e para os governos, a maneira de implementar suas políticas de desenvolvimento e crescimento.

No Congresso Nacional brasileiro existem vários Projetos de Leis que buscam sanar esta situação. O mais antigo destes é o PL 84/99, de autoria do Deputado Federal Luis Pyhauilino, que tramitou há mais de 15 anos, sem que tenha havido acordo entre parlamentares, sociedade civil organizada e governo, para sua aprovação ou rejeição. Destaca-se também o Projeto de Lei que cria o

Artigo original

Hegemonia – Revista Eletrônica de Relações Internacionais do Centro  
Universitário Unieuro

ISSN: 1809-1261

UNIEURO, Brasília, número 16, 2015, pp. 4-21.

Marco Civil da Internet, define direitos e obrigações para os usuários do sistema.

Os crimes cometidos pela internet alcançam também os governos, empresas, sociedade civil e o cidadão, são: as ameaças cometidas por e-mails, injúrias praticadas em redes sociais, a interceptação ilegal de e-mails, a existência de sites com conteúdo racista, as fraudes pela internet, crimes de estelionato ou furto mediante fraude.

Também há muitos casos de crimes contra a honra, crimes de ameaça, racismo, violação ao direito autoral, apologia ao crime ou criminoso, pornografia infantil, entre outros, são os chamados cybers bullying, um tipo de agressão psicológica praticada na rede de forma habitual, traumática e prejudicial à vítima.

Além destes, temos ainda: acesso não autorizado a sistema informatizado protegido por restrição de acesso; obtenção, transferência ou fornecimento não autorizado de dado ou informação; divulgação, utilização, comercialização e disponibilização de dados e de informações pessoais contidas em sistema informatizado com finalidade distinta da que motivou seu registro; destruição, inutilização, deterioração de coisa alheia ou dado eletrônico alheio.

Mais: a inserção ou difusão de código malicioso ou vírus em sistema informatizado; estelionato eletrônico (difundir código malicioso para facilitar ou permitir acesso indevido a sistema informatizado); atentado contra a segurança ou o funcionamento de serviço de água, luz, força, calor, informação, telecomunicação ou outro serviço de utilidade pública.

A MacFee, empresa de segurança de redes, elaborou um relatório com o título "Uma boa década para o cibercrimes"<sup>3</sup>, onde compara o maior assalto cometido nos Estados Unidos contra um carro forte, onde os ladrões saquearam um cofre levando US\$ 18,9 milhões.

Outro exemplo trazido no relatório é o de "Albert Gonzalez que, com uma equipe de hackers chamada Shadowcrew, invadiu os bancos de dados de conhecidos gigantes do varejo, incluindo TJ Maxx, Barnes & Noble e BJ's Wholesale Club, para obter acesso a mais de 180 milhões de contas de cartões de pagamento entre 2005 e 2007". Ele e sua equipe causaram um prejuízo para

---

Artigo original

Hegemonia – Revista Eletrônica de Relações Internacionais do Centro Universitário Unieuro

ISSN: 1809-1261

UNIEURO, Brasília, número 16, 2015, pp. 4-21.

as empresas lesadas de mais de US\$ 400 milhões em reembolsos, perícia e honorários jurídicos.

O Princípio da Legalidade define que ninguém será condenado por crime que não esteja prescrito em lei. Com relação aos crimes cometidos contra as pessoas por meio desta “nova” tecnologia destacam-se a difamação, a calúnia e a injúria, crimes que afrontam o Estado Democrático de Direito e a proteção dos direitos humanos. No Direito Penal a analogia não é permitida, assim sendo, alguém só pode ser punido se existir lei que tipifique o delito.

Além dos crimes descritos acima, temos a pedofilia, a pornografia infantil, o racismo, a intolerância religiosa, a xenofobia, o tráfico de pessoas, o neonazismo, genocídio, e a divulgação de imagens privadas, são delitos comumente praticados nas Redes. Estes dados são frutos de pesquisa recentemente divulgados pela SAFENET.

“SaferNet Brasil - Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos (CND) apontam um crescimento de 264,50% de 2011 para 2012. Em 2012, foram 11.305 endereços denunciados à CND referentes ao Facebook, um aumento de 264,50% comparado à 2011. A maioria (5021 URLs) supostamente abrigava conteúdos de Racismo. Na sequência aparecem Pornografia Infantil (1969 URLs), Apologia e Incitação a crimes contra a vida (1513 URLs), Maus tratos contra animais (697 URLs), Homofobia (635 URLs), Intolerância religiosa (494 URLs), Xenofobia (376 URLs), Tráfico de Pessoas (233 URLs), Neonazismo (186 URLs) e Genocídio (181 URLs). Em 2010, a CND recebeu denúncias de apenas 233 URLs do Facebook. No ano seguinte, foram 4.274 URLs, ou seja um aumento de 1834,33%, em relação ao ano anterior. Em 2012 o Facebook ficou em segundo lugar no ranking global no número de denúncias recebidas no Brasil pelos 7 hotlines integrados à CND, só perdendo para o Orkut, que lidera o ranking desde 2006. Entretanto, ao analisarmos os dados do último trimestre de 2012, percebemos que a tendência é o Facebook assumir a liderança e se consolidar em 2013 como a rede social com o maior número de denúncias de crimes e violações a Direitos Humanos na Internet brasileira.”

Artigo original

Hegemonia – Revista Eletrônica de Relações Internacionais do Centro  
Universitário Unieuro

ISSN: 1809-1261

UNIEURO, Brasília, número 16, 2015, pp. 4-21.

A banalização do direito penal pode oferecer também aos gatunos cibernéticos uma oportunidade de “livrar solto”? Uma vez que assaltar, sequestrar, pixar, agredir, invadir e tantos outros crimes são executados sem a presença física do autor, deixando livre sua rota de fuga, aparentemente sem nenhuma punibilidade.

“La Filosofía penal liberal se concreta en el pensamiento de Beccaría fen una fórmula jurídica que resultaba del Contrato social de Rousseau: el principio de la legalidad ele los delitos y de las penas: nadie podrá ser castigado por hechos que no hayan sido anteriormente previstos por una ley, y a nadie podrá serle impuesta una pena que no esté previamente establecida en la ley.” (ASÚA. 1958. pg.34).

Assim sendo, a cada dia, nascem novos delitos a serem recepcionados pelo Direito Penal, que por sua vez deve respeito ao Contrato Social.

Já o Doutrinador Eugenio Zafaroni se alinha a Teoria Minimalista Penal do Estado. Defende a fórmula garantista donde os propósitos do estado democrático sejam vistos a partir do direito. Estado, com uma intervenção mínima. “Jamais pode o Direito penal ter incidência senão quando absolutamente necessário (princípio da intervenção mínima - Nulla lex poenalis sine necessitate: não há lei penal sem necessidade).”

A discussão trazida por Gabriel Anitua descreve sua preocupação que a Política Criminológica deixe de cumprir o seu papel em detrimento de estudar áreas diferentes da sua. “El objeto de estudio de lá criminologia dejará desde entonces de ser el “delicuyente” y empezará a serlo el de las instancias que “crean” y “administran” lá deliucencia”. (ANITUA, 2010, p 363).

A Doutrina Majoritária é clara em afirmar que não basta que a conduta seja imoral ou pecaminosa, ela deve ofender um bem jurídico e provocar uma grave lesão. Assim é definido o Princípio da Ofensividade. A penalização das ações sociais poderia levar a comunidade a uma revolução.

Artigo original

Hegemonia – Revista Eletrônica de Relações Internacionais do Centro Universitário Unieuro

ISSN: 1809-1261

UNIEURO, Brasília, número 16, 2015, pp. 4-21.

O Marquês de Beccaria, em pleno Século XVII anunciava de forma categórica que “é melhor prevenir do que castigar” e continua, “a finalidade das penas não é atormentar e afligir um ser sensível”, mas sim impedir que novos delitos aconteçam (BECCARIA, 2002, p.43).

Alessandro Barata corrobora com a ideia de que as sanções penais devam esta cunhada no Princípio da Legalidade. “Los límites de lá cominación y de lá aplicación de lá sancón penal, así como las modalidades del ejercicio de la potestad punitiva del Estado, estaban señalados por la necesidad o utilidad de la pena y por el principio de legalidad.” (BARATA, 2009, p.23).

Para Ihering (2004, p.27), “O objetivo do Direito é a paz. A luta é o meio de consegui-la. Enquanto o direito tiver de rechaçar o ataque causado pela injustiça – e isso durará enquanto o mundo estiver de pé – ele não será poupado”.

Para Busato, apenas o simples fato de uma infração de gravidade insignificante não concede ao Estado o poder de agir duramente e procurar flexibilizar suas garantias Constitucionais. “O fato de estar diante de uma infração que não cobra relevância social a ponto de exigir uma intervenção dura, não significa estar com uma situação de direito que pode transigir com garantias, mais sim estar diante de uma situação que, por muito que a lei diga o contrário, não pode e não deve ser considerada Direito penal.” (BUSATO, 2007, p.339).

Segundo especialista de segurança na rede “Atualmente, alguns dos criminosos mais bem-sucedidos não precisam sair do conforto de suas casas para realizar crimes”. “Tudo de que precisam é uma conexão com a Internet, um pouco de conhecimento em tecnologia e muita má-fé”.

Recentemente, no Brasil, a atriz Carolina Dieckmann teve suas fotos divulgadas na internet sem sua prévia autorização. Poder-se-ia supor que como se trata de pessoa pública, não haveria problema algum na divulgação das imagens. Acontece que essas imagens retratam a nudez da atriz na sua intimidade, na sua privacidade.

O fato veio à tona quando os internautas começaram a acessar as redes sociais e se depararam com as fotos íntimas da atriz. Carolina informou que havia enviado o seu computador para concerto em empresa especializada, e por algum motivo desconhecido, suas fotos foram divulgadas. Provavelmente pelos técnicos de computadores da empresa.

Artigo original

Hegemonia – Revista Eletrônica de Relações Internacionais do Centro Universitário Unieuro

ISSN: 1809-1261

UNIEURO, Brasília, número 16, 2015, pp. 4-21.

Na Câmara dos Deputados estava em tramitação desde 29/11/2011, o PL 2793/2011, de autoria do Deputado Paulo Teixeira, do Partido dos Trabalhadores, do Estado de São Paulo, que “Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências”. Este Projeto de Lei foi transformado na Lei Ordinária 12.737, de 30 de novembro de 2012, poucos meses depois do início de sua tramitação.

O caso Carolina foi tema de audiências públicas, entrevistas, matérias diárias nos jornais de grande circulação. As polícias foram acionadas para darem uma resposta rápida e precisa à vítima e à sociedade civil. Várias foram as hipóteses desse crime: violação de direitos humanos, invasão de sistema computacional, chantagem, estelionato, divulgação de imagens não autorizada, furto de propriedade intelectual, quebra de sigilo, quebra de segurança e extorsão. Para os policiais que chegaram aos autores do delito, o que eles queriam na verdade era extorquir dinheiro da atriz.

Para Cláudio Pereira, as políticas de Segurança Pública devem estar sincronizadas com a Carta Magna.

“As leis sobre segurança, nos três planos federativos de governo, devem estar em conformidade com a Constituição Federal, assim como as respectivas estruturas administrativas e as próprias ações concretas das autoridades policiais. O fundamento último de uma diligência investigatória ou de uma ação de policiamento ostensivo é o que dispõe a Constituição. E o é não apenas no tocante ao art. 144, que concerne especificamente à segurança pública, mas também no que se refere ao todo do sistema constitucional. (Cláudio Pereira de Souza Neto).

Os Cybercrimes afetam diretamente a arquitetura das políticas públicas de segurança pública, bem como as políticas de segurança nacional. A primeira, afeta o dia-a-dia dos cidadãos em suas rotinas de transações via internet, navegação nas redes sociais, além do seu uso profissional. A segunda, diz respeito aos supostos ataques terroristas, programados por meio de ataques de hackers aos computadores centrais de bancos, empresas, governos, estação

Artigo original

Hegemonia – Revista Eletrônica de Relações Internacionais do Centro  
Universitário Unieuro

ISSN: 1809-1261

UNIEURO, Brasília, número 16, 2015, pp. 4-21.

de água e luz. A segurança pública não deveria ser tratada de um único segmento, podendo ser um tema multidisciplinar.

## CONCLUSÃO

A preservação dos Direitos Humanos é obrigação do Estado e dever de todos. Assim sendo, dever-se-ia ocupar todos os espaços de decisão, sendo eles: Poder Legislativo, Executivo e Judiciário, além de levar as discussões para as Academias, Centro Universitários, Associação de moradores e a Sociedade Civil organizada. Ou seja, lutar.

Neste trabalho identificou-se que as atualizações Legislativas nem sempre concorrem com os fatos sociais. Vimos também que essa regra tem suas exceções, dentre elas citou-se a Lei Maria da Penha, Lei da Ficha Limpa e Lei Carolina Dickman.

Observou-se também que dependendo do fato social, da personalidade envolvida, da gravidade e da repercussão deste na sociedade, o tempo para criação de Lei ou da sua atualização é razoavelmente reduzido.

Como não poderia deixar de ser a criação da Lei Carolina Dickman, por uma suposta violação dos seus direitos de imagens, teve sua tramitação diferenciada das demais proposições Legislativas. Isto só foi possível porque se estava diante de uma Atriz Global, e como tanto, foi tratada.

Assim sendo, aparentemente a violação aos direitos humanos só é notada quando têm envolvidas Personalidades do meio artístico, político, acadêmico, religioso e empresarial, ou quando uma chacina toma conta dos noticiários.

A arquitetura dogmática da proteção aos Direitos humanos nem sempre se dedica em aprofundar os Tratados Internacionais que versam sobre o assunto, fazendo com que os Estados Membros minimizem suas violações.

Por fim, a comunidade, a sociedade civil, as pessoas, devem estar atentos para preservação dos seus direitos políticos, sociais, econômicos, religiosos, culturais e humanos, para que governos, personalidades, travestidos de boas intenções, não destruam patrimônio tão caro a humanidade.

## BIBLIOGRAFIA



Artigo original

Hegemonia – Revista Eletrônica de Relações Internacionais do Centro  
Universitário Unieuro

ISSN: 1809-1261

UNIEURO, Brasília, número 16, 2015, pp. 4-21.

ANITUA, Gabriel Ignacio. Historia de los pensamientos criminológicos. 1ª ed. 2ª  
reimp. Ciudad Autonoma de Buenos Aires. Editores del Puerto, 2010

BARATA, Alessandro. Criminología crítica y crítica dele derecho Penal. Buenos  
Aires: Ed. Siglo veintiuno, 2009.

BECARIA, Cesare. Dos Delitos e das Penas. Tradução OLIVEIRA, Paulo M. 3ª  
ed. São Paulo: Antena Editora, 1949.

BUSATO, Paulo César. Quem é o inimigo, quem é você? Revista Brasileira de  
Ciências Criminais. V.15. maio-junho 66. São Paulo, editora Revista dos  
Tribunais, 2007.

BUSATO, Paulo César. Modernas Tendências de Controle Social. Revista  
Eletrônica de Ciências Jurídicas. RECJ- 04-03/2007

IHERING, Rudolf Von. A Luta pelo Direito. 4ª ed. Tradução CRETELLA JR. E  
CRETELLA, Agnes. São Paulo: Editora Revista dos Tribunais, 2004.

MONTEIRO, Claudio Pereira - A Segurança pública na Constituição Federal de  
1988: Conceituação Constitucionalmente adequada, competências Federativas  
e Órgãos de execução das políticas.  
<[http://www.oab.org.br/editora/revista/users/revista/12055059741742181819  
01.pdf](http://www.oab.org.br/editora/revista/users/revista/1205505974174218181901.pdf)> acessado em 11/04/2013.

PERRIN, Stephaine. O Cybercrime. Disponível em: <  
<http://vecam.org/article660.html>> <acessado em 09/04/2013>

PIOVESAN, Flávia. Desafios e Perspectivas - Declaração Universal de Direitos  
Humanos.

SAFENET. Indicadores da Central Nacional de Denúncias de Crimes  
Cibernéticos. Disponível em: <<http://indicadores.safenet.org.br/>> acessado  
em 20.04.2013>

SAVINO FILHO, Cárnine Antônio. Evolução do Direito Penal: comentários.  
Revista de Direito do Tribunal de Justiça do Estado do Rio de Janeiro –  
Doutrina e Jurisprudência, out/dez 2001.

Artigo original

Hegemonia – Revista Eletrônica de Relações Internacionais do Centro  
Universitário Unieuro

ISSN: 1809-1261

UNIEURO, Brasília, número 16, 2015, pp. 4-21.

SILVA, Evandro Lins e. DE BECCARIA A FILIPPO GRAMATICA

ZAFARONI, Eugenio Raúl. Humanistas em el Derecho Penal. Revista Superior  
de Justiça, vol. 1, 2011