MUNDO VIRTUAL: leis que regulam a utilização do espaço virtual

Andreia de Brito Pinto

RESUMO

A crescente popularização do uso da internet em grande parte do globo terrestre é uma das principais características do século XXI. Tal popularização apresenta grande relevância e gera impactos sociais, políticos e econômicos na sociedade atual. Assim, faz-se necessário um cuidado, uma cautelosa discussão a fim de encarar essa nova realidade com uma postura crítica e cidadã para então desfrutarmos dos benefíciosque a globalização dos meios de comunicação pode nos oferecer.O objetivo desse trabalho é Compreender o espaço virtual e os crimes cibernético que estão se tornando corriqueiros no nosso país, identificando os seus pressupostos e, por conseguinte, as suas conseqüências, procedendo, para este fim, um estudo para reflexão e discussão.O objetivo específico, Discutir a Lei 12.737 de 2012. É a chamada "Lei Carolina Dieckmann" - apelidada assim por coincidir com um vazamento de fotos íntimas da atriz. O trabalho será realizado usando o método bibliográfico. Através de pesquisa bibliográficas nos códigos, doutrinas, revistas jurídicas ou não, livros e internet.

ABSTRACT

The growing popularity of internet use in much of the globe is a major feature of the XXI century. Such popularization are highly relevant and generates social, political and economic impacts in society today. Thus, it is necessary a caution, a cautious discussion in order to face this new reality with a critical and citizen and then we enjoy the benefíciosque globalization of the media can offer us.The aim of this work is to understand the virtual space and cyber crimes that are becoming commonplace in our country, pointing out their assumptions and therefore its consequences, proceeding, for this purpose, a study for reflection and discussion.The specific objective, Discuss Law 12,737 of 2012. It's called "Law Carolina Dieckmann" - so dubbed because it coincides with a leakage intimate pictures of the actress. Work will be performed using the literature method. Through bibliographical research in codes, doctrines, legal or not magazines, books and internet.

Palavras-chave: Hackers. Cybercrimes. Internet. Crimes virtuais. Computadores.

INTRODUÇÃO

Nos dias atuais, a internet se tornou indispensável para grande parte da população mundial. Mas infelizmente, alguns criminosos têm utilizado esse avanço para realizar práticas delituosas com o intuito de obter para si, vantagem em proveito de outros internautas. A tipificação dos crimes cometidos no ciberespaço é imprescindível para que os poderes públicos possam acompanhar a dinâmica de um mundo globalizado.

Dezoito anos depois de a internet ser apresentada aos brasileiros, o país finalmente reconheceu que alguns crimes podem ser cometidos no ambiente proporcionado pela rede. Na terça-feira, do dia 2 de abril de 2013, o Código Penal passou a contar com artigos que tipificam os chamados "delitos

informáticos" e instituiu penas para quem cometer esses atos. Neste dia entrou em vigor a Lei 12.737 de 2012, que propunha as alterações ao Código Penal. É a chamada "Lei Carolina Dieckmann" - apelidada assim por coincidir com um vazamento de fotos íntimas da atriz. A lei não tem relação direta com o caso da artista, ela é resultado de anos de discussões políticas. Ela surgiu, pelas mãos do deputado federal Paulo Teixeira (PT-SP), principalmente como alternativa à "Lei Azeredo", que apesar de dispor sobre o mesmo tema, vinha sendo considerada perigosa para a liberdade do usuário da rede.

O que muda é que o Decreto-Lei 2.848 de 1940 do Código Penal que agora possui tópicos sobre violação de equipamentos e sistemas - sejam eles conectados ou não à internet - com intenção de destruir dados ou informações, ou instalar vulnerabilidades.Também são instituídas penas, que nos casos menos graves, como "invasão de dispositivo informático", varia de três meses a um ano de prisão e multa.
Já os mais sérios, como invasão para obter “comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas”, podem render de três meses a dois anos de prisão, além da multa. É considerado grave divulgar, comercializar ou transmitir o conteúdo.O ponto positivo disso é o fechamento de uma lacuna, em relação ao fato de que até então não existiam menções ao universo virtual em nosso sistema penal. A invasão nem era uma conduta criminosa.

QUAL A EFICÁCIA DAS LEIS EM VIGOR

Por serem crimes que dependem de perícia, os descritos na lei precisam da máquina policial, o que não é boa idéia, na opinião do jurista e cientista criminal Luiz Flávio Gomes. A polícia só descobre 8% dos homicídios no Brasil, então ela tem de ser mantida longe dos crimes de informática pois, não tem estrutura para isso. O Instituto de Criminalística de São Paulo está um caco. A polícia não tem como atuar agora com a internet.

Há também a existência de 104 termos delicados no texto. Estão entre eles "invasão de dispositivo informático", "mecanismo de segurança", "vulnerabilidades", "interrupção" e "perturbação". Ao ser enquadrado com base

na lei, o acusado pode questionar cada um dos pontos, atrasando o processo. É esse o ponto que restringe a norma.Conforme a redação da lei, só será crime se o dispositivo de segurança foi violado. A invasão de computador sem senha, por exemplo, mesmo que o acesso não tenha sido autorizado, pode não ser punida. E quando se coloca dispositivos de segurança, outras condutas deixarão de ser punidas – como é o caso de conseguir senhas por outros meios, como com base em informações sociais, além da pena prevista na lei ser branda. A lei 12.737 prevê que crimes desse tipo serão punidos com multa mais detenção de seis meses a dois anos. Por isso, acabará sendo absorvida por outro crime. Por exemplo, quando ocorre a invasão e, posteriormente, a extorsão.

PROPOSTA POR PATRICIA PECK PINHEIRO.

Os brasileiros são os campeões, na internet, em solicitações de retirada de conteúdo disponibilizado em redes sociais. Acredito que isto se deva ao fato de sermos um povo com opiniões fortes, mas jocoso, acostumando a ver tudo "acabar em pizza" e á concepção de que, em nosso país, impera a impunidade. Estes fatores, reunidos, permitam criar um perfil de usuários de "moral mais frouxa".

A liberdade de expressão precisa ser ensinada nas escolas: como se expressar de forma ética e juridicamente correta, manifestar a opinião, o direito de protesto ou uma reclamação de consumidor, sem que se transforme em abuso de direito. O limite entre a liberdade e o crime é bem sutil e faz toda a diferença escolher as palavras que divulgarão para o mundo, em tempo real, um pensamento.

Precisamos de inclusão digital, com educação. Em um contexto tecnológico de compartilhamento de informações e produção de conhecimento colaborativo, as "regras do jogo" incluem desde a proteção da reputação e da imagem até os créditos autorais. A grande maioria não reflete sobre o que está comentando, publicando, ou melhor, documentando nas redes sociais. Infelizmente, para estes, é difícil exercer o arrependimento, pois o conteúdo se espalha rapidamente, e se perpetua.

A retirada de conteúdos de rede envolve, principalmente, ofensa digital, exposição de intimidade excessiva (em especial, envolvendo menores) e uso não autorizado de imagem, marca ou conteúdo.

Questão relevante é como orientar os jovens, que entram nas redes sociais, na grande maioria, mentindo a sua idade? O problema ético começa aí, pois os serviços eletrônicos destacam a responsabilidade dos pais de assistir os filhos nos ambientes digitais e estes não sabem, realmente, como os filhosprocedem na “ rua digital”.

A tecnologia não tem um mal intrínseco. Pode ser que este Brasil “digital” seja, de fato, mais transparente e, tão somente, gostemos de nos exibir, falar mal dos outros, fazer piadas de mal gosto e publicar fotos de pessoas sem autorização. Ou, talvez, a geração Y nacional não tenha sido bem orientada, desconhece as leis e as consequências para os seus atos.

Temos de preparar melhor os novos cidadãos da era digital, para o própriocrescimento do País em um cenário de mundo plano, sem fronteiras. Para tanto é essencial garantir a segurança das relações e a proteção dos indivíduos. Toda desavença digital que se torne uma ação de indenização geraprejuízos á justiça e a toda a sociedade, não apenas aos envolvidos.

Devemos investir em duas políticas públicas digitais: de educação e de segurança. No que se refere á primeira, urge a inserção, no conteúdo-base da grade curricular dos ensinos fundamental e médio, de escolas públicas e particulares, dos temas de ética e cidadania digital, abordando-se a proteção da identidade (contra falsa identidade e anonimato); o exercício responsável da liberdade de expressão (contra os abusos); o uso correto de imagens; e a produção e uso de conteúdos digitais, dentro das melhores práticas de direitos autorais (coibindo plágios e pirataria). Os jovens precisam aprender a fazer suas lições sem copiar o conteúdo alheio!

Quanto á segurança, impõe-se a criação de um “time” responsável pela vigilância das “vias públicas digitais”, para identificação rápida de incidentes e maior prevenção. Se o cidadão está na internet, o Poder Público e o Poder de polícia também têm que estar, com ambientes preparados e medidas que garantam a proteção dos usuários.

O País ficou mais justo através da infovia, que projeta artistas ao alcance mundial. Em questão de segundos, o meio pode tornar qualquer pessoa famosa, e propiciar o futuro sonhado que se restringia a poucos.

A mobilidade trazida pela rede, que gerou mais empregos a negócios, já alcança as classes C e D. Permitiu a redução de tarifas e custos, como o acesso a serviços públicos e bancários (inclusive, via celular), mais rápido, eficiente e com menos burocracia.

A conta tecnológica também agradece, pois o uso da Tecnologia da Informação e Comunicação (TIC) minimiza o uso do papel. O ativismo ambiental, crescente nas redes socais, chega a se financiar, através de doações no modelo comunitário-coletivo do "*Crowdfunfing"* (financiamento colaborativo).

Com a Internet, e a relação do eleitor-candidato ficou direta, de fato! A memória coletiva, reavivada nas redes sociais após o pleito, é importantíssima para o amadurecimentodas escolhas políticas e do exercício do direito ao voto. Tudo isso é um ganho!

Claro que o grande investimento em infraestrutura , nos últimos anos, viabilizou um Brasil mais democrático e informatizados, sem o que não teríamos incidentes, nem solicitações de retirada de conteúdo da rede. Mas nãopodemos gerar analfabetos digitais; os usuários têm que ser educados para o uso ético e seguro do ambiente digital.

O ideal não é retirar determinados conteúdos da rede, depois que o estrago foi feito, mas saber como publicá-los, dentro de um modelo mais avançado de cidadania e respeito. Precisamos deixar aos jovens o desejode criar e inovar, e a consciência de que o ferramental tecnológico deve servir ao bem social.

PROPOSTA POR REGINALDO CESAR PINHEIROS

Com a popularização da Internet em todo o mundo, milhares de pessoas começaram a se utilizar deste meio. Contemporaneamente se percebe que nem todos a utilizam de maneira sensata, e acreditando que a Internet é um espaço livre, acabam por exceder em suas condutas e criando novas modalidades de delito: os crimes virtuais.

Também conhecidos por Cybercrimes, estes novos delitos são interpretados, segundo a concepção do Secretário Executivo da Associação de Direito e Informática do Chile, Claudio Líbano Manzur, como sendo todos os atos ilícitos praticados através da Internet que venham a causar algum tipo de dano, seja ele patrimonial ou moral, ao ofendido.

Em um primeiro momento, vem a mente de muitos aplicadores do Direito a máxima "nullapaenanullacrimensinelegge", isto é, enquanto não houver leis específicas de repressão aos crimes virtuais, não será possível que exista por parte do Estado uma atuação coercitiva eficaz. Não se pode olvidar-se, todavia, que na maioria das vezes a Internet é apenas um instrumento de ação dos cybercriminosos. Daí ser conveniente dividi-los em **crimes virtuais puros, mistos** e **comuns.**

Os *crimes virtuais puros,* conforme contempla o advogado Marco Aurélio Rodrigues da Costa, é *"*toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas." (3) Neste ponto é que verifica-se a ação dos hackers*,* que são pessoas com profundos conhecimentos informáticos e que se utilizam desse *know-how* para obtenção de algum benefício ilícito ou simplesmente por vandalismo. Como no caso dos ataques aos *mega-sites* ocorridos recentemente.

Por sua vez, os crimes virtuais mistos são aqueles em que o uso da internet é condição *sinequa non* para a efetivação da conduta, embora o bem jurídico visado seja diverso ao informático. Ocorre, por exemplo, nas transferências ilícitas de valores em uma *home-banking.*

Os crimes virtuais comuns são, pois, assim entendidos, porque utilizam a Internet apenas como instrumento para a realização de um delito já tipificado pela lei penal pátria. A Rede Mundial de Computadores, acaba por ser apenas mais um meio para a realização de uma conduta delituosa. Se antes, por exemplo, a pornografia infantil era instrumentalizada através de vídeos e fotografias, hodiernamente, se dá através das *home-pages*. Mudou-se a forma, mas a essência do crime permanece a mesma.

Há de se destacar, nesse contexto, as enormes dificuldades enfrentadas pelas autoridades responsáveis pela segurança no país para reprimirem este tipo de ação delituosa. Nesse sentido, o professor Antônio Scarance Fernandes

assinala: "Por enquanto a repressão se restringe ao enquadramento desse tipo de infração nos delitos tipificados pelo Código Penal". (4) Ou seja, atualmente, somente os crimes virtuais mistos estão sendo impugnados pelo nosso ordenamento.

Em verdade, a repressão aos cybercrimes também tem encontrado barreiras referentes a conquista de provas materiais. A internet propicia, devido a sua rapidez, a possibilidade de ser eliminada a qualquer momento quaisquer vestígios necessários para a comprovação do delito. Tem-se constatado, independentemente do crime ser puro, misto ou comum, que na maioria das vezes estes delitos ainda permanecem impunes, porque ainda *"continuam a ser novidade"* para os mecanismos coercitivos estatais.

Entretanto, há uma luz ao fim do túnel, isto é, o Direito e o Estado tem trabalhado para a reversão desse quadro anárquico-cibernético. Neste aspecto, o provedor de acesso, é elemento ímpar para a corroboração da punição destes crimes. Nos furtaremos a abordar integralmente a responsabilidade do provedor, mas é importante ressaltar certos aspectos se perfazem relevantes para a tal estudo.

O provedor de acesso, salvo algumas exceções, tem interesse econômico na prestação de serviços de acesso a rede. Logo, todas as informações constantes em seu banco de dados tem alguma relevância. Quando estas informações já não são mais importantes, o provedor as elimina de seu banco de dados. Neste aspecto é que a barreiras surgem, pois independentemente do provedor ser gratuito ou não, estas informações, na maioria das vezes são elementos que comprovam tal conduta delituosa.

A polícia tem conseguido reprimir os cybercrimes se utilizando dos chamados IP (*Internet Protocol),* que identifica através do seu respectivo número a localização do info-marginal. Neste caso o provedor de acesso é obrigado a fornecer a referidas informações para a consubstanciação da prova. Se no caso de ofensa moral a uma pessoa em uma sala de bate-papo, por exemplo, será através deste IP que poderá ser comprovado tal ofensa, para efetivação da punição *a posteriori*. Por isso se faz necessária a existência de mecanismos mais rígidos com relação as atividades do provedor de acesso, sobretudo, exigindo o armazenamento das informações de cada usuário pelo prazo de no mínimo um ano.

Por outro lado, mesmo a Internet sendo uma *Teia de Alcance Mundial*, tem as polícias conseguido punir infrações além-mar, quer dizer, os limites legislativos essencialmente territoriais tem sido superados com o apoio de polícias de outros países e também com o auxílio de organizações mundiais. Mesmo sem existir de fato um tratado internacional, algo que alguns aplicadores do Direito julgavam ser a única forma para tal repressão.

Prova disso, foi a reunião de ministros da justiça e procuradores dos países integrantes da OEA (*Organização dos Estados Americanos*) realizada em março deste ano, na qual um dos principais temas foi a criação de mecanismos para coibir a ação *hacker* na Internet. A OEA, na ocasião afirmava: *"cuidem da segurança dos sites de vocês, senão assim fica mais fácil"* (5) para os cybercriminosos. Assim, o governo brasileiro deseja, o mais depressa possível, criar uma lei que possa punir com maior rigor esses info-delitos.

Tramitam no Congresso Legislativo, por sua vez, cerca de 14 projetos de lei pertinentes aos crimes virtuais, e no entanto, é perceptível o desinteresse do governo perante a matéria. Com a pressão da OEA, porém, acredita-se que ainda este ano se terá um lei vigorando no Brasil referente aos crimes virtuais.

Dois destes projetos vem ganhando a atenção nacional. Um pertencente ao Deputado Luiz Piauhylin e outro do Senador Renan Calheiros. Ambos são vistos com ressalvas, mas entretanto, adverte o próprio senador, dizendo que *"a tipificação desse tipo de delito pelas legislações de todos os países é medida urgente e que não pode esperar mais."* (6)

Deve-se levar em consideração sim, a urgência que se perfaz em nosso contexto, mas sobretudo, não se pode permitir que o Estado, sob o pretexto de atribuir maior segurança aos usuários da rede, viole os direitos de liberdade de expressão do cidadão. Como é o caso de art. 2.º, § 6.º, II e III, do projeto de lei do Senador Renan Calheiros, que define como crimes contra a moral pública e opção sexual, a divulgação de material pornográfico e a divulgação de sons, imagens ou informação contrária aos <u>bons costumes</u>, (7) respectivamente. Ora, se não se trata de pornografia infantil e nem de ofensa de privacidade, porque haveria o legislador de restringi-lo?

No espaço virtual, os defeitos e os atos ilícitos dos internautas se produzem com a mesma facilidade que no espaço real. Todavia, o Direito ao pretender

tutelar o bem jurídico do cidadão precisa, necessariamente acompanhar esta evolução, a fim de possibilitar tal garantia.

Contudo, é preciso que se ampliem os debates sobre a matéria, tanto por parte do governo, quanto pela sociedade civil, no sentido de informar aos usuários sobre os novos tipos de modalidades delituosas que estes estão sujeitos, até porque, os crimes virtuais não se restringem somente a ação dos *hackers*, ela é mais ampla. A tutela do bem jurídico virtual não pode restringir-se somente à produção de legislação específica.

CONSIDERAÇÕES FINAIS

A lei deveria ter sido elaborada com maior cautela, de forma a atender efetivamente às necessidades que a tecnologia vem trazendo para os cidadãos. E como a tecnologia muda a todo instanteprecisamos de termos mais genéricos na legislação em vigor.

As punições poderiam ser maiores para evitar que os criminosos tivessem o benefício do juizado especial criminal. No juizado especial criminal, dependendo de certos requisitos - como não ter sido condenado anteriormente, ou não ter usado esse juizado durante cinco anos - se a pena maior do crime em questão não ultrapassa dois anos, o réu tem direito de, em vez de cumprir pena, pagar cestas básicas ou prestar serviços à comunidade.

REFERÊNCIAS

PECK, PatriciaPinheiro Revista Jurídica CONSULEX 2011,Editora: CONSULEX,

Artigo – Redes sociais – **Liberdade de expressão ou abuso**?,Pag 20.

LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional/**

LIMA, Paulo Marco Ferreira. – Campinas, SP: Millennium Editora, 2005

PINHEIRO, Reginaldo César. **Os crimes virtuais na esfera jurídica brasileira.**
http://jus.com.br/revista/texto/1830/os-cybercrimes-na-esfera-juridica-brasileira

http://tecnologia.uol.com.br/noticias/redacao/2013/04/24/lei-carolina-dieckmann-so-vale-para-eletronicos-com-sistema-de-seguranca.htm

http://blogs.estadao.com.br/radar-tecnologico/2013/04/02/lei-carolina-dieckmann-e-lei-azeredo-entram-em-vigor-hoje-saiba-onde-denunciar/

http://www12.senado.gov.br/noticias/materias/2013/04/16/debatedores-divergem-sobre-necessidade-de-conceitos-de-informatica-no-codigo-penal

http://info.abril.com.br/noticias/seguranca/lei-carolina-dieckmann-entra-em-vigor-entenda-03042013-33.shl

http://jus.com.br/revista/texto/23655/lei-carolina-dieckmann

http://www12.senado.gov.br/noticias/search?SearchableText=lei+12.737

http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=33404&sid=4#.Ub_P8ue-pIg