

Direito Digital: O Impacto da Informação Digital no Mundo do Direito

INTRODUÇÃO

Com certeza, a tecnologia é, uma das condições indispensáveis para a vida moderna em que vivemos atualmente, já que vivemos em um mundo onde a presença de computadores, celulares e demais aparelhos eletro-eletrônicos fazem parte do nosso cotidiano. Isso significa que cada dia está mais dependente do mundo tecnológico e que cada dia vem crescendo mais para atender as necessidades da sociedade digital como também da futura geração informatizada.

Estamos vivendo em um momento onde não sabemos até onde vai nossa liberdade dentro da rede de computadores, ou seja, não sabemos até onde vai a ética legal dentro da sociedade digital e como também usar adequadamente as ferramentas tecnológicas no trabalho. Até onde vai nossa privacidade? Quais as consequências do monitoramento dentro da empresa? Em relação ao email, pode considerar como correspondência? Os dados eletrônicos como “logs”, nós podemos considerá-los como prova criminal? E enviar um “spam” e vírus, significa crime? Quem tem essas respostas e soluções para tantas dúvidas, tem a oportunidade de se diferenciar. Portanto, esse é o papel exigido e cobrado dos operadores do Direito, que sejam advogados, magistrados, promotores, peritos ou procuradores.

Portanto, esse trabalho trata-se de como o Direito pode adequar-se à nova realidade de um mundo digital com freqüentes inovações e totalmente interligados a internet, email, TV interativa, dentre outros.

OBJETIVO GERAL

Podemos encontrar a tecnologia, dentro das nossas casas, escolas, corporações como empresas, banco, serviço público, dentre outros, ou seja, estamos cercados em um mundo totalmente digital. Nossas ruas, avenidas e estradas, enfim, em todos os segmentos sociais, está lá, a tecnologia a nosso alcance. Os recursos trazidos pela televisão, rádio, *internet*, *fax*, equipamentos de áudio e vídeo, *scanner*, telefones fixos e móveis, entre outras maravilhas tecnológicas, vêm distribuindo e agregando conhecimento, informação, cultura, hábitos, valores, ou seja, formando e interferindo, cada vez mais, na formação de pessoas e sociedades. Isso resulta numa dependência, sem limites, do homem aos benefícios que essas máquinas trazem, passíveis de eternas evoluções e revoluções para atender as necessidades humanas.

Porém, apesar de ser rotina para tantos executar ações como enviar um email, seja ela para um amigo ou colega de trabalho, falar ao celular, acessar a internet pelo celular, acessar o Internet Banking, ler uma notícia online, escrever um conteúdo em um Blog, participar de uma rede social, utilizar um *tablet*, participar de um Chat, fazer compras online, tirar uma foto digital, preencher um cadastro em um *Hotsite* de promoção, porém, para muitos essas ações não são claras quando se tratam dos limites de responsabilidades envolvidas nessas atividades. Pois, não é fácil de entender que um email da empresa é o papel timbrado da empresa e que todo conteúdo do escrito na internet é de responsabilidade de seu autor, que enviar uma “fofoca” pelo email ou Chat poderá gerar responsabilidade civil e criminal, que registrar uma palavra-chave com nome de um

concorrente é crime de concorrência desleal, que a comunidade Online nunca se pode falar de questões da empresa protegidas por sigilo profissional, que furto de e-mails da empresa é tão condenável quanto furto de um bem físico.

Entretanto, aprendemos desde criança que não podemos deixar a porta de casa aberta, o que é mesmo que dizer, que não devemos deixar o computador aberto e sem segurança. E que não devemos falar com estranhos, é o mesmo para não abrirmos um e-mail de alguém desconhecido e que não utilizar o cinto de segurança no carro, é o mesmo em dizer que não devemos deixar o computador sem antivírus e firewall.

Aliás, como no mundo real, o crime suspira em cada esquina de nossas casas, na internet o crime está em cada clique de alguém sabendo ou não está praticando. Estamos correndo perigo sem percebermos, pois tudo é apenas um e-mailzinho, apenas um arquivozinho e com isso pode ser uma quebra de sigilo, crime de difamação, de falsa identidade, de fraude, podendo gerar responsabilidades civis, criminais, trabalhistas, tanto para pessoa como para empresa.

OBJETIVO ESPECÍFICO

É de suma importância que da mesma forma que a tecnologia veio para facilitar a vida das pessoas, em uma velocidade imaginária e inteligentemente capacitada para atender todas as nossas necessidades de hoje e futuras, da mesma forma ela pode ser uma ferramenta, uma "arma" onde se comete vários crimes, sejam eles civis ou criminais. Algumas condutas ilícitas, já existentes no mundo real, como pedofilia, racismo, pirataria, com a internet, ou seja, com a rede de computadores, esses crimes propagaram em uma velocidade muito rápida, surgindo muitos crimes ainda não solucionados e praticados na rede de computadores. Bem como, o envio de vírus por e-mails; as fraudes bancárias e de cartões de crédito, etc.

Portanto, existe ainda hoje uma bipolarização em torno de que bem jurídico é fundamentalmente protegido pelo Direito Penal de Informática, se os sistemas ou se as informações.

É importante que o Direito Criminal de Informática com os sistemas de computadores e de comunicação deve-se, fundamentalmente, à proteção dos seus componentes imateriais ou intangíveis, ou seja, o "software" e dados, e os dados que ainda não contam com a mesma proteção do outro componente, o "hardware".

Embora haja uma diferença entre "hardware" e "software", não podemos dizer o mesmo quanto às implicações jurídicas. Em relação ao Direito, este ainda caminha lento em que se trata de um sistema jurídico que proteja os bens incorpóreos e imateriais tão bem como os bens materiais.

Salientando que em relação a bens imateriais, lembramos da propriedade intelectual, como o Direito do Autor, que é um mecanismo de proteção da propriedade imaterial, que objetiva proteger o autor da obra.

MARCO TEÓRICO

Falando da origem da internet, essa surgiu no ápice da 'guerra fria', em meados dos anos 60, nos Estados Unidos, e foi pensada, originalmente, para fins militares.

Tratava-se de um sistema de interligação de redes de computadores que os militares norte-americanos utilizava. À época, denominava-se "Arpanet". Era como uma tática revolucionária em

caso de ataque inimigo a alguma de suas bases militares, as informações no computador existentes não se perderiam, já que não existia lá, uma base de informação.

Depois foi que a internet veio a ser utilizada por civis, mas apenas em algumas universidades norte-americanas, com o objeto dos professores e alguns alunos traçarem informações acadêmicas, como meio de propagar estudos científicos.

Mais ou menos há quarenta anos, a internet não passava de um projeto a ser realizado, o termo “globalização” ainda não era difundido e transmissão de dados por fibra óptica não se cogitava a sua existência. Obter informação era um item caro, pouco acessível e centrado. O cotidiano do mundo jurídico resumia-se a papéis, burocracia e prazos. Com as mudanças ocorridas desde então, ingressamos na era do tempo real.

É importante saber que vivemos em um momento único, tanto no aspecto tecnológico como econômico e social. O profissional de qualquer área, em especial do Direito, tem a obrigação de estar em sintonia com as mudanças que ocorrem com a sociedade.

Toda mudança tecnológica é uma mudança social, comportamental, portanto jurídico.

METODOLOGIA

Tendo em vista que todos esses surgimentos de tecnologia, também vieram os crimes cibernéticos, onde devemos chamar atenção. Como no caso de Fraudes nos meios informáticos, que justamente ocorre quando um determinado indivíduo ao comprar, vender ou investir via Internet é enganado de alguma forma. Como também, quem está vendendo o produto, pode descrever o produto indevidamente, com o intuito de enganar ou pode, ainda, receber o pedido e o dinheiro, mas não entregar o bem ao qual estava obrigado. Esses tipos de crimes são muitos freqüentes.

Estelionato, é outro tipo de fraude, onde um terceiro cria um site falso, por exemplo, um site de banco, para “furar” os dados do cartão do usuário do banco. Ainda, pode acontecer que o usuário enganado, informe dados do cartão ao comprar algo na internet por meio de um site falso, desta forma, chegando até ter seu cartão clonado e desta feita, ser utilizada pelo criminoso indevidamente, criminalmente.

Pode está acontecer de três formas: mercadorias físicas - quando se compra algo pela Internet, por exemplo, como livros; digitais – quando envolve mercadorias digitais, como programas de computador.

Também como Crime contra honra, que são crimes de calúnia, injúria e difamação, presentes nos artigos 138 a 140 do código Penal. Tais crimes podem ser cometidos através de salas de bate-papo, *homepage* e e-mail. As Acesso indevido/ ilegal/ não autorizado – *Hacking*: a violação de dados ou de sistemas é acesso não autorizado de alguém (hacker) a dados, programas e sistemas de natureza pessoal ou confidencial.

Esse tipo de crimes, trata-se de um determinado sistema por particular que tenha permissão insuficiente, ou usuário externo ao sistema, acessando-o sem permissão.

Portanto, ao invadir a privacidade de uma pessoa, esse pode também está possuindo dos dados e bens digitais de outrem. Levando informações sigilosas.

O crime de hacking é quando um criminoso entra em um sistema escolar sem a permissão devida e altera notas dos alunos e colando links onde os alunos possam entrar em sites pornográficos. .

No nosso país, Brasil, esse é um problema muito preocupante pois não há legislação no que se trata da privacidade na internet, pelo fato de que poucos sites se importam com as regras de

privacidade, considerando ainda que, dos poucos que dispõe de alguma política a esse respeito, muitos são os que não a possuem de uma maneira clara para o usuário.

Porém, enquanto não existe nenhuma justiça da informática em nível internacional, temos que, urgentemente, em nível nacional atualizar nossa legislação e aprovar o projeto de lei do Deputado Luis Piauhilino, que dispõe sobre os crimes de informática e que está em tramitação no Congresso Nacional; portanto, seria um bom começo para combater com as fraudes e violações de dados nos sistemas de computadores

CONCLUSÃO

É de suma importância que uma legislação mundial faça um controle da internet, pois com esta, solucionaríamos muitos crimes e fraudes web, fazendo que muito não pratiquem esses tipos de ações. Ainda salientando que é um perigo a internet sem leis, causando um descontrole e podendo ainda que venham a praticar crimes como controlar a humanidade. Uma legislação mundial deve preservar ao máximo os direitos fundamentais, dando grande importância à liberdade individual, ou seja, é necessária uma legislação mundial orientada pela ética e pela liberdade de utilizá-la de forma para o bem da sociedade.

REFERÊNCIAS

Costa, 1995, Costa, Marcos Aurélio. **Jus Navigandi**. HYPERLINK "<http://jus.uol.com.br/revista/texto/1826/crimes-de-informatica/4>" - acessado em 25.05.2011.

Matins, 2011, Martins, **Renata Durval**. Âmbito Jurídico. HYPERLINK "http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=5381" - acessado em 25.05.2011

Pinheiro, 2010, Pinheiro, Patrícia Peck. **Direito Digital**. 4ª edição. Ed. Saraiva. São Paulo, SP.

Proposta de um Software Educacional para Terceira Idade Utilizando IHC PAGE 1

Indicador de seleção