O DIREITO FRENTE ÀS MUDANÇAS NO ESPAÇO CIBERNÉTICO

Fernanda Ribeiro Gildo[1]

Antônio Dhiêgo Carneiro Martins[2]

Sobral–CE
2014

RESUMO

O objetivo do presente trabalho é analisar a rápida evolução do meio digital, sob o enfoque jurídico. São inovações e tendências tecnológicas e sociais que causam preocupação, pois ao passo que evolui, o direito vai ficando para trás, deixando de proteger as relações pessoais e econômicas decorrentes desse meio. Essa evolução propicia o surgimento de uma nova espécie de criminalidade transnacional, que altera a concepção de território, criando o ciberespaço. O principal objetivo desta pesquisa é analisar as transformações que essa nova realidade trouxe em várias áreas, e a legislação a elas aplicadas, verificando também a sua eficácia quando se trata de punir aqueles que agem por meio da facilidade e liberdade que esse novo espaço propõe para cometerem crimes. No decorrer do trabalho iremos analisar o avanço tecnológico e virtual que hoje faz parte do dia-a-dia da humanidade, seu contexto histórico, seus benefícios, bem como os perigos, já que muitas vezes podem causar prejuízos irremediáveis. Com a mudança da sociedade o direito também deve mudar, pois assim como no “mundo real”, estamos correndo perigo a cada esquina, na rede estamos sujeitos a cada clique, e o pior é que na maioria das vezes nem nos damos conta disso e tudo acaba parecendo inofensivo. Diante desses riscos, apesar de nossas leis terem demonstrado bastante evolução, ainda há muito com o que se preocupar, muitas lacunas a serem preenchidas até que nossa imagem e informações estejam seguras na rede, e é isso que iremos abordar.
.

PALAVRAS – CHAVE: *Internet*. Direito Digital. Espaço *Cibernético*. Tecnologia. Crimes Virtuais.

INTRODUÇÃO

Há quase 50 anos, a internet era apenas um projeto, não ouvíamos falar na expressão globalização e não havia transmissão de dados por fibra óptica. A informação era cara, poucos tinham acesso, o mundo jurídico era resumido em folhas de papeis, prazos e procedimentos burocráticos. As mudanças começaram a surgir e a partir de então começamos a adentrar na era do tempo real, na quebra de paradigmas. Essa novidade traz transformações em várias partes da sociedade. Não só mudanças tecnológicas, mas também de conceitos, formas de trabalho e estruturas. O direito também é dominado por essa nova realidade. A dinâmica da era do conhecimento exige do direito uma transformação profunda na própria forma de seu exercício.

O momento que vivemos é único, tanto na esfera tecnológica como econômica e social. Todos os profissionais, independentemente da área, mas em especial os do direito, devem estar em sintonia com as transformações que ocorrem na sociedade, e sabemos que a internet é a principal responsável por esse momento de transformação. A internet não é apenas um simples meio de comunicação formada por uma rede mundial de computadores, mas principalmente formada por indivíduos, que incluem pessoas físicas, empresas, instituições e o próprio governo.

O ano de 1990, época da criação do primeiro Código Brasileiro de Defesa do Consumidor, e 1995 quando o Ministério das Comunicações publicou a norma reguladora do uso dos meios de rede pública de telecomunicações para provimento e a utilização de serviços de conexão a internet, o que marcou o nascimento comercial do sistema do país. Foram fatos históricos cruciais ao amadurecimento de inúmeras questões jurídicas, e colocam o Brasil em condição de alcançar as mudanças globais, em conjunto com as nações de ponta.

Qualquer evolução tecnológica causa mudanças sociais e comportamentais, ou seja, mudanças jurídicas. Quando a sociedade se transforma, o direito também deve se alterar e evoluir. Nesta pesquisa devem ser percebidas as transformações que o direito vem passando, viver esta nova era que é a era digital, e abordar as profundas mudanças que ocorrem na sociedade contemporânea.

NOVOS INSTITUTOS JURÍDICOS DE DIREITO DIGITAL

JUSTIÇA DIGITAL - PROCESSO ELETRÔNICO

Estamos vivendo um marco histórico, que é a migração para o processo eletrônico. Nos últimos tempos, as decisões judiciais vêm se aprimorando em relação aos temas de direito digital, principalmente no que se refere a provas eletrônicas na Justiça.

A Lei n. 11.419/2006 é o marco regulatório da informatização judicial, pois abrange todas as fases e atividades para a fixação do processo judicial informatizado em todo país, em todos os órgãos e graus do Poder Judiciário no Brasil, adotando como válido todo e qualquer ato processual realizado por meio eletrônico, como afirma no caput do seu artigo 11:

> Art. 11° Os documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário, na forma estabelecida nesta Lei, serão considerados originais para todos os efeitos legais.

Na esfera da administração pública, também já se faz uso da digitalização do processo do Tribunal de Contas da União, que se deu início pela PORTARIA – TCU n. 189/2007 que aprova a realização do Projeto processo Eletrônico Administrativo, Segedam Sem Papel e designa o seu gestor.

Para se determinar a autenticidade dos atos processuais eletrônicos há dois modelos, um deles é o uso de um certificado digital da ICP – Brasil. Como podemos ver nas decisões judiciais a seguir:

> CERCEAMENTO DE DEFESA. CONTRARRAZÕES ENVIADAS POR EMAIL SEM CERTIFICAÇÃO DIGITAL. NÃO CONHECIMENTO. Uma vez delimitado na decisão recorrida ter sido utilizado o sistema e-doc de peticionamento eletrônico para o envio das contrarrazões ao recurso ordinário, sem a necessária certificação digital, tal como requerida na Instrução Normativa n. 3/2006 do eg. Tribunal Regional, que regula esse sistema integrado de protocolo de documentos eletrônicos (...) Recurso de revista não conhecido no tema. (TST, RR – 365/2007-148-03-00.0 , Relator Ministro: Aloysio Corrêa da Veiga, j. 26-8-2009, 6ª Turma, Data de Publicação: 4-9-2009).
>
> AGRAVO DE INSTRUMENTO. RECURSO DE REVISTA. IRREGULARIDADE DE REPRESENTAÇÃO. (...) A tese da Recorrente de que o substabelecimento foi digitalizado, não lhe assiste, pois, da análise dos autos, verifica-se que a referida assinatura não lhe confere a indispensável certificação digital que decorreria da utilização de chaves

> criptografadas, o seria possível pelo atendimento do disposto na Instrução Normativa 28/2005 desta Corte. Agravo de instrumento a que se nega provimento. (TST, AIRR – 740/2006-491-05-40.1, Relator Ministro: José Simpliciano Fontes de F. Fernandes, j.17-6-2009, 2ª Turma, Data de Publicação: 31-7-2009).

O outro modelo para se determinar a autenticidade dos atos processuais eletrônicos é o uso de uma senha de usuário previamente cadastrada junto ao Tribunal, o que vem sendo exigido que se faça de início presencialmente, para a verificação de identidade e documentos.

São vários os desafios da Justiça Digital, bem como são vários os benefícios. Um deles é que conseguiremos ter ações mais céleres, tendo em vista que, eliminando os papeis, elide-se boa parte da burocracia. No entanto, a preocupação é a capacidade do ambiente de processo eletrônico do judiciário para garantir a autenticidade, o segredo de justiça e a integridade por meio de segurança da informação evitando adulterações de dados nos sistemas, enfim, criar cultura nos operadores de direito.

Este é o caminho para uma sociedade sem papel, porém não uma sociedade sem documentos, pois o documento é um escrito capaz de ter compreensão humana, independente do material em que ele esteja gravado.

A sociedade digital se torna muito melhor documentada, mas controlada, mais transparente, mas ainda é necessária a quebra de paradigmas culturais e atualizar os usos e costumes, a fim de atender a essa nova realidade.

O Poder Judiciário brasileiro vem se preparando para esta mudança, com o advento do novo Código de Processo Civil que adota o processo eletrônico, cujo trâmite legislativo se encontra no Senado Federal para análise derradeira, antes de sanção pelo Poder Executivo.

FISCO DIGITAL

Nos últimos anos, a vida dos brasileiros contribuintes de imposto de renda mudou quando a receita Federal passou a aceitar a declaração pela internet. Um dos primeiros requisitos que podemos observar é a exigência de uso de um certificado digital com base na ICP-Brasil, que determinou que desde 2010 as empresas de lucro presumido devem enviar declarações e demonstrativos com certificado digital.

Por toda essa característica de aumento de blindagem ou segurança jurídica, já deveria ter-se adotado pelas empresas a inversão do ônus da prova, porém talvez ainda não tenha ocorrido por não possuir um caráter obrigatório.

A intenção é apenas obter o maior número de informações por via do *site* da Receita Federal, evitando a ida a uma Secretaria da Receita, porém ainda há pouca aceitação devido à falta de cultura de uso de arquivamento de documentos pela Internet no site da Receita.

O Sistema Público de Escrituração Digital (SPED) iniciado em janeiro de 2007 foi implementado pelo Programa de Aceleração de Crescimento (PAC 2007-2010) do Governo Federal, como parte das medidas de aperfeiçoamento do sistema tributário e remoção de obstáculos burocráticos ao crescimento econômico (Decreto n. 6022/2007). O mesmo é constituído por três elementos que seguem nos artigos a seguir:

> Art. 1º Fica instituído o Sistema Público de Escrituração Digital - Sped.
>
> Art. 2º O Sped é instrumento que unifica as atividades de recepção, validação, armazenamento e autenticação de livros e documentos que integram a escrituração contábil e fiscal dos empresários e das pessoas jurídicas, inclusive imunes ou isentas, mediante fluxo único, computadorizado, de informações.

A ECD foi instituída pela IN RFB 787/2007 e é o envio de informações contábeis como razão, balancetes, diárias, balanços, fichas de lançamentos e auxiliares e outros. Essas informações são enviadas de forma digital visando a substituição dos livros físicos e sua eventual extinção. Já a EFD é um arquivo digital com informações referentes às operações, prestações de serviços e apuração de impostos do contribuinte.

A verdade é que cada vez mais a tendência é o fisco ser digital na realização de suas atividades. Passamos então a alinhar questões de segurança dessas informações aplicadas a estes ambientes dentro da autoridade fiscal e do Poder Público, como também passamos a questionar os limites de uso e interpretação deles, que não podem ser arbitrários e tampouco ilimitados.

SAÚDE DIGITAL – PRONTUÁRIO ELETRÔNICO

Como já vimos o Judiciário e o Fisco estão cada vez mais digitais e na saúde não é diferente. Essa questão traz discussões sobre Prontuários Eletrônicos, diagnóstico por imagem, uso de biometria para identificar pacientes substituindo o cartão de identificação do plano, criação de um banco de dados único de Saúde, documentações digitalizadas, e eliminação do papel para liberar leitos em hospitais.

A saúde do nosso país é tradicionalmente descentralizada, possui diferentes agentes, e tem como base escritural a documentação em papel. Todavia cada vez mais o uso de Tecnologia da informação na saúde, bem como informações eletrônicas, aumentam o nível de segurança e diminuem as fraudes, além de diminuir a burocracia e por sua vez o tempo para o atendimento, aumentando o padrão de qualidade, beneficiando a todos.

O Conselho Regional de Medicina de Santa Catarina (CREMESC) manifestou-se sobre o assunto desde 1997, sobre o uso da tecnologia para o médico poder cumprir as exigências legais.

O direito aos dados do prontuário médico sempre foi do paciente, e cabe exclusivamente a ele. Porém, a geração do prontuário médico e a sua guarda acaba sendo dos profissionais de saúde. No entanto, é só um paciente ou um familar necessitar de suas informações e já se inicia uma disputa na maioria da vezes jurídica, visto que, aqui há toda uma questão de sigilo médico envolvido.

Outro aspecto importante diz respeito à privacidade. Os dados sobre a saúde de um determinado indivíduo são bastante sigilosos e sensíveis, tendo em vista o impacto que poderão gerar.

Em relação à privacidade desses dados, há muita divergência. Enquanto determinado paciente deseja que saibam o que ele possui de histórico para ser melhor atendido em caso de emergência, de outro lado, temos um responsável pela área de recursos de uma empresa querendo saber se existe alguma doença preexistente que não tenha sido declarada pelo colaborador, para decidir se afirma ou não a sua contratação. No caso de um plano de saúde pode significar uma comprovação de veracidade da declaração de saúde de um novo solicitante do plano.

Essas questões são todas reguladas por leis, como por exemplo o artigo 5º, inciso X, da Constituição Federal de 1988, no tocante a intimidade:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

Em relação ao sigilo profissional o artigo 154 do Código Penal Brasileiro:

> Art. 154 - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem:
>
> Pena – detenção, de três meses a um ano, ou multa.
>
> Parágrafo único – Somente se procede mediante representação

Em especial a Resolução n. 1821/2007 aprova as normas técnicas sobre digitalização e uso de sistemas informatizados para uso, guarda e manuseio dos documentos dos prontuários dos pacientes. Existem duas situação que precisam ser trabalhadas: aquilo que já foi gerado no papel e que deve ser arquivado a longos prazos, e a partir de então para o futuro que o documento já nasceria eletrônico, evitando riscos e custos por sua tramitação em papel.

Não restam dúvidas quanto aos benefícios da saúde digital, mas sim sobre a capacidade de se garantir segurança e privacidade das informações, em que deveria existir controle e restrição aos acessos às informações, havendo autorização dos envolvidos.

No que se refere ao prontuário médico eletrônico, é uma grande evolução, principalmente pela facilidade de leitura, evitando a dificuldade muitas vezes em identificar aquilo que foi escrito a mão pelos médicos. Porém, sabe-se que é um desafio para o setor de saúde, tendo em vista a necessidade de treinamento, de capacitação dos profissionais para uso do computador de forma obrigatória.

A saúde digital é essencial, mas é imprescindível também que haja uma padronização e homologação dos sistemas pelas instituições que regulam a saúde, bem como o investimento em capacitação. Outra característica que não deve deixar de existir é a confiabilidade, ou seja, os dados inseridos devem ser autênticos e íntegros. Havendo um sistema de biometria, ou assinatura digital garantindo que os dados foram inseridos pelo médico. Inclusive, esse assunto já foi objeto de apreciação pelo Conselho Federal de Medicina no Parecer 30/2002 que trata sobre o uso de certificado digital da ICP/Brasil:

> **PROCESSO-CONSULTA CFM Nº 1.401/2002 PC/CFM/Nº 30/2002**
>
> **INTERESSADO**: Dep. E. F.
>
> **ORIGEM**: Congresso Nacional
>
> **ASSUNTO**: Prontuário eletrônico
>
> **RELATOR:** Câmara Técnica de Informática em Saúde do CFM (Cons. Mauro Brandão Carneiro, dra. Beatriz de Faria Leão, dr. Luiz Augusto Pereira)
>
> **EMENTA:** Os prontuários elaborados em meio eletrônico poderão assim permanecer, bem como os novos a serem criados, desde que obedeçam ao disposto em resolução específica do CFM. Os prontuários médicos atualmente existentes em papel somente podem ser destruídos após serem microfilmados observados os trâmites legais. As unidades de saúde deverão constituir Comissão Permanente de Avaliação de Documentos e Comissão de Revisão de Prontuários.

Também é interessante que se acompanhe o Projeto de Lei PLS n. 474/2008, que altera a Lei n. 8.080/90, e dispõe sobre a informação dos serviços de saúde:

> Art. 38-A determina que o uso de meio eletrônico em prontuário de paciente, assim como no registro, na comunicação, na transmissão e na autorização de procedimento ambulatorial e hospitalar de resultado e laudo de exame, de receita médica e das demais informações de saúde serão admitidos nos termos desta Lei.

Portanto, percebe-se o quanto é importante que a saúde acompanhe a evolução digital da sociedade da informação, tomando o máximo proveito disso.

CRIMES ELETRÔNICOS

É delicado falar sobre crimes na era digital, principalmente porque sem a devida redação do novo tipo penal corre-se o risco de se punir alguém inocente. Além disso, sabemos que quando se trata de usar máquinas como se fossem testemunhas não sabemos quando se trata de culpa ou dolo, isso quer dizer que um computador não traz informações sobre o contexto da situação, e muito menos se ação foi com intenção ou não. Um exemplo disso é a tentativa de se tipificar o crime de envio de arquivo malicioso em *e-mail.*

Atualmente existem novas condutas, como também condutas antigas que devem receber uma nova tipificação. Por esse motivo necessitamos para abordar crimes eletrônicos, de uma grande atualização do Código Penal brasileiro, do Código de Processo Penal brasileiro e da Lei de Execuções penais, porém nada disso terá utilidade sem um modelo forte de prova de autoria, de uma identidade digital obrigatória.

O crime eletrônico de início é um crime meio, isto é utiliza-se de um meio virtual. Não é um crime de fim, por natureza, ou seja, o crime cuja modalidade só ocorra em ambiente virtual, à exceção dos crimes cometidos por *hackers*, que de alguma forma podem ser enquadradas na categoria de estelionato, extorsão, falsidade ideológica, fraude, entre outros. Isso significa que o meio de materialização da conduta criminosa pode ser virtual, contudo em alguns casos o crime, não. Fortalecendo esta corrente de pensamento, temos o julgamento pelo Ministro Sepúlveda Pertence, do STF de um habeas corpus (76689/PB 22-9-1998) sobre crime de computador:

> Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminosa, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo.

A maior parte dos crimes que ocorrem na rede também é cometida no mundo real. A internet representa apenas um facilitador, especialmente pelo anonimato que esse meio proporciona.

A depender do bem jurídico tutelado os crimes eletrônicos possuem modalidades distintas. Podemos citar como exemplo o crime de interceptação telefônica e de dados em que se tem como bem jurídico tutelado, os dados, o que se quer proteger é a transmissão de dados e coibir o uso dessas informações para fins delituosos, como por exemplo, o envio de *e-mail bombing*, que é o envio de e-mails imensos ou vários *emails*, que causa atraso na recepção e gasto adicional com conta telefônica, em que é aplicável o artigo 163 do Código Penal: “Destruir, inutilizar ou deteriorar coisa alheia: Pena - detenção, de um a seis meses, ou multa”.

O anonimato na rede é relativo, pois o IP constitui uma forma de identidade virtual para o Direito Digital, porém algumas identidades virtuais não correspondem a identidade real. Por analogia da mesma forma ocorre em contas e empresas fantasmas cuja identidade física pode ser falsa.

No Brasil os crimes mais comuns na rede são o estelionato e a pornografia infantil. O artigo 171 do Código Penal define estelionato:

> **Art. 171** - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
> **Pena** - reclusão, de 1 (um) a 5 (cinco) anos, e multa.

Os e-mails gratuitos são outro agente de expansão, pois seus dados não são necessariamente comprovados. Uma prática recomendável seria obrigar os provedores a identificar suas contas ativas e inativas, ou seja, ter a comprovação dos seus dados, isso com uma prática de cadastro de seus usuário, com o mesmo procedimento usados pelos bancos, permitindo que haja realmente meios de provas confiáveis.

Se observarmos, podemos perceber que diferente dos servidores gratuitos, nos servidores pagos é mais fácil identificar os usuários e restringir as práticas delituosas, pois, os bancos de dados exigem maior detalhamento.

Porém a responsabilidade de operar com senhas difíceis é do usuário, por sua vez cabe ao provedor conferir-lhe um software de criptografia adequado e atualizado.

É importante lembrar que após a internet móvel, a individualização do usuário cresceu, e fez com que o celular se tornasse o prolongamento de sua existência no mundo digital tendo em vista que ele realiza várias ações eletronicamente. O motivo pelo qual o roubo e o furto de celulares vêm crescendo

não é só pelos recursos adquiridos através da venda do aparelho e pelo uso da linha para ligações ilegais, mas sim para assumir a identidade da pessoa proprietária do aparelho por determinado período de tempo.

O maior problema jurídico dos crimes virtuais é a raridade de denuncias e, pior, o despreparo da polícia investigativa e de perícia para apurá-la.

Embora já seja possível fazer boletins de ocorrência pela internet, são poucas as equipes e profissionais preparados para a investigação de um crime virtual. Nos dias de hoje tornou-se muito fácil encontrar na internet o código fonte aberto de um vírus ou trojan. Para alguns é possível até mesmo a clonagem de sites, utilizando-os para roubar informações dos usuários, tais como RG, CPF, endereço, telefones, e-mail, dados bancários, informações suficientes para que o criminoso possa assumir outras identidades em operações comercias com uso de cartão de crédito clonado por exemplo.

A dificuldade para combater esses crimes torna-se difícil por dois motivos, primeiro pela falta de informação, ou mesmo falta de precisão e relevância dessas, quando são passadas as autoridades. Segundo, pela falta de recursos em geral das autoridades policiais.

A maioria das investigações sobre crimes virtuais exige quebra de sigilo. Todos os registros dos usuários que se conectam à rede, mantidos por seus provedores, gozam de proteção podendo ser requeridos apenas pela autoridade competente. Temos uma liminar nesse sentido, concedida pelo Juiz José Ricardo Machado, da 1ª Vara da fazenda Pública Municipal de Goiânia, que determinou que o provedor de serviços de acesso a Internet teria de quebrar o sigilo de cadastro de um de seus clientes para que fosse realizada sua identificação. Neste processo a Procuradoria-Geral do Município relata que, um cliente do UOL, transmitiu uma mensagem na qual divulgou a notícia tida como falsa pela administração pública.

No mesmo sentido, recentemente o STF foi acionado em um processo contra um jovem acusado pelo crime de pedofilia. A promotoria requereu e obteve do provedor, conversas em salas de bate-papo que comprometiam o acusado, o réu alegou quebra de sigilo das comunidades e recorreu. O recurso não foi acatado pelo STF, considerando que o ambiente virtual é informal e está fora do alcance da lei de sigilo e proteção à privacidade.

O Direito Digital possui a obrigação de atualizar-se tecnologicamente, e isso não serve apenas para advogados e juízes, mas também, para delegados, procuradores, investigadores, peritos e todos os demais participantes do processo. Essa mudança de postura é fundamental para alcançarmos uma sociedade digital segura, se isso não acontecer o próprio ordenamento jurídico estará em risco.

Os crimes virtuais ocorrem na maioria das vezes por um estímulo dado pela crença de que o meio digital é um ambiente marginal, um submundo onde rege a ilegalidade. E isso ocorre exatamente pela insegurança que a sociedade tem nesse ambiente, pelo fato de sentirem que o meio não é vigiado suficientemente e que seus crimes não são punidos adequadamente.

A lei n. 12.737, de 30 de novembro de 2012, conhecida como projeto Carolina Dieckmann, foi sancionada sem vetos. A lei ganhou o nome extraoficial, por que na época em que tramitava na Câmara de Deputados, a atriz teve fotos pessoais divulgadas sem autorização. A nova lei classifica como crime justamente casos como esse, em que há a invasão de computadores Dessa forma fica tipificado o uso de dados de cartões de crédito ou débito obtidos de forma indevida ou sem autorização. A Lei equipara essa prática ao crime de falsificação de documento particular. A multa é de 1 a 5 anos e multa.

A lei também criminaliza a invasão de dispositivos eletrônicos alheios conectados ou não à internet, tais como celulares, *notebooks*, *desktops*, *tablets* ou caixas eletrônicos, para obter ou adulterar dados no sistema e conseguir vantagem ilícita. Podemos acompanhar o que diz o artigo 2º da lei a seguir:

> Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:
>
> **“Invasão de dispositivo informático**
>
> 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.
>
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no **caput**.

> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
>
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
>
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
>
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
>
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
>
> I - Presidente da República, governadores e prefeitos;
>
> II - Presidente do Supremo Tribunal Federal;
>
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
>
> "IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."

Apesar do grande avanço que foi dado, infelizmente muitos tipos penais digitais novos, extremamente importantes, não foram aprovados, pois estavam no Projeto de Lei Azeredo. Diferente do Brasil, muitos países já tem discutido o limite que distingue a prática de um crime eletrônico comum e quando ele se torna um *cyberterrorismo* ou de guerra cibernética, já que o ataque internacional a *site* de governo com objetivo de retirar do ar e furtar dados é considerado de altíssima gravidade.

Porém é importante lembrar que além dos crimes considerados grandes, também existem os crimes mais corriqueiros, que todos os usuários correm o risco de cometer sem se dar conta. *E-mails* com informações caluniosas são um exemplo disso.

Outra conquista obtida pelo Ordenamento Jurídico Brasileiro foi a publicação da Lei n. 11.829 de 2008, que trata em seu artigo 241-A:

> "Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou

> telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
>
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
>
> § 1º Nas mesmas penas incorre quem:
>
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
>
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
>
> § 2ºAs condutas tipificadas nos incisos I e II do § 1o deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.

O artigo em epigrafe trata do acesso a internet disponibilizado pela empresa ou órgão publico aos seus funcionários ou colaboradores, podendo haver responsabilidade criminal, em caso de ser encontrado materialidade de crime como por exemplo, material pornográfico e há omissão da empresa ou órgão público diante de tal situação.

Legislar sobre esses novos temas não é fácil. Ainda há desafios conceituais como o crime de furto previsto no artigo 155 do Códico Penal Brasileiro em que se configura o tipo penal tornar indisponível coisa alheia móvel. Logo se questiona, se o ato de copiar e colar configuraria furto. Não existe lei perfeita o que deve ser feito é ver as necessidades que essa nova realidade nos trouxe.

INTERNET MÓVEL

Para atender às necessidades de uma sociedade em que os indivíduos se deslocam o tempo todo e carregam a possibilidade de ser identificados e localizados a qualquer momento surgiu a Internet móvel.

O celular tornou-se um instrumento básico que possibilita desde comprar um refrigerante numa máquina até fazer as mais intricadas operações bancárias. A maioria das pessoas possui mais de um celular, pois assim podem possuir mais de uma identidade eletrônica, onde se pode separar a identidade familiar e pessoal, a do cotidiano e do trabalho.

Essa nova sociedade, a Sociedade Digital Móvel traz acessibilidade vinte quatro horas por dia aos seus usuários, mesmo quando se deslocam de um lugar

para outro. Essa funcionalidade pode de inicio ser vantajosa, no entanto gera um pouco de aflição imaginar que alguém pode saber por onde você esteve durante todo o tempo e o que fez. Mais uma vez estamos diante de uma situação de confronto entre segurança e privacidade.

Todas aquelas questões já analisadas sobre privacidade, publicidade através de dispositivos tomam um caráter muito mais delicado, já que há uma capacidade bem maior de individualização se comparado aos outros mecanismos de comunicação. Seja através do *smartphone*, *tablet*, *vidiogame* ou qualquer outra interface de contato, o consumidor possui a capacidade de ser identificado e localizado com uma precisão bem maior do que anteriormente.

O ser humano tem a necessidade de comunicar-se, compartilhar informações do seu dia a dia, e saber o que esta ocorrendo a sua volta. A internet móvel surgiu e vem exercendo o papel de suprir essa necessidade das pessoas.

AS REDES SOCIAIS E SEUS IMPACTOS

Vivemos hoje a cultura das interfaces gráficas em que a tecnologia, transforma de fato nossa maneira de comunicar-se na era digital. Não mais apelidos e avatás, mas sim verdadeiras redes sociais que surgem cada vez mais, tornando os relacionamentos cada vez mais eletrônicos.

O nome que se dá a este fenômeno é *wikinomics*, ou seja, o poder da colaboração em massa como uma nova forma de infraestrutura, típico de gerações de conhecimento de baixo custo em que pessoas e empresas colaboram de forma aberta impulsiona a inovação.

Há milhares de anos já havia a necessidade de comunicar-se, e assim foram criadas, a fala e a escrita. Com o tempo o homem foi inventando novas grafias e gírias para poder nomear aquelas coisas que ainda não possuíam nomes. Houve também a necessidade de transmitir emoções quando não se estava frente a frente em uma conversa, assim criaram-se os *emoticons*.

Dos primórdios da civilização, em que havia o isolamento de povos e cidades, determinadas pelos acidentes geográficos, direto para a acessibilidade total, sem fronteiras espaciais.

Provavelmente a primeira coisa que a maioria das pessoas fazem quando acordam é pegar o celular, logo cedo, as notificações estão aguardando para serem visualizadas. Primeiro *Whatsapp*, *Instagram*, *Facebook*, *twitter* e assim vai até checar todas as redes sociais possíveis em seu *smartphone* para só depois levantar da cama.

Se tornou indispensável ficar sabendo o que aconteceu no mundo desde que você bloqueou a tela de seu celular e foi dormir até a hora que você acordou. Esse costume já se tornou uma compulsão, já não se sabe quantas vezes por dia as pessoas olham o celular. É como se a vida passasse para a humanidade dentro de um smartphone.

A internet não é mais apenas uma rede de computadores, agora consolidada como uma rede de pessoas. Pessoas que cada vez mais querem participar e se expor seja por meio da divulgação de textos, comentários ou compartilhamento de fotos e vídeos.

Essa interatividade que movimenta o formato atual da web demonstra um panorama completamente novo, pois os produtos são, ao mesmo tempo, o público e este é composto por pessoas que estão expondo ideias , divulgando produtos, ou colaborando com o melhoramento do conteúdo já publicado.

Diante de toda essas mudanças não podemos esquecer que na internet as leis também são aplicadas e que toda essa exposição de imagem e ideias trazem alguns riscos. É necessário que se conheça os direitos e deveres, principalmente no que se refere a liberdade de expressão, intimidade e direitos autorais. Vejamos o voto do relator no STJ. REsp 1117633/RO, Rel. Ministro Herman Benjamin, Segunda Turma, julgado em 09/03/2010, DJe 26/03/2010).:

> A internet é o espaço por excelência da liberdade, o que não significa dizer que seja um universo sem lei e sem responsabilidade pelos abusos que lá venham a ocorrer. No mundo real, como no virtual, o valor da dignidade da pessoa humana é um só, pois nem o meio em que os agressores transitam nem as ferramentas tecnológicas que utilizam conseguem transmudar ou enfraquecer a natureza de sobre princípio irrenunciável, intransferível e imprescritível que lhe confere o Direito brasileiro.

Recentemente acompanhamos alguns casos de jovens que tiveram imagens e vídeos íntimos divulgados na rede e causaram bastante repercussão, chegando algumas delas a terem suas vidas destruídas literalmente, muitas delas chegando a cometerem suicídio tendo em vista a gravidade das consequências causadas.

Em decorrência de todos estes acontecimentos, ainda em outubro de 2013, o deputado Romário (PSB/RJ) apresentou o Projeto de Lei (PL) 6.630/13, que altera o Código Penal tipificando a conduta de divulgar fotos ou vídeos com cena de nudez ou ato sexual sem autorização da vítima:

> Art. 1º Esta lei torna crime a conduta de divulgar fotos ou vídeos com cena de nudez ou ato sexual sem autorização da vítima.
>
> Art. 2º O Decreto-lei nº 2848, de 7 de dezembro de 1940, passa a vigorar acrescido do seguinte art. 216-B: divulgação indevida de material íntimo
>
> Art. 216-B. Divulgar, por qualquer meio, fotografia, imagem, som, vídeo ou qualquer outro material, contendo cena de nudez, ato sexual ou obsceno sem autorização da vítima.
>
> Pena – detenção, de um a três anos, e multa.

A Constituição Federal de 1988 assegura o direito à inviolabilidade da intimidade, vida privada, honra e imagem das pessoas, no entanto o número de pessoas que tem suas imagens íntimas expostas na rede, por seus companheiros por ato de vingança, humilhação ou autopromoção é incontável.

Todo cuidado é pouco quando se edita um conteúdo a ser publicado, para que não se promova a prática de ofensas que podem até caracterizar crimes como difamação, calúnia e injúria, bem como o uso de imagens de outras pessoas ou até mesmo colocar em risco a própria imagem.

CONCLUSÃO

Diante do que foi abordado chegamos à conclusão da importância que se tem em analisar essa nossa nova realidade, que é a sociedade digital. O mundo evoluiu, e devemos acompanhar essa evolução.

A realidade mudou, o tempo real invadiu o dia a dia de trabalho e nossas relações pessoais. Não se relacionamos da mesma forma que nos relacionávamos, às vezes parece que nossa vida passa dentro de nossos computadores, tablets ou smartphones.

É preciso saber tanto de tantas coisas que temos a sensação de estarmos desatualizados. As novas regras de conduta nascidas da tendência crescente de proteção da privacidade, segurança da informação e governança corporativa trouxeram novas exigências para o profissional do Direito em especial.

Percebemos que estamos atravessando um momento de ruptura, de quebra de paradigmas, na qual se desenham novos valores que devem ser protegidos e ensinados.

Este trabalho teve a intenção de problematizar o impasse em que se encontra o Direito diante da informatização e o impactos causados por ela em todos os sentidos uma vez que a Internet não tem fronteiras, tampouco quaisquer espaço delimitadores de territórios.

Um dos pontos mais importante desse trabalho foi buscar em nossa legislação atual uma forma de proteção aos direitos fundamentais, diante desse novo ambiente, sem comprometer a liberdade, sabendo da dificuldade que a nossa legislação encontra frente a rápida evolução tecnológica, que por vezes torna-se possível alcança-la.

É de fundamental importância se destacar que o advento das novas tecnologias requer mudanças comportamentais, dos próprios usuários da Internet, é necessário ter cautela ao disponibilizar informações ou dados pessoais junto a serviços oferecidos na web, uma vez que o fim a que se destinam muitas vezes é incerto e pode trazer consequências gravosas à sua intimidade e vida privada. Todavia, algo se mostra extremamente importante em todo o contexto apresentado

que é a necessidade de um aperfeiçoamento legislativo com a fim de garantir o respeito aos direitos fundamentais que são constantemente violados em face das novas tecnologias.

O Direito Digital deve ser estudado não só para fins profissionais, mas para a formação dos cidadãos desta nova era, a fim de poder continuar a exercer a liberdade individual sem prejuízos da vida coletiva em uma sociedade totalmente conectada, em que a ação de um pode gerar efeitos e conseqüências em cascata para todos.

Por fim, a Internet salienta a realidade que chegou para todos, sobretudo no que tange à liberdade e à responsabilidade. A educação para o exercício da liberdade é o grande desafio dos dias atuais. A liberdade responsável, com a mínima intervenção do Estado, no sentido de haver uma legislação sobre o assunto que sirva como norte, e não como controle, tende a gerar uma sociedade mais consciente e amadurecida.

REFERÊNCIAS

ALMEIDA, José Carlos de Araújo. **Manual de informática jurídica e direito da informática,** Rio de Janeiro: Forense, 2005.

BARROS, Marco Antonio de. **A busca da verdade no processo penal,** 1. ed. São Paulo: Revista dos Tribunais, 2005.

BLUM, Renato Opice; DAOUN, Alexandre Jean. **Cybercrimes**. **Direito & Internet – Aspectos jurídicos relevantes**, São Paulo, Edipro, 2000.

CARLI, Vilma Maria Inocêncio. **Teoria e Direito das obrigações contratuais:** uma nova visão das relações econômicas de acordo com os códigos civil e consumidor. Campinas: Bookseller, 2005.

FERREIRA, Ivette Senise. A criminalidade informática. In: DE LUCCA, Newton, SIMAO FILHO, Adalberto (orgs.). **Direito & internet:** aspectos jurídicos relevantes. Bauro: Edipro, 2000.p.21-100.

PEREIRA, Marcelo Cardoso. **Direito à Intimidade**. Curitiba, Editora Juruá, 2005.

VIANNA, Tulio Lima. **Dos crimes por computador.** Disponível em: <www.mundo juridico.adv.br/cgi-bin/upload/texto259.rtf.> Acesso em: 05 junho 2014.

WOLF, Karen Emilia Antoniazzi. **A possibilidade de incidência do ICMS nas operações da Internet.** Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1811> Acesso em: 16 julho 2014.

ZAFFARONI, Eugenio Raul; PIERANGELI, Jose Henrique. **Manual de Direito Penal Brasileiro, Parte Geral,** 1. ed. São Paulo: Editora, 2004.

ZANETTI, Robson. **Internet em benefício do acesso a informação jurídica**. Disponível em: <http://s.www,cbeji.com.br/br/novidades/artigos/main.asp?id=178> Acesso em: 16 maio 2014.