ASPECTOS JURÍDICOS DO COMBATE AOS CRIMES DA TECNOLOGIA DA INFORMAÇÃO NO URUGUAI

THE LEGAL ASPECTS ON THE ACTION AGAISNT THE INFORMATION TECHNOLOGY CRIMES IN URUGUAY

Aglais Cristina Gondim Tabosa Freire[1]
João Araújo Monteiro Neto[2]

Sumário: Introdução; 1 Sociedade, tecnologia e direito; 2 Aspectos gerais dos crimes de tecnologia da informação; 3 Aspectos jurídicos do combate aos crimes de tecnologia da informação no Uruguai; Conclusão; Referências.

Resumo: A difusão da utilização de recursos da tecnologia da informação modificou sensivelmente a forma de organização social moderna, influenciando de forma profunda o contexto das relações sociais, econômicas e culturais. O desenvolvimento de novas formas de circulação de informações, em especial as de caráter pessoal, comercial e financeira, fomentou, entretanto, a prática de inúmeras condutas lesivas a manutenção dessa nova forma de organização social. Funcionando como fator criminógeno, os recursos de tecnologia da informação, potencializaram práticas criminosas já previstas nas ordens jurídicas nacionais, ou permitiram a perpetração de condutas ilícitas ainda não tuteladas pelo direito penal, o que exige, por parte do Estado, uma resposta rápida na tutela dos chamados crimes de tecnologia da informação. Contudo, em virtude de seu caráter transnacional, o crime de tecnologia da informação não pode ser punido de forma isolada pelos Estados, posto que a ausência de tratamento simétrico por parte dos Estados permitiria a migração dos criminosos, com um simples click, para Estados onde tais condutas não são consideradas criminosas. Nesse esteio, em busca de fomentar o estudo de uma legislação supranacional, o primeiro passo é o conhecimento das realidades jurídicas locais, por intermédio do estudo dos preceitos penais incriminadores relacionado à matéria. Assim, em virtude ser considerado um país de tendências avançadas, bem como por ser dos precursores da regulamentação do Direito da Tecnologia da Informação na América do Sul, o presente artigo visa analisar, por meio de pesquisa bibliográfica e documental, a legislação penal Uruguai relacionada aos delitos de tecnologia da informação.

Palavras-chaves: tecnologia da informação; legislação penal; Uruguai.

Abstract: The dissemination of resource use of information technology noticeably change the shape of modern social organization, thus influencing the social, economic and cultural context. Developing new ways of circulating information, particularly those of personal, commercial and financial, encouraged, however, the practice of many conduits affecting the maintenance of this new form of social organization. Functioning as criminogenic factor, resources for information technology, criminal practices have worsened already provided under domestic law or allowed the perpetration of illegal conduct does not tutored by criminal law, which requires, by the state, a rapid response in the protection so-called crimes of information technology. However, due to its transnational nature, the Crime Information Technology cannot be punished by states in isolation, since the absence of symmetrical treatment by the states would allow the migration of criminals with a simple click, to states where such conduct are not considered criminal. In such a mainstay in search of promoting the study of a supranational law, the first step is the knowledge of local legal realities, through the study of criminal statutes related to the incriminating material. Therefore, due to be considered a country of advanced trends, as well as being the precursors of the rules of law of Information Technology in South America, this article aims to analyze, through research literature and documents, the criminal law relating Uruguay the offenses of Information Technology.

Key words: information technology; criminal Law; Uruguay.

Introdução

A tecnologia da informação como agente transformador das relações humanas vem reclamando a mobilização do Direito no sentido de regular as relações sociais, civis e comerciais perpetuadas no ambiente digital com o objetivo principal conferir-lhes segurança jurídica, bem como tutelar os novos bens jurídicos surgidos com o advento da chamada sociedade da informação. Assim, diante dessa nova

[1] Aluna do quinto semestre do curso de Direito da Universidade de Fortaleza-UNIFOR.cristabosa@hotmail.com.
[2] Professor do Curso de Direito da Universidade de Fortaleza. joaoneto@unifor.br.

realidade, não somente novas práticas lícitas, mas acima de tudo, o surgimento de condutas lesivas à utilização da tecnologia da informação demandou a necessidade de instrumentalizarem-se por meio da regulamentação jurídica medidas preventivas, e acima de tudo punitivas, para essas novas práticas.

Inicialmente, o presente trabalho abordará o impacto do desenvolvimento tecnológico no contexto socio-jurídico, em especial sua influência na seara criminológica, funcionando, acima de tudo, como fator potencializador e inovador de práticas ilícitas, bem como as controvérsias acerca da repercussão da utilização desses recursos no plano jurídico. Em seguida, serão analisados os aspectos gerais dos crimes de tecnologia da informação, abordando-se especialmente seu conceito, sua classificação, e os modelos legislativos de tratamento a essas condutas. Por fim, serão abordados os aspectos jurídicos do combate aos crimes de tecnologia da informação à luz da legislação penal uruguaia, em especial observando-se à normatização dessas condutas, bem como a forma como o ordenamento jurídico uruguaio se propõe a tratar essa matéria.

1 Sociedade, tecnologia e direito

Embora as transformações decorrentes do desenvolvimento da tecnologia da informação não tenham ocorrido de forma repentina, mas resultado da evolução das relações sociais e produtivas, ela foi capaz de afetar a sociedade de tal forma que provocou uma reestruturação da forma como as pessoas se relacionam, de seus hábitos, do modo *on-line* como realizam suas transações econômicas e financeiras, de produzir riquezas, do relacionamento entre os poderes políticos, entre o Governo e as empresas e entre esse e os cidadãos, que podem fiscalizar exigir, receber serviços e informações dos órgãos públicos. (MONTEIRO NETO, 2008)

O ambiente digital é apenas uma extensão da vida real. Em ambos podemos compartilhar, comprar, comunicar, pagar contas, e, inclusive, traficar drogas, instigar ao suicídio, ofender a honra, entre outros. Assim, as pessoas, as boas maneiras exigidas, os crimes e as leis aplicadas são os mesmos em ambas as comunidades. (MENDES, 2007)

As relações tornam-se tão impessoais que amigos e familiares, passam a se comunicar apenas por meio de canais de bate-papo ou sites de relacionamento. Os serviços disponíveis no ambiente virtual permitem ao usuário criar uma *Second Life*, uma nova vida, com identidade, trabalho, status social e financeiro, completamente diferente e autônoma do plano real. (GREIS, 2007)

O nascimento da sociedade da informação, termo que denomina a sociedade contemporânea influenciada e excessivamente vinculada à tecnologia da informação, fez surgir novos valores, novas relações, novos bens e interesses que precisam ser tutelados juridicamente. Novos direitos, novas responsabilidades nas diversas áreas do Direito, por exemplo, cível, penal, consumeirista e novos confrontos, que necessitam de regulação e respaldo jurídico. A própria informação sofreu um reforço a sua, então precária proteção jurídica, posto que nesse novo modelo de produção econômico cultural, sua valoração foi potencializada.

Ao mesmo tempo em que a *Internet* confere celeridade e praticidade à obtenção de informações que transitam no meio virtual e ao modo como os indivíduos interagem entre si, ela também, em muitos casos, serve como veículo para a prática de condutas lesivas a coletividade, funcionando assim como um fator potencializador da criminalidade.

Quando um delito é realizado, por meio virtual, ganha uma dimensão maior, não só pela natureza do bem jurídico informacional, mas sim, pelo alcance quase que imensurável da lesividade da prática, pois um código malicioso como um *trojan horse*, pode em segundos circular o mundo de forma que milhões de pessoas sejam lesadas.

O acelerado crescimento dos índices acerca dos crimes de tecnologia da informação encontra respaldo basicamente em dois fatores. O primeiro relaciona-se à falsa ideia de que o mundo da tecnologia da informação, em especial a Internet, é um mundo sem lei, uma espécie de faroeste virtual, sentimento esse potencializado pela errônea impressão de que tudo que é praticado na rede reveste-se do véu de anonimato de um monitor. Ledo engano. Mesmo que lentamente, o maquinário jurídico dos Estados já iniciou o processo de criminalização dessas condutas, seja adaptando-as aos dispositivos incriminadores já existentes, seja criando novas condutas típicas, entretanto, por se tratar de um processo lento suas

conseqüências, só serão sentidas a médio e longo prazo. O segundo fator está associado à mudança de perfil do criminoso de tecnologia da informação, posto que hoje a maioria das condutas seja perpetrada por grupamentos criminosos organizados que utilizam os recursos tecnológicos para praticarem condutas objetivando amealhar recursos para financiar outras ações ilícitas, ou para lavar capital oriundo de outras condutas criminosas. Ademais, ante a pluralidade de tratamento normativo conferido pelos Estados à matéria, os criminosos se aproveitam de países de menor capacidade legal e tecnológica, aumentando vertiginosamente os índices de crimes praticados via computador nos últimos anos.

Nesse diapasão, embora a legislação ordinária brasileira abarque, total ou parcialmente, a grande maioria das condutas criminosas praticadas por meio da tecnologia da informação, ou uma pequena parte, extremamente nociva, ainda não têm punição legalmente prevista. Consiste, principalmente, em acessos indevidos e invasões a sistemas privados, ocasionando, assim, grande preocupação, e ensejando o debate pela necessidade de uma urgente alteração nas legislações penal nacional. Isso para possibilitar o enquadramento dessas novas figuras criminosas e a realização de convênios internacionais entre os órgãos de investigação e punição dos delitos da tecnologia da informação (COSTA, 2010) e de cooperação entre as instituições internacionais, como Organização dos Estados Americanos e a União Europeia, no sentido de elaborar normas e procedimento padronizados acerca da matéria.

Como os crimes de tecnologia da informação são considerados transnacionais, em razão da capacidade de o *iter criminis* se fracionar em diversas regiões do mundo ou mesmo se consumar, ao mesmo tempo, em lugares de jurisdições diversas, esses delitos se tornam um problema global, o que torna complexa a tarefa de criar de um sistema punitivo eficaz ao combate dessas infrações.

Nesse contexto, surge o Direito da Tecnologia da Informação não como uma espécie normativa autônoma, mas como uma mera evolução do ordenamento jurídico vigente, sendo composto por institutos, normas e princípios gerais, que se diferencia apenas por introduzir elementos e valores próprios às relações praticadas no meio virtual. (PINHEIRO, 2009)

2 Aspectos gerais dos crimes de tecnologia da informação

Diante das divergências doutrinárias acerca da conceituação deautomatizado de la misma crime da tecnologia da informação, serão apresentadas as duas das principais correntes. A primeira corrente classifica tal espécie delituosa como crimes de meio. Assim, os referidos crimes são definidos por Jijena Leiva (RODRÍGUEZ, 2010) como toda ação típica antijurídica e culpável para cuja consumação é utilizadas tecnologias informáticas ou que afeta informações contidas em sistemas de tratamento automatizado das mesmas. Tais condutas podem ser praticadas contra pessoas físicas ou jurídicas, por meio da utilização de alguma ferramenta eletrônica no transcorrer do iter criminis, destinada a produzir um dano, seja patrimonial ou moral, produzindo, mesmo que indiretamente, lesões a diversos valores jurídicos e benefícios ilícitos para o agente que a pratica, seja ou não de caráter financeiro.

Dessa forma, apesar de ser indispensável que a pratica do delito se desenvolva no ambiente virtual, é irrelevante a natureza eletrônica do bem jurídico diretamente atingido ou o momento da utilização de recursos tecnológicos, podendo ocorrer na preparação, na execução ou na consumação do delito, uma vez que se configura em um crime de meio, e não um crime de fim. (PINHEIRO, 2009)

Essa teoria, por sua vez, divide esses delitos em puros ou impuros, de acordo com a natureza do bem jurídico ameaçado ou tutelado. São crimes puros, também denominados de crimes eletrônicos propriamente ditos, aqueles que visam, diretamente, à violação de um recurso tecnológico, como o acesso indevido às informações contidas no banco de dados do computador; enquanto que os impuros são crimes que, embora praticados com a utilização de ferramentas tecnológicas, atingem bens jurídicos que não constituem recursos tecnológicos, como a difamação praticada em sites de relacionamento, uma vez que o objeto juridicamente tutelado não é a máquina, mas a honra da vítima. (ARAS, 2009)

Quanto às condutas já tipificadas se dão por instrumento da tecnologia da informação, de forma a ampliar o seu potencial ofensivo, é perfeitamente possível adequar às normas vigentes a abarcar essas situações especiais, guardando, assim, as devidas diferenças; entretanto, quando tais condutas atingem novos bens jurídicos e não encontram no ordenamento tipificação, trata-se de um novo instituto, devendo, em nome da ordem pública e da paz social, ser criados novos tipos penais que descrevam tais condutas e lhes imputem as devidas sansões. (RODRÍGUEZ, 2010)

Dentre tais condutas impuras, ou crimes comuns mediados por recursos tecnológicos, praticadas com maior frequência estão:

- Fraudes, por meio da apropriação e utilização de senhas de terceiros para acesso a sites pagos ou para conexões à rede, do comércio ilegal ou irregular de mercadorias e da contratação de serviços, sem que haja nenhuma formalização ou garantia.

- Pornografia infantil, de modo a utilizar a Internet como veículo virtual para a satisfação da lasciva sexual de pedófilos.

- Crimes contra a honra, que se dá pela divulgação de materiais (reais ou adulterados) de textos, imagens, vídeos e áudio, com o intuito de agredir a honra de terceiros, podendo se apresentar pela injúria, pela calúnia ou pela difamação[3], em blog, sites de relacionamento, salas de bate-papo ou e-mails.

- Racismo, praticado por meio da incitação à violência, divulgação de ofensas, instigação ou indução à aversão a determinados grupos de pessoas.

- Pirataria de áudios, vídeos e programas informáticos, que consiste na utilização de recursos informáticos para difundir, na Internet, de músicas, programas de computadores e vídeos, em desrespeito às licenças de uso e aos direitos autorais dos criadores e produtores. (COSTA, 2010)

A segunda corrente considera como crimes de tecnologia da informação apenas os denominados crimes puros, isto é, aqueles cujos objetos ameaçados ou violados são bens jurídicos de natureza tecnológica, como o software, as informações contidas nos banco de dados e outros, excluindo, assim, os denominados crimes impuros, da tutela do Direito da Tecnologia da Informação, por não se tratarem de novos tipos penais, mas de delitos que ofendem bens jurídicos não tecnológicos ou informacionais.

A Organização das Nações Unidas (ONU), para solucionar as controvérsias acerca da conceituação desses delitos se posicionou sobre o tema reconhecendo como crimes de tecnologia da informação apenas os denominados tipos puros, aqueles que somente visam violar recursos tecnológicos, dividindo-os ainda em 3 (três) às categorias: fraude, falsificação e dano ou alteração de programas ou dados. (PATERLINI, VEGA, GUERRIERO, 2010)

As fraudes são cometidas por meio da manipulação de banco de dados presentes nas máquinas e se distinguem em manipulação de dados de entrada e de saída, de programas ou de outros recursos informáticos. Enquanto a falsificação se dá pelo ingresso indevido a sistemas informáticos, a fim de alterar ou suprimir, de modo intencional e sem permissão, informações ali contidas na forma de dados, de modo a aparentar autenticidade e produzir efeitos legais. Já o dano ou a alteração de sistemas se classifica como ações distintas, tipo a sabotagem informática, o envio de vírus, os acessos não autorizados e a reprodução não autorizada de programas ou dados contidos nas máquinas. (PATERLINI, VEGA, GUERRIERO, ipud)

No plano do direito comparado na América Latina, os ordenamentos jurídicos nacionais se diferem quanto ao modelo legislativo adotado para o tratamento dos delitos de tecnologia da informação, ora adotam a elaboração de leis específicas, ora optando por inserção dos dispositivos incriminadores no bojo dos códigos penais.

O sistema de leis especiais implica na criação de novos dispositivos elaborados para regular essa especificidade delitos, como ocorre na Venezuela (lei n. 37.313 de 30 de outubro de 2001) e no Chile (mediante a lei de delitos informático n. 19.223 de 28 de maio de1993).

O modo de tratamento pela atualização dos códigos penais, os quais sofreram modificações, normalmente por meio da inserção de normas expansivas ou de circunstâncias agravantes aos crimes que, embora anteriormente tipificados, se diferenciam quanto à utilização de recursos no decorrer do iter criminis. Essa forma de tratamento pode se apresentar de maneira difusa, em artigos esparsos, como no Paraguai, ou concentrada, por meio da elaboração de capítulos especiais, como na Bolívia.

Da mesma forma, alguns países optaram por adotar um tipo misto, que adota tanto o sistema de leis especiais quanto a reforma dos códigos penais, como é o caso do Brasil (projeto de lei n. 76 de 2000) e da Argentina (lei n. 26.338 de 04 de junho de 2008).

[3] O Código Penal brasileiro define os crimes contra a honra: calúnia é imputar, falsamente, a alguém a prática de um fato definido como crime (artigo 138); difamação é imputar a alguém fato ofensivo à sua reputação (artigo 139); e injúria é atribuir a outrem qualidade negativa, ofensiva de sua dignidade ou decoro (artigo 140).

Diferentemente da Argentina, o Brasil ainda não aprovou o projeto de lei que visa à criação de normas especificas para regular as novas condutas delituosas vinculadas à tecnologia da informação. Conta tão somente com alguns dispositivos já inseridos no Código Penal, ou na legislação extravagante.

A situação especial do ordenamento jurídico uruguaio será analisada a seguir com uma maior precisão.

3 Aspectos jurídicos do combate aos crimes de tecnologia da informação no Uruguai

Pode-se dizer que o Uruguai é um país de tendência avançada ou próspera quanto ao Direito da Tecnologia da Informação, isto é, têm como características o esforço do Poder Legislativo em regular as relações decorrentes do uso da tecnologia da informação e a consolidação desse novo ramo do Direito na legislação, na doutrina e na jurisprudência nacional, levando inclusive à Suprema Corte questões envolvendo a referida matéria.

O Uruguai criou o CINADE (Centro de Informática Aplicada ao Direito) que, dirigido por Marcelo Bauzá Reilly, sediou o VI Congresso Iberoamericano de Informática y Direito, celebrado em maio de 1998, cujo objetivo foi promover estudos jurídicos acerca das novas tecnologias da informação, e onde se desenvolvem importantes projetos de lei acerca do Direito da Tecnologia da Informação. (CANTU, 2000)

Dentre as referidas normas estão:

- Lei n. 16.736 (5 de janeiro de 1996): dispõe acerca dos Expedientes Eletrônicos.

- Lei n. 17.243 (29 de junho de 2000): estabelece a validez e a eficácia das firmas eletrônicas e digitais no Sistema Informático do Estado.

- Lei n. 17.616 (13 de janeiro de 2003): altera as regras inerentes aos Direitos do Autor e Direitos Conexos, assim como a Lei de Propriedade Literária e Artística.

- Lei n. 17.805 (26 de agosto de 2004): altera a lei n. 9.739 Lei de Copyright.

- Lei n. 17.948 (8 de janeiro de 2006), sobre informações sobre pessoas, empresas e instituições incorporadas nos registros do Banco Central do Uruguai.

- Lei n. 18.331 (6 de agosto de 2008): estabelece a proteção de dados pessoais contidos em bancos de dados públicos e regula a ação de habeas data.

- Lei n. 18.600 (15 de setembro de 2009): autoriza o uso de registros eletrônicos, documentos eletrônicos, software simples tecla, assinatura eletrônica, assinatura digital, comunicações eletrônicas e endereço eletrônico constituído, em todos os processos judiciais e administrativos pendentes no sistema judicial. (CUERVO, 2010)

Um dos grandes precursores do movimento uruguaio de criminalização da s condutas ilícitas praticadas por intermédio de mecanismos da tecnologia da informação foi o deputado, durante o período legislativo de 1995-2000 pelo Partido Colorado, advogado e mestre em direito internacional pela *American University*, *Washington College of Law*, Jorge Pacheco Klein. O referido parlamentar apresentou projeto de lei dispondo sobres à tipificação de Delitos Informáticos, cujo objetivo era criminalizar o acesso não autorizado (doloso e culposo) a sistemas de computação, a fraude informática, o furto informático, a obtenção indevida de vantagens econômicas por meio eletrônico, penalizando também a tentativa desses delitos, bem como atribuindo agravantes diante da condição do agente (funcionário público no exercício de sua função) ou da natureza do bem jurídico ameaçado ou atingido (recurso tecnológico pertencente à entidade estatal).

O projeto foi considerado como um ponto de partida para a regulamentação dos crimes de tecnologia da informação no plano uruguaio, contudo sofreu a rejeição do Congresso Nacional uruguaio ainda na legislatura passada. (RODRÍGUEZ, 2010)

Assim, concretamente, no que tange a criminalização dos crimes de tecnologia da informação a primeira norma de alteração do Código Penal Uruguaio (CPU) foi a lei n. 16.002 (25/11/1988) que regula em seus artigos 129 e 130 a autenticidade e a prova dos documentos transmitidos à distância por meios

eletrônicos entre dependências oficiais, penalizando a falsificação de documentos expedidos digitalmente. O artigo 130 do referido diploma normativo equipara a transmissão eletrônica de textos falsificados ou alterados entre as dependências oficiais documento aos crimes de documentação documental previstos nos artigos 236 a 239 do CPU[4], imputando a esses crimes as respectivas sanções penais. A Lei n. 16736 (5/1/1996) ampliou o artigo 129, CPU, ao substituir a terminação "medios electrónicos" por "medios informáticos y telemáticos" e ao eliminar o termo: "entre dependencias oficiales", tornando genérica a aplicação dessa regra. A lei n. 25.930 inseriu ao artigo 173 do CPU a redação do seguinte inciso:

El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciese por medio de una operación automática.[5]

Tal dispositivo inicialmente se refere à proposta de criar como figura típica a fraude informática, a qual fazia parte do projeto de lei de delitos informáticos que fora elaborado pela secretaria de comunicações do Uruguai. Tal norma solucionou, mesmo que apenas parcialmente, o dilema da insegurança jurídica nas relações comerciais e da atipicidade dessas condutas danosas.

No ordenamento jurídico uruguaio, embora não haja um tipo específico quanto ao acesso não autorizado em sistemas informáticos, muitos profissionais forenses defendem, de forma equivocada, a utilização da analogia, para enquadrar tal conduta no tipo incriminador inserto no artigo 300 do CPU, que se refere ao "conhecimento fraudulento de secretos". No mesmo sentido chega-se a defender o enquadramento típico da conduta de pedofilia no tipo inserto no artigo 278 do C.P.U., que se restringe à regular de mogo genérico o delito de exibição pornográfica.

Esse entendimento, entretanto, não encontra respaldo no princípio norteador do Direito Penal que é a legalidade, de modo que não há crime sem uma lei anterior que o defina, considerado como um dos pilares do Direito contemporâneo, que se estrutura em torno dos princípios da dignidade da pessoa humana e do devido processo legal.

Quanto à aplicabilidade das figuras típicas apresentadas pelo Código Penal Uruguaio aos delitos de tecnologia da informação, destacam-se os seguintes dispositivos:

Artigo 340 (Furto): El que se apoderare de cosa ajena mueble, sustrayéndosela a su tenedor, para aprovecharse o hacer que otro se aproveche de ella, será castigado con tres meses de prisión a seis años de penitenciaría.

Em virtude do princípio da legalidade já comentado, é defesa ao juiz a interpretação extensiva a fim de aplicar o referido dispositivo ao delito de furto de informações, contidas em banco de dados de máquinas, assim como ao crime de subtração valores, por meio da transferência eletrônica de fundos de poupança ou conta corrente, uma vez que o conceito de coisa, configura-se como algo tangível, palpável, não recepcionando-se assim a ideia de informação, mesmo que está corporifique o patrimônio.

Artigo 347 (Estelionato): El que con estratagemas o engaños artificiosos, indujere en error a alguna persona, para procurarse a sí mismo o a un tercero, un provecho injusto, será castigado con seis meses de prisión a cuatro años de penitenciaría.

[4] Artículo 236. (Falsificación material en documento público, por funcionario público) El funcionario público que ejerciendo un acto de su función, hiciere un documento falso o alterare un documento verdadero, será castigado con tres a diez años de penitenciaría. Quedan asimilados a los documentos, las copias de los documentos inexistentes y las copias infieles de documento existente.
237. (Falsificación o alteración de un documento público, por un particular o por un funcionario, fuera del ejercicio de sus funciones) El particular o funcionario público que fuera del ejercicio de sus funciones, hiciere un documento público falso o alterare un documento público verdadero, será castigado con dos a seis años de penitenciaría.
238. (Falsificación ideológica por un funcionario público) El funcionario público que, en el ejercicio de sus funciones, diere fe de la ocurrencia de hechos imaginarios o de hechos reales, pero alterando las circunstancias o con omisión o modificación de las declaraciones prestadas con ese motivo o mediante supresión de tales declaraciones, será castigado con dos a ocho años de penitenciaría.
239. (Falsificación ideológica por un particular) El que, con motivo del otorgamiento o formalización de un documento público, ante un funcionario público, prestare una declaración falsa sobre su identidad o estado, o cualquiera otra circunstancia de hecho, será castigado con tres a veinticuatro meses de prisión.
[5] RIQUERT, op. cit.

O dispositivo citado apresenta como elemento do crime de estelionato o engano da vítima. Como não é possível que uma máquina, como um sistema informático bancário, posse ser ludibriada, em razão de estratégias e artifícios fraudulentos, ela não pode ser sujeito passivo do crime de estelionato. Não obstante, o entendimento atual dos juristas admite a aplicação desse delito diante dessa espécie de fraude informática, uma vez que toda máquina é comandada por uma pessoa natural que a produziu, o programador, que seria, nessa situação, a vítima do engano.

Artigo 358 (Dano): El que destruyere, deteriorare o de cualquier manera inutilizare, en todo o en parte, alguna cosa mueble o inmueble ajena, será castigado, a denuncia de parte, cuando el hecho no constituya delito más grave con multa de 20 U.R. (veinte unidades reajustables) a 900 U.R. (novecientas unidades reajustables).

A norma referida estabelece como objeto do crime de dano coisa móvel ou imóvel. Os dados, os programas ou as informações contidas em sistemas informáticos não podem ser classificados como tal, por não se tratarem de bens incorpóreos, de natureza virtual, portanto não é possível aplicar esse dispositivo aos delitos de dano perpetrados contra esses objetos. (RODRÍGUEZ, 2010)

Diante da lacuna da legislação penal uruguaia acerca da criminalidade tecnológica, resta ao magistrado, em virtude do princípio da legalidade, aplicar os princípios hermenêuticos às normas vigentes para que as violações de direitos perpetradas no ambiente digital não sejam excluídas da apreciação judicial.

Conclusão

Em razão do impacto das novas tecnologias da informação nos diversos setores das relações humanas, que proporcionou o surgimento de novos relacionamentos, valores e bens carentes de tutela jurídica, aparece o Direito da Tecnologia da Informação, como um ramo autônomo do Direito. Diante da ofensa a esses novos bens jurídicos e da insegurança das relações no ambiente digital, surge a necessidade do Estado tutelar juridicamente esses novos bens e valores sociais.

No caso do Uruguai, embora considerado um país de tendências avançadas ou prósperas quanto à regulamentação da tecnologia da informação, depreende-se quase nenhum esforço normativo para tipificar os crimes de tecnologia da informação.

Verifica-se um vazio normativo que impede uma efetiva tutela da prestação jurisdicional, resultante, principalmente, do fracasso do projeto de lei de delitos informáticos do Deputado Pacheco Klein e das singelas modificações realizadas no Código Penal uruguaio.

Diante do princípio da legalidade, a ausência de tipificação dos delitos de tecnologia da informação, se configura como um entrave ao desenvolvimento e a exploração dos mecanismos de tecnologia da informação, posto que insegurança e a falta de credibilidade desses meios inibem a sua potencial exploração, colocando em risco o desenvolvimento do modo de produção informacional.

Faz-se necessária, portanto, a criação de mecanismos que reduzam os riscos de invasão de sistemas informáticos e de órgãos estatais que fiscalizem as relações no ambiente digital, como medida preventiva aos ataques perpetrados por meios informáticos, garantindo uma maior segurança na utilização dos recursos eletrônicos.

Devido ao fracionamento do *iter criminis* desses delitos em locais de jurisdições diversa, é essencial a elaboração de tratados internacionais, a fim de unificar a regulamentação dos diversos ordenamentos jurídicos nacional, conferindo segurança jurídica e eficácia da prestação jurisdicional diante das ofensas e ameaças praticadas por instrumento das novas tecnologias da informação, assim como de prevenir futuros conflitos de jurisdição.

Referências

ARAS, Vladimir. Crimes de informática: uma nova criminalidade. **Revista Informática Jurídica.** 1998-2009. Disponível em: <http://www.informatica-juridica.com/trabajos/artigo_crimesinformticos.asp>. Acesso em: 15/fev./2010.

BLUM, Renato Opice. Informação dada pelo advogado em entrevista ao site Consultor Jurídico. **Advocacia Bittar**. Disponível em: <http://www.advocaciabittar.adv.br/index.php?option=com_content&task=view&id=254&Itemid=1>. Acesso em: 20/fev./2010.

CANTU, Ricardo. Tendencias actuales de la Informática y el Derecho a Nivel Internacional. **Alfa-Redi**. Jan./2000. Disponível em: <http://74.125.45.132/search?q=cache:pViiSX5-2bQJ:www.alfa-redi.org/rdi-articulo.shtml%3Fx%3D398+proyecto+de+ley+de+klein+delitos+informaticos&cd=5&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 2/abr./2010.

COSTA, Elizete Escolástica Ferreira da. Aspectos da criminalidade na Internet. **Buscalegis**. Disponível em: <http://www.buscalegis.ufsc.br/revistas/index.php/buscalegis/article/viewFile/5588/5157>. Acesso em: 20/fev./2010.

CUERVO, Victor. Legislación Uruguay. **Informática jurídica**. Disponível em: <http://www.informatica-juridica.com/anexos/anexo1508.asp>. Acesso em: 2/abr./2010.

GREIS, Luciano kercher; Faria Elaine Turk. Second Life: uma proposta de utilização pedagógica. **Colabor@- A Revista digital da CVA- RICESU**. v.4. n.15 set. 2007. Disponível em: < http://www. ricesu.com. br/colabora/n15/artigos/n_15/pdf/id_01.pdf >. Acesso em: 17/nov./2009.

MENDES, Carolina de Aguiar Teixeira. Crimes Contra a Honra. **Brasil Escola**. Goiânia, mai./2007. Disponível em: < http://www.brasilescola.com/informatica/crimes-contra-a-honra.htm >. Acesso em: 18/out./2009.

MONTEIRO NETO, João Araújo. **Aspectos constitucionais e legais do crime eletrônico.** Fortaleza: Universidade de Fortaleza, 2008. Dissertação de Mestrado. Dissertação de Mestrado. Disponível em: <http://uol11.unifor.br/oul/ObraBdtdSiteTrazer. Acesso em: 17/nov./2009.

PATERLINI, Nora; VEGA, Carolina; GUERRIERO, Gabriela; VELÁZQUEZ, Mercedes. **Delitos informáticos:** antecedentes Internacionales para una Legislación Nacional Proyectos Legislativos. Asociación Argentina de Derecho de Alta Tecnología. Disponível em: <http://www.aadat.org/delitos_informaticos20.htm>. Acesso em: 15/fev./2010.

PINHEIRO, Patrícia Peck. **Direito digital**. 3.ed. São Paulo: Saraiva 2009.

RIQUERT, Marcelo A., Estado de la Legislación contra la Delincuencia Informática en el Mercosur. **Alfa-Redi**. Disponível em: <http://www.alfa-redi.com/rdi-articulo.shtml?x=10136>. Acesso em: 25/fev./2010.

RODRÍGUEZ, María José Viega. Delitos informáticos. **vLex**. Disponível em: <http://comunidad.derecho.org/mjviega/deli_inf.htm>. Acesso em: 15/fev./2010.