

Relatório Painei “A responsabilização Civil e Penal dos Usuários que Cometem Ilícitos na Internet”.

Karina Figueiredo (Polícia Civil do Pará):

A Polícia Civil do Pará, conta com uma divisão especializada de combate a crimes cibernéticos, que contam com algumas frente de trabalho, dentre elas a capacitação e a aperfeiçoamento.

Não pode ser esquecida da parte de prevenção dos crimes cibernéticos, sobretudo sobre a população ter ciência sobre essas questões para enfrentamento da criminalidade cibernética. Uma das medidas seria proferir palestrar a população.

Questionada a palestrante sobre indicadores sobre a punição de crimes cibernéticos, ela respondeu que não possui dado específico sobre a criminalidade cibernética no Estado do Pará, que provavelmente o grau de resolução de crimes é diferente em comparação com o Estado de São Paulo. A Unidade de crimes cibernéticos da Polícia Civil do Estado do Pará é procurada desde quem teve uma ofensa numa mídia social, até questões de grandes fraudes, pornografia etc. Em muitos casos, a polícia não recebe as informações dos provedores, e a ineficiência da investigação dos ciber Crimes não se da por causa da polícia, e sim por causa de terceiros.

Leonardo Reis (Solintel)

O seu trabalho é voltado para atendimento de pequenos provedores na Solintel, o papel dos provedores de conexão para auxiliar as investigações criminais, é importante o provedor cumprir o que está no Marco Civil da Internet, principalmente na guarda dos registros de conexão e logs.

Outra dificuldade técnica é o esgotamento do IPV4, onde um número IP é compartilhado entre vários usuários.

Entende que a implementação do IPV6 é muito custosa para os pequenos provedores, mas é um cenário que resolveria a questão da identificação de usuários na internet.

Uma alternativa importante na questão da implementação do IPV6, seria o governo facilitar linhas de crédito para os provedores investirem em tecnologia.

Ao ser questionado ele vê a falta de educação digital e se os provedores podem alegar ignorância da lei para se defenderem em processos? Argumentou que está certo o posicionamento da Anna Gardemann, e que temos uma dificuldade de interpretação e

implementação das regras jurídicas. O provedor e o empresário de internet, deve buscar um conhecimento especializado de quem entenda as leis.

Anna Gardemann (Gardemann e Vidotti Advogados)

Os provedores fazem tudo que está no alcance para controlar os registros dos usuários, mas importante ponto é a consequência da responsabilidade civil dos provedores.

A legislação é muito pujante em relação aos crimes virtuais, e existe uma responsabilização muito grande das empresas, principalmente em relação aos pequenos provedores, sendo que eles precisam investir muito em segurança cibernética.

Não existe uma questão específica na legislação em que de uma espécie de especialização pelo poder público de pessoas que combatem os crimes na internet.

Questionada sobre como ela vê a falta de educação digital e se os provedores podem alegar ignorância da lei para se defenderem em processos? Na visão dela a educação é uma necessidade, e que os argumentos de ignorância e falta de conhecimento da lei, somente podem ser usados por consumidores. O setor empresarial não pode alegar a ignorância da lei. Os provedores devem sempre estar atentos a legislação exposta no Marco Civil da Internet, sobretudo os empresários adotarem em casos judiciais todas medidas previstas no MCI.

Flávia Lefèvre (Intervozes)

Existem problemas de jurisdição e limites territoriais já foram parar no STF, e que essas questões no plano transfronteiriço da internet, acabam sendo mais complexos.

Existem algumas plataformas de internet, que são transnacionais (planetárias), como por exemplo, o Youtube, Facebook, WhatsApp e Instagram. Só o Facebook tem 2,7 bilhões de usuários que comparados com o continente africano você tem 1 bilhão e 600 milhões de pessoas.

Esses desafios têm levado muitos países a se unirem na Internet Jurisdiction Policy Network, da qual o CGI.br participa. Esse projeto existe tem uma participação ampla de países e atores multisetoriais.

Essas empresas (Facebook, Google etc), pelo artigo 170 da Constituição Federal e Pelo Código de Defesa do Consumidor, inclusive com precedentes do STJ, impõem que elas se submetem a legislação brasileira.

Inclusive no artigo 11 §2º do Marco Civil de Internet, impõe a essas empresas a aplicação da legislação brasileira.

Além disso devemos observar o Decreto 3810/2001, que internacionalizou o MLAT, acordo de cooperação em matéria penal, e mesmo havendo esse acordo, existem discussões sobre aplicabilidade de seus termos por conta das previsões previstas nos termos do Marco Civil da Internet.

Por isso, existe a Ação Declaratória de Inconstitucionalidade nº 51 onde reclama-se que se respeite o MLAT, que foi internalizado por um decreto legislativo.

Além disso o Inquérito 4781 do STF sobre as fakenews, onde foi determinada a suspensão de conteúdo e páginas de determinados usuários, onde num primeiro momento houve uma resistência em cumprimento por parte do Facebook e do Twitter, pois a decisão estaria extrapolando os limites territoriais do Brasil.

Para ela a decisão do Ministro Alexandre de Moraes está correta, uma vez que a decisão incide aos usuários com acesso a internet e IP's localizados aqui no Brasil, e a resistência das empresas nesse caso parece ser ilegal e injustificada.

Outro tema importante é a questão de acesso de dados de usuários da internet (das aplicações e de conexão) nos termos do artigo 13 e artigo 15 ambos do Marco Civil da Internet, devendo-se lembrar que apesar de existir um limite para guarda legal desses dados, que utilizando-se o poder de cautela um Juiz pode determinar a guarda por mais tempo, e o acesso a esses dados deve ser dado através de ordem judicial.

Questionada sobre a sua visão da dificuldade de entrega de dados por parte dos provedores, respondeu que as plataformas de conexões e aplicações tem na maioria das vezes entregue os dados às autoridades.

Alfonso Presti (Ministério Público do Estado de São Paulo)

A questão da cibercriminalidade é muito complexa, pois 3% de todos os delitos em maneira geral recebem punição, ou seja, temos como regra a impunidade.

O maior entrave que temos no Brasil, são entraves de aceitação ao processo digital no Brasil.

Outra questão é a carência dos legisladores em fornecer ferramentas adequadas ao combate aos crimes da internet, onde é difícil caracterizar os tipos penais incriminadores, pois não temos uma legislação penal que tragam conceitos.

Temos o artigo 5º do Marco Civil da Internet, que confrontam um pouco com a Lei Carolina Dieckmann.

Quando se fala em ciberdelitos, falamos internet como ferramenta para prática de crimes, falamos de crimes comuns, crimes específicos, mas falamos em ciberdelitos enquanto um espaço, enquanto um locus.

O MPSP, em sua grande maioria enfrenta muitas dificuldades para resolver essas questões de ciberdelitos, pois é necessário autorização judicial para quase tudo. Os pequenos provedores dificilmente acabam enviando informações necessárias. Tanto é verdade que o MPSP buscou através de inquérito civil e ação civil pública a responsabilização de provedores que tenham utilizado nocivamente os seus serviços.

Quando chega para um Promotor de Justiça uma informação de crime cibernético é um problema dramático, elevando em muito a eficiência da punição de crimes.

O MPSP criou o CYBERGAECO, para tratamento das questões cibernéticas, incluiu também as promotorias de interesses difusos para que o crime cibernético seja enfrentado sob o ponto de vista civil e criminal.

Temos uma deficiência legislativa enorme em relação aos crimes cibernéticos, como por exemplo normas penais em branco nos crimes cometidos pela e na internet.

Também é necessária a capacitação dos operadores do direito (Juizes, Promotores e Delegados) para que eles tenham esses novos conceitos sobre a criminalidade cibernética.

Questionado se existe um corpo técnico que auxilia os Promotores de Justiça, uma vez que eles possuem formação do direito e não formação de engenheiros, respondeu que primeiramente as questões relacionadas a porcentagem de impunidade, deve-se chamar o NEV da USP para tratar as estatísticas. Além disso, existe um corpo técnico chamado Caex que auxiliam os promotores, ressaltando que muitos casos as demandas (notícia de crime) acabam não chegando.

Marco Antonio Marques da Silva (PUC-SP)

O tema internet, é um tema transdisciplinar, como por exemplo a educação digital que serve como um código de comportamento de como se portar na internet, e o que seria uma educação digital?

A sociedade deveria desmistificar a questão da internet ser um território sem lei.

Nos crimes cometidos pela internet não existe a presencialidade, territorialidade e materialidade, fatos esses que pode gerar uma sensação de impunidade e que o crime compensa.

A grande dificuldade da cibersegurança é de investigar, prosseguir (processar) e punir, ou seja, uma resposta com caráter pedagógico e educativa para evitar esses tipos de delitos.

Também concorda com o ponto de vista que o Marco Civil Da Internet não trouxe elementos e conceitos para a área penal, mas o MCI possui o art. 7º que o acesso à internet é essencial ao exercício da cidadania e assegura os direitos, sendo esse artigo quase que uma espinha dorsal do MCI.

No tocante aos crimes cibernéticos, sejam eles próprios ou impróprios, se visa proteger a confidencialidade, integridade e disponibilidade do sistema.

Considera que o Inquérito do STF, é um monstro jurídico, pois a própria vítima pode investigar, determina providências, pode dar medidas e depois julgar, sendo que existem órgãos destinados na Constituição para a investigação policial.

Questionado sobre a educação digital, os pais pecam em deixar os filhos na frente de celulares e computadores? A nova geração é educada olhando para frente, para o além. Antes da pandemia, especialistas falavam que era necessário ter um limite quanto as crianças e adolescentes utilizarem dispositivos eletrônicos e a internet, porém esse cenário foi totalmente alterado por conta da pandemia.

Ricardo Vieira de Souza (PUC-SP)

O fenômeno deve ser entendido sob o ponto de vista tecnológico, sociológico e do direito, porque envolve tecnológica, relações sociais e as leis.

Atualmente as pessoas podem se comunicar estando localizadas em diversas partes do mundo, e a união dos cabos submarinos que permitem as pessoas se conectarem em diversas localidades do mundo, é reconhecida pelo Marco Civil da Internet como a escala global da rede.

Além disso, por se falar em transfronteiriço, existe a questão da transferência internacional de dados pessoais, como por exemplo o Facebook transferir dados da União Europeia para os Estados Unidos, para se esquivar a uma legislação mais rígida de proteção de dados pessoais.

Afirma ser incoerente o discurso do Facebook em não querer acatar a decisão do STF em bloquear mundialmente as contas relacionadas a Fakenews, mas utilizar o dispositivo da transferência internacional de dados pessoais.

O problema da jurisdição na internet, na verdade deve ser visto como a falta de jurisdição estatal e a falta de cooperação entre Estados. É necessária uma lei que internacionalize as questões relacionadas a internet, como por exemplo a Convenção de Budapeste, que é um importante instrumento de cooperação.

É necessário se discutir a adoção do Brasil a Convenção de Budapeste.

Deve-se censurar por exemplo, o WhatsApp, que acha que não deve cumprir a legislação brasileira, uma vez que eles têm escritório no Brasil, ganham dinheiro com as eleições, mas acham que não precisam ser cumpridas as determinações judiciais.