Entrevista: Renato Opice Blum, especialista em Direito Eletrônico

Spacca" data-GUID="renato-opice-blum.jpeg">

A legislação ordinária brasileira cobre, total ou parcialmente, 95% dos crimes eletrônicos. Os demais 5% que ainda não têm previsão legal são motivos de grande preocupação. “É um mundo sem leis”, diz **Renato Opice Blum**, um dos poucos advogados especializados em Direito Eletrônico no país.

Ele revela que depois das acusações de calúnia e difamação online, as principais ações do chamado Direito Eletrônico no Judiciário tratam de invasões de sistemas e vazamento de informações, dois tipos de ilícito sem tipificação específica na legislação penal brasileira.

Se o *cracker* invadir um sistema privado sem causar prejuízo, não há crime. Trata-se de um fato atípico. No caso de vazamento de dados, a pena é de um ano, não proporcional ao efeito multiplicador quando o vazamento se dá na internet.

Em entrevista à **Consultor Jurídico**, o advogado diz que o Judiciário brasileira tem suprido as lacunas da legislação com muita imaginação e sabedoria jurídica. Segundo ele, o Brasil não tem leis como Estados Unidos, União Européia e mesmo como os vizinhos Argentina, Chile e Colômbia. Mas tem muito mais casos e decisões judiciais. Em suas contas já chegam a 17 mil os julgados em matéria de Direito Eletrônico no país.

A falta de legislação específica é apenas um dos elementos que fazem com que a Era da Tecnologia possa ser considerada a Era da Insegurança. Um clique em falso e, em minutos, todos os seus vizinhos, colegas de trabalho e amigos com acesso à internet poderão ver, ouvir e comentar o seu segredo. Anos de investimento na segurança do sistema vão por água abaixo depois de alguns esforços de um *cracker***,** que quebra as barreiras e senhas e tem acesso a todas as informações sigilosas da empresa.

Por isso é necessário criar mecanismos de proteção aos dados pessoais, que integram milhares de cadastros feitos por empresas, sites, cartões de crédito. Opice Blum cita a lei do estado de Nevada, nos Estados Unidos, em que todos os dados devem ser criptografados assim que coletados. Já que a possibilidade de vazamento não pode ser descartada, que eles se tornem incompreensíveis aos serem

repassados inadvertida ou ilegalmente.

Renato Opice Blum tem 39 anos e três filhos. Começou a vida acadêmica na faculdade de engenharia. Levou quatro anos para perceber que o Direito era a carreira que mais lhe agradava, talvez por influência do pai, desembargador do Tribunal de Justiça de São Paulo. Inquieto, decidiu estudar Economia ao mesmo tempo. Não concluiu engenharia na FEI, de São Bernardo do Campo (SP), mas formou-se em direito na FMU e em economia na Faap. Seu destino foi traçado logo no primeiro ano da faculdade, quando foi estagiar em um escritório que advogava para uma fabricante de computadores.

Uma passagem pelo Tribunal de Justiça de São Paulo, como estagiário do juiz aposentado Luiz Flávio Gomes reforçou a opção. “Ele adora tecnologia. Presenciei a primeira coleta de depoimento que fez usando videotexto”, um precursor da videoconferência. Desde 1997, em sociedade com o pai, mantém um escritório que conta com 61 profissionais.

Participaram da entrevista, os jornalistas Gláucia Milício e Mauricio Cardoso

Leia a entrevista:

ConJur — Há necessidade de legislação específica para tratar da internet?
Renato Opice Blum — O Direito Eletrônico merece atenção especial, porque tem muitas peculiaridades. É uma área que já existe na prática, com reflexos importantes para a sociedade como um todo. O Brasil vive uma situação *sui generis*. Não tem legislação específica, mas tem muitos casos interessantes julgados, o que não acontece em países que já têm legislação para a internet. Há alguns anos, crimes que aconteciam lá fora, aqui não existiam. Hoje, também acontecem dentro do Brasil. Os Estados Unidos e a União Europeia têm legislação específica prevendo a coleta, o tratamento, a guarda e o eventual compartilhamento de dados pessoais coletados pelo governo, por empresas e no comércio eletrônico. Sem dúvida, tem de haver leis próprias para isso. Cada vez mais fornecemos os nossos dados e não percebemos os riscos disso. Todo mundo tem cartão de crédito, e-mail, Twitter, Orkut, Flickr, MSN. Nossos dados estão disponíveis para estas empresas quando fazemos o cadastro. Estamos aceitando perder nossa privacidade sem perceber.

ConJur — Esses dados estão se tornando cada vez mais valiosos.
Opice Blum — A informação vale muito hoje, mas não existe interesse pelo seu tratamento no Brasil. Uma lei do estado de Nevada (EUA) prevê que determinadas informações devem ser automaticamente criptografas depois de coletadas. As empresas, o governo, os sites têm de respeitar as condições de coleta, sob pena de serem responsabilizadas e multadas. O grande problema é a questão do vazamento dos dados. O Legislativo de Nevada entendeu que, por mais que haja segurança, os dados podem vazar. Portanto, que vazem de forma incompreensível. O Brasil tem de dar este passo. Andar de acordo com a evolução tecnológica. Argentina e México já aprovaram leis nesse sentido.

ConJur — A legislação brasileira não trata da questão?
Opice Blum — Não. Aqui usamos uma legislação genérica. Temos de nos concentrar no detalhamento dessas situações e dar mais atenção aos projetos relacionados com tecnologia, Direito Eletrônico, internet. São questões muito sensíveis. Há um mês estive no Peru, para um congresso. Há uma rede internacional de escritórios que trabalham com Direito Eletrônico, TI e propriedade intelectual. Eu e

minha sócia tínhamos 45 minutos para falar, mas a nossa exposição levou duas horas e meia. Notamos que todos os países que estavam lá, especialmente da América Latina, tinham legislação específica para crimes eletrônicos, proteção de dados. No Brasil, apesar de ainda não existir, temos em torno de 17 mil decisões judiciais relacionadas às novas tecnologias, o que despertou o interesse de quem estava no congresso.

ConJur — E como o Judiciário brasileiro está analisando essas questões?
Opice Blum — Apesar de todas as dificuldades, os tribunais brasileiros estão indo muito bem. Já decidiram questões que nos outros países foram pouco discutidas. A validade da prova pericial é uma delas. A polícia faz uma busca e apreensão e prende o computador do acusado. Ele diz que entre os dados apreendidos há um e-mail pessoal, que não está relacionado com as acusações. O Judiciário tem entendido que o uso dessa prova vai depender da análise de um perito. Se ele achar que pode ter relação com as acusações, pode ser usado. Em outros países, não. Entende-se que o e-mail não poderá entrar nas investigações, porque configura invasão de privacidade.

ConJur — O provedor pode ser responsabilizado pelos e-mails enviados pelos usuários?
Opice Blum — Os tribunais brasileiros têm entendido no sentido de que *lan houses* e *cyber cafes* devem ter o registro de quem está usando o provedor e o seu sistema. Essa interpretação é feita com base no princípio básico de segurança. Nestes casos, as *lan houses* podem ser responsabilizadas por crimes cometidos por seus usuários. O Código Civil brasileiro diz apenas que se você for negligente e cometeu o ilícito, deve indenizar. E que há responsabilidade objetiva quando a atividade for de risco. Em cima desta previsão genérica, os advogados têm de fazer a sua interpretação e criar uma tese para levar aos tribunais. Na União Europeia, por exemplo, este entendimento ainda não existe. Lá o arcabouço legal é bem interessante, formado por diretivas, que direcionam as leis de cada país. Existem diretivas sobre assinatura de planos, de comércio eletrônico, de privacidade, de tratamento de dados e até de responsabilidade do provedor no comércio eletrônico. Mas não há decisões nesse sentido, nem nos Estados Unidos.

ConJur — No caso de e-mails corporativos, o Tribunal Superior do Trabalho já entendeu que a empresa pode ter acesso.
Opice Blum — Este é um caso em que a legislação não existe, mas a situação está acontecendo e os tribunais tiveram de dar uma resposta. Num primeiro momento, os tribunais entenderam que a empresa não poderia monitorar o e-mail do funcionário. A reversão total desta posição se deu nos tribunais superiores. Esta é uma decisão correta. Uma questão que ainda está se formando nos tribunais é o uso da internet corporativa para acesso, por meio de artifícios, a sites bloqueados pela empresa, como e-mail pessoal. A empresa pode controlar esses acessos? Mesmo ao e-mail pessoal? Ela pode argumentar que está monitorando o registro do funcionário: “Entrei no webmail porque ele fraudou o sistema”. É uma discussão sensível, porque de fato há uma conduta irregular.

ConJur — A dificuldade é adequar a repressão ao potencial ofensivo?
Opice Blum — Exatamente. Calúnia, injúria e difamação pela internet têm um potencial ofensivo enorme. Nos Estados Unidos, há pouco tempo, uma adolescente de 13 anos se matou depois de sofrer o chamado *cyber-bullying*. A vizinha criou um perfil falso no MySpace e passou a ofendê-la. A agressora foi condenada a um ano de prisão. Não foi proporcional.

ConJur — E qual a responsabilidade do site, neste caso?
Opice Blum — Existe a responsabilidade inconsciente, que presume o não conhecimento. Quando o provedor dá apenas o meio técnico para a publicação do conteúdo, defendo que não tem de ser responsabilizado. Não pode ser diferente. Caso contrário, ninguém vai querer prover conteúdo ou o serviço será caríssimo. A ideia é a seguinte: quando não se conhece o conteúdo, não há responsabilidade. A partir do momento que toma conhecimento do conteúdo impróprio, tira do ar ou será responsabilizado. Situação diferente é quando a *lan house* não guarda os registros de conexão. Ela não pode alegar que não sabia. A situação é diferente.

ConJur — Já houve casos em que a conexão *wireless* da *lan house* foi usada para cometer irregularidades na internet. O estabelecimento responde nesses casos?
Opice Blum — Quando a *lan house* oferece conexão *wireless*, deve criar senhas ou autenticar o acesso de alguma forma. Se não o fez, responde pelas irregularidades. Não importa se o acesso é sem fio ou não. Quem trabalha com meio eletrônico tem de conhecer o seu funcionamento. Agora, se alegar que o usuário quebrou a criptografia da rede, a situação muda. É preciso buscar as causas da invasão. Se for por negligência da *lan house*, ela responde.

ConJur — Quando a situação acontece de forma reiterada, vale a alegação de que o provedor não sabia?
Opice Blum — Esta é uma questão interessante do ponto de vista jurídico. O artigo 187 do Código Civil prevê punição em casos de abuso de direito. Esta, no entanto, deve ser uma discussão mais profunda. Fala-se em inclusão digital, mas não se discute a educação digital. Não é possível dar um computador e internet e dizer “usa”. A pessoa tem de saber dos riscos, dos limites, do que pode e não pode fazer. Um rapaz no Rio Grande do Sul se suicidou com dicas que recebeu de internautas em um *chat*. Há situações extremas que causam preocupação. Não podemos descuidar. O meio eletrônico é muito bom, mas é sensível e tem riscos, com graves consequências.

ConJur — Então, todos os envolvidos no processo de acesso e uso da internet têm responsabilidade sobre abusos cometidos?
Opice Blum — O Tribunal de Justiça do Rio Grande do Sul tem uma decisão interessante. Um consumidor entrou com ação contra a companhia telefônica. Seu nome foi parar no serviço de restrição ao crédito porque se recusou a pagar uma conta com diversas ligações para Ilhas Salomão, em 2003. A companhia conseguiu provar que o autor da ação acessou sites pornográficos por meio de uma conexão nas Ilhas Salomão. Ele baixou um programinha e, ao invés de se conectar em Porto Alegre, o acesso foi feito por aquele país. O tribunal decidiu que quem acessa a internet e não usa antivírus é responsável. Por isso, acho que todos nós temos um grau de responsabilidade. No caso de crianças e adolescentes, os pais podem responder, dependendo das circunstâncias. O Código Civil prevê graus de responsabilidade.

ConJur — A internet não foi feita com o princípio de não ter controle?
Opice Blum — Mais do que isso. Foi feita para não cair nunca, ficar sempre no ar. A internet no início era um projeto militar, que depois foi ampliado para os nossos meios e chegou até à tecnologia da informação. Hoje é preciso pensar em procedimentos de segurança e trabalhar em cima de prevenção. O exemplo do estado de Nevada vai nesse sentido. A informação vai ser tratada, coletada, mas se por ventura não der certo, se sair do controle, que saia de uma forma controlada. Temos a Wikipedia, que é

uma enciclopédia colaborativa. O conteúdo em sua maioria é muito bom, mas existem coisas que não procedem. Então, é preciso cuidado, comparar o conteúdo com outras fontes.

ConJur — Criaram até uma enciclopédia, que ironiza a Wikipedia, com um conteúdo totalmente inventado.
Opice Blum — Quando é brincadeira não tem problema. A questão é quando se extrapola e cai na humilhação, difamação. A internet oferece muito conhecimento mas cria problemas na mesma proporção por conta da interatividade global.

ConJur — Um dos problemas da internet é o difícil controle da autoria tanto de criações como de crimes, não é?
Opice Blum — Do ponto de vista jurídico, do Direito Penal, não se pode condenar sem que haja comprovação da autoria. Sentada atrás do teclado e da tela do computador a pessoa se sente segura para fazer o que quiser. Uma pessoa tímida, que ao vivo jamais seria suspeita, pode cometer crimes pela internet. Às vezes a pessoa se sente tão segura que acaba deixando pistas, em favor da percussão penal e da Justiça. É muito fácil criar um perfil falso numa rede social para destruir outra pessoa. A identificação é difícil e quando acontece o acusado pode alegar que foi uma brincadeira. Nesta linha, a legislação brasileira é muito precária. Apesar do que, existe previsão legal para 95% das situações criadas dentro do Direito Eletrônico. Em 60% a cobertura é total. Em 35%, parcial. Em 5%, não há qualquer previsão. É um mundo sem leis.

ConJur — Para quais casos não há lei?
Opice Blum — Uma pessoa que invade um sistema (que não seja na administração pública) só para olhar e não faz nada, não pode ser condenada. Este é um fato atípico. Mas existe previsão para os casos em que o sujeito entra no sistema e vaza uma informação. A Lei de Propriedade Intelectual (Lei 9.279), em seu artigo 195, trata da situação de vazamento de informação sigilosa a que uma pessoa teve acesso indevido. A pena é de um ano de prisão. No entanto, há uma distorção. Se alguém quebrar o IP *[Internet Protocol, o número de identidade de cada computador que acessa a rede]* de 20 milhões de pessoas, a pena é a mesma. Ele será condenado a pagar cestas básicas. Esse é um caso em que há previsão parcial. Outra situação preocupante é a pena para a pessoa que colocar vírus em uma urna eletrônica: 5 a 10 anos de prisão. É uma punição extremamente severa, maior que para homicídio.

ConJur — Onde está prevista?
Opice Blum — Na legislação eleitoral. A legislação em relação à administração pública já é melhor. Se o servidor emprestar a senha de acesso ao sistema para terceiro, a pena é de dois anos. Razoável. A norma que trata do peculato eletrônico (Lei 9.983) é interessante. Se houver alteração de um dado ou informação da administração pública em troca de vantagem indevida, o servidor pode pegar de dois a 12 anos de prisão. Esta lei nasceu depois da violação do placar do Plenário do Senado. O Legislativo discutiu e aprovou rapidamente a legislação depois do episódio. Conseguiu fechar algumas lacunas dentro da administração pública. Neste ponto houve evolução. Mas também é preciso evoluir na esfera privada, para que haja uma proteção mínima.

ConJur — Quais são os pontos importantes destes 5% de situações em que não há qualquer previsão legal?
Opice Blum — A primeira coisa que precisa ser regulamentada é o acesso indevido, a invasão de

sistemas privados. Não se pode permitir que alguém quebre uma senha e invada o sistema. No mundo inteiro é regulamentado. Aqui, se a invasão não causar prejuízo, não aconteceu nada. É um fato atípico, não tem o que fazer.

ConJur — Mas no mundo físico, se eu invadir a casa de outra pessoa, mesmo sem levar nada, é crime.
Opice Blum — Perfeitamente. Este crime está previsto o Código Penal: crime de violação e invasão de domicilio. O probleminha é que no Direito Penal é vedado o uso da analogia. Então, ainda que seja a mesma coisa, no código está escrito casa e não meio eletrônico. Não é possível usar analogia.

ConJur — Os juízes estão preparados para julgar crimes pela internet?
Opice Blum — A maioria está. As decisões do Judiciário têm sido acertadas. Quando o juiz não se sente confortável para julgar, nomeia um perito para fazer esclarecimentos técnicos. É claro que muito disso depende do advogado fazer o convencimento, de fazer a sua tarefa prévia. Nessa área, estamos intimamente ligados aos profissionais técnicos. Dificilmente se discute uma questão de Direito Eletrônico sem um parecer técnico. São atividades complementares. A profissão de perícia eletrônica tende a crescer aqui, como nos Estados Unidos. No Brasil, existem poucos peritos com conhecimento profundo, capazes de fazer uma boa análise de um dispositivo que está sendo periciado. Principalmente, quando envolve tecnologia que mistura problemas de computadores, banco de dados e dispositivos eletrônicos. A análise deve integrar todas essas áreas, e é muito difícil, porque o profissional tem que ter conhecimento de um pouco de cada situação.

ConJur — Criar e disseminar vírus é crime?
Opice Blum — Essa é uma questão que gera muitos debates. Hoje, se alguém criar um vírus e houver provas de que foi para destruir um sistema, e dependendo do sistema que atingir, é possível condená-lo. Se for uma tentativa de prejudicar um serviço, é crime. Mas a pena é mínima. Já a criação de um vírus, em si, é um fato atípico. Ao editar a lei, o legislador terá que levar em conta o potencial ofensivo, tratar do dolo. Não que a legislação vá impedir que o crime aconteça. Há pena para homicídio e isso infelizmente continua acontecendo. A ideia é criar uma organização dentro do sistema do Direito Eletrônico.

ConJur — Há algum projeto no legislativo que esteja caminhando neste sentido?
Opice Blum — O Brasil tem vários projetos, mas o Legislativo precisa ser mais ágil. O projeto que teve mais discussão é o do senador Eduardo Azeredo *[PSDB-MG]*. Nunca vai existir uma legislação perfeita, que atenda todo mundo. Isso é da própria natureza do Direito. A lei é feita para ser questionada, sempre haverá várias formas de interpretação. Mas um marco tem de existir. Há ainda projetos inspirados em leis de outros países da América Latina. A lei argentina é muito parecida com a peruana, que, por sua vez, é muito parecida com a da União Europeia. Há uma sinergia que é importante. A interatividade é extrafronteiras hoje. É preciso haver mecanismos de colaboração e repressão semelhantes. Os tratados e convenções internacionais foram criados para atender essa necessidade. A mais conhecida no âmbito do Direito Eletrônico é a Convenção de Budapeste, que o Brasil ainda não assinou. Apesar de ter 100% de condições de aderir. A Alemanha entrou recentemente.

ConJur — O Brasil não coopera com os outros países?
Opice Blum — Não coopera da forma que está prevista na convenção, mas coopera de outras formas.

Há um sistema de monitoramente conhecido como 24×7. A Polícia Federal tem um profissional disponível 24 horas por dia, sete dias por semana, para receber pedidos de investigação de outros países. É claro que para que isso aconteça, é necessário ter autorização judicial. Há uma discussão apaixonante em torno disso. Um policial de outro país, disfarçado, se diz interessado por pedofilia. Identifica o acusado, coleta provas e descobre que o IP dele fica no Brasil. Quando o pedido de colaboração chega ao Judiciário, o juiz não concede a permissão: "Olha, esta é uma prova preparada. O policial se passou por uma pessoa que não era". A figura da prova preparada existe no nosso Direito Penal, com muita intensidade. É um desafio equalizar todas essas questões. Mas reitero que a Justiça brasileira vai bem nessa matéria. Existe muita gente condenada e muita gente absolvida, corretamente, inclusive.

ConJur — A polícia brasileira está preparada para lidar com este tipo de crime?
Opice Blum — A polícia é muito esforçada. Com a estrutura que possui, faz muito mais do que a capacidade deles. Mas é preciso melhorar as condições de trabalho. Não dá para ter apenas uma delegacia especializada. O ideal seria um núcleo especializado. É uma área que exige colaboração integrada, seja na acusação ou na defesa. O advogado e a vítima devem fornecer subsídios para que a polícia possa trabalhar. Além disso, a polícia científica tem também de ser investigativa. Deve ainda haver promotorias e varas especializadas em delitos eletrônicos. Nessa área, é preciso rapidez. Uma, duas semanas para obter uma informação não é muito para os padrões do Judiciário, mas está longe do ideal para a investigação de crimes eletrônicos. O processo eletrônico será uma reviravolta.

ConJur — Quais são os crimes que mais ocorrem?
Opice Blum — Hoje, as questões não se restringem a calúnia, injúria e difamação. Estas continuam sendo situações de extrema gravidade, porque quando acontecem pela internet, propiciam uma propagação muito grande. Mas há situações mais graves, como invasão de sistemas e vazamento de informações. Há muito investimento para manter dados em sigilo e, de repente, eles vazam e não há como saber onde foram parar. Isto é muito sério. Seja quanto aos investimentos, seja quanto à segurança econômica, seja quanto ao uso indevido por terceiros. A grande preocupação das empresas é em relação ao funcionamento e à proteção dos sistemas. Elas querem a segurança da informação e de que não haverá nenhuma intrusão externa no sistema. Internamente, a preocupação é quanto ao uso indevido e vazamento de dados.

ConJur — E isso acontece com frequencia?
Opice Blum — Já vi situações em que profissionais da área de segurança de informação, sem querer, sem querer mesmo, deixaram vazar informações altamente sigilosas. A pessoa foi trabalhar em casa, deixou um sistema de guarda de arquivos aberto, o Google foi lá e indexou. Outro problema frequente é a manipulação de provas e evidências.

ConJur — Com tanta tecnologia, o senhor se preocupa com grampo telefônico?
Opice Blum — Eu me preocupo mais com o grampo ambiental. Por isso, procuro ser 100% correto em tudo o que falo e faço. Hoje, há câmeras, gravadores, celulares em todos os lugares. Qualquer coisa pode cair na internet, no *YouTube*, no mesmo momento em que você fez. Além do que, pela minha profissão, sou obrigado a manter sigilo. Tenho de tomar medidas de segurança, ter um sistema seguro e me preocupar com o que digo. Mesmo tendo cautela você corre riscos, muitos riscos.

ConJur — No seu escritório, como as informações, os e-mails são protegidos?
Opice Blum

— Temos um sistema de criptografia, regras de boas práticas e um senhor regulamento de segurança da informação. Tudo isso para cumprir com o dever de sigilo dos advogados. Como a tecnologia evoluiu tão rapidamente, pode ser que um dia alguma informação vaze, mas daí vaza de forma incompreensível. Existem empresas especializadas nesses sistemas de segurança para escritórios. Muitos ainda não pensaram nisso. Eu penso porque trabalho muito com segurança da informação.

ConJur — Podemos dizer que a privacidade não existe mais?
Opice Blum — O conceito de privacidade mudou. Está restrito a situações especificas em que você vai lá e coloca o selo "confidencial", "sigiloso". Todos saberão que aquele documento está protegido. De resto, temos de interpretar caso a caso. Se a janela está aberta, alguém pode filmar de fora. Por que deixamos a janela aberta? Mas se a cortina estiver fechada e o vizinho usar um espectro que vara a cortina, aí é invasão de privacidade. Teve aquela discussão do caso do Supremo, em que os ministros estavam trocando mensagens durante a sessão plenária e o fotógrafo do *[jornal] O Globo* registrou as imagens. Nós temos que tomar cuidado com essas situações, a cada dia, a cada momento. Um casal nos Estados Unidos processou o Google Maps, porque encontrou uma imagem da casa deles, de cima. O casal perdeu a ação. É um ambiente público. Mesmo se o Google Maps flagra uma pessoa nua tomando sol na cobertura do prédio. Não se pode tomar sol nu. Se a pessoa está lá, não tem expectativa de privacidade.

ConJur — Então, o mundo virou um grande Big Brother?
Opice Blum — E nós somos os operadores do Big Brother. (risos) Todo mundo está vendo tudo de todo mundo o tempo todo. A palavra chave é expectativa de privacidade. O primeiro caso de expectativa de privacidade nos Estados Unidos foi o de um casal que comprou uma casa nos arredores de Manhattan. Como eles gostavam de andar nu pela casa, construíram um muro a cinco quilômetros de distância da casa. Uma pessoa colocou uma escada no muro e os fotografou. No tribunal, o acusado disse que não houve invasão, porque estava antes do muro. O casal contestou, dizendo que houve invasão a partir do momento que construíram o muro com a expectativa de que ninguém tivesse acesso à casa. O tribunal entendeu que, de fato, havia expectativa de privacidade.

ConJur — Outra questão complicada na internet é a da propriedade intelectual. Quem é o dono do que está na internet?
Opice Blum — Esse é um problema. Pela legislação você só pode dispor daquilo para o que você tem autorização legal ou de quem tem os direitos autorais. Quem imprime um site pode estar violando os direitos autorais. A pessoa pode acessar, navegar. Só pode imprimir se tiver autorização. É constante a violação dos direitos de propriedade intelectual na internet. As pessoas acham que não estão fazendo nada de errado. Quem coloca uma música, um vídeo num site P2P para outras pessoas baixarem pode receber punição de 2 a 4 anos de reclusão. Há decisões no Brasil nesse sentido. O problema é controlar isso. Esta é uma questão mundial. Se não for disseminada a cultura de que isso não pode ser feito, ninguém vai querer criar mais nada.

ConJur — Os novos meios eletrônicos modificaram o conceito de propriedade intelectual. Hoje estão à disposição todos os meios necessários para que as pessoas possam reproduzir músicas, filmes, vídeos. Como vamos tratar essa questão agora usando as regras dos tempos do vinil?
Opice Blum — Acima de tudo, temos que respeitar os princípios gerais do Direito e o Estado Democrático de Direito. Se a legislação proíbe esse tipo de circunstância, até que seja alterada, ou que

haja posicionamento jurisprudencial mais flexível, temos que defender o seu cumprimento.

ConJur — E quando a legislação não está adequada aos novos meios?
Opice Blum — Ela pode ser atualizada. Mas em alguns casos, a atualização não se faz necessária. Quando as coisas se dão de forma tão rápida, as infrações acontecem e o Estado não consegue dar conta nem da repressão. Por não conseguir frear, acaba tolerando. A legislação poderia evoluir no sentido de permitir reproduções para uso pessoal, já que hoje esta é uma realidade. É diferente da reprodução para comercializar, distribuir. Em alguns casos de propriedade intelectual, mudanças legislativas podem ser feitas. No entanto, alguns pontos vão permanecer para sempre. O sujeito que criou e quer que a sua obra fique protegida para sempre, tem esse direito. A criação intelectual é um dos maiores dons do ser humano. Todo o desenvolvimento da sociedade está ligado à criação intelectual.

Date Created
22/03/2009