e-book

DIREITO DIGITAL & LGPD

INSTITUTO DE DIREITO CONTEMPORÂNEO

OPICE BLUM ACADEMY

SUMÁRIO

1 - DIREITO DIGITAL

1.1 - O DIREITO DIGITAL FRENTE ÀS NOVAS TECNOLOGIAS E COMO MEIO DE CONFORMIDADE, PREVENÇÃO E REPRESSÃO

1.2 - MARCO CIVIL DA INTERNET, LIMITES E OBRIGAÇÕES DE USUÁRIOS E PROVEDORES

1.3 - CONTRATOS ELETRÔNICOS E PROVAS DIGITAIS

1.4 - RELAÇÕES TRABALHISTAS E COMPLIANCE DIGITAL: COMO PROTEGER SUA EMPRESA DE RISCOS INTERNOS

1.5 - CYBERCRIME E CYBERATAQUES: COMO MITIGAR RISCOS E COMO REAGIR

2 - LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

2.1 - LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA

2.2 - DADOS PESSOAIS E DIREITOS DOS USUÁRIOS

2.3 - TRATAMENTO DOS DADOS DE FORMA LÍCITA E O PAPEL DO DPO/ ENCARREGADO DE DADOS

2.4 - COMO REAGIR A UM INCIDENTE?

DIREITO DIGITAL

O DIREITO DIGITAL FRENTE ÀS NOVAS TECNOLOGIAS E COMO MEIO DE CONFORMIDADE, PREVENÇÃO E REPRESSÃO

Em poucas décadas e de maneira expressiva, as ciências tecnológicas evoluíram consideravelmente desde a criação da Internet.

Os sistemas de inteligência artificial, realidade aumentada e realidade virtual invadiram irreversivelmente o mercado brasileiro. Experiência de consumidores que pareciam ser raras foram exponencialmente popularizadas a partir de 2018, principalmente, seja através de produtos wearables (tecnologias vestíveis), seja através de equipamentos domésticos de IoT, como em games e brinquedos em geral.

Entretanto, a era digital e suas promessas de melhorias à vida pessoal e profissional de milhões de usuários também representam inseguranças e uma fatídica exposição daqueles que um dia se permitiram as mudanças de um mundo que, há poucas gerações passadas, desconhecia os impactos que a utilização de determinadas ferramentas representaria para a sociedade.

Dessa forma, a educação é a chave para que essas inseguranças e riscos sejam mitigados e o melhor da tecnologia e Internet possa ser devidamente explorado. A contextualização do Direito Digital, portanto, é imprescindível e permite um conhecimento melhor das medidas preventivas e repressivas em casos de invasão de sistemas, vazamentos de dados, direito ao esquecimento, cybercrimes, dentre outros.

Assim, nessa linha, é inquestionável que os desafios futuros passam pela compreensão da legislação atual, assim como pela adequação de todo um sistema voltado ao planejamento empresarial e familiar, sendo inafastável e urgente a compreensão do Direito Digital e de como ele alcança a conformidade, prevenção e repressão.

MARCO CIVIL DA INTERNET, LIMITES E OBRIGAÇÕES DE USUÁRIOS E PROVEDORES

A Lei Federal nº 12.965/2014, comumente tratada por Marco Civil da Internet, trouxe inovações e maior segurança à sociedade como um todo quando do estabelecimento de princípios e da consolidação de direitos e deveres para o uso da Internet em território nacional.

Certamente, apesar de não esgotar o tema, essa legislação setorial (Internet) foi e é motivo de entusiasmo pela sociedade e profissionais da área do direito digital e tecnologias, na medida em que, como já pontuado por Renato Opice Blum, "a abrangência da internet é incalculável" e, por isso, iniciativas do legislativo que, de fato, contribuam para as políticas de segurança nesse setor devem ser incentivadas e suas repercussões debatidas em prol de um prospecto mais positivo a médio e longo prazo.

Ademais, em razão do grande fluxo de troca de informações, disponibilização de conteúdo sensível e de prestação de serviços pelas plataformas digitais, a imposição de limites para usuários e provedores é medida que se impõe e deve ser invariavelmente respeitada, sob pena de aplicação de sanções previstas na legislação civil e criminal atualmente em vigor.

Sendo assim, o que precisa ser considerado para que, em tempo hábil, haja melhor respaldo à sociedade quanto ao que pode ou não ser permitido ao usuário? Como reagir frente à necessidade de preservação dos direitos civis, sobretudo quanto às obrigações e responsabilidades impostas por força da lei? Qual a efetividade do Marco Civil da Internet nos cases práticos? Esses, dentre outros, são objetos de especial atenção na exposição desse tema.

CONTRATOS ELETRÔNICOS E PROVAS DIGITAIS

A compreensão dos contratos eletrônicos e da sua validade ainda é algo que causa muitas dúvidas, as quais, invariavelmente, são suscitadas quando se necessita que determinado documento digital seja utilizado como prova em um processo administrativo, judicial ou arbitral.

A bem da verdade, tem-se que um contrato digital possui a mesma validade jurídica que um contrato físico, de tal sorte que o desafio está em se compreender as diferentes modalidades de contratação pela via eletrônica, assim como, e especialmente, os cuidados essenciais para se garantir, por exemplo, a integridade e disponibilidade desse documento.

Nesse viés, vale se questionar:

Será que, ao aceitar os termos de uso de um app, estamos firmando um contrato?

Ao acessar um site, estamos construindo uma prova?

E ao utilizar o GPS do celular?

Ou, quem sabe, ao acessar um programa de streaming de filmes?

Será que a impressão de um e-mail é suficiente para provar uma conversa? Ou talvez o seja o seu encaminhamento direto para o e-mail do cartório?

Essas são algumas perguntas que permeiam uma das aulas do nosso curso e sobre as quais o aluno poderá refletir e responder.

RELAÇÕES TRABALHISTAS E COMPLIANCE DIGITAL: COMO PROTEGER SUA EMPRESA DE RISCOS INTERNOS

É inquestionável que, atualmente, o mercado de trabalho é um dos maiores destaques para inúmeras das questões inerentes ao Direito Digital. O combate à prática de atos lesivos no meio corporativo deve ser uma constante e medidas preventivas devem ser sempre priorizadas, para que, por consequência, esse ambiente não seja comprometido por uma violação à segurança da informação, da marca, reputação, dados pessoais, entre outros importantes valores e ativos empresariais.

É nesse cenário que a sistemática de um compliance digital tem o condão de permitir a prevenção e resolução dos efeitos de condutas lesivas, negligentes, culposas ou mesmo não intencionais.

Para tanto, mister que se tenha em mente o desenvolvimento ou revisão das políticas internas, aplicando o Direito Digital às relações trabalhistas em prol dos padrões éticos, morais e de segurança da empresa, considerando, inclusive, os novos ambientes de trabalho e conceitos como BYOD (Bring Your Own Device) e BYOC (Bring Your Own Cloud).

Diante de um incidente, crime ou ilícito que tenha partido de dentro de uma empresa, sem dúvidas, será o compliance digital um importante aliado para estabelecer e limitar a responsabilidade dos envolvidos, na medida em que o compliance não é um ato isolado, mas um processo que alia o treinamento de pessoas, a implantação de sistemas e o monitoramento do processo.

CYBERCRIME E CYBERATAQUES: COMO MITIGAR RISCOS E COMO REAGIR

Nos dias de hoje, quase não se fala em expansão digital sem que sejam considerados eventuais atos criminosos, que são cada vez mais propagados por meio do uso dessas novas fontes. É por isso mesmo que a crescente disponibilidade de dados nas redes e a facilidade de acesso a tais informações tornou-se um chamariz para agentes mal-intencionados.

Os motivos para isso são inúmeros. Os setores afetados pelos cybercriminosos, na sua maioria, guardam relação direta com ativos financeiros, mas a violação à privacidade, inclusive de cunho sexual, vazamento de dados sensíveis, cyberbullying e determinadas modalidades de fake news, também ocupam a lista dos principais ilícitos da atualidade, cujo resultado depende diretamente das ferramentas digitais.

A Norton Cyber Security chegou a reportar recentemente que o Brasil se destaca em seu radar como um dos países com maior índice de cometimento de crimes cibernéticos no mundo, concorrendo com países tais como China, Estados Unidos e Rússia. Também é relevante pontuar que a Microsoft chegou à conclusão, após um estudo promovido em 23 países, de que cerca de 30% dos "crimes online" estão ligados a amigos ou mesmo parentes das vítimas. Trata-se de uma surpresa aos menos avisados, mas o que mais pode impressionar é que o grupo de maior exposição, de acordo com essa referência, compreende a faixa etária de 18 a 34 anos. Ou seja, apesar de se tratarem de pessoas incluídas em uma categoria jovem, com maior acesso à internet e demais mídias e que, portanto, poderiam estar melhor instruídas sobre esses perigos, são justamente as mais vitimadas.

Em atenção também a isso, os poderes legislativo e judiciário procuram coligar esforços para repudiar tais práticas e puni-las, por meio da condenação dos agentes. As penas e respectivas execuções variam e nem sempre cumprem um papel pedagógico, tendo em vista a recorrência crescente dessa prática.

Naturalmente, cresce também a importância das abordagens com viés educacional e preventivo, para que novas condutas de consequências irremediáveis às vítimas sejam evitadas. Eis um exemplo clássico e irrefutável de uso benéfico da tecnologia, a fim de que a propagação desses, dentre outros eventos criminosos, sejam gradativamente inibidos.

Como identificar o ilícito ou o crime, como reagir e como mitigar os riscos e os danos são lições essenciais em uma sociedade conectada.

LGPD

LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA - LGPD

Em primeiro plano, o Regulamento Europeu Geral de Proteção de Dados – GDPR (General Data Protection Regulation) desempenhou papel protagonista para a consolidação dos artigos reunidos na Lei Federal nº 13.709/2018, a Lei Geral de Proteção de Dados brasileira – LGPD, que visa proteger os dados pessoais das pessoas físicas, humanas, identificadas ou identificáveis.

A compreensão do que isso representa em meio às demais matérias do Direito Digital não pode ser menosprezada e, portanto, explanações conceituais sobre a lei federal que passará a vigorar em 2020, inclusive com exposição dos princípios que regem a legislação, é condição para que demais pontos, tais como o papel da Autoridade Nacional de Proteção de Dados (ANPD) e o âmbito de aplicação da lei também possam ser trabalhados.

Antes do advento da LGPD, o Marco Civil da Internet previa apenas uma única possibilidade de coleta e tratamento de dados pessoais, qual seja: com o consentimento do titular. A ampliação dessa hipótese para um rol de pelo menos dez possibilidade distintas representa inegável ganho às empresas, que efetivamente poderão coletar dados mesmo sem o consentimento do titular, desde que assim o faça com propósito justificável.

Por outro lado, não obstante as vantagens que a LGPD traz às empresas, é preciso que o empresário inicie, desde logo, a adequação de seus procedimentos, rotinas, sistemas, e atividades em geral de coleta e tratamento de dados pessoais, à nova legislação, para que fiquem em conformidade, evitando qualquer tipo de sanção.

Certamente estamos diante de um "novo tempo" de proteção de dados no Brasil, e ainda haverá um grande amadurecimento de empresas e pessoas naturais quanto à coleta e tratamento de dados pessoais, sendo de grande relevância a aprovação da LGPD.

DADOS PESSOAIS E DIREITOS DOS USUÁRIOS

Mas, afinal, o que seriam dados pessoais?

Por uma perspectiva simplificada, define-se por quaisquer informações referentes ao seu titular que o identifiquem ou possam identificá-lo, conforme previsto no artigo 5°, I, da LGPD.

O titular dos dados possuem inúmeros direitos, consolidados especialmente pela LGDP, tais como o direito de conhecer quem detém seus dados, de negar o tratamento dos seus dados pessoais, direito de ter acesso a eles, de pedir retificação e exclusão dos seus dados pessoais, dentre outros.

De fato, a proteção da LGPD, nesse aspecto, poderia ser considerada uma releitura de alguns direitos também previstos em outros diplomas legais que aqui merecem citação, como a própria Constituição Federal Brasileira de 1988, que sempre garantiu os direitos fundamentais, mais precisamente em seu artigo 5°, dada a importância da preservação do indivíduo nas interações e relações virtuais.

Essa repetição, todavia, não é nenhum demérito, reforçando, isso sim, os direitos dos titulares, inclusive para estabelecer limites ao uso dos seus dados, bem como prazos para eventuais respostas aos seus questionamentos.

Porém, para quem trabalha com tecnologia ou direito digital, logo surgem inúmeras perguntas a respeito dos direitos dos titulares: como saberei quem está com os dados, diante da facilidade de transferência? Como garantir que os dados foram excluídos? Como cumprir os prazos? Qual o limite da informação que precisa ser prestada? E se eu não possuir o consentimento, mas precisar dos dados?

TRATAMENTO DOS DADOS DE FORMA LÍCITA E O PAPEL DO DPO/ ENCARREGADO DE DADOS

A boa notícia é que para todas – ou quase todas – essas dúvidas há uma resposta ou, ao menos, uma diretriz, sendo certo que o objetivo da lei não é impedir que os dados sejam tratados, principalmente quando houver justo motivo para tratá-los e isso ocorrer de forma transparente, respeitando os limites legais.

Para entender o que seria esse justo motivo, a própria LGPD traz as hipóteses para tratamento dos dados, tais como obrigação legal, obrigação contratual, consentimento e legítimo interesse.

A complexidade e peculiaridades de cada uma das hipóteses, especialmente o legítimo interesse, reclama análise mais acurada, motivo pelo qual dedicamos uma aula sobre esse tema em nosso curso, seguida da compreensão do papel e responsabilidade do DPO (Data Protection Officer)/Encarregado de Dados, do Operador e do Controlador do tratamento dos dados pessoais, bem como do mapeamento dos dados pessoais tratados (afinal, para se verificar com precisão se algo está sendo feito correta e licitamente, antes é imprescindível entender o que exatamente está sendo feito).

COMO REAGIR A UM INCIDENTE?

Muito embora o Brasil seja um dos 100 países que possuem legislação específica e destinada à proteção de dados, determinados incidentes são frequentes e, portanto, com amparo justamente dessa legislação, a melhor medida preventiva seria a de conscientização dos

envolvidos e o desenvolvimento de planos que mitiguem o risco de vazamento de dados.

O controle é fundamental, já que não há ambiente absolutamente impenetrável e, portanto, plenamente seguro. Em determinados casos, é compulsória a notificação do incidente, assim como o desenvolvimento de um plano de contenção dos danos.

Apesar de a LGPD, que ainda não está em vigor, trazer diretrizes e obrigações diante de um incidente, tem-se que o próprio mercado e a sociedade já realizam certo julgamento de empresas envolvidas em vazamento de dados, sendo que, dependendo do volume e tipo de dados vazados, a reputação dos envolvidos é comprometida a ponto de inviabilizar a continuidade do negócio ou do emprego. A este respeito, basta lembrarmos de casos conhecidos sobre vazamento de dados médicos de pacientes ou da lista de clientes de uma empresa de relacionamentos extraconjugais.

Assim, se alguém ainda duvida que a LGPD veio para ficar e para "pegar", ousamos dizer que ela já pegou e que, se hoje ainda é um diferencial competitivo já estar compliant com ela, muito em breve, o mercado anuncia, não passará de uma obrigação comum, cuja não observância terá importantes e cruciais consequências.

INSTITUTO DE DIREITO CONTEMPORÂNEO

OPICE BLUM ACADEMY