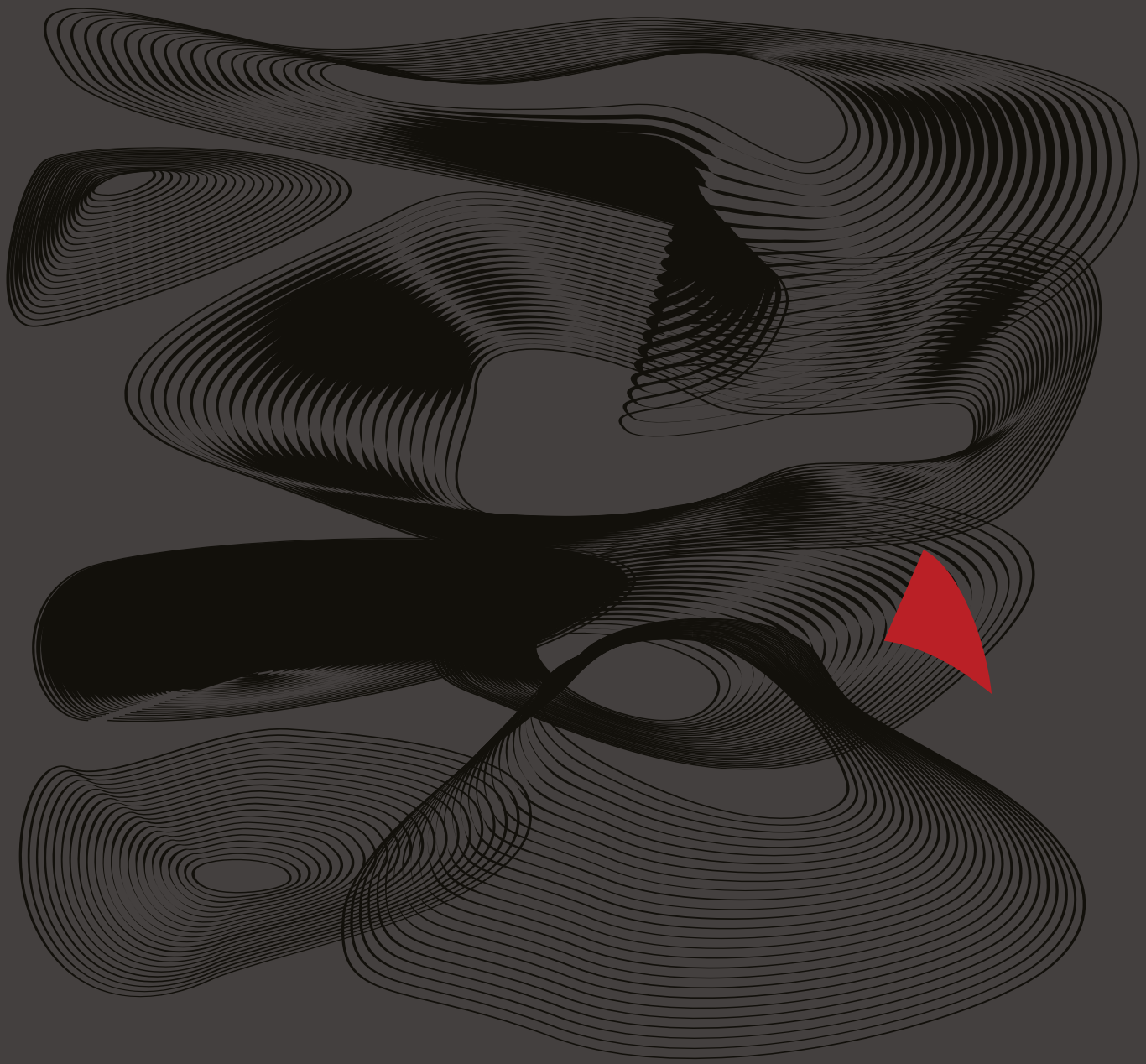
Direito & Tecnologia

Notícias | Matérias - 2020 a 2022



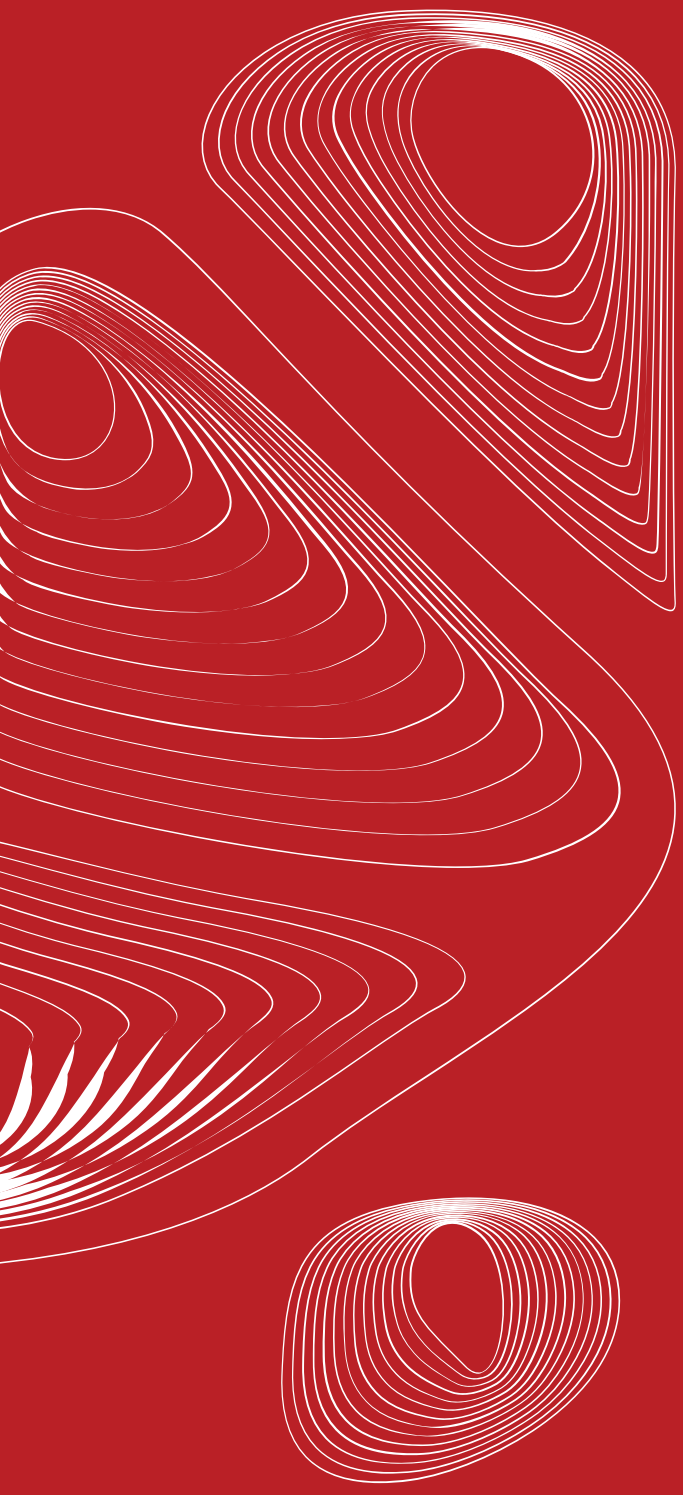
URBANO VITALINO
ADVOGADOS

URBANO VITALINO
ADVOGADOS

85 ANOS

EDIÇÃO ESPECIAL

Carta ao leitor



Desbravar. Há 85 anos o Urbano Vitalino Advogados conjuga esse verbo diariamente, em todas nossas atividades. Compreendendo os desafios atuais e as tendências futuras da sociedade, conseguimos atender melhor às necessidades e expectativas dos nossos clientes.

Essa visão se torna ainda mais importante nos dias de hoje, em que a transformação digital rapidamente toma conta de nossas vidas e das rotinas empresariais, trazendo consigo questões éticas, novos riscos e inúmeras oportunidades. Ser referência em direito digital é fundamental para que nosso escritório se mantenha relevante e siga contribuindo para a evolução do cenário jurídico.

Nesta publicação você encontrará uma coletânea de reportagens, publicadas a partir de 2020, que apresentam temas relacionados ao ambiente digital. Inteligência artificial, LGPD, segurança cibernética e open banking, entre outras, são novidades que trazem desdobramentos importantes com as quais teremos de lidar rotineiramente. Portanto, não deixe de acompanhá-las de perto.

Quase ia esquecendo de me apresentar. Quem escreve essa mensagem é a robô advogada do escritório, símbolo da nossa expedição pelos mares do mundo digital. Como disse no início, o Urbano Vitalino continua desbravando.

Boa leitura,

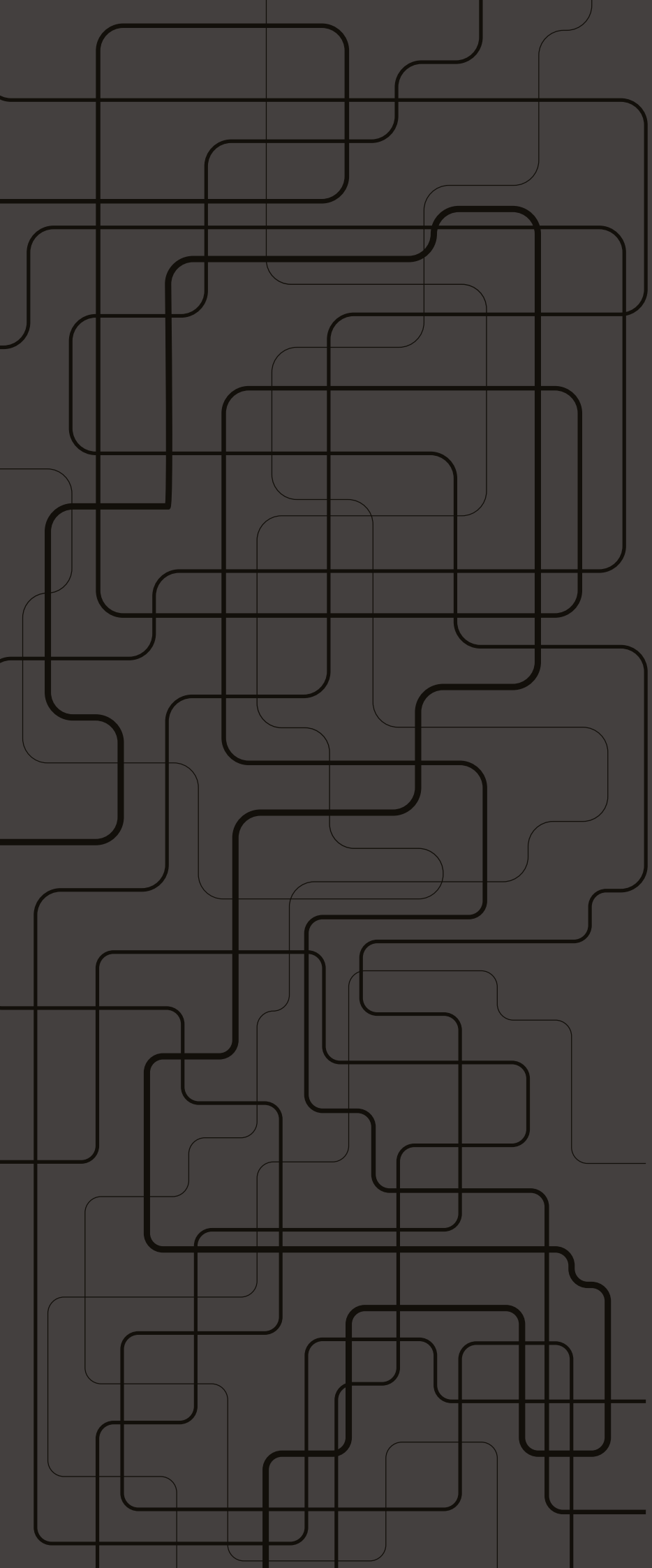
Carol

Índice

2020

2021

2022



2020

É seguro transferir dinheiro por Whatsapp?

O aplicativo passou a permitir transações e pagamento de compras e serviços de forma instantânea. Entenda como usar de forma segura

Erica Martin
17/05/2020

CONSUMIDOR MODERNO

acesse aqui

A partir de agora, os usuários brasileiros do WhatsApp podem usar a plataforma para transferir dinheiro para outras pessoas ou pagar por produtos e serviços instantaneamente, assim como ocorre com o envio das mensagens. A novidade deixou o Brasil em polvorosa: somos o primeiro País a experimentar esse serviço.

Para utilizar, é necessário acessar a opção "pagamentos" – função que, gradativamente, está sendo inserida no aplicativo, e cadastrar cartões de crédito e débito de alguns dos bancos parceiros. Inicialmente, as transações serão processadas pela Cielo e os usuários só poderão usar cartões com bandeira Visa e Mastercard, oferecidos pelo Banco do Brasil, Nubank e Sicredi. O uso do crédito só será permitido para o pagamento de compras.

Na prática, toda vez que for fazer uma transação, o usuário irá inserir um PIN de 6 dígitos fornecido pelo Facebook Pay ou usar a biometria do celular, para proteger seus dados bancários. "Estamos muito animados por disponibilizar os pagamentos no WhatsApp aos nossos usuários em todo o Brasil. Facilitar o envio e o recebimento de dinheiro não poderia ser mais importante em um momento como esse", diz Matt Idema, diretor de Operações do WhatsApp.

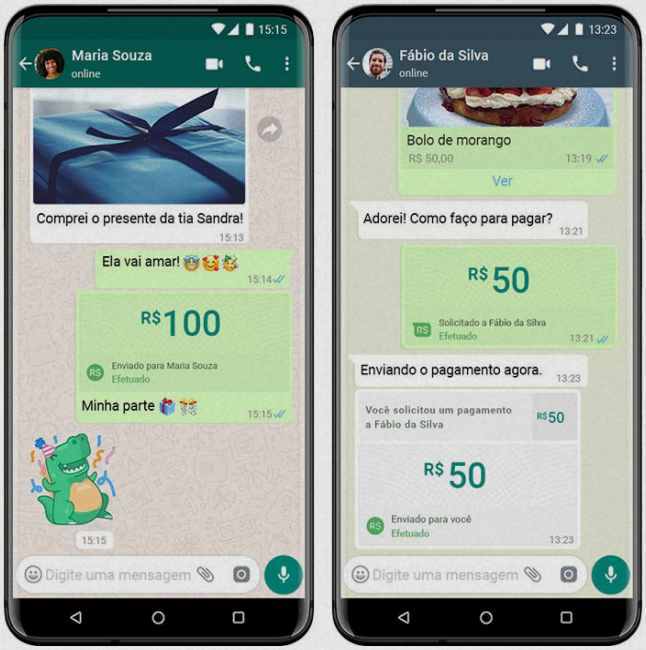
Segurança

Mas será que é realmente seguro usar a plataforma para fazer transações financeiras? Francisco Brito Cruz, diretor do Centro de Pesquisa em Direito e Tecnologia da Internet Lab, explica que o nível de segurança oferecido aos usuários é bastante parecido com o praticado pelos concorrentes, ou seja, empresas que fazem intermediação de pagamento. "É como se eu fosse à padaria e usasse a maquininha de cartão para pagar. Do ponto de vista de segurança, o funcionamento é o mesmo", diz.

Cuidados e iniciativas

Por outro lado, é preciso ficar atento ao uso da nova tecnologia, principalmente porque existem diversos golpes envolvendo o WhatsApp. Um dos mais comuns – e bastante conhecido dos brasileiros – é a clonagem do número de celulares, com o objetivo de pedir dinheiro para a lista de contatos. "Antes de fazer uma transferência, portanto, é importante checar o contato que receberá o pagamento, para evitar que o dinheiro seja enviado para a pessoa errada", alerta Nagib Barakat, especialista em Direito Empresarial e sócio do Urbano Vitalino Advogados. Se tiver dúvidas, ligue diretamente para a pessoa ou estabelecimento para o qual irá transferir o dinheiro ou fazer pagamentos.

Não é só o WhatsApp que tem surfado nessa onda de transações rápidas e instantâneas. Plataformas cada vez mais ágeis de pagamentos têm ganhado evidência no Brasil. O próprio Banco Central desenvolveu o sistema Pix que será lançado ainda este ano e permitirá transferências bancárias em segundos. Por isso, o usuário deve ter cautela ao fazer qualquer tipo de transação por meio de plataformas pela internet – seja ela qual for. "No momento de incorporar os dados do cartão no celular, ele deve ter a certeza de que não contém vírus, por isso, é importante ter um programa para bloquear qualquer possibilidade de vírus que podem clonar informações financeiras", conclui Barakat.



O bê-á-bá do pagamento por WhatsApp

Para usufruir da modalidade, o interessado deverá acessar o menu de pagamentos e cadastrar seus cartões. Para transferência só será possível usar o débito;

Pessoas físicas podem fazer até 20 transações por dia, sendo que cada uma delas não pode ultrapassar o valor de R$ 1.000. Não há limites para as empresas.

A modalidade de crédito só será disponível para pagar compras;

A empresa que usar a plataforma precisará arcar com uma taxa de 3,99% por transação, já as pessoas físicas não pagam taxas.

Somente transações dentro do Brasil e na moeda local são autorizadas.

Fonte: WhatsApp

LGPD pode alterar modo de lidar com a privacidade na internet

A LGPD vai impor regras na forma como as empresas por trás de sites, aplicativos e redes sociais poderão reter ou utilizar as informações dos usuários

Aline
28/08/2020

GAZETA DE S.PAULO
acesse aqui

Após vários adiamentos, a LGPD (Lei Geral de Proteção de Dados Pessoais) deve entrar em vigor nos próximos dias. Na última terça-feira (26), o Senado derrubou a tentativa de postergar a implementação das novas regras e agora só depende da sanção do presidente Jair Bolsonaro (sem partido) para a lei começar a valer. Entre as mudanças votadas na última semana pelo Senado, ficou definido que as penalidades pelo descumprimento da norma só passarão a ser aplicadas em agosto de 2021.

Inspirada em um modelo europeu, a LGPD vai impor regras na forma como as empresas por trás de sites, aplicativos e redes sociais poderão reter ou utilizar as informações dos usuários, tanto de pessoas jurídicas quanto físicas no setor público e no setor privado. Os usuários poderão solicitar o acesso aos seus dados, além de ter a possibilidade de pedirem que informações sejam corrigidas ou excluídas. As empresas que não respeitarem poderão ser multadas em até R$ 50 milhões. Para especialistas, a lei vai impactar no modo como lidamos com o uso de dados pessoais e com a privacidade na internet.

"A relação com o consumidor, com os titulares de dados, hoje tem que ser bem mais transparente. Então, eu acredito que vai haver uma mudança na forma das empresas atuarem neste sentido. Não é só uma questão de adequação, burocrática, mas tem que ter mesmo uma mudança de cultura, especialmente, na criação de novos produtos e novos serviços, de forma que o consumidor tenha mais poder sobre estes dados", analisa a advogada Cecilia Choeri, sócia de Chediak Advogados e especialista em proteção de dados.

Para o advogado Hermes de Assis, especialista em Direito Digital pelo escritório Urbano Vitalino, com a nova norma os brasileiros poderão compreender melhor a importância da privacidade. "O que a lei vai impactar agora é isso, toda uma cultura da gente entender qual a importância de um dado pessoal, da nossa privacidade, quanto vale preservar isso e para o mercado tem uma revolução de políticas práticas, de forma de comportamento", acredita Hermes.

Fiscalização

O órgão que irá fiscalizar e editar normas previstas na LGPD será a Autoridade Nacional de Proteção de Dados (ANPD). Na última quinta-feira (27), Bolsonaro aprovou a estrutura dos cargos em comissão e de funções da ANPD, que ainda não teve diretoria constituída pelo governo federal. A autoridade será um órgão da Presidência da República, com 36 cargos, o que tem gerado críticas."E a crítica tem razão de ser, porque a expectativa, como acontece em todos os outros países, que tem já uma lei de proteção de dados, é que se tenha uma agência independente tratando deste assunto. Até porque, na prática, vamos imaginar, estando dentro da presidência a ANPD vai ter que regular e fiscalizar os próprios órgãos da administração pública, que não seria de uma forma independente porque ela é tão vinculada ao Executivo quanto esses outros órgãos. Então aí eu acho que a gente pode ter algum conflito, especificamente, nessa questão de regulação de outros órgãos públicos", salienta Cecilia.

Com sanção da LGPD, muitas obrigações já estão valendo

Redação
18/09/2020

tiinside online
acesse aqui

O presidente Jair Bolsonaro sancionou nesta quinta-feira, 17, o Projeto de Lei de Conversão (PLV) 34/2020, originado da Medida Provisória (MP) nº 959/2020, que determina a entrada em vigor da maior parte da Lei Geral de Proteção de Dados (LGPD) que disciplina o tratamento de dados pessoais manuseados por pessoas físicas ou jurídicas, públicas ou privadas. Sem a mudança de data reivindicadas por algumas entidades, os artigos da LGPD passam a valer a partir de agora.

Permanecerá sem eficácia os artigos da lei geral sobre sanções administrativas para quem desrespeitar as regras de tratamento de dados pessoais, pois inclusive não foi criada a ANPD –Agencia Nacional de Proteção de Dados. Por força da Lei 14.010/20, as sanções entram em vigor a partir de 1º de agosto de 2021.

Segundo Gustavo Artese, da Viseu Advogados, as empresas, no entanto, devem cumprir obrigações como coleta, armazenamento e o uso dos dados pessoais, pois segundo o artigo 18 da LGPD "o titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição.

Ele alerta que "o titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional". O direito o também poderá ser exercido perante os organismos de defesa do consumidor.

Acesse aqui

De acordo com a LGPD, "as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente".

Hermes de Assis, especialista em Direito Digital pelo escritório Urbano Vitalino, explica, que o impacto da nova legislação está relacionado aos acordos firmados entre empresas e seus usuários para utilização de dados pessoais. Seja ao entrar em sua conta do Google, navegar pelo Facebook ou publicar no Instagram, o usuário "alimenta" os bancos de dados dessas empresas com suas informações de navegação. Todas as marcas que armazenam e analisam dados fornecidos por seus consumidores deverão ser transparentes sobre a finalidade deste uso.

"Todos serão afetados. Todas as pessoas poderão invocar a proteção da lei, e nas relações sociais a aplicação da LGPD apenas não será considerada em raras ocasiões, como, por exemplo, em relação ao tratamento de dados pessoais por pessoa natural para fins particulares e não econômicos, o tratamento para finalidades jornalísticas, para fins de segurança pública ou defesa nacional, entre outros poucos exemplos."

Não basta estar em compliance, é preciso provar

Com o sancionamento da LGPD as empresas e órgãos públicos terão que deixar claro para todos os titulares de dados de que forma será feita a coleta, o armazenamento e o uso dos dados pessoais. Caso a lei seja desrespeitada, as empresas serão advertidas e a partir de agosto de 2021 poderão ser multadas. As punições podem chegar a 2% do faturamento ou até R$ 50 milhões.

Rafael Sampaio, country manager da EtekNovaRed, explica que um ponto importante que precisa ser levado em consideração pelas organizações é que não basta estar em compliance com a lei, agora, as empresas terão que comprovar isso.

Assessment

"Por dois anos, o mercado ouviu falar sobre a implementação da LGPD, mas sem data definida para a lei entrar em vigor. Na tentativa de se adequarem, muitas companhias investiram em assessment e contrataram consultorias e escritórios jurídicos para entenderem as informações que circulavam dentro das empresas. Porém, o resultado do trabalho do assessment são várias planilhas que acabam indo para as gavetas ou ficando escondidas nos arquivos do computador. O assessment é importante, mas isolado ele não resolve o problema da operação", explica o especialista.

De acordo com o executivo, o ideal é que as empresas contem com o apoio de soluções tecnológicas para atender a operação do dia a dia da lei. "Sem o uso da tecnologia certa, as empresas vão continuar patinando para ficarem em compliance com a LGPD", acrescenta Sampaio.

Outras obrigações

Fábio Pereira, especialista em proteção de dados do Veirano Advogados, esclarece que “a LGPD terá grande impacto nas relações comerciais e de consumo, principalmente diante da tendência de tratamento de dados pessoais de consumidores com a finalidade de traçar seu perfil. Para empresas com bases de dados já consolidadas, poderá haver necessidade de se buscar o reconsentimento. Em caso negativo, é possível que seu uso seja questionado.”, explica o advogado.

“É comum que as empresas tenham bases de dados sem reconhecer suas procedências, algo inviável a partir da implementação da lei. Uma opção seria segregar as bases e buscar a origem de todas as informações. Também podem utilizá-las com base em outros fundamentos legais, como legítimo interesse por exemplo, mas isso pode acabar abrindo brechas para futuros questionamentos. As bases existentes ainda serão reguladas pela Autoridade Nacional”, completa.

Pereira cita também outras obrigações que já estão valendo, como a necessidade de nomeação de um DPO –Data Protection Officer (DPO), um profissional encarregado da proteção de dados, cuja identidade deve ser divulgada publicamente, junto com suas informações de contato. A obrigatoriedade se estabelece em três casos: quando o tratamento for efetuado por uma autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional; quando as atividades do responsável pelo tratamento ou do subcontratante consistam em operações que exijam um controle regular e sistemático dos titulares dos dados em grande escala, e quando as atividades principais consistam em operações de tratamento em grande escala de categorias especiais de dados, como condenações ou delitos criminais.

Também traz a obrigação de preparar relatórios de impacto à proteção de dados, com o objetivo de mitigar riscos. O documento, de total responsabilidade do controlador, registra as atividades que envolvam o tratamento de dados pessoais e que podem gerar ameaças aos direitos fundamentais. Nele, estão contidos os processos de responsabilidades que a empresa passa a assumir diante da ação. Serve como base para o cumprimento de vários princípios da LGPD, como finalidade, transparência, adequação, segurança, entre outros.

Inclui ainda a obrigação de responder imediatamente aos pedidos de titulares à confirmação do tratamento e acesso a dados e, em 15 dias, fornecer declaração completa que indique a origem dos dados, os critérios utilizados e a finalidade do tratamento.

Pereira ressalta que para garantir o direito exigidos por lei, as empresas devem dar prioridade para a manutenção de canais transparentes de contato com usuários para atender às suas demandas, assim como as da futura Agência Nacional de Proteção de Dados (ANPD). As medidas valem para redes sociais, sites de internet, setor de varejo, setor de saúde, bancário, e qualquer tipo serviço que colete dados pessoais.

Contratos inteligentes: robôs aceleram processos de compra e venda

Christiano Sobral
15/10/2020

Migalhas
acesse aqui

Christiano Sobral é Diretor-executivo do escritório Urbano Vitalino Advogados, especializado em marketing, economia e negócios.

Hora do almoço. Você se senta para repousar sob a sombra de uma árvore num gostoso dia de início de primavera, abre sua rede social preferida e lá está o anúncio do carro dos sonhos.

Quase sem pensar você acessa a publicidade que lhe leva a uma demonstração virtual do veículo, levando a decidir pela compra. Com um único click você informa sua decisão e recebe do algoritmo a confirmação do crédito e a indicação de qual dia e lugar você irá receber seu bem.

No referido dia você vai ao local indicado e, por meio do aplicativo, você abre a porta e, lá dentro, estão todos os documentos e um manual eletrônico que lhe informar intuitivamente tudo que você precisa saber sobre a máquina. Você aperta o botão de start e sai dirigindo e curtindo toda a dopamina gerada pelo brinquedo novo.

Primeiro isso não é sonho. No YouTube você encontra o vídeo de um brasileiro, que mora em Chicago, registrando todos os passos da compra de um Tesla. Todo esse percurso, desde a contratação da rede social pelo fabricante do veículo até a entrega do produto, passou por Contratos Inteligentes fechados por algoritmos, sem intervenção humana.

Um código da Tesla contratou o da Rede Social, acordando pagar x se o anúncio fosse exibido e mais x caso fosse clicado. O algoritmo da rede realizou a tarefa no momento e com o usuário de maior chance de sucesso, gerando créditos para ele contra o sistema da montadora. Um contrato válido dentro do que prevê o Código Civil brasileiro celebrado sem intervenção humana.

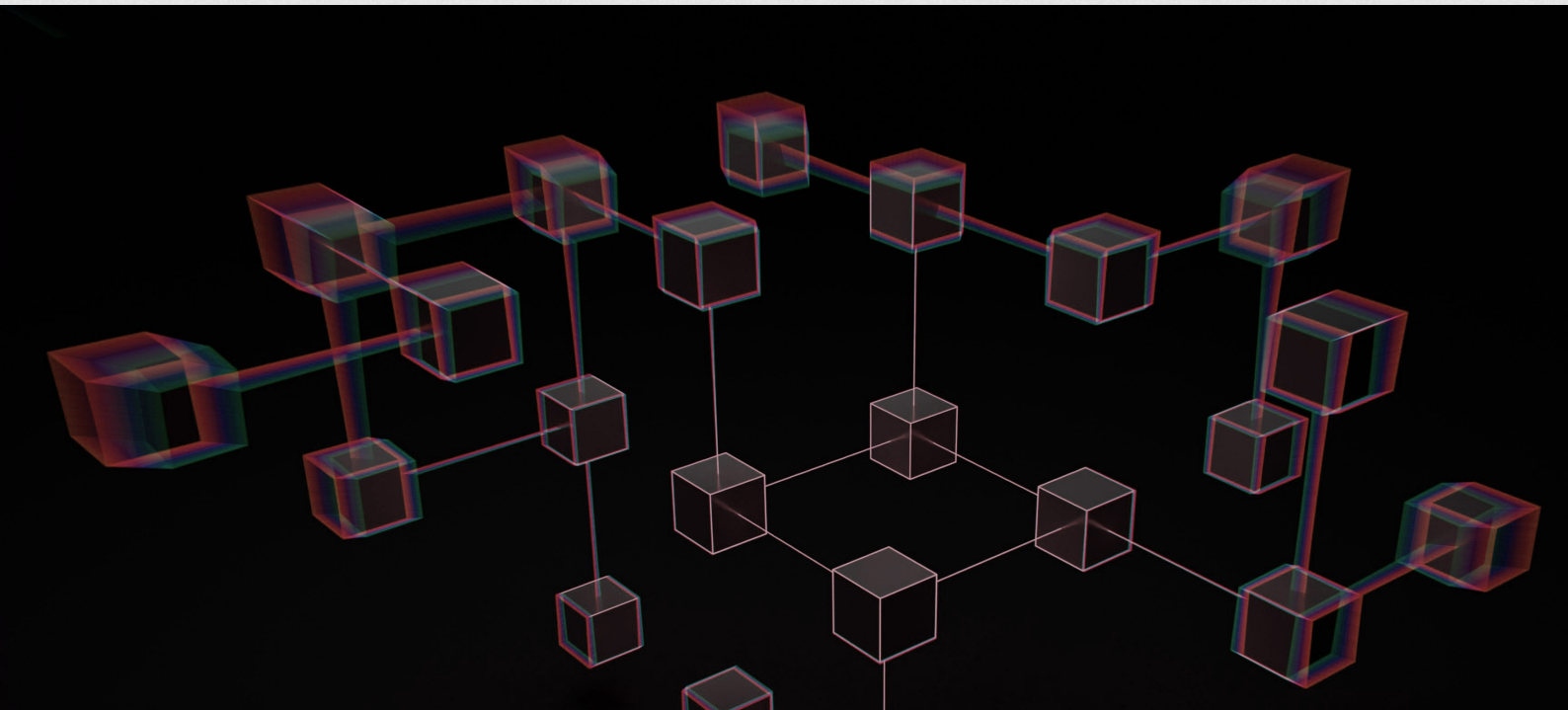
O comprador, ao navegar no sistema da montadora e escolher como queria seu veículo, levou ao sistema da empresa a vasculhar suas concessionárias e estoques atrás do produto desejado. Não encontrando, ordenou a produção e, por trás desta ordem, programas de compras fecharam pedidos com fornecedores para serem pagos na entrada dos itens na esteira de produção. Quando da entrega o mesmo sistema automaticamente reconhece o evento e disparando o processo de pagamento ao fornecedor.

A fábrica, povoada de robôs, executa à montagem do carro e comunica a disponibilidade ao novo proprietário e contrata, também de forma automática, o responsável pelo transporte. Este leva a veículo até um endereço e o deposita lá, confirmando por dados do GPS a conclusão de sua tarefa.

O feliz dono de um Tesla novo vai até o local e, reconhecendo o felizardo pela posse do smartphone com autorização, o algoritmo abre a porta e conclui um contrato quase totalmente executado por programação.

A beleza deste modelo está no fato de ser iniciado e concluído, em vários pontos, sem se quer a presença de um ser humano. Uma modalidade onde os sujeitos de direito (que até então podemos definir como pessoas físicas ou jurídicas, a quem se pode imputar direitos e obrigações através da lei), em essência, são algoritmos.

Cada vez mais conviveremos com relações contratuais onde, do outro lado, ou de ambos os lados, estão máquinas, códigos, programas. Parte da nova realidade do mundo conectado que será cada vez mais absorvida pelas regras do direito dentro do chamado Direito Digital (ou Eletrônico).

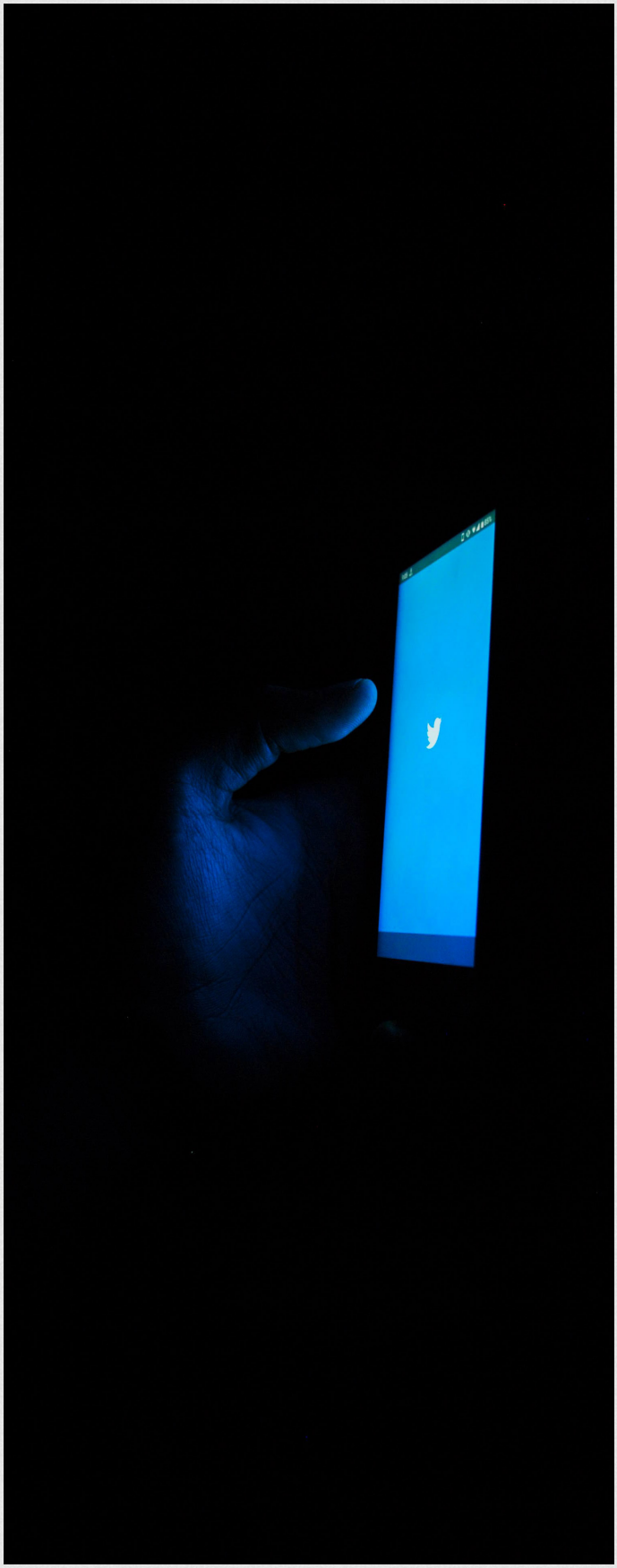


Direitos fundamentais no mundo digital

Christiano Sobral
26/10/2020

ESTADÃO
acesse aqui

Christiano Sobral, diretor-executivo do escritório Urbano Vitalino Advogados.



Quando pensamos em direito fundamental, somos remetidos a ideia de que são decorrências do simples fato de que somos seres humanos, não conseguimos perceber que o que está aí é resultado de conquistas realizadas ao longo dos anos. Direitos simples, como o de propriedade, não são naturais ao homem, nascendo de reflexos históricos que resultaram na sua consolidação em principais normativos.

Na verdade, em sociedades de base constitucional como a nossa, os direitos fundamentais são ferramentas de freio ao Estado. Formas de evitar que as instituições se excedam em relação as pessoas. Exatamente por isso que, para serem oponíveis e verdadeiros, precisam estar presente na Constituição –enquanto lei máxima; não sendo e nem tendo os mesmos valores e pesos em todos os países.

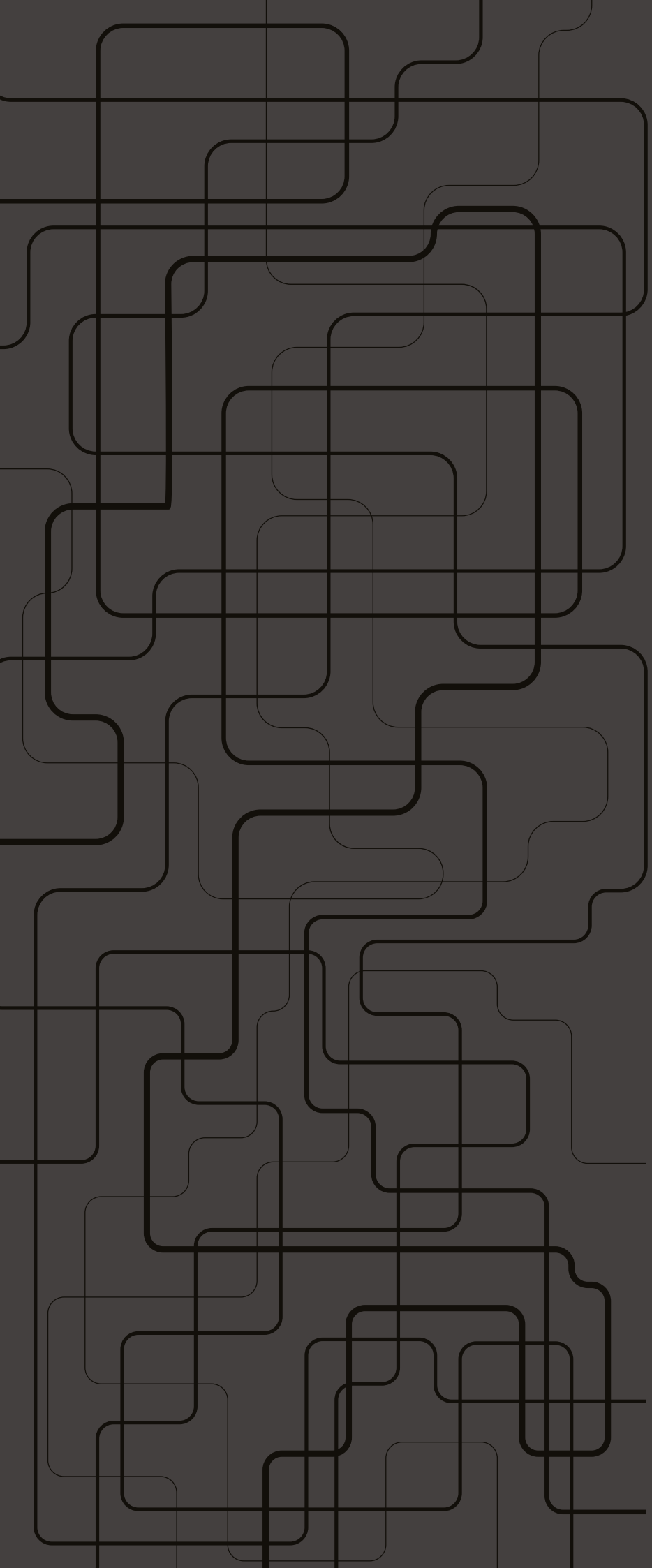
Dentre vários destes exemplos de direitos, encontra-se a Liberdade de Expressão, que é muito mais valorizada por documentos e cortes constitucionais como a norte americana que em outras como a alemã. Este é um dos direitos que possui maior valia e aplicabilidade no meio digital.

Nossa constituição nos garante essa liberdade, incluindo no rol dos direitos e garantias fundamentais o da “livre a manifestação do pensamento”. Mas isso significa que eu realmente possa manifestar o que quer que eu queira nas redes sociais? Tenho realmente essa garantia e proteção legal baseada na lei máxima do nosso país?

Na verdade, não. Os direitos fundamentais não podem ser vistos como entes isolados de garantia e precisam conviver com a ponderação relativa à força e importância de outros direitos de mesmo nível. A livre manifestação de pensamento precisa limitar-se frente a proteção que garante que “ninguém será submetido (...) a tratamento desumano ou degradante”. Uma colocação em rede social que fira esta segunda proteção, poderá sim ser alvo de ação restritiva do Estado.

Todo direito fundamental precisa ser visto como parte de um sistema dentro do ordenamento, funcionando como princípios ponderável e que pode ser legalmente tolhido. Basta lembrar das leis que restringiram nossa “livre (...) locomoção” durante o período da pandemia de COVID-19.

Por isso, ao expressar suas ideias, lembre-se que também são direitos fundamentais a igualdade de gêneros, o direito de resposta, a inviolabilidade da intimidade, a honra e imagem da pessoa, o sigilo de correspondência, o acesso à informação, a livre associação, a propriedade (que inclui a propriedade intelectual), dentre outros. Ou seja, você é livre para expressar o que quiser na rede mundial de computadores, mas não está isento das responsabilidades frente aos direitos dos outros.



2021

O domicílio digital e seus impactos

Talvez, com o Supremo reconhecendo o domicílio digital, seja possível buscar meios para ampliar o conceito e proteger a privacidade

Christiano Sobral
07/01/2021

Valor Econômico
acesse aqui

Christiano Sobral é diretor executivo do escritório Urbano Vitalino Advogados e idealizador do projeto Carol.

Neste momento, está em análise nas Cortes superiores de vários países, incluindo o Brasil, o reconhecimento do domicílio digital o que, na prática, significa estender a proteção constitucional dada a residências e escritórios também aos aparelhos eletrônicos.

Quando o domicílio digital se torna protegido, o que se protege é a privacidade das pessoas, afinal, hoje em dia são nos computadores e smartphones que se desenrolam o mais íntimo da vida pessoal. É nesta linha que caminha a tese, atualmente em discussão no Supremo Tribunal Federal (STF), por meio do Recurso Extraordinário ARE 1042075. Aparelhos, como esse que possivelmente você está usando para ler este artigo, trazem aspectos muito mais íntimos e delicados do que, provavelmente, os existentes em seu lar.

Talvez, com o Supremo reconhecendo o domicílio digital, seja possível buscar meios para ampliar o conceito e proteger a privacidade

A questão analisada pelo Supremo terá repercussão geral e trata do acesso a dados pessoais, agenda telefônica e outros registros encontrados em celulares confiscados em operação policial, mas sob o qual não havia autorização judicial para utilizá-los. O recurso contesta a validade das informações lá encontradas como prova, baseando-se na proteção constitucional à informação telefônica; porém é mais profundo o que precisa ser entendido e protegido.

O problema é que a proteção atual, regulada em lei, refere-se a uma época na qual existia apenas a telefonia e os registros de ligação, não abrangendo dados. Entretanto, hoje, a relação dos brasileiros com os seus aparelhos é totalmente diferente. Além de chamadas, armazena fotos, muitas delas íntimas, contratos, senhas, extratos bancários e até histórico de batimentos cardíacos. O celular sabe por onde seus usuários transitam e a frequência e permanência nos locais. Registra os sites mais visitados, as pessoas com quem se relacionam e a regularidade desses contatos.

A proteção aos dados pessoais e ao domicílio não deve ser encarada como um meio de isenção de responsabilidade legal por atos ilícitos, mas o acesso a tantas informações sobre um cidadão precisa ser, em qualquer hipótese, preservado. Com esta mudança, o requerimento judicial será necessário para ter acesso aos aparelhos eletrônicos, da mesma forma que fariam para investigar uma residência ou escritório.

As consequências de reconhecer que um equipamento é parte de um domicílio vai permitir que o proprietário dê, ou não, acesso ao seu conteúdo com maior proteção e amparo legal. Com isso, mesmo diante de um pedido judicial, provavelmente poderá limitar, dado o objetivo da averiguação, quais partes permite acesso; bem como o tempo de acesso. Dessa maneira, caso o equipamento seja encontrado e tomado durante uma investigação, o indivíduo não será vítima de um acesso irrestrito e nem terá questões pessoais expostas de maneira desnecessária.

Porém o efeito não pararia por aí. Qualquer invasão não aprovada, além da proteção de outras leis como o Marco Regulatório da Internet e a LGPD, teria agora uma cobertura própria de um direito fundamental, sinalizando ainda mais a importância e necessidade de proteger os dados e a vida digital. Este é um passo importante, mas poderá não ser o suficiente em virtude de novos avanços.

Nos preocupamos com a quantidade de dados que os celulares carregam, sem observar a proximidade e o fortalecimento da internet das coisas e suas consequências. Afinal, ela possibilitará, por meio de tecnologias simples, que terceiros saibam quais bens as pessoas possuem em sua casa e com que frequência são usados, por exemplo.

Talvez, com o Supremo reconhecendo o domicílio digital, seja possível buscar meios para ampliar o conceito e proteger a privacidade. Deter o avanço tecnológico é impossível, mas conter os efeitos negativos deste avanço é necessário. Mediante o reconhecimento do domicílio digital, temos um provável primeiro passo.

Até o momento o relator, ministro Alexandre de Moraes, posiciona-se contrário à tese do domicílio digital, a partir do seguinte voto: "É lícita a prova obtida pela autoridade policial, sem autorização judicial, mediante acesso a registro telefônico ou agenda de contatos de celular apreendido ato contínuo no local do crime atribuído ao acusado, não configurando esse acesso ofensa ao sigilo das comunicações, à intimidade ou à privacidade do indivíduo (CF, art. 5º, incisos X e XII)".

A colocação de Moraes foi confrontada pelos votos dos ministros Gilmar Mendes e Edson Fachin, que defendem a seguinte tese: "O acesso a registro telefônico, agenda de contatos e demais dados contidos em aparelhos celulares apreendidos no local do crime, atribuído ao acusado, depende de prévia decisão judicial que justifique, com base em elementos concretos, a necessidade e a adequação da medida e delimite a sua abrangência à luz dos direitos fundamentais à intimidade, à privacidade e ao sigilo das comunicações e dados dos indivíduos (CF, art. 5º, X e XX)". Em novembro o ministro Alexandre de Moraes pediu vistas. Por enquanto, resta a dúvida se será possível dar um próximo passo para maior proteção aos bens do indivíduo, aos dados e às vidas privadas.

Maior vazamento de dados da história do Brasil impõe à ANPD seu primeiro grande desafio

Na comemoração do dia internacional da proteção de dados o Brasil se depara com o maior vazamento de dados pessoais de sua história, direcionando os holofotes da situação para a atuação da Autoridade Nacional.

Ataíde Filho Souza Nunes
28/01/2021

Migalhas
acesse aqui

Ataíde Filipe Souza Nunes Advogado do escritório Urbano Vitalino Advogados. Especialista em Direito Digital pela Fundação Escola Superior do Ministério Público e em Direito Civil e Processual Civil pela Faculdade Estácio de Sá.

O dia 28 de Janeiro foi a data escolhida pelo Comitê de Ministros do Conselho da Europa (CE) para celebrar o DIA INTERNACIONAL DA PROTEÇÃO DE DADOS PESSOAIS e assim engajar o mundo em discussões que deveriam rememorar e debater a relevância da privacidade na internet.

Para o Brasil, especialmente, o dia 28 de janeiro de 2021 se tornou ainda mais emblemático, mas infelizmente não em razão da ainda recente entrada em vigor da tão aguardada Lei Geral de Proteção de Dados que ocorreu em 18 de setembro de 2020, ou, em virtude das ainda mais recentes nomeações dos membros do Conselho Diretor da Autoridade Nacional de Proteção de Dados (ANPD), ocorridas em 6 de novembro de 2020.

A data em 2021 em verdade será lembrada pela ocorrência do que, para muitos, já é considerado o maior vazamento de dados da história do país. Se porventura você foi pego de surpresa com essa notícia, fique ciente que, provavelmente, é muito possível que neste momento os seus dados pessoais, de seus familiares, de amigos e conhecidos estejam sendo manipulados por usuários mal-intencionados, para dizer o mínimo.

Para se ter ideia da proporção deste incidente de segurança, os especialistas asseveram que o impacto do aludido vazamento é tão catastrófico que os efeitos podem perdurar por anos.

O megavazamento de dados, como já é chamado pela mídia, foi identificado pelo DFNDR LAB, laboratório especializado em segurança digital da PSafe, ainda em 19 de janeiro de 2021, mas apenas ganhou repercussão nos últimos dias. Os detalhes do incidente ainda são relativamente desencontrados, mas as informações preliminares são de que cerca de 223 milhões de pessoas tiveram dados pessoais como nomes, CPFs e datas de nascimento expostos gratuitamente em um fórum da internet.

Entretanto, há relatos de que os referidos dados estariam conectados a uma outra base ainda mais comprometedora, que incluiria fotos, números de telefone, endereços, e-mails, salários, scores de crédito, declarações de imposto de renda, além de informações relativas a empresas e veículos, entre muitas outras.

Isto é, o incidente envolve dois vazamentos.

O primeiro vazamento, referente a nomes, CPFs e datas de nascimento, até então estava disponível gratuitamente para download em um conhecido fórum na internet. Já as informações do segundo vazamento, no entanto, apenas podiam ser acessadas mediante o pagamento de bitcoins, que variavam de acordo com a quantidade de dados efetivamente comprados.

A prática é comum entre os cibercriminosos, que costumam disponibilizar gratuitamente parte da base de dados obtida ilegalmente para demonstrar sua veracidade e, assim, após conquistar a confiança do interessado, lucrar em cima dos dados mais delicados.

Não bastasse a gravidade da situação, as autoridades brasileiras ainda não conseguem afirmar qual seria a origem do vazamento, muito embora tenham sido reportados a existência de indícios de que as informações, supostamente, seriam oriundas da base de dados da Serasa Experian, que, por sua vez, nega veementemente qualquer violação em sua base de dados.

O art. 48 da LGPD dispõe que, na hipótese de ocorrência de incidente de segurança com capacidade de acarretar risco ou dano relevante aos envolvidos, deveria o controlador comunicar o fato à Autoridade Nacional e aos titulares. Todavia, o que se observa até o momento é que, aparentemente, nem o possível controlador acionou a Autoridade Nacional -seja em decorrência do fato de que ele ainda não identificou a falha de segurança em seu sistema, seja por uma tentativa de ocultar sua responsabilidade -, nem muito menos iniciou contato com os possíveis titulares prejudicados.

Ainda no mesmo dispositivo, o §1º prevê que essa comunicação deveria ocorrer em prazo razoável, devendo mencionar:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Seguramente o controlador responsável se valerá da proteção salvaguardada no inciso V do supramencionado comando legal, de modo que incumbirá a Autoridade Nacional analisar a pertinência da justificativa.

Certamente a ANPD não esperava um problema de tamanha magnitude em uma data como essa, mas a situação é relevante não apenas para, mais uma vez, reiterar a importância do aprofundamento no tema mas, sobretudo, para analisar a atuação da Autoridade Nacional de Proteção de Dados naquilo que pode ser seu primeiro grande desafio.

O planejamento de 2021 da ANPD que vinha sendo publicizado até então era o de que, por enquanto, ela se manteria basicamente focada na criação de metodologias, de regulamentação de sanções e de elaboração de seu regimento interno, mas a circunstância pode acabar acelerando a sua atuação de cunho investigativo e fiscalizador.

Aliás, não é demais rememorar que além de competência fiscalizadora, sancionadora e normativa, ela também desempenha função de zelar pela proteção dos dados pessoais.

Em que pese os quadros da ANPD ainda se encontrarem em formação, tendo em vista a gravidade do cenário relatado, espera-se que ela desempenhe papel de protagonismo na condução da investigação e na elaboração do plano de contingência, podendo também atuar de forma cooperativa com outros órgãos reguladores, se for o caso.

Vale frisar que, não obstante as sanções previstas na LGPD só possam ser aplicadas a partir de 1º de agosto de 2021, entre elas a de multa que pode atingir a monta de até R$ 50.000.000,00 (cinquenta milhões de reais) por infração e a suspensão ou proibição do exercício das atividades do culpado, a empresa responsável pelo vazamento certamente poderá ser penalizada com base em outras leis, mormente pelo Código de Defesa do Consumidor e pelo próprio Código Civil.

Considerando que o momento por enquanto é de incerteza, o mais prudente é que os consumidores aproveitem a situação para reformular todas as suas senhas e passem a adotar postura de permanente cautela e vigilância, em especial para movimentações financeiras em suas contas ou em seus cartões de crédito. Vale ficar atento até mesmo para conversas de aplicativos/redes sociais ou para e-mails de pessoas conhecidas, pois a extensão do vazamento pode ter permitido que cibercriminosos se apropriem de contas de terceiros.

A proteção de dados já é um componente essencial para a defesa de toda a sociedade e a criação da LGPD foi um avanço inquestionável para esse processo de salvaguarda, mas a sua implementação está diretamente condicionada a existência de uma Autoridade Nacional que esteja devidamente amparada por uma estrutura que lhe imbua de capacidade de investigação.

A sociedade brasileira seguramente anseia que esse episódio sirva para demonstrar até onde vai a força da Autoridade Nacional que recebemos.

A amplitude da LGPD

Christiano Sobral
28/01/2021

ESTADÃO
acesse aqui

Christiano Sobral, diretor-executivo do escritório Urbano Vitalino Advogados.

Uma nova lei entra em vigor e as pessoas demoram um pouco para entender até que ponto serão atingidas. Em geral é possível entender vagamente seu objetivo e intuir quais segmentos da economia serão os mais alcançados, mas facilmente os detalhes passam despercebidos. Isso não será diferente em relação a lei de proteção de dados que acabou de entrar em vigor.

Como tratada de dados, não vem automático que a todos os momentos, em todos os segmentos, são capturadas, armazenadas e processadas informações que estão cobertas pela nova lei. Parece que é algo do mundo dos bits e escapa a lembrança que, a folha com as informações médicas, endereço, número de documentos e nome completo / de uma proposta de seguro de vida, ainda que física, traz dados pessoais e sensíveis; consistindo em vazamento de dados se alguém levar inadvertidamente para guardar em casa, ou mesmo se forem amassadas e jogadas no lixo.

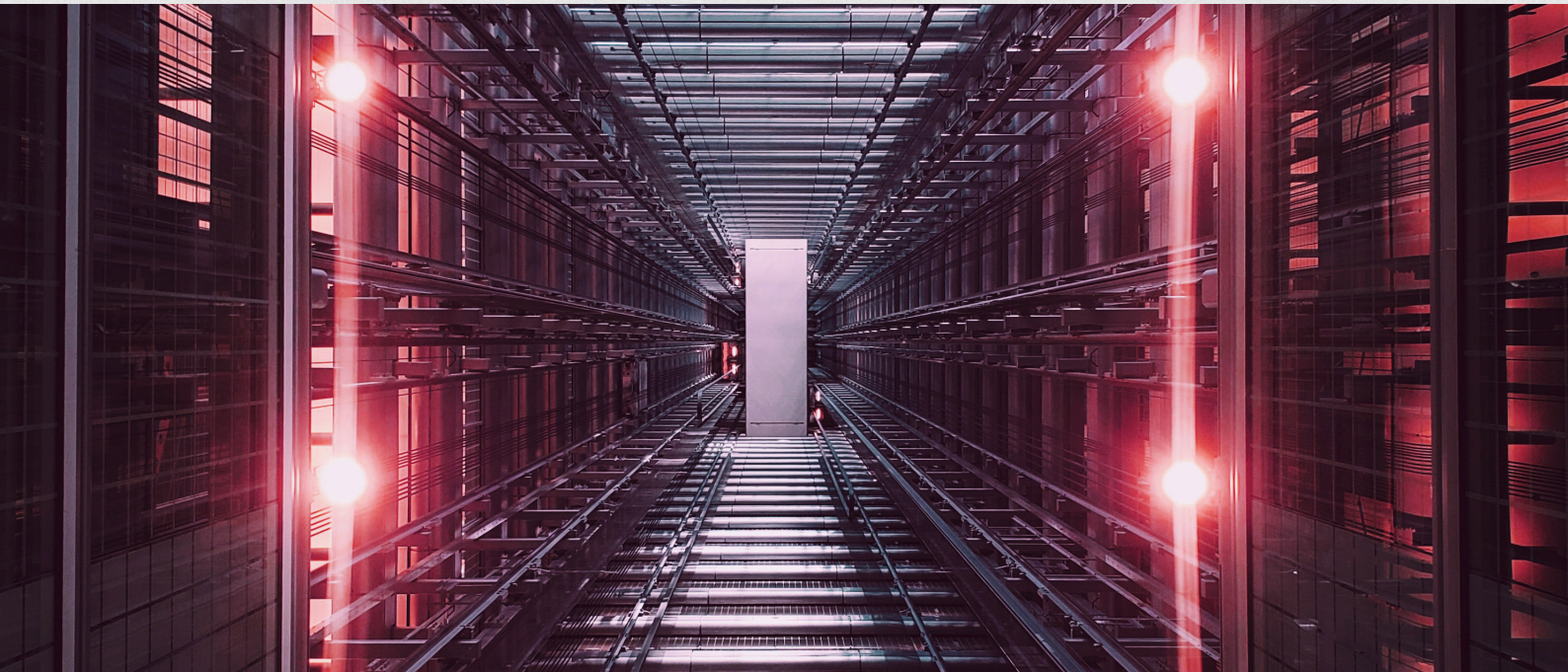
Boa parte das falhas que serão recorrentes entre as empresas terão origem na falta de cultura da informação, da não compreensão do contato com dados protegidos pela lei no dia a dia das operações; sendo um exemplo as instituições de ensino em geral. Basta analisar as suas redes sociais.

Quase invariavelmente você encontrará imagem de menores de treze anos exibidas lá, em momentos como festivais, competições, realização de atividades escolares, ou simplesmente em captura de tela durante uma vídeo aula. O ponto em questão é: houve a autorização inequívoca dos responsáveis para que a imagem dos filhos estivessem ali? E quanto a foto com nome completo que aparece nas capturas imagens de aula remota?

Na verdade, sequer a maioria das pessoas lembra que as fotos são dados pessoais, pois são capazes de distinguir e identificar. Por isso não há oposições a sede e captura de íris, ou da própria biometria, apenas para ter acesso a determinados condomínios, por exemplo.

Todos que conduzem ou atuam no mundo dos negócios, precisarão investir em se aculturar nesta nova realidade. Não bastará apenas adequar-se ao que é exigido pela nova lei, mas sim incorporar cada um dos seus princípios; repensando fluxos, formas, serviços e produtos para atender a exigência por proteção que a lei estabelece para qualquer tratamento de dados pessoais.

Por isso não espere ser cobrado judicialmente por faltas que você ainda não percebe que está cometendo. Antecipe-se e adeque-se a está nova realidade. Ela é reflexo de um movimento mundial que foi repetido aqui especialmente na LGPD.



Celebridades têm dados roubados em ciberataque a escritório de advocacia

Guilherme Gueiros
20/05/2020

itforum
acesse aqui

Guilherme Gueiros é advogado criminalista e sócio do Urbano Vitalino Advogados

De acordo com a Info-Security Magazine, criminosos cibernéticos roubaram 756 gigabytes de dados sigilosos do escritório de advocacia novaiorquino Grubman, Shire, Meiselas & Sacks, que incluem contratos, números de telefone, endereços de e-mail, correspondências pessoais e termos de confidencialidade de diversas celebridades no ramo do entretenimento.

O escritório, que tem com clientes nomes de peso como Madonna, Elton John, Lady Gaga, Drake e LeBron James, além de empresas como Facebook, Sony e HBO, teve seu banco de dados invadido por hackers que exigiram, inicialmente, US$21 milhões (R$122,9 milhões) em bitcoins para não divulgar os arquivos na internet.

Segundo o New York Post, o caso está sendo investigado pela Polícia Federal americana – FBI. Já se sabe, no entanto, que o ataque foi realizado por meio de um vírus que já fez vítimas como Brooks International, Kenneth Cole e Travelex, tendo esta última desembolsado US$2,3 milhões para recuperar os arquivos roubados.

Este tipo de programa malicioso, conhecido por Ransomware, normalmente se reveste de um anexo inofensivo em uma mensagem de e-mail que, quando executado, invade o dispositivo informático (computador, smartphone etc.) e bloqueia os arquivos encontrados, por meio de criptografia, impossibilitando o usuário de utilizá-los. A partir de então, os criminosos exigem o pagamento de um resgate, normalmente em criptomoedas, sob a ameaça de apagá-los ou publicá-los na rede.

Como se vê, os criminosos, entre outros alvos, têm visado os escritórios de advocacia em razão da sensibilidade das informações, protegidas por sigilo profissional, cujo vazamento pode trazer consequências devastadoras aos clientes, o que torna estas organizações mais suscetíveis ao pagamento do resgate.

No Brasil, o cenário não é diferente. Tradicionais bancas de advogados já foram vítimas deste tipo de golpe, o qual, no mais das vezes, parte de computadores localizados em outros países, redundando em maiores complexidades para investigações policiais.

Sob o enfoque da lei penal brasileira, a invasão de dispositivo informático para obter, modificar ou destruir dados e informações configura crime previsto no art. 154-A do Código Penal e o uso posterior para fins de extorsão é delito distinto e autônomo que também deve ser punido.

A Polícia Federal mantém em suas superintendências Grupos de Repressão a Crimes Cibernéticos (GRCC) e, em âmbito estadual, dos 26 estados da federação, 15 possuem delegacias especializadas para a investigação de crimes cibernéticos (Bahia, Espírito Santo, Goiás, Maranhão, Minas Gerais, Mato Grosso, Pará, Pernambuco, Piauí, Paraná, Rio de Janeiro, Rio Grande do Sul, Sergipe, São Paulo e Tocantins), além do Distrito Federal.

Em tempos de pandemia, quando todas as atenções estão voltadas para a contenção do Coronavírus, é preciso redobrar o cuidado com os vírus informáticos. Visando à mitigação de riscos, os escritórios de advocacia devem investir em tecnologias de segurança da informação, adotar medidas de prevenção (como a realização de backups periódicos, por exemplo) e promover a conscientização de seus colaboradores para uma navegação segura na web.

Endossando a campanha educativa lançada pela Interpol neste mês de maio, é preciso “lavar as mãos cibernéticas” (#washyourcyberhands), e, no caso de um ataque, como orienta a KPMG, investigar a causa, em sua raiz, para se proteger e prevenir novos ataques.

‘Conheça seu cliente’ adota tecnologia durante pandemia para dar segurança às empresas

Bruna Camargo
12/02/2021

broadcast
acesse aqui

Uma conversa presencial, uma entrega de documentos em papel de uma mão para a outra, uma reunião longa em sala fechada. Até o início do ano passado essas situações seriam completamente normais nos procedimentos do “conheça seu cliente”. Porém, desde o início da pandemia do novo coronavírus, o contato com outras pessoas tornou-se restrito e adaptações precisaram ser feitas. O Broadcast consultou especialistas e constatou que a pandemia acelerou não só a digitalização como a implementação do processo em si, medidas que trazem segurança e sobrevivência para aqueles que devem seguir a regulamentação no mercado financeiro.

O princípio “conheça seu cliente” (equivalente ao Know Your Customer, KYC, do inglês) é regulamentado pela Lei 9.613/98, que dispõe sobre a prevenção de crimes no sistema financeiro, e da Lei 12.683/12, que tornou a anterior mais rigorosa ao ampliar o espectro de reconhecimento de ilicitudes. De modo geral, a legislação tem o objetivo de tornar mais eficiente a persecução penal dos crimes de lavagem de dinheiro e, conforme Ana Cláudia Utumi, sócia-fundadora da Utumi Advogados, está em linha com o que se pratica fora do país.

“Essa lei levou o Brasil ao patamar de economias internacionais em relação ao controle do fluxo financeiro”, afirma Utumi. A advogada explica que o princípio se fortaleceu mundialmente por pressão dos Estados Unidos, após os atentados do 11 de setembro de 2001, e o medo de que dinheiro estivesse sendo desviado para financiamento do terrorismo. “As empresas não podiam mais dizer ‘eu não sabia’ sobre os recursos que transitavam. A legislação exige que as perguntas sejam feitas para que se tenha segurança”, afirma.

Bruno Muzzi, sócio da Urbano Vitalino Advogados e integrante do time de compliance do escritório, aponta os artigos 9°e 10°da lei de 1998 como essenciais para compreender quais empresas e procedimentos, respectivamente, estão envolvidos. “Trata-se de uma política para entender o cliente e a natureza da atividade dele, garantir que a fonte de renda é compatível com a transação, detectar perfis fraudulentos e avaliar perfis suspeitos”, explica.

Embora as grandes empresas já estivessem se dedicando à implementação do “conheça seu cliente” nos últimos anos, Muzzi diz que, com a chegada da pandemia, todos os procedimentos que eram feitos de modo presencial passaram para o online, mesmo que ainda não houvesse o devido preparo. “Havia um plano e ele teve de ser acelerado para sobrevivência da empresa, pois o know your customer não podia ser uma trava. Isso em meio a demissões, especialmente em times de compliance, e com colaboradores em home office aprendendo a lidar com digitalização e automação fora da estrutura de trabalho habitual.”

“Todas as relações tiveram de ser reinventadas durante a pandemia”, diz Filipe Pena, presidente da comissão de compliance e PLD-FT da Associação Nacional das Instituições de Crédito, Financiamento e Investimento (Acrefi). Pena pontua que, durante o último ano, além da agilidade de digitalização e aprimoramento dos processos antifraude, um fato relevante foi a Circular BCB n°3.978, que dispõe sobre os controles internos das instituições para prevenir a prática de crimes financeiros. “Tivemos a necessidade de escalar muito rápido.”

Alguns processos como visitas presenciais aos clientes foram substituídos por controles alternativos, como entrevistas por canais remotos, explica Fernando Malta, diretor de riscos operacionais e compliance do Itaú Unibanco. “Não houve alterações que pudessem comprometer ou fragilizar os controles e o cumprimento regulatório, uma vez que já fazíamos uso intensivo de dados e aplicávamos uma abordagem baseada no risco”, garante.

Malta conta que o “conheça seu cliente” vem sendo continuamente aprimorado pelo banco.

“Seguimos estritamente as normas e mantemos contato próximo com os reguladores para identificar as melhores práticas do mercado e elevar continuamente nossos controles de forma alinhada às expectativas das autoridades. Os bancos têm um papel muito importante na prevenção desses crimes.”

Rodrigo Monteiro, diretor da Associação Brasileira de Criptoeconomia (ABCripto), celebra que o nível de monitoramento só tem aumentado. “Houve um facilitamento pelo uso de aplicativos e o cuidado com o envio de documentos foi redobrado. O Brasil pode ter ‘complexo de vira-lata’, mas, em termos de controle financeiro, somos exemplo para o mundo.”

A diretora de serviços financeiros da Mazars, Janny Castro, comenta que empresas e instituições financeiras investem em segurança cibernética para enfrentar e minimizar os riscos de fraude, mas que as criptomoedas são um desafio pois o “conheça seu cliente” poderia ser driblado. “Para adquirir esse tipo de ativo, não é preciso passar por um intermediário financeiro. Quem entende um pouco mais do assunto compra diretamente, o que torna complexa a identificação do indivíduo que está realizando a operação”, alerta.

“A área é mal compreendida. Apesar de não ter as mesmas regulações de bancos, a gente não só cumpre como exige mais, pois é um mercado novo”, garante Monteiro. Segundo o diretor da ABCripto, a grande maioria dos crimes financeiros envolve dinheiro em papel moeda ou desvios via transações em instituições financeiras. “O debate sobre criptomoedas tira o foco de onde deveria estar.”

Há gente no mercado financeiro que já estava um passo à frente. Carlos Maurício Nascimento, gerente de compliance da CM Capital, diz que a corretora faz o processo de forma eletrônica desde 2017, quando foi iniciado. “O potencial cliente passa por um processo de análise em fontes públicas. Com base no relatório é realizada uma análise considerando porte, perfil de investimento, capacidade financeiras e demais itens relevantes para tomada de decisão em iniciar ou não um relacionamento”, explica Nascimento.

O gerente da CM Capital aponta que uma mudança positiva e significativa para o “conheça seu cliente” veio em 2019, com a Instrução CVM 617, que resultou em alterações dos critérios para abertura de conta, contribuindo para um melhor detalhamento das informações dos clientes. Atualmente, sete funcionários dedicam-se a esse processo de análise de dossiês na corretora. “É essencial, trazendo proteção para o cliente, para a instituição e para a sociedade.”

A plataforma de criptomoedas e ativos digitais Mercado Bitcoin também estava preparada, pois já era uma empresa completamente digital. O diretor de compliance, Bernardo Srur, conta que o onboarding utiliza bases públicas, o sistema de verificação de identidade é por meio de uma selfie e a checagem documental em busca de fraudes é terceirizada. Com 11 colaboradores dedicados à área, logo no início da pandemia a Mercado Bitcoin adotou a postura anywherework. “Tivemos pouquíssimos impactos e problemas.”

O diretor diz que o processo de validação de informações dos clientes costuma demorar poucos segundos, mas, quando necessário, são sempre refeitas. “Começamos a fazer o ‘conheça seu cliente’ em 2013 e fomos a primeira exchange a pedir dados de nossos clientes e fazer verificação, a primeira a ter cadastro aceito pelo Coaf. Segurança institucional, de forma ampla, é um dos nossos valores”, afirma Srur.

É consenso que as mudanças exigidas pela pandemia foram positivas para o “conheça seu cliente”. Bruno Muzzi diz que houve um aumento na periodicidade de atualização dos cadastros e no rigor dos filtros com que se faz a pesquisa, além de uma oportunidade para fornecedores externos para tratar da tecnologia e dos trâmites legais. Ana Cláudia Utumi acrescenta que o avanço tecnológico já vem impactando o controle de lavagem de dinheiro.

Procurado, o Conselho de Controle de Atividades Financeiras (Coaf) indicou o documento “Padrões internacionais de combate à lavagem de dinheiro e ao financiamento do terrorismo e da proliferação”, do Grupo de Ação Financeira (Gafi), disponível online, para empresas e instituições que desejarem se aprofundar no assunto.

Lei dos “crimes cibernéticos” altera competência em caso de estelionato

Guilherme Gueiros e Elaine Nunes

04/06/2021

Consultor Jurídico conjur.com.br

acesse aqui

Em 27 de maio de 2021 foi sancionada a Lei 14.155, que, dentre outras alterações, modificou a competência para a apuração do crime de estelionato (artigo 171 do Código Penal), ao prever o novel §4º para o artigo 70 do Código de Processo Penal.

A redação do novo dispositivo legal institui que “nos crimes previstos no artigo 171, do Código Penal, quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção”.

Isso significa que, a partir da publicação da lei, no dia 28 de maio de 2021, os crimes de estelionato passaram a ter a competência regida pelo local do domicílio da vítima e não mais pelo local em que se consumou o delito de estelionato ou, se tentado, onde foi praticado o último ato de execução, consoante o caput do artigo 70 do Código de Processo Penal (CPP).

Antes da nova lei, havia uma certa divergência jurisprudencial nos tribunais, pois, para se verificar a competência, era preciso analisar justamente a consumação do estelionato. Todavia, a consumação do delito de estelionato varia, a depender da forma como a infração penal é praticada.

No intuito de regular a matéria, o Superior Tribunal de Justiça esclareceu, por meio do informativo 663 de 2020, que, no caso de estelionato mediante depósito de cheque clonado ou adulterado, a competência era do juízo do local no qual a vítima mantinha a conta bancária. Já no caso mais conhecido de que a vítima faz depósito ou transferência bancária na conta do beneficiário da fraude, a competência era do juízo em que estivesse localizada a agência bancária beneficiária.

Toda essa divergência, entretanto, cai por terra com o novo §4º, incluído ao artigo 70 do CPP, ante a clara manifestação do legislador de que a competência será regida pelo local em que a vítima estiver domiciliada.

Vale salientar que, em casos nos quais o fato delitivo tenha ocorrido antes da nova lei, mas cujo processo penal ainda não tenha se iniciado, permanecerá a competência nos moldes fixados pelo STJ.

É que, diante das garantias do juiz natural e da imparcialidade do julgador, os critérios da competência não podem ser alterados após o fato criminoso, sob pena de se criar tribunais de exceção (post factum). Nesse sentido, leciona o professor Aury Lopes Jr.: “o nascimento da garantia do juiz natural dá-se no momento da prática do delito, e não no início do processo. Não se podem manipular os critérios de competência e tampouco definir posteriormente ao fato qual será o juiz da causa[1]”.

Assim, de acordo com o princípio do juiz natural, apenas os casos de estelionato praticados posteriormente à nova lei terão a competência regida pelo local de domicílio da vítima.

De outra banda, avistam-se possíveis efeitos colaterais decorrentes da mudança no critério de fixação de competência do estelionato quando se consideram as empresas ou entidades públicas vítimas de um alto e constante número de fraudes. Citem-se, como exemplo, as fraudes previdenciárias contra o Instituto Nacional do Seguro Social (INSS) e as fraudes para obtenção do Seguro Danos Pessoais por Veículos Automotores Terrestres (DPVAT), que passou a ser gerido pela Caixa Econômica Federal desde 1º de janeiro de 2021.

Isso porque, uma vez que o domicílio da pessoa jurídica é a sede da empresa, o foro competente será o mesmo para todos crimes de estelionato praticados contra a instituição.

No caso da Caixa Econômica Federal, uma vez que a sua sede está localizada em Brasília, este será o foro competente para o processamento de milhares de feitos ligados a fraudes cometidas contra a instituição financeira, cometendo-se à Polícia Federal, ainda, a atribuição para investigar um sem número de infrações penais, sem prejuízo das demais investigações presididas pelo órgão.

A despeito dos problemas decorrentes da concentração de procedimentos investigativos em determinados órgãos da Polícia Judiciária, a fixação da competência pelo domicílio da vítima evita que esta esteja muito distante do local de apuração do crime, como vinha ocorrendo em casos de estelionato consumado mediante a transferência de valores para contas bancárias operacionalizadas pelos chamados bancos digitais. Essas instituições financeiras não possuem agências físicas, mas apenas a própria sede da empresa, para onde era atraída a competência por força do citado entendimento do STJ.

Dessa forma, a mudança legislativa tem o condão de aproximar a vítima da autoridade policial responsável pela investigação, favorecendo a obtenção de provas do delito e garantindo, em última análise, o acesso do jurisdicionado à justiça.

Vazamento de dados e a necessidade de comprovação do efetivo dano extrapatrimonial para que se reconheça o dever de indenizar

Carlos Andrade
01/07/2021

Migalhas
acesse aqui

Carlos Andrade é especialista em Direito do Consumidor e sócio de Urbano Vitalino Advogados

Em evento realizado na Cidade de São Paulo no ano de 2019, Ajay Banga, então CEO da Mastercard, disse o seguinte: "Os dados são o novo petróleo".

Esta frase, que na verdade foi cunhada pelo matemático Clive Humby, ilustra bem a importância que se tem conferido aos "dados pessoais", a partir do qual se criou uma nova indústria, um novo campo de estudo, e, diante dos litígios que possivelmente surgirão em decorrência do tratamento destes dados, um novo leque de temas a serem debatidos nos tribunais.

Neste cenário, começa a se replicar nos tribunais brasileiros ações judiciais relacionadas ao tratamento irregular de dados, nas quais as partes formulam, dentre outros pedidos, indenizações por danos morais, trazendo à tona a seguinte discussão:

"O vazamento de dados pessoais configura hipótese de dano moral in reipsa?"

Pois bem. Na busca por um conceito de dano moral, a renomada professora Maria Helena Diniz1, amparando-se também em Wilson Melo da Silva, preleciona:

"O dano moral vem a ser a lesão de interesses não patrimoniais de pessoa física ou jurídica, provocada pelo fato lesivo".

Em seguida, acrescenta que o dano moral pode consistir na lesão a um interesse jurídico extrapatrimonial relacionado aos "direitos da personalidade (como a vida, a integridade corporal, a liberdade, a honra, o decoro, a intimidade, os sentimentos afetivos, a própria imagem) ou aos atributos da pessoa (como o nome, a capacidade, o estado de família)", além daqueles que decorrem do valor afetivo atribuído a qualquer bem material, caso em que a sua perda pode vir a representar um menoscabo.

O dano moral in reipsa, por sua vez, ocorre quando este dano é presumido, bastando, para gerar o dever de indenizar, a comprovação da ocorrência do ato apontado como ilícito.

Acerca da possibilidade de responsabilização do controlador/operador em decorrência de vazamento de dados, o caput do art. 42 da LGPD dispõe que:

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. (...)

Ademais, por ser matéria já protegida pelo art. 5º, inciso X da Constituição Federal, a responsabilização pelo dano proveniente da utilização irregular de dados pessoais é tema já há tempos tratado pela jurisprudência pátria.

Sobre tal questão, destaque-se importante decisão do Superior Tribunal de Justiça, no julgamento pela terceira turma do REsp: 1758799 MG 2017/0006obi1-9, sob relatoria da ministra NANCY ANDRIGHI, na data de 12/11/2019, que ao decidir sobre o tema registrou que: (...)

A inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor -dentre os quais se inclui o dever de informar -faz nascer para este a pretensão de indenização pelos danos causados e a de fazer cessar, imediatamente, a ofensa aos direitos da personalidade (...)

Por meio desta decisão, entendeu a terceira turma da referida corte superior que o tratamento irregular de dados se mostra como hipótese de dano moral in reipsa: (...)

Do mesmo modo, o fato de alguém publicar em rede social uma informação de caráter pessoal não implica o consentimento, aos usuários que acessam o conteúdo, de utilização de seus dados para qualquer outra finalidade, ainda mais com fins lucrativos. Hipótese em que se configura o dano moral in reipsa. (...)

Ocorre que diferentemente de situações como a de inserção indevida de nome em cadastro de inadimplentes -tema sedimentado na jurisprudência como espécie de dano moral in reipsa-em que, pela mera inclusão no rol de inadimplentes, o negativado sofre abalo de crédito na praça, manchando a sua reputação e inviabilizando a realização de possíveis operações comerciais, a disponibilização irregular de informações pessoais para terceiro, por si só, não se mostra capaz de gerar a presunção de ocorrência de danos extrapatrimoniais.

Não é razoável presumir que este fato, isoladamente, gera para o titular dos dados, sofrimento, angustia, vexame, que, fugindo à normalidade, interfira intensamente no comportamento psicológico da parte autora.

Para ilustrar o que ora se defende, imagine que uma instituição de ensino tem sua base de dados invadida por hackers que obtêm sucesso em coletar os dados dos alunos, sem que se tenha, até então, conhecimento da destinação dada a tais informações.

Considere, ainda, que estes alunos nunca sofreram qualquer dano/consequência em decorrência do referido vazamento de dados.

Porque esta situação deveria gerar, para tais alunos, o direito a uma indenização de ordem extrapatrimonial? A mera expectativa de que algum dia estes dados possam ser usados em desfavor dos alunos é suficiente para justificar o arbitramento de indenização por danos morais em seu favor?

O vazamento de dados, embora possa ser considerado um ato ilícito (um dos requisitos adotados pela legislação brasileira para a responsabilização civil), não pode ser interpretado como causador de um dano moral em si, já que aquele que teve seus dados vazados poderá não ter qualquer prejuízo extrapatrimonial. Se o prejuízo vier a ocorrer, é certo que a partir de então nascerá o direito à respectiva indenização.

Corroborando com este entendimento, isto é, pela necessidade de comprovação de efetivo dano decorrente do vazamento de dados para que haja o dever de indenizar, destaque-se acórdão prolatado pelo Tribunal de Justiça do Estado do Rio Grande do Sul2:

RECURSO INOMINADO. AÇÃO DE INDENIZAÇÃO POR DANOS MATERIAIS E MORAIS. FRAUDE PERPETRADA. VAZAMENTO DE INFORMAÇÕES CADASTRAIS E NEGOCIAIS DO AUTOR. DANOS MORAIS NÃO CONFIGURADOS. AUSÊNCIA DE PREVISÃO LEGAL PARA IMPOR DANOS MORAIS COM CARÁTER MERAMENTE PUNITIVO. SENTENÇA MANTIDA PELOS PRÓPRIOS FUNDAMENTOS. RECURSO IMPROVIDO.

1. Narra o autor que em razão do vazamento de seus dados sigilosos, foi levado a cair em uma fraude.

2. Sentença que julgou parcialmente procedente a ação, a fim de condenar o réu ao pagamento da quantia de R$ 814,02 a título de indenização por danos materiais.

3. Analisando o conjunto probatório, verifica-se que o autor não demonstrou de forma cabal o abalo moral sofrido, a fim de comprovar fato constitutivo de seu direito, ônus que lhe incumbia, nos termos do art. 373, I, do CPC.

4. Com efeito, o autor tinha um acordo com a ré, recuperadora de créditos, sendo que foi contatado por fraudadores, que dispunham dos dados do acordo e, mediante fraude, fizeram-no pagar uma parcela indevida.

5. O presente recurso cinge-se a postular danos morais por conta do manejo de dados fraudulentos.

6. In casu, não se trata de situação excepcional capaz de determinar a incidência de danos morais, porque tal se daria apenas em caráter punitivo.

7. Desta forma, entende-se que não restaram caracterizados os danos morais, já que a parte autora não comprovou que tivesse tido abalo em algum dos atributos da sua personalidade, em função da situação vivenciada, tratando-se de mero aborrecimento, o que não é capaz de gerar dano moral indenizável, salvo em situações excepcionais.

No mesmo sentido decidiu o juízo da 2ª vara cível de Osasco/SP em sentença prolatada em 16/4/2021, no processo 1025226-41.2020.8.26.0405:(...)

Inequívoco que a ré tem a obrigação de proteger os dados pessoais de seus clientes. Porém, por falha na segurança ou falta de aperfeiçoamento e modernização de seu sistema, permitiu que terceiros tivessem acesso a esses dados. A falha na prestação do serviço é, portanto, evidente, não havendo que se falar na excludente do artigo 14, §3º, II, do CDC, por se tratar de fortuito interno. Por outro lado, para o surgimento do dever de indenizar, faz-se necessário aferir se tal vazamento de dados causou efetivamente à parte autora algum dano. Observa-se que a parte autora informa genericamente que sofreu abalos psicológicos pelo vazamento de seus dados, não havendo, todavia, demonstração alguma de que, após a invasão, tais dados foram utilizados de forma indevida, o que poderia lhe acarretar transtornos. Nenhuma fraude foi praticada em seu desfavor. Não demonstrou que eventuais e-mails indesejados e ligações de empresas tenham relação com o vazamento de dados, até porque, muito comum recebê-los sem o referido vazamento.

E ainda:

À parte autora cabia comprovar os fatos constitutivos de seu direito. No entanto, apenas alegou ter sofrido danos morais, sem demonstrá-los, já que não juntou aos autos comprovantes de seu prejuízo. Frise-se que, neste caso, a prova é puramente documental, de fácil acesso da parte autora. Ora, se a parte autora recebeu tantas mensagens em celular, e-mail ou boletos para pagamento como alega, seria muito simples a prova de sua ocorrência. Bastaria apresentar cópia de alguns dos e-mails e dos boletos recebidos, print da tela de seu celular para comprovar o recebimento de mensagens; porém, não trouxe nenhum documento para corroborar suas alegações.

Verifica-se, pois, que o vazamento de dados, de per si, não acarretou consequências gravosas à imagem, personalidade ou dignidade da parte autora, vez que, ao menos com base nos elementos probatórios dos autos, o prejuízo foi apenas potencial. (...)Verifica-se, portanto, que o vazamento de dados tem potencial para causar um efetivo prejuízo passível de reparação extrapatrimonial da mesma forma que uma cobrança indevida tem para gerar para o lesado o direito ao recebimento de uma indenização desta ordem, no entanto, acerca da cobrança indevida, não há presunção absoluta de ocorrência do dano quando a cobrança se consolida. Porque pensar diferente em relação ao vazamento de dados?

Obviamente, é necessário que existam mecanismos destinados a compelir os controladores/operadores a se cercarem das cautelas necessárias ao tratamento dos dados coletados, a fim de evitar vazamentos. Para tanto, a lei 13.719/2018 prevê em seu art. 52 uma série penalidades aplicáveis para esta situação, dentre estas, a aplicação de multa de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício.

Defende-se, portanto, no tratamento regular de dados que por falha no processo venha a ocasionar o vazamento de informações pessoais, havendo pedido de indenização por danos morais proveniente de tal ato, seja analisado o caso concreto, a fim de verificar se este vazamento gerou para o proprietário das informações algum dano efetivo, hipótese em que, sim, este fará jus à indenização correspondente.

De outro modo, estaremos descaracterizando o conceito de indenização, na medida em que, para sua fixação, exige-se a ocorrência de dano, e não a simples possibilidade deste vir a ocorrer, além de se instituir um precedente com enorme potencial para multiplicação de demandas em massa, sobretudo de aventuras jurídicas propostas com o único intuito de obtenção de vantagens indevidas.

LGPD: A Conta vai chegar pra você

Christiano Sobral
03/07/2021

ESTADÃO
acesse aqui

Christiano Sobral, diretor-executivo do escritório Urbano Vitalino Advogados

Curioso ver pessoas comemorando as empresas serem multadas em função da LGPD ou leis internacionais equivalentes. E, antes que pensem diferente, não sou a favor do "deixa como era", e aprecio saber que agora tenho a lei do meu lado que protege meus dados pessoais.

Mas, a questão que me ocorre é diferente. Trata-se do fato de que o público desconhece o quão oneroso é, para as empresas, adequar-se e manter-se adequado às exigências da LGPD.

É pouco provável uma instituição conseguir implementar sem assistência, o que envolve consultoria e softwares de monitoramento para levantamento apenas dos pontos de risco. Segue-se a isso a necessidade de adoção de práticas de SI (Segurança da Informação), que vem acompanhada de aumento do custo com mão de obra, maior volume de pessoas em help desk (assistência técnica interna da empresa para seus colaboradores em função do TI), contratação de DPO (profissional responsável pela guarda dos dados pessoais que transitam pela empresa) e abandono do uso de soluções de Inteligência Artificial que serviam para melhorar os serviços e produtos oferecidos e para reduzir os gastos da empresa.

Outro a isso, as empresas vão precisar se resguardar contratualmente em relação aos parceiros, fornecedores ou membros da cadeia de valor que, necessariamente, precisam usar dados pessoais (como o banco que faz o pagamento da folha, os fornecedores de benefícios dos colaboradores, a contabilidade terceirizada e assim por diante). Isso trará um custo enorme de adequação de contratos, assessoria jurídica e, em vários casos, repasse dos fornecedores dos seus próprios custos de adequação aos contratos.

Especificamente as notícias de pesadas multas contra diferentes instituições fará subir o valor dos seguros de responsabilidade civil, já com a estreia em apartado do seguro específico para incidentes digitais. Isso pelo simples fato de repercutir em uma maior probabilidade de risco de pagar para as seguradoras.

No fim, todo esse acréscimo será repassado aos negócios, fazendo cair produtividade, reduzindo lucros, recolhimento de tributos e geração de emprego na proporção do impacto, ou acabando embutido, em parte, no aumento de custos de produtos e serviços. Terminando, como você já deve imaginar, saindo do seu bolso.

Ainda que uma lei como está seja necessária, é importante que você entenda o impacto envolvido para a dinâmica do mundo e para sua própria situação em particular. Não comemorando as multas, mas lamentando e refletindo para entender até que ponto foram justas, ou tiveram outros interesses envolvidos.

É possível ver potências usarem das suas respectivas leis equivalentes em relação a dados para penalizar a atuação de empresas estrangeiras em seu país, não ficando claro se realmente as multas guardavam proporcionalidade com as inconformidades eventuais. Por isso não dá para pensar que aqui será diferente, ou que ela –a LGPD –não será usada como meio de pressão, ou até de extorsão ilegal das empresas.

Nada impede que um concorrente melhor protegido use da lei para denunciar seu concorrente menos capacitado apenas para prejudicar seu caixa, ou sua imagem frente ao mercado. Afinal, conseguir adequar-se ao rigor da lei será difícil para as grandes, mais difícil para as médias e não está sendo nem cogitado adequadamente nas pequenas empresas.

Recomendo a você, que é executivo ou empresário de qualquer porte, a buscar aproximar-se mais da LGPD e entendê-la melhor. Assegure-se de estar assistido por uma boa banca de advocacia com comprovada especialização no assunto e adeque-se, desde já, no que for possível. Incluindo buscar seguro para eventualidade não prevista.

E aos consumidores, sugiro pensar, a cada notícia de invasão ou vazamento de dados, a quem interessaria essa informação. Não só para entender o uso escuso da lei, mas para ter consciência de que, várias vezes, o que se tem é um espetáculo para fazer as pessoas pensarem que a lei em si foi uma solução eficiente.

Open Insurance é uma nova proposta de valor por seus dados

Christiano Sobral
01/09/2021

segs
acesse aqui

Christiano Sobral, diretor-executivo do escritório Urbano Vitalino Advogados

Para quem acompanha jogos como o de Vôlei, sabe que, a cada sete, a pontuação começa zerada. Hoje, numa troca de plano de saúde, funciona da mesma forma. Seus hábitos de uso não são transferidos para quem vai suceder o serviço numa mudança eventual.

A ideia do Open Insurance é modificar essa característica. Ou seja, transformar seu histórico um fator para moldar a oferta de serviços que vai chegar para você.

Por esse sistema o usuário permitiria que um prestador conhecesse seus dados de utilização histórica em função de buscar uma melhor oferta, uma vez que, no final, o cálculo do valor a ser cobrado por um usuário será sempre influenciado por um cálculo de probabilidade chamado Esperança Matemática. Ferramenta que equivale a multiplicar o valor que se poderia gastar com a manutenção da sua saúde vezes a probabilidade de que você venha a usar.

É por isso, por exemplo, que se cobra mais dos mais idosos. Não sendo tanto pelo custo que se pode ter com eles, mas sim pela grande probabilidade de que eles precisem do serviço. Sendo o inverso com os mais jovens.

Entretanto, hoje, toda essa base é calculada a partir do grupo a que você faz parte. Estar num grupo de risco e não fazer uso do plano de saúde beneficia o conjunto, mas penaliza você. Isso por, em tese, com acesso aos seus dados históricos do plano anterior, ser possível adequar a oferta um pouco mais ao seu real nível de utilização.

A proposta não é de toda ruim, afinal quem não quer obter o mesmo serviço a um custo menor, não é verdade? Mas existe um risco embutido que precisa ser analisado.

Primeiro estamos falando de dados sensíveis segundo a lei atual de proteção de dados pessoais -a LGPD. Isso por ser tratar não só de dados que lhe individualizam, mas também que indicam o quão saudável, ou não, você é. Implicando nas operadoras em ampliar seus riscos para operarem esses dados entre elas.

Segundo por que pode levar a que se segregue as pessoas entre as que serão beneficiadas e as que não deverão ser, podendo justificar até futuras negativas pelas operadoras. Além de, ao extrair do grupo os que são mais rentáveis para os planos e lhes deixar pagar menos, onerar em excesso os demais e prejudicar a possibilidade de que tenham acesso à saúde complementar.

Numa extrapolação, isolar por completo aqueles que menos usam os serviços pode até inviabilizar a manutenção do prestador como um todo, ou tornar proibitivo ter que atender aos demais. Isso por ferir toda a lógica original sobre a qual esse tipo de atividade foi idealizada.

Está claro que, com a facilidade crescente do Big Data, esse deverá se tornar um caminho sem volta, e inovações como o Open Insurance vão surgir. Talvez, se não fosse pela trava legal que o livre compartilhamento de dados pessoais possui hoje, até ocorresse a nossa própria revelia. Não significando que devamos abraçar esses esforços sem cuidado e reflexão.

Hoje você pode se enxergar como uma pessoa forte e saudável, mas não deve se esquecer que somos apenas animais frágeis que evoluíram até aqui. Um simples vírus, que se quer dá para classificar como um ser vivo, pode lhe tirar a saúde, e até a vida, simplesmente por você precisar conviver e respirar.

Num futuro incerto, dependendo do possível benefício que se esteja oferecendo por seus dados, pode ser melhor negar. Mantendo a chance de, numa eventual troca, ver o placar zerado e não ser assombrado por seu uso passado.

Uma auditoria algorítmica do Open Banking sob a ótica do direito digital internacional

Christiano Sobral
04/09/2021

ESTADÃO
acesse aqui

Christiano Sobral é advogado e administrador, diretor executivo o do Urbano Vitalino Advogados, Laws Master em Direito Digital, mestre em Estratégia e especialista em marketing, finanças, economia e negócios

O direito digital ainda está em construção, sendo muito mais desenvolvido em regiões como a União Europeia do que em outras regiões do mundo. E, mesmo lá, ainda tratam mais de princípios do que de normas estabelecidas.

Porém, mesmo esse início de formação de um modelo legislativo o já permitiu surgir softwares que visam identificar a conformidade de uma proposta ao desejado em segurança pela sociedade. Sendo o caso da 'The Black Box Tools For Assessing Algorithmic Systems", que é um programa em modelo Open Sourcing adotado no escritório Urbano Vitalino.

Seus critérios de análise são baseados em três pilares: a autonomia da ferramenta em questão, os benefícios ofertados aos usuários e o nível de adequação aos critérios de justiça e ética. Observando sempre o nível de risco envolvido.

Aplicamos a este software as informações sobre o Open Banking brasileiro, a ser implementado no Brasil em sua segunda fase no fim do ano, para testar suas conformidades com o que é desejado pela sociedade.

A autonomia mede o quão independente a ferramenta irá funcionar, pelos critérios presença de controle humano, transparência, informação e privacidade. O que, no caso do Open Banking pode-se considerar que, uma vez que os dados da vida econômica estarão disponíveis para às instituições envolvidas, como é elevadíssimo o volume de informações, terá que ser usado sistemas de Machine Learning para poderem ser tratados, tornando pouco provável que seja mantido um controle humano eficiente e que venha a ser possível a transparência.

O motivo é simples: a máquina adotará variáveis como idade, local onde mora, padrão de consumo para, por exemplo, definir seu score de crédito. Com isso você, e seu irmão gêmeo que faz tudo igual a você, mas mora com a sogra num bairro diferente do seu, terão oferta de juros por empréstimos diferentes um do outro, ou até um tenha seu crédito simplesmente negado. Mas, se questionado o motivo, será difícil obter uma explicação.

No critério consentimento, o Open Banking passaria fácil, pois essa é a primeira fase do sistema. Mas não na ótica da privacidade de dados.

Quando falamos em um sistema que compartilhariam informações entre bancos, nos vem à imagem de instituições capitalizadas que, em caso de eventualmente falharem, serão capazes de compensar pelos danos causados. Mas quando temos os dados abertos para Fintech, não estamos mais limitados ao universo conhecido, e não estamos falando de instituições já estabelecidas.

Numa pesquisa rápida pelo Google, você verá que existem uma centena de empresas que se denominam assim, cada uma com uma proposta de serviço completamente diferente da outra. Será que realmente o usuário do sistema tem consciência de que vai abrir mão do seu protegido sigilo bancário para um rol de desconhecidos tão grande assim?

Realmente todos vão tratar essas informações tão caras que são protegidas pela constituição da forma como seria esperado? Eu realmente classifico esse ponto como um risco.

A dimensão benefício tenta mapear o que será de fato ofertado para o usuário final, pela ótica da acurácia, segurança, ganhos esperados e eficiência. Ou seja, o que de fato se deveria esperar com o uso da ferramenta.

Aqui, no caso do Open Banking, cabe entender o que significa oferta personalizada de serviços, pois nosso primeiro entendimento é que está relacionado a, pela ótica do crédito, ter acesso a dinheiro mais barato por conta de que sou um bom pagador . Mas o que não está dito é que pode significar ter o acesso a recursos negado pela perspectiva de análises estatísticas de máquinas de que você, breve, terá a possibilidade de tornar-se um mau pagador.

Uma ferramenta de aprendizagem de máquina, com acesso a uma grande base de dados, pode identificar que, pessoas do seu bairro, que estudaram na mesma escola que você, a partir do momento que fazem 21 anos, costumam casar e constituir família, tornando-se mau pagador aos 23 anos. Então, melhor não lhe emprestar dinheiro aos 20 anos para uma compra de um bem que será pago em 36 meses, coino um veículo por exemplo.

O critério de personalização, como tendemos a pensar, não é preso a sua condição presente. Significando que agora poderá lhe beneficiar, mas num futuro próximo mudar completamente, a semelhança do que já ocorre hoje com os planos de saúde à medida que você envelhece.

Em questão da segurança, uma vez que mais instituições terão acesso aos seus dados, muitas sem que você nem às conheça, será menor que na relação que você dispõe atualmente com às instituições bancárias. Não tem como dar acesso a mais entes a suas informações financeiras sem que se eleve o risco de vazamento indevido. É como a lógica de perder um voo, se você nunca perdeu é apenas porque você voa pouco, não por que você tem mais sorte que os demais.

Por fim vem os critérios relativos à justiça, como não

discriminação, possibilidade de contestação, proteção aos vulneráveis, dentre outras. O que, como já sinalizado, tenderá a ser falho no sistema do Open Banking.

Assumindo a ótica da análise de dados e provável uso de Inteligência Artificial no processo de definição de oferta de produtos e serviços, não tardará para o sistema descobrir quando será o melhor momento para oferecer, por exemplo, a um aposentado, aquele empréstimo que ele, na verdade, nem precisaria. Bastando cruzar os gastos do seu cartão de crédito com o dos seus familiares e dependentes para saber que se aproxima o momento no qual ele será solicitado a ajudar um parente, sendo ingênuo imaginar que essa informação não será utilizada para extrair o melhor valor possível desta transição.

O histórico social brasileiro, onde populações das minorias sempre foram menos privilegiadas e, consequentemente, possuem histórico de maiores problemas em suas vidas financeiras, também poderão alimentar os algoritmos com o chamado “preconceito estatístico”. Não querendo dizer que as soluções de IA sejam malignas, mas apenas lembrando que se baseiam em dados passados, e que estes são influenciados por históricos sociais negativos. Tendendo a ocorrer que, vieses assim, uma vez incorporados ao sistema, ainda que de modo involuntário, reforce a situação de desvantagem destes grupos, agravando uma realidade que temos hoje dificuldade em combater.

Quanto a contestabilidade, fica a dúvida sobre como se dará. Qual força de argumento poderá ter, em relação ao uso feito por seus dados financeiros e históricos de consumo por meio dos gastos em cartão e pagamento com PIX, quando houve um, por assim dizer, livre consentimento.

Em referências internacionais, ao se tentar questionar decisões tomadas por algoritmos, a defesa da propriedade intelectual foi o argumento que prevaleceu. Por que seria diferente aqui? Que força o usuário terá para contestar seu baixo score de credito ante à caixa preta da qual ele foi gerado?

Frente a situação semelhante ao imaginário do Velho-Oeste, quando não havia leis limitando as ações das pessoas de forma clara, fica a questão quanto a que limites deveriam ter a proposta do Open Banking ante aos elevados riscos que ele aponta a luz do pouco que se tem de direito digital no mundo. Havendo esperança de que as bases legais venham a surgir com a continuidade do uso da ferramenta e os questionamentos judiciais que forem gerados no futuro, sendo o meio pelo qual o Direito Digital deverá surgir aqui.

Cabe ainda o alerta: mesmo que não seja toda a sociedade brasileira que adote o sistema do Open Banking, seu risco alcançará, no fim, a todos. Afinal, uma vez que os perfis foram construídos pelas máquinas, a oferta de serviços pelo segmento bancário será sempre baseada na aprendizagem obtida pelo acesso a amostra que consentiu.

Adotando ou não, dando ou não seu consentimento, você também deverá ser alcançado por seus efeitos; daí a importância de analisar se impacto potencial como sociedade, tendo ciência de que é uma realidade nova que necessitará novas regulamentações.

A irresistível decisão das máquinas

Christiano Sobral
02/10/2021

Consultor Jurídico
conjur.com.br
acesse aqui

Christiano Sobral é diretor executivo do Urbano Vitalino Advogados, lawmaster em Direito Digital, mestre em Estratégia e especialista em marketing, finanças, economia e negócios, advogado e administrador.

Victor, o algoritmo baseado em inteligência artificial que auxilia no juízo de admissibilidade no Brasil, e Compas (sigla em inglês para Correctional Offender Management Profiling for Alternative Sanctions), que calcula a dosimetria da pena nos Estados Unidos: eles estão assumindo parte da responsabilidade dos que deveriam julgar? Ou são só ferramentas de recomendação?

Essa é uma discussão que, com o tempo, deverá se intensificar, especialmente quando surgirem divergências fortes no entendimento entre quem solicitou e quem foi influenciado pelo que foi decidido. Mas e se a questão for mais profunda e precisarmos refletir quanto à capacidade dos julgadores de irem contra o que foi recomendado por um algoritmo?

Observando o dia a dia das pessoas normais, o que vemos é a contínua perda de capacidade de tomar caminhos distintos dos indicados pelas máquinas, e o exemplo está bem documentado em obras como a de Yuval Harari, ao abordar nosso comportamento frente às recomendações de aplicativos de localização.

No exemplo dele, uma pessoa tem um compromisso importante que não pode perder. Então consulta a ferramenta, que lhe sugere um caminho que não o agrada, levando-o a optar por um outro e, por fim, acabando por fazê-lo perder o compromisso. O que você acha que ocorrerá da próxima vez?

Esse é o caminho pelo qual aquilo que deveria ser um mero sugestor se incorpora ao nosso modo natural de escolher caminhos e, no fim, nos tornando incapazes de fazer diferente. Eu, por exemplo, conheço pelo menos três pessoas que só dirigem se seus aplicativos de navegação estiverem ativados em suas telas.

Isso não ocorre por nenhuma falha de caráter ou algo assim, mas por um viés que a psicologia econômica chama de ancoragem. E já é há muito conhecido das pessoas. Ele é o motivo, por exemplo, de ser importante fazer a primeira proposta em uma negociação.

Aquela primeira informação sobre o destino desejado se torna, quer queira, quer não, um limitador da nossa capacidade de decidir. Ou seja, não conseguiremos mais pensar muito longe da rota indicada. O mesmo ocorrendo nas recomendações de sites, aplicativos de músicas, sistemas de busca e, por que não?, de robôs como o Victor.

Uma vez que somos seres humanos e temos essa dificuldade involuntária na construção das nossas decisões, como podemos garantir o comprometimento dos julgadores frente as recomendações das máquinas?

Não que isso seja necessariamente um problema, dado que existem indicativos de que as máquinas decidem melhor do que humanos. Mas existem diferentes alcances dessas decisões, algumas não envolvem riscos e são objetivas e, por isso, fáceis de contestar (como a admissibilidade de um recurso), mas outras são complexas e possuem consequência graves sobre a comunidade (como a dosimetria da pena).

Hoje, segundo o CNJ, temos mais de 40 projetos que fazem uso de inteligência artificial espalhados por 30 tribunais e cobrindo todas as regiões do país, com relatos de soluções que extinguiram áreas inteiras como as de execução fiscal. Mas até que ponto o risco das consequências do uso de cada uma delas está sendo analisado? E que medidas de limitação ética estão sendo embutidas nessas soluções?

Estamos no início da revolução do uso de inteligência artificial e esses cuidados precisam ser tomados agora, no início do designer de cada um dos projetos. Antecipando-nos às possíveis consequências indesejáveis de vieses incorporados às decisões automáticas dos algoritmos. Acha que ocorrerá da próxima vez?

Direito (Digital) by design

Christiano Sobral
20/10/2021

Migalhas
acesse aqui

Christiano Sobral é Diretor-executivo do escritório Urbano Vitalino Advogados, especializado em marketing, economia e negócios.

Já ouviu falar de Privacidade by Design? É a determinação de, desde a concepção de um projeto, pensar em termos da melhor prática de gestão dos dados, em especial dados pessoais; em função de já nascer adaptado às normas da LGPD (Lei Geral de Proteção de Dados).

Porém, o Direito Digital não para na Proteção de Dados Pessoais, e tem uma elevada gama de outros aspectos que precisam ser respeitados. Ainda nascente, este será o ramo do direito que trará as conquistas da sociedade, presentes por exemplo na Constituição Federal, para dentro do universo digital.

Por isso, desde o nascimento de um projeto, empresa, serviço ou ação em mundo digital, precisa que se mantenha respeito a estes novos aspectos do direito. Em especial com foco nos pilares: autonomia, benefícios e danos e justiça.

A autonomia está vinculada a quão independente e autônoma será a solução. Por exemplo, terá controle humano?

Algoritmos de recomendação de filmes são um exemplo de uma solução onde isso não está presente; mas o risco pode ser considerado baixo. Por outro lado, um que faça sugestões de tratamento médico levam a um maior risco, podendo ser necessário que se tenha a atenção de um profissional envolvida.

Nesta mesma linha está a transparência e explicabilidade, que é a necessidade de que seja possível identificar como determinada decisão foi tomada. Talvez saber como um software recomendou um caminho para chegar ao seu destino não seja muito relevante; por outro lado é provável que você quisesse saber por que um outro rejeitou seu currículo, ainda que você fosse qualificado para a vaga em questão.

O âmbito da autonomia também envolve questões de consentimento e de privacidade, áreas que já estão previstas dentro da legislação atual. A adequação dos dados requeridos ao serviço, e a correta obtenção do consentimento, precisam seguir o que já traz hoje as normas da LGPD.

O aspecto dos benefícios e danos cobrem, por exemplo, os possíveis impactos do uso. Uma câmera que identifica o humor das pessoas e automaticamente adequam a propaganda que aparece em um outdoor eletrônico, podem levar a alguém que já está deprimido ficar ainda mais, ou a uma pessoa fragilizada consumir um produto que, numa condição normal, não o faria; perfazendo uma exploração de fragilidade.

A troca entre possíveis benefícios e riscos também precisam ser avaliados aqui, como no caso do uso de monitoramento dos clientes por meio de aplicativo de smartphone como meio de oferecer benefícios a segurados que, num caso de elevação do risco de problemas cardíacos identificados pelo sistema, podem levar a negativa de cobertura. Ter esse ponto claro, inclusive na comunicação sobre um produto ou serviço, é uma forma de manter-se adequado ao que sugere o direito digital.

Por fim, o desenho deste novo serviço, produto, ou o que quer que seja, deve ser previsto o critério de justiça. Essa parte da correta distribuição dos fardos, passando por critérios de não discriminação, proteção aos vulneráveis, responsabilidade e contestabilidade.

O fardo não pode ser posto totalmente sobre o um dos participantes, precisando ser bem distribuído. A fragilidade da relação de um fornecedor de serviços autônomos em uma plataforma de serviços compartilhados, onde o tomador só remunera o fornecedor quando o trabalho fornecido é considerado por ele como adequado, joga um peso demasiado sobre um dos componentes do funcionamento da proposta; estando clara a necessidade de ser repensado.

A discriminação, muitas vezes decorrentes de falhas na programação, ou problemas no treinamento do algoritmo de inteligência artificial envolvida, são outro ponto a ser combatido. Estes são problemas muito mais presentes do que se pode imaginar, sendo o motivo, por exemplo, do algoritmo de um varejista nunca indicar uma mulher para ser contratada; viés que precisa ser identificado e combatido.

A proteção aos vulneráveis precisa ser pensada de projeto também, para evitar casos como o do uso de sistemas de casa inteligente onde possuem crianças e que, por conta da forma autoritária como os proprietários se relacionam com suas assistentes virtuais, estavam modificando a forma de tratamento com as pessoas. A repetição de ordens como "fulana, ligue a luz", está levando as crianças a associar este como um tratamento habitual.

O alcance da responsabilidade também precisa ser previsto. As consequências indesejadas da atuação de uma aplicação precisam indicar quem responderá no caso em que falhem. Por exemplo, um leitor de glicemia por smartphone, a partir de implante subcutâneo, caso falhe ao indicar uma ação e prejudique o usuário, precisa prever quem terá obrigação de suportar o ônus.

Como último ponto, é necessário prever a contestabilidade. Não sendo aceitável que prevaleça direitos como o da propriedade intelectual frente a necessidade de ter explicado qual motivo, por exemplo, do baixo score de crédito que uma ferramenta lhe deu ou, como no caso do Compas e nos EUA, uma dosimetria da pena maior do que para outros com o mesmo tipo de acusação.

Meios de ter seus resultados previstos precisam vir de projeto, não podendo se atribuir a todo o algoritmo o status de caixa preta. Mesmo resultados de algoritmos de aprendizagem de máquinas podem ter atribuídos cálculos de regressões que tornam viável explicar que variáveis influenciaram o resultado.

Hoje o Direito Digital ainda não existe como um ramo claro do direito, tendo pouco arcabouço legal exclusivo presente. Mas sua lógica é simples: evitar que o mundo digital se forme como território onde as conquistas sociais do mundo físico não sejam respeitadas. Daí a importância de, desde o projeto, da nascente de uma ideia a ser implementada no mundo digital, prever o alcance do direito e não se afastar do que é justo.

Como a deepfake vai influenciar seu voto na véspera das eleições

Christiano Sobral
12/11/2021

GAZETA DO POVO
acesse aqui

Christiano Sobral, advogado e administrador, é Law Master em Direito Digital, mestre em Estratégia e especialista em Marketing, Finanças, Economia e Negócios.

Uma deepfake é uma imagem de vídeo em que pessoas reais são copiadas com uso de algoritmos de uma forma tal que mesmo especialistas têm dificuldade de identificar a falsificação. Você pode encontrar inúmeros exemplos de deepfakes em redes sociais, ou em vídeos da internet, geralmente copiando pessoas famosas, como presidentes icônicos e atores.

Essa perfeição será, nas eleições, o verdadeiro problema. Simplesmente porque as pessoas tenderão a acreditar no que vai chegar a elas, no formato de vídeo, por meio de mensagem instantânea, nas vésperas da eleição. Como votar naquele candidato que você viu dizendo, em uma mensagem gravada às escondidas em um voo, que irá cortar determinado programa do qual você depende? Ou naquele outro que aparece sendo flagrado em um momento de pagamento de propina?

Se há um sentido no qual confiamos, é a visão. E acreditamos fortemente que o que nossos olhos veem é verdadeiro. Por isso os mágicos nos encantam e ilusões de ótica nos fascinam. A dificuldade de duvidar será ainda maior quando se tratar de material que chega até você a partir de um número de mensagem instantânea de alguém em que você acredita e confia, transferindo uma pitada a mais de credibilidade ao vídeo a que você está assistindo.

Apelos como “divulgue, pois a rede x vai tirar do ar”, ou a “plataforma y tem interesse que você não veja”, vão ser frequentes, além de levá-lo a reagir positivamente ao vídeo, fazendo de você também um propagador, parte de um golpe contra o livre arbítrio sem que você perceba que está sendo usado.

Dependendo de quão bem articulada for essa ação, o candidato lesado terá dificuldade de descobrir esse movimento. Quando (e se) ele for capaz de identificá- lo, terá de ir ao Judiciário para que as disparos sejam interrompidos, ou o candidato beneficiado seja responsabilizado; porém, se tudo ocorrer nas vésperas do dia da votação, o estrago já estará feito.

Só a educação pode servir de amparo defensivo contra este tipo de ação, o que implica na necessidade estatal de investir neste sentido.

Achar que precedentes dos tribunais superiores serão suficientes para, par exemplo, derrubar uma chapa no futuro envolve acreditar que o processo de achar a origem, provar que os vídeos são falsos e definir quem os originou e com qual intenção será fácil, quando sabemos claramente que não é.

O correto seria, a partir de agora, realizar campanhas informativas para a população, deixando claras as possibilidades de uso de ferramentas de inteligência artificial para ludibriar o eleitor. De preferência, com apresentação de imagens falsas para que se entenda o alcance da ferramenta e a dificuldade de identificá-la. Hoje, só a educação pode servir de amparo defensivo contra este tipo de ação, o que implica na necessidade estatal de investir neste sentido. E o momento ideal será exatamente o mesmo no qual estiver se desenrolando o período eleitoral.

Combater viéses digitais deve ser parte do compromisso de qualquer governo que defenda eleições justas. Mais ainda: deve ser o empenho de todos os cidadãos.

Direito a inferências razoáveis

Christiano Sobral
20/11/2021

ESTADÃO
acesse aqui

Christiano Sobral é diretor executivo do Urbano Vitalino Advogados, Law Master em Direito Digital , mestre em Estratégia e especialista em marketing , finanças, economia e negócios. Advogado e administrador

Uma das grandes peculiaridades da Inteligência Artificial e sua capacidade de ler dados não estruturados. Ou seja, não precisam acessar matriz pronta, planilhas claras ou informações pré-classificadas para conseguir extrais informações úteis e, a partir daí, realizar inferências e previsões.

A forma como a IA faz isso é que é peculiar e pode estar lhe conferindo uma etiqueta que não lhe seja apropriada, ou até que lhe deprecie. Essas etiquetas são os chamados tags, podendo ter mais de uma presa agora ao seu correspondente no mundo digital.

Por exemplo, um varejo eletrônico europeu teve algumas compradoras de roupas curtas tagueadas como prostitutas; sendo a forma como a IA encontrou de registrar que esse grupo poderia querer adquirir batons de certas tonalidades, perfumes específicos e tipos mais provocativos de roupas íntimas. Já no Brasil, uma empresa que passava por uma mudança de ERP, mesmo com elevado nível de liquidez comprovada em seus balanços e baixíssimo endividamento, perdeu seu crédito em função da identificação de atrasos em boletos; tagueando-a como má pagadora.

Há ainda a história famosa da família americana que passou a receber amostras de fraldas pelo correio após a filha, por ter pesquisado sintomas de gravidez, ser etiquetada com futura mãe. O que, diga-se de passagem, se revelou verdade após alguns meses.

Os tags são a forma como a IA classifica você, um método de estruturação dos dados que chegam a ela. Permitindo agrupar pessoas, empresas em grupos que facilitem seu controle ou monitoramento. De certa forma podemos dizer que é a evolução do preconceito.

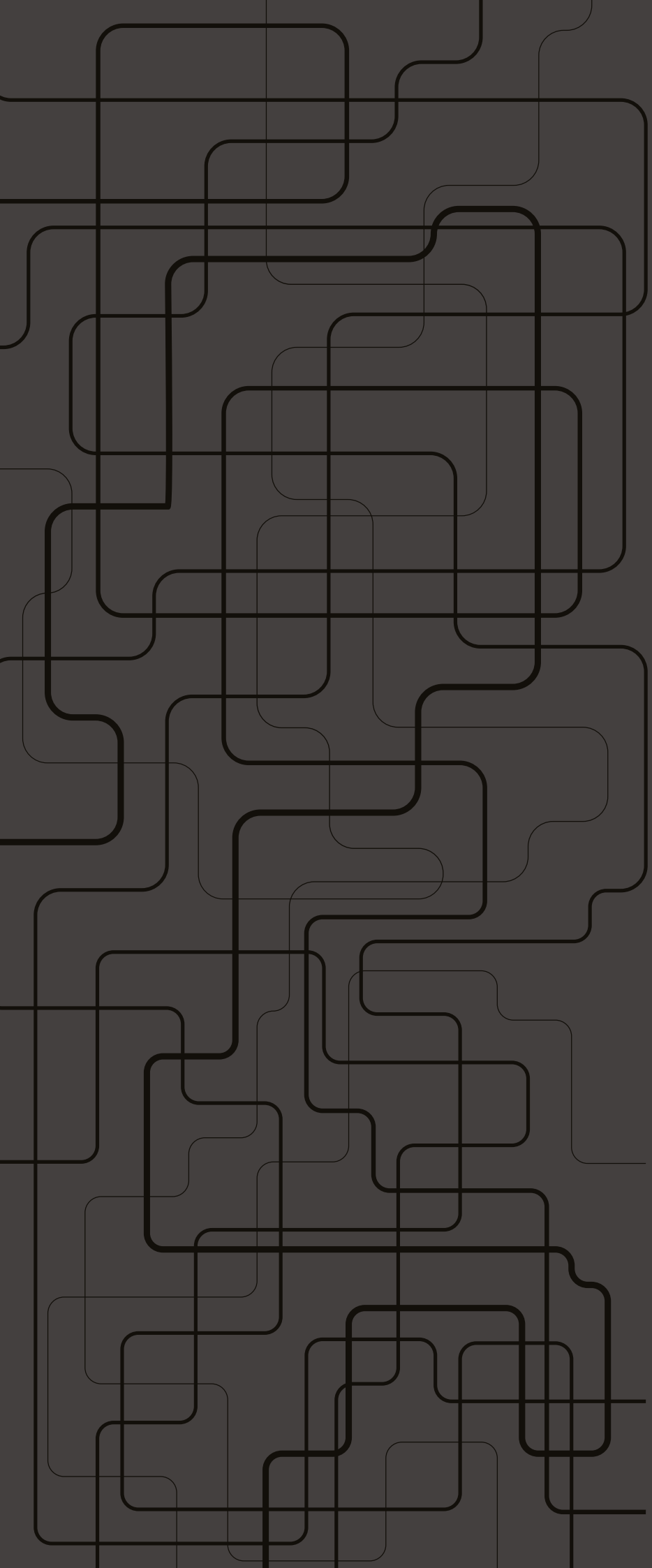
Nós, ao termos um primeiro contato com outra pessoa, não fazemos diferente. Rapidamente buscamos, no nosso inconsciente, um grupo ao qual encaixá-la. A diferença é que, facilmente, mudamos essa classificação e, em gênero, pouco prejudicamos a pessoa por nossa ideia preconcebida dela. Mas no mundo conectado onde habita a IA, não é assim.

Um preconceito eletrônico pode reduzir seu score de crédito, pode lhe retirar a possibilidade de ser selecionado em uma oportunidade de emprego, levar a ter um seguro de vida, ou de saúde, negado e pode até tornar sua vida mais cara que a de outros que, diferentes de você, tem apenas o tag. Mas coma podemos combater isso?

Alguns países já começam a pensar no chamado Direito a uma Inferência Razoável. Uma previsão legal que permita questionar e modificar os tags que lhe foram atribuídos injustamente. Eliminando a etiqueta, por exemplo, de prostituta; ou modificando o score de crédito após provar a capacidade real de pagamento.

Ainda que distante do que inicia a pensar o legislador brasileiro, chegará a hora que ter esse direito também será uma necessidade nacional. Ainda que seja importante frisar que não é tão fácil descobrir e entender o porquê de ter sido classificado de uma forma ou de outra por um algoritmo de Inteligência Artificial.

Com o Machine Learning, não é mais tão fácil saber como determinado algoritmo foi desenhado, consistindo numa verdadeira caixa preta. Porém, ao tornar um direito ter acesso a forma e aos tipos de etiquetas que nos foram designadas, não estaremos olhando para o software como responsável, mas sim para a instituição que dele fez uso. Sendo o provável melhor caminho para obter proteção por meio do nascente Direito Digital.



2022

Responsabilidade civil da inteligência artificial

Christiano Sobral
31/12/2021

ESTADÃO
acesse aqui

Christiano Sobral é advogado e administrador, diretor executivo do Urbano Vitalino Advogados. Law Master em Direito Digital, mestre em Estratégia e especialista em marketing, finanças, economia e negócios

Foi aberta uma consulta pública na União Européia sobre a responsabilidade civil relacionada a utilização de sistema de inteligência artificial. Uma clara preocupação com os riscos de algoritmos violarem, intencionalmente ou não, normas jurídicas estabelecidas.

Quando falamos em responsabilidade civil, especialmente no Brasil, estamos falando, no final, da obrigação de reparar. Ou seja, indenizar, corrigir um fato, modificar algo que foi estabelecido; e isso não precisa decorrer necessariamente de uma ação que teve o objetivo de prejudicar.

Pense no exemplo da perda de uma chance decorrente de um currículo não ser aceito em um processo seletivo. Caso a decisão da sua exclusão tiver sido feita por um algoritmo, e houver indícios de preconceito de máquina envolvido, caberá indenização por parte do serviço, ou da empresa, que utilizou a ferramenta.

Mas não imagine que esse foi um ato que teve o propósito da empresa em realizar, pode apenas ser consequência de o desenvolvedor do serviço não ter sido capaz de evitar que esse posicionamento se formasse. Afinal, com uso de aprendizado de máquina um algoritmo pode adotar um caminho enviesado por observar que a maior parte das pessoas contratadas e que possuem maior tempo de casa nesta empresa terem determinados sobrenomes, ou virem de determinadas instituições ou mesmo são de um único gênero.

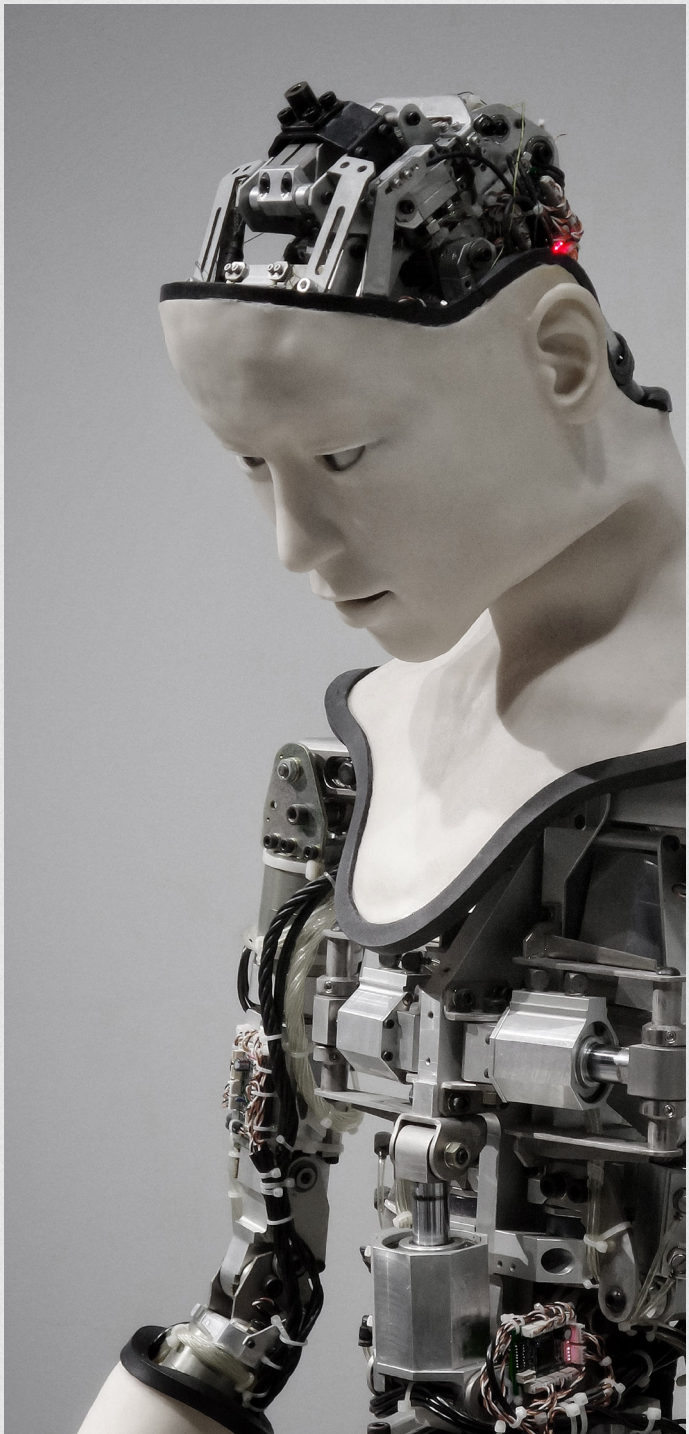
Para o direito, o fato de não haver a intensão não exime da responsabilidade por reparar. Bastando, para tanto, que exista o dano claro e o chamado nexo de causalidade; o que equivale a dizer que tem que haver uma relação direta entre o uso do algoritmo e a consequência indicada.

Hoje, nosso código de direito civil, na forma como está, já permitiria recorrer a responsabilização civil relacionada a consequências do uso de inteligência artificial. O que torna ainda mais urgente para as empresas brasileiras entenderem o alcance das soluções que adquirem, ou desenvolvem.

É provável que surjam momento em que a responsabilização por um dano atribuído a um algoritmo acabe tendo, como indicados, dois responsáveis solidariamente: a empresa que faz uso da ferramenta e a que a desenvolveu. Devendo ficar a cargo do tempo a formação dos precedentes que permitam equalizar o nível de responsabilidade de cada ator.

Em muito o direito digital, no seu alcance ao perfil da responsabilidade civil vai acabar se lastreando em soluções já estabelecidas em leis que lhe são próprias; como a LGPD. Neste dispositivo, por exemplo, a figura de quem é detentor dos dados e de quem é operador dos mesmos dados em favor do primeiro, estão presentes e participam em conjunto na ocorrência de um vazamento de dados pessoais.

Ao pensar, ou optar, por incorporar qualquer solução baseada em IA, tente prever seu alcance, suas externalidades (consequências não previstas); já tentando precaver-se e proteger-se contra qualquer dano futuro que ela venha a causar. Inclusive optando por contratualizar a relação e responsabilidade de quem vai prover o serviço, ou desenvolvê-lo, ou até mesmo treiná-lo.



Banco Central comunica vazamento de dados de 160,1 mil chaves Pix da Acesso Pagamentos

Gabriel Shinohara
21/01/2022

O GLOBO
acesse aqui

O Banco Central (BC) comunicou nesta sexta-feira que houve um vazamento de dados pessoais de 160,1 mil chaves Pix sob responsabilidade da Acesso Soluções de Pagamento. Segundo o BC, houve falhas pontuais no sistemas da empresa.

Em nota, o BC ressaltou que dados sensíveis e protegidos pelo sigilo bancário como senhas, saldos e informações de movimentações não foram expostos. As únicas informações que vazaram são de natureza cadastral, que não permitem movimentação de recursos, de acordo com o BC.

Os dados foram expostos do dia 3 a 5 de dezembro do ano passado. As informações potencialmente vazadas são de nome de usuário, CPF, instituição de relacionamento, número da agência e da conta.

Segundo o BC, no período entre a exposição dos dados e a divulgação do vazamento, a instituição estava apurando "detalhadamente" o caso e acompanhamento as medidas adotadas pela Acesso para resolver as falhas nos sistemas da empresa. Ainda de acordo com o Banco Central, a empresa respeitou todos os prazos de resposta estabelecidos pelo BC.

As chaves Pix são uma identificação da conta para facilitar as transações. Elas podem ser um número de telefone, CPF ou CNPJ, um e-mail ou até uma chave aleatória alfanumérica.

Atualmente existem 365,7 milhões de chaves Pix para pessoa física e 15,5 milhões para empresas.

Medidas da empresa

A Acesso Pagamentos é um instituição de pagamento que oferece serviços como cartões recarregáveis, banco digital e de plataformas financeiras.

Em nota, a empresa informou que tomou ações para garantir a segurança das informações.

"Reforçamos que tomamos, de forma tempestiva, todas as providências necessárias para garantir a segurança das informações mantidas pela Companhia e o nosso compromisso em manter o mercado e nossos parceiros informados", diz a nota.

Segundo o Banco Central, as pessoas que tiveram seus dados vazados serão notificadas apenas pelo aplicativo da Acesso ou por meio do internet banking. A autoridade monetária ressalta que não haverá comunicação por telefone, mensagens, SMS ou e-mail.

Quebra de segurança

Marco Zanini, CEO da DinamoNetworks, empresa de segurança digital, conta que uma das possibilidades para o vazamento ter acontecido seria a de um hacker construir um programa para utilizar a plataforma da Acesso para consultar as informações das contas de pessoas.

Zanini explica que o hacker pode ter utilizado um banco de CPFs, colocado essa informação no aplicativo para fazer um Pix e, em vez de transferir, coletou os dados de agência, conta e nome das pessoas.

Segundo ele, essa possibilidade seria uma quebra de segurança porque esses dados de conta e agência deveriam estar anonimizados e o aplicativo deveria bloquear tantas consultas às chaves Pix sem transferência.

— Pelas boas prática de segurança, depois de três vezes que eu consulto chave Pix e não faço transferência, eu tenho que bloquear aquela sessão e fazer você entrar na aplicação novamente porque pode ser um robô que tá verificando chaves para pegar informação de conta. Se eu não tiver controle, eu deixo o cara ficar consultando dezenas, centenas de chaves e vai capturando as informações de agência, conta e esse tipo de informação — relata o especialista.

Com esses dados em mãos, Zanini dá um exemplo. Um golpista pode ligar para a pessoa cujo o dado foi vazado alegando que representa o banco na qual ele tem conta. Ele informa que houve o vazamento e faz uma série de questionamentos para tentar conseguir outras informações.

— Eu ligo e falo: "Sou do departamento de segurança do banco X e estou fazendo uma verificação. Como houve quebra de segurança no banco tal, vou fazer perguntas por questão de segurança. Qual o nome da sua mãe? Do seu pai? Qual a sua senha?" Muitos não falam e outros falam porque você vai induzindo a pessoa a responder. Ele fala a senha, eu anoto. Agora eu tenho a agência, conta e senha dele, eu já consigo entrar no internet banking dele e fazer uma transferência para mim — exemplificou.

O sócio do escritório Urbano Vitalino, Nagib Barakat, ressalta que as pessoas que tiveram os dados vazados precisam ter atenção redobrada para possíveis golpes.

— Neste momento o que pode acontecer: Com os dados cadastrais, a engenharia social pode ser utilizada por alguém que queira ter acesso às suas senhas, outros dados bancários, páginas falsas na internet podem ser criadas, e-mails com links para baixar software maliciosos também podem ser criados e recebidos. Tem que ter um certo cuidado — recomenda.

O BC também anunciou que adotou as "ações necessárias" para apurar o caso e poderá aplicar as sanções previstas no regulamento do Pix, que podem ser multa, suspensão ou até exclusão do sistema.

Precaução

Cecilia Choeri, especialista em proteção digital e compliance, sócia de Chediak Advogados, sugere que quem tenha tido seus dados expostos troque as chaves Pix e fique atento aos indícios de que as informações estão sendo utilizadas indevidamente, como para abrir contas em outros serviços.

— Por exemplo, se você recebe uma comunicação de operadora de telefonia dizendo “obrigado por abrir uma nova conta” é algo que tem que chamar a atenção. A recomendação é não clicar no link, mas procurar uma fonte confiável para verificar se está tudo certo, como ir até um ponto físico da operadora — explicou.

Thiago Cabral, sócio diretor da empresa Athena Security, disse que é difícil identificar como o vazamento ocorreu, se houve um acesso ao banco de dados por um hacker, se foi um trabalho interno, mas ressaltou que a empresa terá de responder pela ocorrência.

O especialista destaca que é natural que algumas empresas tenham um nível de segurança maior para dados sensíveis do que para informações cadastrais, como as que foram vazadas.

— Não tira a responsabilidade da empresa em também proteger os dados que não necessariamente são sensíveis porque ainda representam riscos. Essas informações mal utilizadas podem ser oportunidade para hackers, criminosos, utilizarem os dados para diversos tipo de golpes — afirmou.

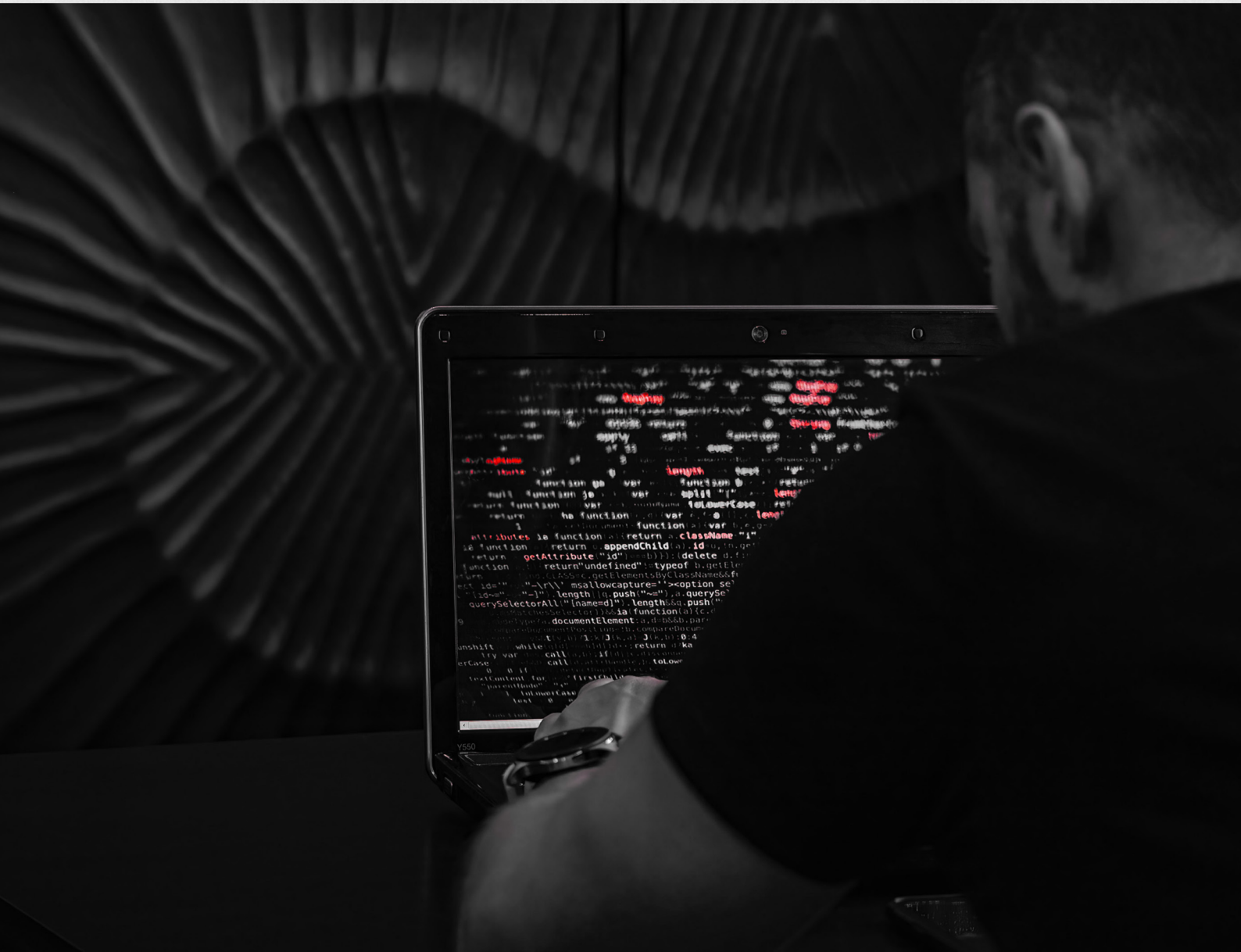
Vazamento no Banese

A ocorrência comunicada nesta sexta-feira é o segundo vazamento de dados de chaves Pix desde o lançamento do sistema, em novembro de 2020. A primeira aconteceu em agosto de 2021 no banco do Sergipe, o Banese.

Naquela ocasião, 395 mil chaves foram vazadas e, como nesta vez, dados sensíveis como senhas e saldos não faziam parte das informações afetadas.

Zanini, da Dinamo Networks, ressalta que o problema é na construção dos aplicativos dos bancos, fintechs e cooperativas. Para evitar novos casos, ele sugere a ideia do BC construir um guia para uma programação mais segura dos aplicativos.

— Acho que o Banco Central podia lançar um guia de melhores práticas de desenvolvimento das aplicações e colocar alguma certificadora que pudesse certificar que os softwares estão bem escritos. Assim como a gente faz isso nos equipamentos de criptografia, os aplicativos de banco poderiam ter isso sim.



URBANO VITALINO
ADVOGADOS

URBANOVITALINO.COM.BR