Retrospectiva TMT | 2018

Azevedo Sette 50 Anos
ADVOGADOS

Somos +50 • We are +50

RECONHECIDO ENTRE OS ESCRITÓRIOS BRASILEIROS QUE MAIS ASSESSORAM OPERAÇÕES DE COMPRA E VENDA DE EMPRESAS.

Rankings de M&A da Bloomberg, Thomson Reuters e Mergermarket

“ELES TÊM AMPLO CONHECIMENTO E ENTENDIMENTO SOBRE O AMBIENTE DE NEGÓCIOS DOS CLIENTES, ALÉM DE MUITOS ANOS DE EXPERIÊNCIA DE MERCADO NO ATENDIMENTO EMPRESARIAL.”

Chambers Latin America

“UM CLIENTE DESCREVE O ESCRITÓRIO COMO MUITO CAPACITADO, COM ADVOGADOS DE PRIMEIRA LINHA COM AMPLO CONHECIMENTO JURÍDICO E SEMPRE DISPONÍVEIS PARA ATENDER AOS CLIENTES.”

Latin Lawyer 250

“O ESCRITÓRIO TEM UM IMPRESSIONANTE PORTFÓLIO DE DE CLIENTES NACIONAIS E MULTINACIONAIS COM NOMES REALMENTE REPRESENTATIVOS.”

The LegaL 500

Escritório Azevedo Sette São Paulo

Prefácio

Com grande *expertise* nos segmentos de TMT e atento à constante evolução tecnológica, à expansão desses mercados e à complexidade das normas regulatórias do setor, Azevedo Sette Advogados conta com uma equipe experiente e especializada no atendimento às crescentes demandas dos clientes nas áreas de Internet, Mídia, Tecnologia e Telecomunicações.

Somos um dos escritórios pioneiros na especialização de demandas jurídicas para o segmento, com um longo *track record* de operações realizadas na prática de Fusões e Aquisições e no atendimento de demandas em todas as práticas do Direito, com *expertise* em questões regulatórias específicas do setor. O escritório conta, ainda, com profissionais advindos do jurídico de companhias multinacionais de tecnologia, o que contribui para o entendimento das necessidades dos clientes de forma empresarial e única.

Com a complexidade das demandas de nossos clientes, atuamos de forma multidisciplinar com as áreas Societária, Tributária, Contratual, Bancária e Contenciosa, atendendo globalmente as questões.

Escritório Azevedo Sette São Paulo

Colaboradores nesta edição

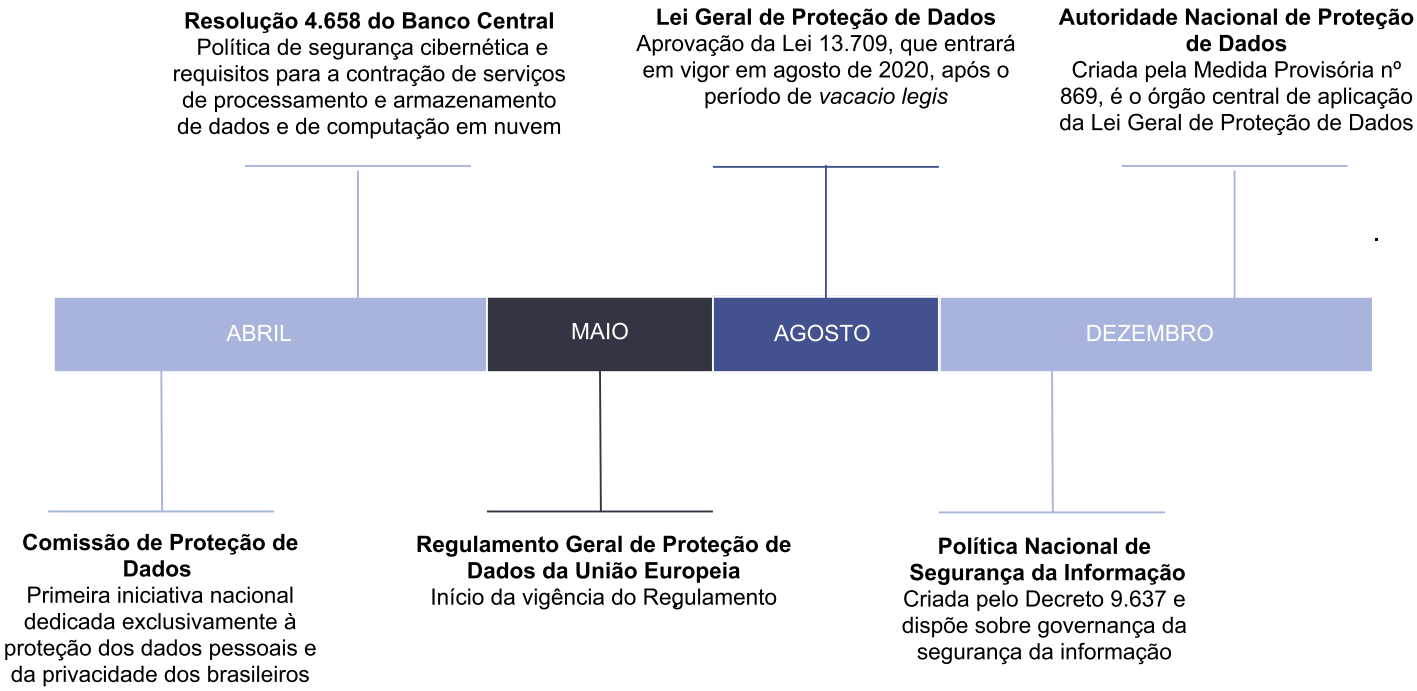
Ricardo Barretto Ferreira da Silva, *sócio coordenador da área de TMT*
Lorena Pretti Serraglio, *advogada*
Vitor Rodolfo Koketu da Cunha, *interno*

2018 e o foco na privacidade e proteção de dados

O ano de 2018 foi marcante para o panorama regulatório de privacidade e proteção de dados, no Brasil e no mundo.

Necessário relembrarmos que o tema ganhou grande relevância com a modernização das tecnologias, advento de aplicativos e mudança do próprio comportamento social. A informação passou a ser o novo elemento estruturante da sociedade.

Nesse contexto, em um movimento de adequação aos fatos sociais, teve início, em maio de 2018, a vigência do Regulamento Geral de Proteção de Dados da União Europeia (General Data Protection Regulation - GDPR). No cenário nacional, deparamo-nos com a Resolução 4.658, do Banco Central; com a aprovação da Lei Geral de Proteção de Dados no Brasil e com a Medida Provisória nº 869, que criou Autoridade Nacional de Proteção de Dados (ANPD):



Órgãos, regulações e legislações nacionais

A **Comissão de Proteção de Dados Pessoais** é uma iniciativa do Ministério Público do Distrito Federal e Territórios. Pautada nas funções constitucionais do próprio Parquet, tem atuado em inúmeros incidentes, calcada em 07 pilares:

- **Pilar Opinativo**, sugerindo diretrizes para uma Política Nacional sobre o tema;
- **Pilar Informativo**, de modo a informar a população, as empresas e os órgãos públicos sobre as normas e as políticas públicas de proteção de dados e privacidade;
- **Pilar de Estudos**, promovendo estudos nacionais e internacionais, mormente diante da ausência de fronteiras no que tange à utilização dos dados;
- **Pilar de Cooperação**, cooperando com as autoridades de proteção de dados, inclusive internacionalmente;
- **Pilar de Notificação**, recebendo comunicações sobre ocorrência de qualquer incidente de segurança que venha causar prejuízo aos titulares dos dados;
- **Pilar Investigativo**, instaurando procedimento preparatório, inquérito civil público e procedimento administrativo, também em conjunto com o promotor natural.
- **Pilar Sancionador**, propondo as competentes ações judiciais, juntamente ao promotor natural da causa.

Ainda no tocante à proteção do consumidor, podemos citar a **Secretaria Nacional do Consumidor (SENACON)**, órgão integrante do Ministério da Justiça, com atribuições previstas no Código de Defesa do Consumidor (CDC), tendo atuado em alguns casos relacionados à privacidade e proteção de dados no ano de 2018.

Além disso, normas específicas foram criadas para setores particulares da economia. O Banco Central do Brasil, por exemplo, publicou a **Resolução nº 4.658/2018**, que trata da política de segurança cibernética e dos requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a serem observados pelas instituições financeiras e demais instituições autorizadas a atuar no ramo.

O objetivo dessas regulações, tal como a do Banco Central, é controlar como organizações, empresas e o próprio governo utilizam a massiva quantidade de dados pessoais produzidas, com o propósito de proteger os usuários/indivíduos de usos não autorizados, inadequados e maliciosos. Sem regras estabelecidas e sem a fiscalização das autoridades competentes, os dados coletados podem ser utilizados de forma indevida, trazendo riscos e eventuais prejuízos para os usuários, consumidores que são.

A **Lei Geral de Proteção de Dados**, sancionada em agosto de 2018, será essencial supedâneo a embasar a atuação das autoridades competentes. Sua vigência, prevista apenas para agosto de 2020, garante um período de *vacatio legis* para as empresas se adequarem à nova regulamentação de proteção de dados. E engana-se quem pensa que o período é longo. O modo de atuação das empresas será diretamente impactado, razão pela qual um olhar mais aprofundado sobre a dinâmica dos dados será essencial, culminando, necessariamente, em um projeto de adequação.

Assim, do ponto de vista legislativo e regulatório, percebemos que o Brasil está atento à virtualização da informação, de modo a adequar sua base legal aos atuais fatos sociais, garantindo que os cidadãos tenham o devido acompanhamento e suporte, quando necessário.

Atuação sistemática do MPDFT

Como visto, o ano de 2018 foi marcado pela atuação frequente do Ministério Público do Distrito Federal e Territórios (MPDFT), que criou Comissão de Proteção dos Dados Pessoais, atual Unidade Especial de Proteção de Dados e Inteligência Artificial – ESPEC, primeira iniciativa nacional dedicada exclusivamente à proteção dos dados pessoais e da privacidade dos brasileiros. A Comissão atuou sistematicamente em diversos casos envolvendo vazamento e uso indevido de dados pessoais.

Um dos primeiros casos cuida-se do vazamento de dados da empresa de e-commerce Netshoes. Naquela oportunidade, 2 milhões de clientes foram afetados, com exposição de dados como nomes, CPF, e-mail, data de nascimento, código de compra e valor do produto. O vazamento tornou público não apenas dados que individualizam o usuário como, também, o perfil de consumo de cada um deles.

Apesar de não existir, atualmente, nenhuma obrigação na legislação que determine a comunicação do vazamento de dados aos usuários afetados e ao público em geral (mormente diante do *vacatio legis* da LGPD), o Ministério Público, pautado em princípios legais e levando em conta a gravidade do incidente e os riscos decorrentes da exposição dos dados pessoais, recomendou, por meio da Comissão de Proteção de Dados Pessoais, que a empresa de e-commerce Netshoes:

- Informe aos clientes afetados pelo incidente de segurança, através de correspondência, com aviso de recebimento (AR), ou por meio de ligação telefônica, quais dados pessoais foram comprometidos (sendo que o descumprimento dessa recomendação implicaria no ajuizamento de Ação Civil Pública por danos morais e materiais causados aos consumidores [1]);

- Abstenha-se de efetuar qualquer tipo de pagamento ao suposto autor do incidente de segurança, sob pena de configuração de crime de fraude processual [2].

A Comissão também averiguou o vazamento de dados da empresa Uber, que afetou 57 milhões de contas de motoristas e clientes da empresa ao redor do mundo, e expôs dados de 156 mil usuários brasileiros, incluindo nome, telefone e e-mail. A Comissão, através de um documento enviado ao Diretor-Geral da Uber no Brasil, questionou a empresa acerca dos dados de motoristas e clientes brasileiros comprometidos. Após a conduta da Comissão, a Uber optou por notificar os clientes envolvidos no incidente, informando-os do ocorrido.

No caso do vazamento de dados do Banco Inter, a Comissão ajuizou uma Ação Civil Pública (ACP) em face da instituição bancária, pedindo a condenação da empresa ao pagamento de indenização por danos morais no valor de R$ 10 milhões, por não ter tomado os cuidados necessários para garantir a segurança dos dados pessoais dos clientes e não clientes da instituição.

De acordo com a ACP, o Banco Inter informou que efetivamente houve um incidente de segurança, onde dados pessoais de clientes e colaboradores foram vazados. A Comissão recebeu do Banco Central do Brasil os dados vazados dos clientes, que incluem Banco, CNPJ/CPF, agência, número da conta e nome completo da pessoa física ou jurídica titular da conta. Aproximadamente 13.000 contas/clientes tiveram os dados bancários comprometidos e estes dados estavam sendo vendidos na Deep Web.

Em 18 de dezembro de 2018 a Justiça homologou um acordo entre o MPDFT e o Banco Inter. O acordo prevê o pagamento de R$ 1 milhão, que será destinado a instituições públicas que combatem crimes cibernéticos, e R$ 500 mil, que serão destinados a instituições de caridade.

Além dos casos descritos acima, a Comissão também está investigando alguns incidentes de segurança e o uso indevido de dados pessoais (quadro disponível na próxima página).

Atuação sistemática do MPDFT

USO INDEVIDO DE DADOS PESSOAIS

Inquérito Civil Público
Investigar as circunstâncias e as causas do provável uso ilegal de dados pessoais de brasileiros

Cambridge Analytica

Inquérito Civil Público
Investigar o tratamento de dados de crianças brasileiras por parte do YouTube

YouTube

Inquérito Civil Público
Investigar o uso da tecnologia de reconhecimento facial de usuários e não usuários do Facebook

facebook

Inquérito Civil Público
Investigar o uso de bancos de dados biométricos para fins comerciais, e os algoritmos de reconhecimento facial

CredDefense
Certibio
Acesso Digital

Inquérito Civil Público
Investigar a legalidade da ferramenta de rastreamento de smartphones no Brasil

inlocomedia

Ação Civil Pública
Comercialização ilícita de banco de dados pessoais de brasileiros pela internet

tudosobretodos

INCIDENTES DE SEGURANÇA

NETSHOES

Inquérito Civil Público
Recomendação para informar 2 milhões de usuários afetados pelo vazamento no Brasil

UBER

Procedimento Preparatório
Acordo para informar 196 mil brasileiros afetados pelo incidente no Brasil

twitter

Requisição de informações
Informações solicitadas tendo em vista os 300 milhões de usuários afetados pelo incidente no mundo

BANCO inter

Ação Civil Pública
Acordo no valor de 1,5 milhão a título de danos morais coletivos pelo vazamento de dados de 13 mil clientes

C&A

Procedimento Preparatório
Acompanhamento das consequências do incidente envolvendo 2 milhões de usuários afetados no Brasil

MyHeritage DNA

Requisição de Informações
Informações solicitadas tendo em vista o vazamento de dados de 3.5 milhões de usuários afetados no Brasil

SKY

Inquérito Civil Público
Investigação do possível incidente de segurança envolvendo dados de 32 milhões de clientes

FIESP

Inquérito Civil Público
Investigação de incidente de segurança envolvendo dados de 34 milhões de brasileiros

g+

Inquérito Civil Público
Investigação do comprometimento de dados pessoais dos usuários brasileiros no incidente de segurança envolvendo 52 milhões de usuários no mundo

Atuação da SENACON e do PROCON/MG

Além dos casos acima descritos, outras entidades relacionadas à proteção do consumidor atuaram em casos envolvendo vazamento e/ou utilização indevida ou desautorizada de dados pessoais.

A Secretaria Nacional do Consumidor (SENACON) multou o site Decolar.com em R$ 7,5 milhões por oferecer preços diferentes para reservas de hotéis, a depender da localização do consumidor (prática conhecida como geo pricing) e por ocultar a disponibilidade de acomodações a consumidores brasileiros, em favor de consumidores estrangeiros (prática conhecida como geo blocking). A SENACON considerou que as práticas são abusivas e discriminatórias, e infringem a legislação consumerista, que define que é vedado ao fornecedor de produtos ou serviços:

- Recusar atendimento às demandas dos consumidores, na exata medida de suas disponibilidades de estoque;
- Recusar a venda de bens ou a prestação de serviços, diretamente a quem se disponha a adquiri-los mediante pronto pagamento;
- Elevar sem justa causa o preço de produtos ou serviços.

Além da multa, foi determinado que a empresa cessasse imediatamente a prática abusiva e discriminatória, sob pena de suspensão da atividade, bem como a retirada do site do ar.

Em outro caso envolvendo o uso indevido de dados pessoais, a rede de farmácias Drogaria Araújo foi multada em R$ 7 milhões pelo Procon-MG, por condicionar descontos ao fornecimento do CPF do consumidor no ato da compra, sem dar informações claras e adequadas sobre a abertura do cadastro.

A condenação ocorreu após investigação dos fatos e recusa da empresa em ajustar sua conduta. Segundo a decisão, essa prática viola o direito do consumidor à informação clara e adequada sobre o serviço ofertado, uma vez que a farmácia não informa adequadamente ao consumidor os termos de uso, políticas de privacidade, e os riscos à segurança de dados do programa.

Dados de consumo de drogaria podem revelar informações sensíveis sobre a saúde e a vida do consumidor e levar a práticas abusivas de empresas. Doenças, distúrbios psíquicos e outras informações sensíveis podem ser deduzidas a partir dos hábitos de compra de medicamentos, e tais informações não são esclarecidas ao consumidor. Dessa maneira, o consumidor, hipossuficiente na relação, não tem as informações necessárias para consentir de forma adequada com a coleta de seus dados pessoais em troca do desconto.

Segundo o promotor de Justiça de Defesa do Consumidor de Belo Horizonte, Fernando Ferreira Abreu, “o escopo principal do suposto programa de fidelidade é o de captar e capturar os CPFs dos consumidores e não desenvolver, em si, um programa de vantagens ou fidelidade”, o que configura prática abusiva, pois a concessão de descontos não pode estar condicionada ao fornecimento de dados pessoais.

De acordo com a decisão, “a captura constante dos hábitos de consumo do consumidor de forma oculta e sem informação prévia representa severo risco à intimidade e vida privada do consumidor, além de sujeitá-lo a riscos das mais variadas espécies”.

Os casos acima comprovam que o período de vacatio legis da LGPD não tem sido óbice para as investigações e responsabilizações das empresas, de modo que as movimentações vistas no ano de 2018 são pequena amostra do que está por vir, principalmente com a vigência dos regulamentos de proteção de dados, a nível nacional e internacional.

O que esperar para 2019?

De acordo com um estudo (1) da consultoria Gartner, os gastos com produtos e serviços ligados à segurança da informação chegarão a $124 bilhões em 2019, um crescimento de 8.7% em relação a 2018. Essa projeção reflete, sem precedentes, os desafios relacionados à segurança cibernética e à proteção de dados enfrentados pelas empresas (de todos os portes, é bom frisar).

As ameaças digitais evoluem em compasso com o progresso tecnológico. Não falamos, aqui, de uma realidade distante, mas, sim, daquilo que nos cerca em nosso dia a dia: tecnologias cada vez mais comuns na sociedade digital como reconhecimento facial, internet das coisas, internet 5G, drones, big data, inteligência artificial, mapeamento genético, carros autônomos, smartphones, relógios inteligentes.

Todas as tecnologias listadas estão mudando os limites e as expectativas de privacidade, trazendo diversos desafios para a sociedade civil, governo, órgãos reguladores, empresas e organizações. E se o ano de 2018 trouxe à tona tantos incidentes, foi para tornar clara a real situação, qual seja, a de atenção e ação quanto à proteção dos nossos dados, estejamos nós na figura de titulares, operadores ou controladores.

A segurança da informação é fator chave para transformação digital da sociedade. E, diante do que foi até aqui estudado, alguns comportamentos podem ser essenciais aos ambientes corporativos para prevenção de problemas futuros, como a observância das regulações, nacionais e internacionais, ligadas à proteção de dados; a análise dos riscos dos negócios digitais, e a proteção de propriedade intelectual no ambiente online. Adotar uma conduta compliant às legislações e regulações é o primeiro passo para diminuição de tantos riscos.

E com relação ao ano que se inicia, o que podemos esperar? Bem, as primeiras semanas de 2019 já reuniram dois grandes acontecimentos. Em 17 de janeiro, um pesquisador de segurança digital descobriu uma base de dados com aproximadamente 773 milhões de e-mails únicos e 21 milhões de senhas únicas (2), em um dos maiores vazamentos de dados da história. Em 21 de janeiro, a CNIL (Autoridade de Proteção de dados da França) impôs à Google uma multa de 50 milhões de euros, por falta de transparência e consentimento válido dos anúncios, além de informação inadequada.

Assim, é nítido que empresas que lidam com dados estão sujeitas a incidentes de segurança. E, aqui, incluem-se todas elas: as gigantes da tecnologia e o pequeno empreendimento do nosso bairro. O custo dos incidentes é alto: identificação do problema, notificação aos usuários, multas regulatórias, perda de reputação e negócios.

Tais considerações nos fazem concluir que a conduta preventiva ainda é a melhor estratégia a ser adotada. Conheça seu negócio, saiba quais dados são coletados e de que forma são tratados. Olhe com atenção às ferramentas que você já possui e, se necessário, procure um especialista.

1 Disponível em inglês
https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019,

2 Disponível em inglês
https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

BELO HORIZONTE (MG)

Rua Paraíba, 1000 | Térreo
30130-141 | Tel.: +55 11 3261.6656

BRASÍLIA (DF)

Setor Hoteleiro Sul, Quadra 6, Conj. A, Bl. C | 20º andar
70316-109 | Tel.: +55 61 3035.1616

GOIÂNIA (GO)

Rua 10, 250 | Conj. 507, Edifício Trade Center, Setor Oeste
74120-020 | Tel.: +55 62 3096.4573

RECIFE (PE)

Av. Gov. Agamenon Magalhães, 4575 | 4º andar
50070-160 | Tel.: +55 81 3019.0020

RIO DE JANEIRO (RJ)

Rua Sete de Setembro, 99 | 17º andar,
20050-005 | Tel.: +55 21 3550.5900

SÃO PAULO (SP)

Av. Pres. Juscelino Kubitschek, 2041 | Torre E | 16º andar
04543-011 | Tel.: +55 11 4083.7600

Azevedo Sette 50 Anos
ADVOGADOS

www.azevedosette.com.br

Somos +50 • We are +50