# Direito Digital: 2022, a LGPD e as garras da ANPD

O ano de 2021 foi marcado pelo hercúleo trabalho realizado pela Autoridade Nacional de Proteção de Dados (ANPD). Ao longo do ano, o regulador apurou casos de vazamento de dados pessoais de grande repercussão envolvendo mais de 220 milhões de pessoas, dados de operadoras de telefonia, de cartão de crédito, do Sistema de Pagamentos Instantâneos (Pix), fechando o mês de dezembro com a investigação do incidente de segurança do Ministério da Saúde e do aplicativo Conecte SUS. Por ocasião do seminário promovido pelo Tribunal de Contas da União (TCU) sobre a LGPD, a ANPD informou que recebeu 116 notificações de incidentes de dados entre janeiro e outubro de 2021. Miriam Wimmer, diretora da Autoridade, apontou que o órgão recebeu 391 reclamações que demandam algum tipo de ação e fiscalização.


O órgão também abriu uma importante frente de diálogo com a sociedade por meio de diversas consultas públicas. Em janeiro, a ANPD iniciou a tomada de subsídios sobre microempresas com o objetivo de receber contribuições da sociedade para posterior regulamentação do tratamento de dados pessoais efetuado por essa categoria de empresas. No mesmo mês, a órgão regulador lançou edital convocando os membros da sociedade a compor o Conselho Nacional de Dados Pessoais e da Privacidade (CNPD), cujos membros — entre os quais o autor destas linhas — foram designados pelo presidente da República em agosto do mesmo ano. Em maio, a Autoridade abriu inscrições para que a sociedade participasse de reuniões técnicas sobre o Relatório de Impacto de Proteção de Dados Pessoais e, no mesmo mês, abriu a consulta pública sobre o seu Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador, em vigor desde outubro de 2021.

Em fevereiro a ANPD divulgou o seu planejamento estratégico para o período de 2021 a 2023 por meio do qual anuncia três dos seus principais objetivos: 1) promover o fortalecimento da cultura de proteção de dados pessoais; 2) estabelecer o ambiente normativo eficaz para a proteção de dados pessoais; e 3) aprimorar as condições para o cumprimento das competências legais. Em março, a ANPD publicou seu regimento interno e um alerta sobre envio de e-mails falsos em seu nome como tentativa de *phishing* . Ainda houve a publicação de importantes documentos de referência, como o guia orientativo sobre agentes de tratamento e encarregado, o "Guia de Como Proteger os Seus Dados Pessoais", em parceria com a Secretaria Nacional do Consumidor, e o "Guia de Segurança da Informação para Agentes de Tratamento de Pequeno Porte".

2021 também foi marcado pela assinatura de diversos acordos estruturantes. Em março a Autoridade e a Secretaria Nacional do Consumidor (Senacon), celebraram acordo de cooperação técnica visando a garantir maior agilidade nas investigações de incidentes de segurança, seguido pelo acordo de cooperação técnica entre ANPD e o Conselho Administrativo de Defesa Econômica (Cade) visando a conjugar esforços para garantir a livre concorrência nas atividades que envolvam o tratamento de dados pessoais. Em julho, o Núcleo de Informação e Coordenação do Ponto BR (NIC.br) e a ANPD assinaram um acordo de cooperação para intercâmbio de informações sobre incidentes de segurança na internet e poucos meses depois a Autoridade fechou o ano com a celebração de acordo de cooperação técnica outro com o Tribunal Superior Eleitoral versando sobre a aplicação da LGPD no âmbito eleitoral.

Finalmente, no âmbito internacional, em outubro a ANPD assinou memorando de entendimento com a Agência Espanhola de Proteção de Dados, tornando-se membro da Rede Ibero-Americana de Proteção de Dados, e em novembro integrou a Global Privacy Enforcement Network (GPEN), rede de reguladores de privacidade e proteção de dados cuja missão é otimizar e ampliar a cooperação na aplicação das leis internacionais sobre o tema.

Diante desse impressionante volume de trabalho realizado, diga-se de passagem, realizado por um reduzido grupo servidores extremamente dedicados e competentes, só nos resta constatar: a ANPD está pronta, e com garras afiadas.

Por outro lado, para a maior parte das empresas e organizações brasileiras o ano de 2021 ainda foi um ano de transição. Salvo algumas exceções, a maior parte dessas empresas e organizações postergou o início do seu processo de adequação à lei por diversos motivos: a pandemia, os prazos para a entrada em vigor das sanções previstas pela LGPD, a ausência do regulamento de sanções da ANPD etc.

Contudo, a quantidade de incidentes de segurança envolvendo dados pessoais que assolou o Brasil em 2021 revela a necessidade gritante de ações concretas de reforço da segurança da informação. Os ataques cibernéticos à empresas brasileiras cresceram 220% no primeiro semestre, de acordo com a pesquisa do grupo MZ [1]. As companhias de energia elétrica e o setor de saúde foram os mais afetados pelas invasões, visto que ambos os nichos possuem dados cobiçados pelos cibercriminosos. O crescente número de ataques está relacionado ao aumento exponencial do trabalho remoto durante a pandemia, visto que diversas pessoas se viram forçadas pela circunstâncias a utilizar seus dispositivos pessoais e redes wi-fi domésticas para acessar dados corporativos, vulnerabilidades bem exploradas pelos *hackers*.

Os incidentes mais recorrentes são os ataques de *phishing*, por meio dos quais os *hackers* enviam uma "isca’" por meio de um link encaminhado para o e-mail que, se acionado, viabiliza a invasão do dispositivo por parte dos criminosos. Outro ataque comum consiste no *ransomware*, uma espécie de *malware* que bloqueia ou codifica os dados da vítima, impedindo o seu acesso. O contágio do sistema pode ocorrer por meio de vulnerabilidades de aplicações, cliques em links maliciosos ou anexos em e-mails de armadilha, de modo que o criminoso contata a vítima após criptografar ou bloquear os seus arquivos e exige o pagamento de um resgate para a liberação do acesso. O Instituto Nacional de Telecomunicações e o Ministério da Saúde foram vítimas desse tipo de ataque nesse ano.

Diversas técnicas e ferramentas de tecnologia da informação devem ser conjugadas para reforçar a segurança da informação, como a instalação de um *firewall*, a manutenção de *backups*, a estruturação de um plano de respostas a incidentes e de continuidade de negócios, o isolamento de redes, o uso de antivírus, o monitoramento de ativos digitais e sobretudo ações de conscientização e treinamento do pessoal de todos os níveis da organização.

Esse contexto hostil, conjugado com o crescente grau de consciência dos titulares dos dados pessoais em relação aos seus direitos criados pela LGPD e com as garras já afiadas da ANPD não deixa escolha às organizações brasileiras. A adequação à LGPD em 2022 não é mais uma escolha: antes era treino, agora é jogo!

**Date Created**
10/01/2022