RETROSPECTIVA 2020

PRINCIPAIS ACONTECIMENTOS EM PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

PEDRO BASTOS LOBO MARTINS
DAVI TEOFILO NUNES OLIVEIRA
MARIANA RIELLI

DataPrivacyBR

DataPrivacyBR RESEARCH

Introdução

O ano de 2020 foi um ano, no mínimo, muito agitado para a proteção de dados pessoais. Marcado pela entrada em vigor da Lei Geral de Proteção de Dados (Lei 13.709/18) após uma série de reviravoltas, e pela criação da Autoridade Nacional de Proteção de Dados, o Brasil finalmente conta com uma estrutura jurídica e institucional para a consolidação e sistematização da área.

Neste relatório iremos destacar, em cinco diferentes tópicos, os principais acontecimentos de 2020 no universo da privacidade e proteção de dados pessoais. Além disso, iremos demonstrar como a atuação do Data Privacy Brasil se manteve conectada com os principais acontecimentos do Brasil e do mundo.

Esperamos que esse material possa ser útil como documentação histórica e que possa se tornar uma prática anual. Boa leitura!

Normas de Proteção de Dados

No que diz respeito a leis de proteção de dados, o ano começou com a entrada em vigor, em 1º de janeiro, do CCPA - California Consumer Privacy Act - legislação do estado da Califórnia que prevê uma série de direitos à privacidade nas relações de consumo.

No Brasil, a Lei Geral de Proteção de Dados (LGPD) tinha sua entrada em vigor prevista para o mês de agosto, após a prorrogação feita pela Medida Provisória 869/2018. Contudo, em razão da pandemia do COVID-19, houve um movimento para adiar ainda mais a vigência da legislação.

O Senado aprovou, em abril, o PL 1179, inaugurando esse movimento. O texto previa o adiamento da LGPD para janeiro de 2021 e gerou grande repercussão na área, com posicionamentos públicos contra a prorrogação por parte do Ministério Público Federal e entidades como a Coalizão Direitos na Rede. Quando chegou à Câmara dos Deputados, o Projeto de Lei foi alterado, mantendo-se o adiamento apenas para as sanções administrativas previstas na lei, para agosto de 2021.

Antes da mudança na Câmara, contudo, a Presidência da República editou a Medida Provisória 959/2020, que adiou a entrada em vigor da LGPD para maio de 2021. Depois disso, a saga da vigência da LGPD sofreu ainda mais reviravoltas na reta final, em agosto. A Câmara dos Deputados, ao apreciar a Medida Provisória 959, decidiu pela entrada em vigor em 31 de dezembro de 2020. Porém, o Senado considerou que essa questão estava prejudicada, pois já teria sido deliberada na tramitação do PL 1179. Assim, o artigo sobre o adiamento foi retirado da versão final do projeto.

Com essa última reviravolta, a LGPD entrou em vigor em 18 de setembro de 2020, no momento da sanção da Lei nº 14.058/2020, originada pela MP 959/2020.

O mês de agosto trouxe também outras emoções para a proteção de dados. No dia 26, a Presidência da República editou o Decreto nº 10.474, criando, enfim, a estrutura da Autoridade Nacional de Proteção de Dados. Dois meses depois, em outubro,, a Presidência indicou os 5 diretores da Autoridade, sendo três deles militares. Após Sabatina no Senado, os cinco nomes foram aprovados: Waldemar Gonçalves Ortunho Junior como diretor-presidente e Arthur Pereira Sabbat; Joacil Basilio Rael; Nairane Farias Rabelo Leitão e Miriam Wimmer.

Sobre esse ponto, a Associação Data Privacy Brasil de Pesquisa produziu um estudo acerca do perfil de autoridades de proteção de dados ao redor do mundo, e constatou que apenas China e Rússia possuem militares na composição desse órgão.

Após o Decreto de estruturação da Autoridade, porém antes da nomeação dos diretores, o Data Privacy Brasil ofereceu o curso Autoridade Nacional de Proteção de Dados: Estruturas e Competência com os professores Fabrício da Mota Alves e Laura Schertel Mendes.

Na reta final do ano, a comissão de juristas formada para elaborar um Anteprojeto de Lei de proteção de dados pessoais na segurança pública e persecução criminal, presidida pelo ministro do STJ Nefi Cordeiro e com relatoria de Laura Schertel Mendes, enviou o texto do anteprojeto para o Presidente da Câmara dos Deputados, Rodrigo Maia (DEM-RJ).

A Associação Data Privacy de Pesquisa elaborou uma Nota Técnica sobre o Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal.

A jornada legislativa na área de proteção de dados pessoais não se restringiu à Lei Geral de Proteção de Dados. Ainda em junho, o Senado aprovou o PL 2630/2020, conhecido como "PL das Fake News", que propõe, dentre outros pontos, a criação de mecanismos de rastreabilidade de metadados. O projeto causou polêmica e dividiu especialistas. A Associação Data Privacy de Pesquisa elaborou uma Nota Técnica sobre o PL 2630/2020, em que são pontuadas críticas aos mecanismos de rastreabilidade. Ainda, o Data Privacy Brasil ofereceu uma aula aberta sobre o PL das Fake News com a participação da Professora Clara Iglesias Keller.

Pandemia

Se existe um acontecimento de 2020 que ficará para sempre marcado é a pandemia causada pela SARS-CoV-2 (COVID19). A escala e intensidade da pandemia alterou de forma significativa a forma como a sociedade se organizou ao longo de todo ano, com efeitos que serão duradouros. Os impactos nas áreas da saúde, educação, economia e trabalho afetaram, por consequência, as discussões sobre privacidade e proteção de dados no Brasil e no mundo.

Os debates envolvendo rastreamento de contato, monitoramento de empregados, adoção de ensino remoto pelas instituições de ensino e crescimento do comércio eletrônico passaram todos, em algum momento, pelo regramento da proteção de dados.

Em março, com as medidas de isolamento social, as Autoridades de Proteção e Dados da Europa começaram a emitir uma série de guias, direcionamentos e diretivas para que o fluxo de dados não fosse interrompido em um momento tão delicado, especialmente para fins de pesquisas e produção de estatística, e, ao mesmo tempo, para que esse fluxo não ameaçasse direitos fundamentais e regras de proteção de dados. Reino Unido, França e Itália são só alguns exemplos de países que contaram com orientações de sua Autoridade Nacional de Proteção de Dados nesse contexto.

Ao longo do ano, a Associação Data Privacy Brasil de Pesquisa lançou 29 Boletins em que, dentre outras informações, monitorou as novidades das Autoridades do mundo inteiro.

Já no cenário brasileiro, o movimento gerado foi justamente no sentido contrário. Com as diversas tentativas de adiar a vigência da LGPD, e o adiamento das sanções, a Autoridade Nacional de Proteção de Dados só foi criada no segundo semestre do ano, e não teve a oportunidade de atuar, de fato.

Um dos principais desafios ao longo do ano foi o uso de tecnologias baseadas em dados para o combate à COVID-19, o que inclui desde monitoramento por geolocalização, formação de mapas de calor, até o desenvolvimento de soluções de rastreamento de contato (*contact tracing*). Um ponto de atenção, que apareceu no Brasil e no mundo, foi o compartilhamento de dados pessoais do setor privado para o setor público para o desenvolvimento de tais iniciativas e como isso impacta a privacidade e a proteção de dados pessoais.

A Associação Data Privacy de Pesquisa, nesse contexto, realizou o projeto "Os Dados e o Vírus" em que diversos produtos foram gerados, incluindo oito informes sobre COVID-19, novas tecnologias e dados pessoais, uma aula aberta "Contact Tracing e a COVID-19", o relatório "Privacidade e Pandemia: recomendações para o uso legítimo de dados no combate à COVID-19" e o livro de ensaios "Os Dados e o Vírus - Pandemia, proteção de dados e democracia".

Proteção de Dados e Cortes Superiores

Como já visto até aqui, 2020 foi um ano agitado no campo da privacidade e proteção de dados. Naturalmente, essas tensões se refletiram nas cortes superiores.

No Brasil, a Ação Direta de Inconstitucionalidade (ADI) 6.387, conhecida também como "Caso IBGE", julgada pelo Supremo Tribunal Federal (STF) em maio de 2020, já é considerada um julgamento histórico para a Corte e para o cenário de proteção de dados no Brasil. Em abril, a Presidência da República editou a Medida Provisória 954/2020, determinando o compartilhamento de dados por empresas de telecomunicações com o IBGE, "para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus".

O Plenário do STF considerou a MP inconstitucional, ressaltando a importância da proteção de dados no contexto de pandemia, e alçando a proteção de dados ao *status* de direito fundamental autônomo. A Associação Data Privacy Brasil de Pesquisa participou do julgamento como *Amicus Curiae*.

Além do caso IBGE, o STF deu início também ao julgamento da Ação de Descumprimento de Preceito Fundamental (ADPF) 403 e na Ação Direta de Inconstitucionalidade (ADI) 5527. As ações tratam dos bloqueios de aplicativo de mensagem, como o Whatsapp, pelo não fornecimento de registros e conteúdo de mensagens trocadas no aplicativo. A utilização de criptografia está no cerne do debate. O julgamento foi suspenso pelo pedido de vista do Min. Alexandre de Moraes.

Até o momento, os Ministros Edson Fachin e Rosa Weber já proferiram seus votos. A ministra Rosa Weber afirmou que "seria um inadmissível contrassenso, e mesmo retrocesso, tornar ilegal ou limitar dessa maneira o uso de criptografia." No mesmo sentido, o Min. Fachin reforçou a importância da criptografia em uma sociedade democrática: "A criptografia é, portanto, um meio de se assegurar a proteção de direitos que, em uma sociedade democrática, são essenciais para a vida pública.". Assim, o entendimento até então é de que não há embasamento legal para o bloqueio de aplicativos pela impossibilidade de fornecer dados protegidos por criptografia.

Não foi só no Brasil que as cortes tiveram decisões históricas e importantes. O Tribunal de Justiça da União Europeia julgou o caso "Max Schrems v. Data Protection

Commissioner", conhecido como Schrems II, um dos principais julgamentos do ano, relacionado à transferência internacional de dados.

O caso inicialmente surgiu de uma reclamação apresentada pelo ativista austríaco de proteção de dados Maximillian Schrems à autoridade supervisora irlandesa, visando proibir a transferência de seus dados pessoais do Facebook Ireland para o Facebook Inc, localizado nos Estados Unidos, com o fundamento de que a lei e as práticas estadunidenses não forneciam proteção adequada contra o acesso a dados pessoais por parte das autoridades públicas.

Esse compartilhamento de dados entre União Europeia e Estados Unidos era facilitado pelo Privacy Shield, acordo entre o governo estadunidense e a Comissão Europeia, realizado em 2016, para a transferência internacional de dados entre o país e o bloco, estabelecendo salvaguardas e medidas a serem adotadas.

O caso foi levado ao Tribunal de Justiça da União Europeia, que em sua análise concluiu que as práticas de vigilância estatal estadunidenses representam uma violação aos direitos fundamentais, especialmente à privacidade, de forma que o Privacy Shield não pode continuar a ser usado para legitimar essa transferência internacional. Desta forma, o Privacy Shield foi efetivamente anulado, e os controladores de dados da UE devem buscar outros mecanismos e instrumentos legais para a transferência internacional para território estadunidense.

Devido ao caso, o EDPB publicou novas orientações relativas à transferência internacional, visando guiar os controladores e operadores e trazendo menos incerteza e mais segurança jurídica. O documento traça um teste de 06 (seis) fases que inclui desde o mapeamento do fluxo global de dados até a reavaliação e atualização das salvaguardas adotadas para tanto.

Em outubro de 2020, pouco após a decisão no caso Schrems II, a Associação Data Privacy Brasil de Pesquisa fez o primeiro webinário da série LGPD em movimento: temas chave de implementação, que tratou do tema das transferências internacionais de dados.

Incidentes, violações e enforcement.

Um dos pontos centrais das discussões sobre privacidade e proteção de dados, sem dúvidas, são os incidentes de segurança e violações à privacidade e proteção de dados. As reportagens na mídia, discussões em grupos especializados, posicionamentos institucionais, etc. demonstram o impacto e repercussão desses casos na rotina das organizações.

Sobre esse tema, 2020 foi agitado e apresentou uma série de novos desafios, ficando marcado como um ano que trouxe uma série de mudanças estruturais nas organizações no Brasil e no mundo e demonstrou a importância das discussões sobre segurança e privacidade, além de também consolidar uma série de interpretações e ações de *enforcement* por autoridades e órgãos de controle.

Em 2020, grandes organizações dos mais diversos setores, públicas e privadas, sofreram ataques e foram vítimas de incidentes no Brasil e no mundo. A lista de formas de ataques e vulnerabilidades é inesgotável, mas esse ano destacamos o aumento expressivo do ataque do tipo ransomware. Segundo pesquisa da Kaspersky, o Brasil é o país mais atingido por ataques de ransomware em toda a América Latina. Dos mais de cinco mil golpes desse tipo que acontecem todos os dias na região, 46,6% são registrados em nosso país, o que também nos coloca entre os territórios mais visados de todo o mundo.

O objetivo deste capítulo é trazer um breve panorama de incidentes e violações no Brasil e no mundo, buscando destacar alguns casos notórios, mas não exaustivos. Além de incidentes de segurança, também selecionamos alguns casos de violações às normas relativas à privacidade e proteção de dados pessoais.

Início do ano

No início do ano, no âmbito internacional, podemos destacar alguns acontecimentos importantes nos Estados Unidos da América (EUA). Em Janeiro a Equifax foi condenada a pagar US $380 milhões em uma ação coletiva derivada de um incidente de segurança. Ainda nos EUA, o Facebook fechou um acordo de US $550 milhões referente a ação coletiva sobre o uso de tecnologia de reconhecimento facial em Illinois.

No Brasil, podemos destacar a ação proposta pelo Intervozes contra a operadora de telefonia Vivo, por conta de uma falha que expôs dados pessoais de clientes no portal Meu Vivo, incluindo nome, endereço completo, data de nascimento, RG, CPF e e-mail.

Também destacamos a Ação judicial contra câmeras de reconhecimento facial no Metrô de SP proposta em conjunto por Defensoria Pública do Estado de São Paulo, Defensoria Pública da União (DPU), Instituto Brasileiro de Defesa do Consumidor (Idec), Intervozes e ARTIGO 19, com apoio do Coletivo de Advocacia em Direitos Humanos (CADHu). A ação discute a implementação de um sistema de câmeras com reconhecimento facial que custaria R$ 58,6 milhões aos cofres públicos e tinha o potencial de atingir cerca de 3,7 milhões de passageiros. Ainda no começo do ano também tivemos a suspensão do site BaseUp, site que vendia dados pessoais por R$ 299, após investigação do MPDFT.

Outro ponto de atenção foi a divulgação de e-mails relacionados à Cambridge Analytica no Brasil. Os e-mails traziam detalhes da vinda da empresa para o Brasil, antes do escândalo que a fechou, após acusações de interferências em várias eleições pelo mundo.

No período também ocorreu a notificação da Senacom ao Grindr e Tinder, por suposta venda de dados pessoais de usuários. No dia 15.01, a Secretaria Nacional do Consumidor (Senacon), do Ministério da Justiça e Segurança Pública, notificou os aplicativos para prestar esclarecimentos sobre o suposto compartilhamento ilegal de dados pessoais dos usuários, identificado pelo Conselho de Consumidores da Noruega no relatório Out of Control.

Houve, ainda, a multa aplicada pelo PROCON-SP à Decolar pela prática de *geopricing*. De acordo com o Procon, a empresa teria cobrado preços diferentes para um mesmo serviço de hospedagem a depender da localização do usuário. A prática foi considerada abusiva, violando o art. 39 do Código de Defesa do Consumidor por discriminação em razão do perfil do consumidor.

Pandemia

Com o início da pandemia, o Congresso Nacional iniciou os debates sobre o PL 1179/2020, que dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do Coronavírus (Covid-19). . O PL já foi tratado no "Capítulo 1: Normas de proteção de dados", mas reforçamos a sua

importância, já que originou a lei que adiou a entrada em vigor das sanções da LGPD e, impactando na resolução dos incidentes e violações.

Devido a pandemia, uma série de novas preocupações surgiram para as organizações. Com a expansão do trabalho remoto, houve um aumento significativo de ataques cibernéticos e das preocupações, em geral, relativas à privacidade e proteção de dados dos usuários das plataformas.

Um dos principais destaques de incidentes e violações no início da pandemia foi o aplicativo de videoconferências Zoom, questionado por uma série de questões de segurança e privacidade. As discussões e questionamentos estavam relacionados a uma série de vulnerabilidade da plataforma , como por exemplo, um erro no kit de desenvolvimento de software que possibilitou exploração de dados, além da principal crítica: uma falsa publicidade de criptografia ponta a ponta.

Foi nesse contexto que a Secretaria Nacional do Consumidor (Senacon), do Ministério da Justiça e Segurança Pública, notificou a empresa de teleconferências no dia 06.04.2020, solicitando que prestasse determinadas informações sobre suas práticas de compartilhamento de dados.

Outro destaque do contexto da pandemia foram as tentativas de fraude ao auxílio emergencial, com a veiculação de iniciativas fraudulentas com o objetivo de confundir a população. Com o início dos programas de auxílio, medidas foram desenvolvidas para conscientizar a população sobre os golpes.

No âmbito internacional, um dos principais incidentes do ano foi o ataque ao Twitter. O ataque,direcionado a contas de pessoas públicas, comprometeu contas no Twitter de personalidades como Bill Gates, Elon Musk, Jeff Bezos e Barack Obama, sendo considerada a maior na história da rede social. O ataque aconteceu após vários funcionários da rede social terem suas credenciais roubadas por meio do golpe “spear phishing”, em que mensagens habituais para verificação de segurança parecem vir de uma fonte confiável.

No Brasil, no início do segundo semestre, o STJ obrigou o Google a fornecer dados de usuários que pesquisaram termos chave ligados à investigação do assassinato da vereadora Marielle Franco. O caso foi paradigmático e levantou uma série de discussões sobre quebra de sigilo e privacidade.

LGPD em vigor

No dia 18 de Setembro, a LGPD entrou em vigor, mas com as sanções adiadas para 2021. A partir desse momento, algumas ações foram propostas com base na legislação, além de haver uma grande cobertura da mídia em casos relacionados à proteção de dados pessoais.

O primeiro caso de Ação Civil Pública proposta com base na LGPD veio do MPDFT, em uma ação contra a Infortexto, por comercializar dados pessoais. Entretanto, após a ação, o site ficou fora do ar e a ação foi suspensa. Pouco depois, tivemos a primeira multa aplicada, em que a Cyrela foi condenada por descumprir a Lei Geral de Proteção de Dados (LGPD), com uma juíza paulista decidindo por uma indenização de R$ 10 mil a um cliente que teve seus dados compartilhados com parceiros sem autorização.

No Brasil, o Procon-SP notificou o Facebook em relação a um possível vazamento de dados de crianças e adolescentes e questionou a adequação da plataforma à LGPD. Nesse período, iniciaram-se também os preparativos para as eleições municipais e o TSE firmou uma série de parcerias com empresas de tecnologia para combater a desinformação nas eleições. Outro destaque no Brasil foi o incidente da Prudential Brasil, que anunciou um acesso indevido em sua base de dados e criou um canal de comunicação com os titulares afetados.

Mais um caso marcante para as discussões sobre privacidade e proteção de dados foi o caso Serasa Experian, em que foi aplicada a LGPD. O caso discutia a legalidade da comercialização de dados pessoais por R$0,98 em serviços do Serasa. Uma decisão de antecipação de tutela em segundo grau decidiu pela suspensão do compartilhamento de dados com base na LGPD.

Com a entrada em vigor da LGPD pode-se perceber uma intensa movimentação dos atores de *enforcement* no cenário nacional, mesmo sem a ANPD instalada. Esse movimento foi objeto de um curso do Data Privacy Brasil, "LGPD nas Cortes", em que o Professor Rafael Zanatta abordou justamente as intersecções da atuação desses atores com as principais teses que podem vir a ser decididas pelo poder judiciário, já no cenário de LGPD em vigor.

Fim do ano e poder público

O final do ano foi delicado no que diz respeito a incidentes no Brasil, principalmente no âmbito do poder público. Apenas em novembro e dezembro, pelo menos cinco grandes ataques ocorreram contra o poder público no Brasil. Destacamos o ataque ao STJ, em que o Tribunal foi alvo de um ransomware, tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento.

Ainda no âmbito do poder público, destacamos o vazamento de dados do Ministério da Saúde, um dos principais incidentes de segurança da história do Brasil. Estima-se que 16 (dezesseis) milhões de brasileiros tiveram seus dados comprometidos. O vazamento ocorreu após um funcionário do Hospital Albert Einstein divulgar uma lista com usuários e senhas que davam acesso aos bancos de dados de pessoas testadas, diagnosticadas e internadas por COVID-19 nos 27 estados da federação.

Em dezembro, outro vazamento do Ministério da Saúde foi noticiado pela mídia, que alega que dados de mais de 200 milhões de brasileiros que compõem a base cadastral do SUS ficaram expostos por seis meses, também devido à publicação indevida de login e senha de um sistema. Nesse contexto, a Comissão Externa de Enfrentamento à Covid-19 da Câmara dos Deputados realizou uma audiência interativa para discutir os desafios da tecnologia da informação e segurança de dados no contexto da pandemia. O evento ocorreu após as denúncias na imprensa sobre o vazamento de dados sigilosos do Ministério da Saúde.

Nesse mesmo período, no âmbito internacional, as discussões sobre antitruste e empresas de tecnologia se intensificam com o fim do ano e o Senado americano intimou Mark Zuckerberg, Sundar Pichai e Jack Dorsey para audiência sobre a seção 230 CD. Além disso, o Departamento de Justiça Americano processou o Google por abuso de poder econômico. Todo esse contexto culmina em um em relatório com mais de 500 páginas do subcomitê da Câmara dos EUA que diz que Big Techs se aproveitam do "poder de monopólio".

Na União Europeia, a Autoridade Alemã multou a multinacional H&M Hennes & Mauritz em €35,3 milhões (o equivalente a cerca de R$ 228,91 milhões de reais) por violação à GPDR. O caso levantou uma série de discussões sobre vigilância de colaboradores, sendo um dos principais julgados sobre o tema no mundo.

Principais Julgados e Proteção de Dados

O objetivo deste capítulo é trazer uma breve sistematização de alguns dos principais casos envolvendo a aplicação da LGPD no Brasil e da GDPR no cenário Europeu.

Brasil:

Caso	Acesso	Tema
Infortexto	https://bityli.com/qvgPC	Venda de dados pessoais;
Cyrela	https://bityli.com/b36lL	Compartilhamento indevido de dados pessoais;
Serasa Experian	https://bityli.com/b36lL	Compartilhamento indevido de dados pessoais;

Europa:

Caso	Acesso	Tema
H&M Autoridade de Hamburgo	https://bityli.com/UNJFt	Vigilância e coleta excessiva de dados de colaboradores;
Carrefour - CNIL	https://bityli.com/0aPzP	Falta de informação e transparência no programa de fidelidade;
Amazon e Google - CNIL	https://bityli.com/uNk1z	Falta de informações relativas à coleta de cookies.

Outros Acontecimentos.

Além dos marcos destacados nos tópicos anteriores, diversos outros acontecimentos movimentaram o ano da privacidade e proteção de dados e a atuação do Data Privacy Brasil. Comentaremos de forma mais breve alguns deles:

Eleições: Em 2020 ocorreram as eleições municipais no Brasil, o primeiro pleito com a Lei Geral de Proteção de Dados em vigor. A resolução 23.610/19 do TSE já havia incorporado algumas das previsões da LGPD, e inclusive faz menção expressa à lei. Nesse cenário, o Data Privacy Brasil realizou o curso "Eleições e Proteção de Dados" para discutir os principais impactos da LGPD nas campanhas políticas de 2020. A Associação Data Privacy Brasil de Pesquisa também lançou, junto ao InternetLab e o Instituto Liberdade Digital, o documento Proteção de dados nas eleições: democracia e privacidade.

Inteligência Artificial: A inteligência artificial continuou a ganhar novos desenvolvimentos em 2020. Em fevereiro, a Comissão Europeia lançou o White Paper on Artificial Intelligence: a European approach to excellence and trust, traçando alguns princípios da abordagem europeia para o futuro do desenvolvimento da tecnologia de IA.

Além disso, no Brasil, a consulta pública para a Estratégia Brasileira de Inteligência Artificial, aberta no fim de 2019 pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), recebeu submissões até março de 2020. Dentre elas, a Associação de Pesquisa Data Privacy Brasil enviou a Contribuição à Consulta Pública da Estratégia Brasileira de Inteligência Artificial.

O Data Privacy Brasil realizou, ainda, o curso Inteligência Artificial: Aspectos Práticos e Teóricos de Governança, que contou com uma Aula Magna aberta ministrada pelo Professor Virgílio Almeida.

Corrida para a adequação: Com a entrada em vigor da LGPD as organizações começaram uma verdadeira corrida para sair do atraso. Nesse período, o Data Privacy Brasil lançou de forma pioneira o "Curso Prático de Adequação à LGPD".

Seminário de Privacidade e Proteção de Dados do CGI.BR: Após 10 edições realizadas, o Seminário de Proteção à Privacidade e aos Dados Pessoais é considerado o mais importante evento sobre o tema no país. Neste ano, em virtude da pandemia COVID-19 e suas repercussões na organização de eventos, a 11ª edição foi realizada pela primeira vez em formato totalmente on-line, de 17 a 20 de novembro. O Data Privacy Brasil participou de um painel em que apresentou uma pesquisa sobre a importância do Seminário para a consolidação de uma cultura de proteção de dados no Brasil.

Lives Data Privacy Brasil: Esse ano, com a pandemia, expandimos nossas lives e produzimos diversos conteúdos que estão disponíveis em nosso canal do youtube.

- Confira em nosso canal do youtube.

Newsletter Data Privacy Brasil: Chegamos a 60 edições da nossa newsletter esse ano. Temos muito orgulho de semanalmente apresentar os principais acontecimentos de privacidade e proteção de dados para a comunidade.

Boletim do Observatório: É com enorme orgulho que neste ano apresentamos o 29º Boletim, com publicações, diretrizes, opiniões, artigos científicos, projetos de lei e decisões judiciais sobre privacidade e proteção de dados pessoais.

Podcast Dadocracia: Nosso podcast, o Dadocracia, chegou a 39 edições e estamos muito felizes com o caminho que o podcast tem tomado. No fim do ano, o podcast foi agraciado pela chamada de produção de podcasts do instituto Goethe.