ASSOCIAÇÃO BRASILEIRA DE PROPRIEDADE INDUSTRIAL

Programa de Educação Continuada curso Privacidade e Proteção de Dados

Aula 7 – 07 de julho de 2020.

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS – RIPD

Professores: PAULO VIDIGAL E LUIZ FERNANDO CHAVES – Daniel Advogados, Privacy Challenge, Privacyquiz e LGPDrive.

Monitora: NATANE SANTOS – graduanda de curso Direito da FND/UFRJ e pesquisadora na área de Proteção de Dados.

Relatório de impacto é um tema que gera inúmeras dúvidas, pois a lei foi bastante sucinta. Leva-se em consideração muito o que há na Europa em relação à atuação das autoridades.

LGPD *art. 5º XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;*

Apenas o controlador precisa elaborar o relatório de impactos? A princípio sim, porque seria uma obrigação primária do controlador, mas na prática há contratos com cláusulas onde se coloca a assistência do operador nessas questões, ou seja, o operador assistir o controlador para realização do relatório de impactos.

Quais impactos e hipóteses que serão abordados ou necessários especificamente no relatório de impacto? Não ficou muito claro, há pessoas que defendem que seria nas ocasiões em que se faz o tratamento com base no legitimo interesse ou quando trata dados sensíveis. O relatório serve para afirmar que houve uma reflexão em cima de algum risco identificado na sua atividade.

Qual é o conteúdo do relatório de impacto?

Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a ***descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.***

A lei aborda o conteúdo mínimo de forma genérica: descrição dos tipos de dados, metodologia e a análise do controlador “grande coração do relatório” medidas de salvaguarda para mitigar riscos. Entender os riscos e tomar as medidas correspondentes para mitigação. Não se prender apenas este conteúdo mínimo, na prática o relatório será maior. Leva-se em consideração o que há de melhor prática na Europa.

Seis menções da expressão relatório de impacto:

1) *Art. 4º§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.*

   A LGPD não se aplica em algumas hipóteses, como operações de tratamento de dados para fins de segurança pública. Nestes casos ainda que a LGPD não se aplique seria prudente em alguns casos a realização do relatório de impacto.

2) *Art. 5º XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;*

3) *Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:*

   § 3º A ***autoridade nacional poderá solicitar ao controlador relatório*** *de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.*

4) *Art. 32. A autoridade nacional* ***poderá solicitar a agentes*** *do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.*

5) *Art. 38. A autoridade nacional* ***poderá determinar ao controlador que elabore relatório*** *de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.*

6) *Art. 55-J. Compete à ANPD: XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei;*
   (Incluído pela Lei nº 13.853, de 2019).

POLÊMICAS:

Não confundir relatório de gestão com relatório de impacto a proteção de dados, pois este é por ou para cada atividade de tratamento.

LIA – teste de legítimo interesse/ importação da doutrina estrangeira (Bruno Bioni e Renato Leitte) – teste para ver se uma atividade está dentro ou não dos aspectos relacionados ao legítimo interesse. Esse teste não está mencionado expressamente na legislação.

LIA é diferente de relatório de impacto.

É importante fazer um relatório de impacto para alguns processos envolvendo ou não legítimo interesse e dentro deste relatório de impacto ter um campo para avaliar a eventual aplicabilidade do legítimo interesse. Trabalhar com o que consta na lei que é o relatório de impacto.

Diante do legítimo interesse precisa fazer LIA e/ou relatório de impacto, documentar de alguma forma?

Há divergências. O legislador no art. 10 afirmou poderá solicitar relatório de impacto e no art. 38 poderá discriminar que se elabore o relatório de impacto. A LGPD não é algo matemático ou binário, não podemos ter uma interpretação simplista da lei. O relatório de impacto visa redução de riscos, atentemos para cada situação na prática.

Opinião do Luiz Fernando: não precisaria fazer relatório de impacto de acordo com a base legal, mas precisa fazer quando o tratamento ensejar um risco elevado para o titular de dados. Às vezes está enquadro no consentimento e ainda assim o risco é elevado porque há dados sensíveis ou se vazar sujeitará a pessoa a discriminações, por exemplo.

Várias atividades simples são amparadas pelo legítimo interesse como, por exemplo, RH. Ao passo há que muitas atividades que também são relevantes, por exemplo, como análise de crédito, e também requer atenção. Não basta focar apenas no legítimo interesse, mas em todas as atividades que envolvem alto risco.

Elaborar preventivamente o relatório de impacto ou esperar que a autoridade solicite?

Arts 10,32 e 38 discussão. A própria descrição/conceito de relatório de impacto no art. 5 aponta para um dever de boa prática, então seria prudente conduzir este relatório do momento zero para demonstrar após se necessário que a análise dos riscos, mitigação e implementação de medidas, sem prejuízo de eventual defesa posteriormente.

A LGPD já é uma legislação muito discutida e o MP pode solicitar informações para instituições. O MPDF e Territórios determinaram que pelo menos duas empresas fizessem relatório de impacto de proteção de dados. Uma empresa apresentou, outra recorreu, por fim as duas apresentaram.

Outro caso importante: O STF julgou uma ADIN de uma MP que determinava o compartilhamento de dados entre operadoras de telefonia móvel e IBGE, dados cadastrais dos

clientes das operadoras para fins de realização de pesquisa e amostral. Reconheceu-se na decisão o direito a proteção de dados como autônomo no Brasil. A Corte não possuía este entendimento, atualizou sua jurisprudência. O ministro Fux afirmou que não fazia sentido fazer um relatório de impacto de mitigar riscos depois que a atividade já foi performada, pois não teria sido preventivo, apenas remediaria o risco. O STF deu a entender então que este relatório só faz sentido de existir de for feito antes, no momento inicial para preservar a privacidade e os dados pessoais. Fazer posteriormente seria contraproducente.

O relatório prestação de contas, mostrar que diligentemente se mediu riscos, tomou providências, medidas práticas para mitigar riscos. Atentar para as questões de compliance, a lei tem uma lógica de cuidado, diligência e equilíbrio. Cada instituição precisará encontrar a sua própria régua de risco.

Como funciona no GPDR?

Deve ser feito quando a atividade potencialmente resultar num alto risco para os titulares envolvidos.

Verificar o art. 35 do GPDR

Pelo menos três hipóteses obrigatórias:

- Profile: Quando causa efeitos significativos aos titulares;
- Tratamento em larga escala de dados sensíveis;
- Monitoramento de áreas publicamente acessíveis. (vigilância)

Estudar a atuação das autoridades na Europa – ver os slides e sites.

Perguntas para turma: Há necessidade ou não do relatório de impacto?

A) Uma instituição cria um banco de dados de classificação de crédito ou fraude em nível nacional, esta atividade reclamaria um relatório de impacto? Como aconselhar esta empresa?

Sim. Faz sentido ter o relatório de impacto porque tem impacto em dados sensíveis, alto risco, a questão da não discriminação do dado, portabilidade entre bancos, extensão dos dados nível nacional, dentre outros aspectos.

B) Um site de comércio eletrônico exibindo anúncios de peças de carros antigos envolvendo perfis limitados a partir de visualizações ou compras a itens feitas em seu próprio site.

Considerando apenas ao enunciado NÃO precisa produzir relatório, pois não há um impacto significativo na privacidade do titular. Apenas uma criação de perfil para oferecimento de serviços, mas o cliente pode cancelar a inscrição a qualquer tempo. Atenção: No caso concreto verificar como são criados os perfis e se seriam eventualmente compartilhados dados.

OBS: Cuidado com vazamentos de dados e o modelo de negócio, às vezes o problema não é o dado em si mas o contexto do tratamento. Exemplo do site de encontros amorosos, vazou

apenas nome e e-mail das pessoas não vazou senha, a priori não seria um vazamento de alto risco, mas dependendo de onde vazou a informação contextual pode gerar sérios riscos.

C) Uma revista online usando lista de e-mails para enviar resumo diário genérico para seus assinantes.

Não precisa de relatório. Atividade rotineira sem altos riscos.

D) Uma empresa monitorando sistematicamente atividades de seus funcionários, incluindo o monitoramento de estação de trabalho, navegação na Internet etc.

Precisa de relatório. Na Europa eles são bem conservadores quanto a essa questão por causa do respeito à privacidade.

LISTA DO WORKING PARTY 29: Na combinação de dois desses critérios há necessidade de relatório de impacto.

1. Avaliação ou Scoring

2. Dados sensíveis ou registros criminais

Nossa lei não aborda os registros criminais. Será que as delegacias teriam que elaborar um relatório de impacto se a LGPD fosse aplicada aos registros criminais? Lembrar da não aplicabilidade em assuntos de segurança publica, haverá um lei específica com consulta pública em sua elaboração. Se a LGPD fosse aplicada as delegacias, seria importante este relatório de impacto, mas os registros criminais também são utilizados por empresas privadas que fazem o Background check, por exemplo, para análise de sócios e funcionários/contratação. São informações delicadas que demandaria o relatório tendo em vista a mitigação de riscos. Coletar menos dados, por exemplo, não se precisa saber necessariamente o prédio e o número do apartamento para calcular o frete de uma pessoa.

Background check tema controverso nas empresas, ter um equilíbrio em relação ao que o TST estabeleceu.

3. Dados de crianças ou vulneráveis. Cautela: o que serão os vulneráveis? Talvez se houver apenas dois vulneráveis não precisaria do relatório.

4. Combinação de bases de dados (e fontes de dados) - Obtidos de maneira lícita, questão da transparência principalmente se foi coletado de maneira indireta.

5. Uso de novas tecnologias ou soluções inovadoras - usar um nova tecnologia para uma nova finalidade, provavelmente há impactos desconhecidos desta nova tecnologia, por isso atenciosamente fazer um relatório de impacto. Caso: App Secret para pessoas deprimidas desabafar e receber mensagens positivas, aqui no Brasil o uso teve efeito contrário, utilizado por algumas pessoas como meio de ofensa. Houve ações judiciais

pedindo o banimento. O problema não era o app, mas o comportamento de terceiros. Um modelo de negócio inicialmente pode não enxergar todos os riscos.

6. Tratamento em larga escala – porque a extensão do tratamento impacta diversas pessoas em distintas localidades e /ou com um volume expressivo.

7. Monitoramento sistemático

8. Tratamento automatizado com efeitos significativos – direito à revisão de decisões automatizadas.

9. Tratamento que impeça ou limite exercício de direitos ou ingresso a contratos – medir se as decisões são justas, bem como se estão em harmonia com as bases e as premissas do tratamento para mitigar qualquer tipo de risco.

Retirada da revisão humana do texto da LGPD

Opinião do Luís Fernando – a princípio era a favor da revisão humana, mas depois de conversar com pessoas da área de inteligência artificial, chegou à conclusão que os humanos não podem se desvincular 100% dos seus vieses e isso afetaria até tecnologia, por outro lado está se investido em algoritmos mais livres de vieses. Há testes que mostram que certas decisões tomadas por algoritmos seriam menos discriminatórias que decisões tomadas por humanos. Colocar um humano para revisar, pode dar a entender que os desenvolvedores da tecnologia não precisariam fazer algoritmos livres de vieses porque na ponta haveria um humano para corrigir eventuais falhas da tecnologia. A revisão humana na ponta mostraria que não houve privacy by design efetivo. O GDPR talvez seja mais conservador neste aspecto, possivelmente não dialogaram o suficiente com desenvolvedores de tecnologias. Ver o site LGPDdrive e alguns estudos na área.

Paulo Vidigal – GPDR conservador, afirma que o titular não precisaria se sujeitar a uma decisão pautada apenas em decisão automatizada.

EXERCÍCIO

Uma empresa produziu um urso de pelúcia com câmera, microfone,funções liga e desliga, conectação com wifi, comunicação com o app vinculado ao smartphone e ao tablete, reconhecimento de voz, chip, possibilidade da criança se comunicar com os pais e amigos, postar fotos e áudios, vigilância-babá. Experiência interativa com a criança que ganha o presente de Natal. A criança faz uma conta, o urso começa a captar os dados, uma plataforma recebe e processa os dados da aplicação, devolve através da fala do urso por meio de uma pergunta por exemplo, análise da interação(ex. a criança não reagiu bem), entende o que ela quer ou gosta, etc.

Relatório de impacto – mitigar riscos.

Será que preciso deste cardápio todo de informações?

Verificar dados cadastrais, segurança, evitar vazamento de dados, cuidado com os dados sensíveis, consentimento dos pais, informações claras dos dados da criança, linguagem acessível para criança, atentar aos arts. 6 e 14, conta da criança vinculada a conta do adulto.

Minimização dos dados – eliminar o sobrenome, não precisa da data de nascimento, trabalhar com a faixa etária, etc.

Mapear os impactos indevidos, mitigar riscos possíveis (jurídicos, técnicos) – acesso indevido, subtrair os dados do servidor por falha da empresa que administra, sequestro de conta, recuperar dispositivos descartado indevidamente, discriminação, ameaças, vazamentos e fraudes.

Como mitigar essas possíveis ameaças: medidas técnicas, criptografia, controle de acesso, recursos de segurança de informação da empresa, testes periódicos do brinquedo e da plataforma, atender o melhor interesse da criança e não o da empresa ou dos pais apenas, documentos de política de proteção de dados, boas práticas, duplo valor vinculado a uma conta email, senha digital, exigir um padrão mínimo de segurança de quem está usando o app, autenticações frequentes, etc.

Pensar fora da caixa, não basta à empresa verificar apenas na segurança o usuário. Refletir em todos os cenários possíveis riscos físicos, digitais, o que vem do cliente e de fora do cliente. Qual conteúdo os funcionários da empresa tem acesso?

Outras mitigadoras: controle de acesso, plano de respostas em casos de incidentes, desativação temporária do brinquedo, uma trava para a criança não manipular sem a supervisão dos pais, controle do acesso do banco de dados pelos funcionários, minimização dos dados e tempo de retenção deles, ter uma regra clara de quando serão apagados, conscientização e supervisão dos empregados, notificação em casos de acidentes, etc.

A avaliação de riscos é algo subjetivo, varia conforme as ameaças, atentar ao contexto como um todo. A Agência de Segurança Europeia tem um material interessante que analisa o impacto de um vazamento de dados, um dos fatores levados em consideração é a possível intenção do agente que praticou a ação. A diferença em um técnico de informática apontando apenas a vulnerabilidade de um modelo de negócio, mas não fará nada com os dados em contraste com outra pessoa que invade um banco frauda, furta ou pede resgate para devolver os dados. Não basta apenas atentar para leis, mas é importante fazer uma análise contextual.

Alguns links: Brinquedo interativo: https://www.youtube.com/watch?v=AHhZGJc4CxI

Projeto LGPDrive: https://www.lgpdrive.com.br/cap-iii-arts-17-22#h.jjkk11p6j3fy

European Data Protection Board: https://edpb.europa.eu/about-edpb/about-edpb_pt

https://indicca.com.br/lgpd-compliance-protecao-de-dados/