UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE INFORMÁTICA
ESPECIALIZAÇÃO EM CIÊNCIA DE DADOS E SUAS APLICAÇÕES

LAÉRCIO SANTO DE ARAUJO

O IMPACTO DA LEI GERAL DE PROTEÇÃO DE DADOS NA CIÊNCIA DE DADOS APLICADA A AREA DE SAUDADE

CURITIBA
2021

LAÉRCIO SANTO DE ARAUJO

O IMPACTO DA LEI GERAL DE PROTEÇÃOD DE DADOS APLICADA A CIENCIA DE DADOS NA AREA DE SAÚDE

Proposta de Trabalho de Conclusão de Curso apresentado a Especialização em Ciência de Dados e suas Aplicações da Universidade Tecnológica Federal do Paraná, como requisito parcial para a obtenção do título de Bacharel.

Orientador: Prof. Dr. Leandro Batista de Almeida.

CURITIBA

2021

Ministério da Educação
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
UTFPR - CAMPUS CURITIBA
DIRETORIA-GERAL - CAMPUS CURITIBA
DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO - CAMPUS CURITIBA
DEPARTAMENTO DE APOIO DAS ESPECIALIZAÇÕES LATO-SENSU DOS CURSOS DE INFORMÁTICA - CAMPUS CURITIBA
CURSO DE ESPECIALIZAÇÃO EM CIÊNCIA DE DADOS E SUAS APLICAÇÕES

TERMO DE APROVAÇÃO

O IMPACTO DA LEI GERAL DE PROTEÇÃO DE DADOS NA CIÊNCIA DE DADOS APLICADA A AREA DE SAUDE.

por

Laércio Santo de Araujo

Este Trabalho de Conclusão de Curso foi apresentado às 21h30min do dia 28 de julho de 2021 por videoconferência como requisito parcial à obtenção do grau de Especialista em Ciência de Dados e suas Aplicações na Universidade Tecnológica Federal do Paraná - UTFPR - Campus Curitiba. O aluno foi arguida pela Banca de Avaliação abaixo assinados. Após deliberação, a Banca de Avaliação considerou o trabalho aprovado.

_____

Prof. Dr. Leandro Batista de Almeida(Presidente/Orientador – DAINF-CT/ UTFPR-CT)

_____

Profa. Dra. Rita Cristina Galarraga Berardi (Avaliadora 1 – DAINF-CT/ UTFPR-CT)

_____

Prof. Msc. Christian Carlos de Souza Mendes (Avaliador 2 – DAELN-CT/ UTFPR-CT)

O Termo de Aprovação assinado encontra-se no sistema SEI- Processo nº 23064.031964/2021-93

Dedico este trabalho à minha família, e em especial a minha esposa que é minha grande incentivadora.

AGRADECIMENTOS

Agradeço aos meus professores, que cada um a seu modo, me apresentou uma nova perspectiva, não apenas quanto as matérias em si, mas também na forma de abordar de modo simples, assuntos demasiadamente técnicos e por vezes difíceis.

Agradeço ao meu orientador Prof. Dr. Leandro, pela sabedoria, perspicácia e objetividade com que me guiou nesta trajetória, inclusive na escolha do tema, o que reconheço nem sempre é fácil.

Agradeço a coordenadora e professora Dra. Rita Denardi que com muita sabedoria e resiliência, soube administrar e manter o curso e a turma firme, mesmo considerando os momentos tão adversos que passamos devido a pandemia de COVID-19. Além disso, ela "acendeu" uma luz no final do túnel quando até achei que não conseguiria finalizar esse trabalho.

Ao meu colega de curso Roderlei Vendrametto, que muito me ajudou nos trabalhos e nas tarefas do curso.

Gostaria de deixar registrado também, o reconhecimento e gratidão à minha filha Anna Luisa, que curiosamente também está escrevendo seu trabalho de conclusão de curso (TCC) do seu curso de graduação e sempre me incentivou a escrever mais e melhor.

O que o trouxe até aqui não será o que o levará adiante.
(Marshall Goldsmitth)

RESUMO

Vivemos numa era em que a informação é de enorme relevância para o cidadão e para as empresas. A informação assertiva e tempestiva, pode determinar o sucesso ou o fracasso de uma empresa e tem sua origem no adequado tratamento dos dados. Por sua vez, os dados a cada dia são obtidos de maneiras nunca imaginadas. Equipamentos de uso pessoal, sistemas de coletas automatizadas que muitas vezes não são percebidos pelos usuários e cadastros que se auto complementam, tornam a captura e processamento de dados mais poderoso e preciso. Nesse contexto a promulgação da LGPD – Lei Geral de Proteção de Dados; Lei nº13.709/2019 –, trouxe consigo consideráveis impactos ao tratamento dos dados de modo geral. Esse impacto não foi menor no tratamento dos dados no para instituições que trabalham em assistência ou pesquisa em saúde. Nesse contexto, o tratamento de dados passou a ser ainda mais criterioso e cuidadoso no tocante a proteção da identificação da pessoa ou paciente Tecnologias de extração, tratamento e anonimização de dados tornaram-se obrigatórias, para evitar o descumprimento da legislação. Muitos desses cuidados embora já fossem observados devido a existência de normas e regulamentos de entidades classes e associações que atuam no segmento da saúde, ampliaram ainda mais preocupação quanto a proteção dos dados históricos e a identidade do indivíduo. Por fim, a autorização para processamento autorização para processamento dos dados e para utilização desses dados em pesquisas clínicas assumiu relevância e destaque ainda maior.

Palavras-chave: LGPD. Informação. Dados. Anonimização. Pseudoanonimização

ABSTRACT

We live in an era in which information is of enormous importance for citizens and companies. Assertive and timely information can determine the success or failure of a company and has its origin in the proper processing of data. In turn, the data each day is obtained in ways never imagined. Equipment for personal use, automated collection systems that are often not noticed by users and records that complement each other, make the capture and processing of data more powerful and accurate. In this context, the enactment of the LGPD – General Data Protection Law; Law No. 13.709/2019 - brought considerable impacts to the processing of data in general. This impact was not smaller in the treatment of data for institutions that work in health care or research. In this context, data processing became even more judicious and careful with regard to protecting the identification of the person or patient. Data extraction, processing and anonymization technologies became mandatory, to avoid non-compliance with legislation. Many of these precautions, although they were already observed due to the existence of norms and regulations of professional bodies and associations that work in the health sector, increased even more concern regarding the protection of historical data and the individual's identity. Finally, the authorization for processing authorization for data processing and for the use of these data in clinical research took on even greater relevance and prominence.

Keywords: LGPD. Information. Data. Anonymization. Pseudoanonymization

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS, SIGLAS E ACRÔNIMOS

LISTA DE ABREVIATURAS

ART. Artigo

LISTA DE SIGLAS

GPDR	Regulamento Geral de Proteção de Dados
LGPD	Lei Geral de Proteção de Dados
CE	Comunidade Europeia
HIPAA	Health Insurance Portability and Acconuntability – Lei de Portabilidade e Responsabilidade de Saúde
HHS	Health and Human Service – Departamento de Saúde e Serviços Humanos
PHI	Personal Health Information – Informação Pessoal de Saúde
ANS	Agência Nacional de Saúde
CFM	Conselho Federal de Medicina
CRM	Conselho Regional de Medicina
COREN	Conselho Regional de Enfermagem
TCLE	Termo de Consentimento Livre e Esclarecido
TC	Termo de Consentimento
CPF	Cadastro de Pessoa Física
PL	Projeto de Lei
RG	Registro Geral
IP	Internet Protocol - Protocolo de Internet
MP	Medida Provisória

LISTA DE ACRÔNIMOS

ONU	Organização das Nações Unidas
EUA	Estados Unidos da América

SUMÁRIO

1 INTRODUÇÃO

Em uma sociedade cada vez mais digital e conectada, as informações sobre as pessoas tornaram-se a cada dia um bem mais valioso.

> "Desde o início da vida a informação é um elemento fundamental para s sobrevivência dos seres de todas as espécies e mais especialmente para a raça humana. A informação permitiu descobertas como o fogo, a roda e tantas outras que são consideradas comuns nos dias de hoje, A informação é parte das nossas vidas. Chegamos até aqui porque a informação foi compartilhada de geração a geração". [PONTES, EDISON, 2012]

Facilitadas por tecnologias que automatizam a coleta e o processamento, muitas organizações coletam diariamente uma assombrosa quantidade de dados.

"Os relacionamentos sociais foram energizados por um fluxo informacional que não encontram mais obstáculos físicos distanciais". [BIONI, BRUNO RICARDO, 2019, p. 5]

Dados pessoais, tais como: dados demográficos, hábitos de consumo, dados financeiros, deslocamentos, comportamento social, passa tempos e uma infinidade de outros e entre esses, dados relativos à saúde são coletados, armazenados e processados com velocidades e acurácia até então inimagináveis.

Essa expressiva quantidade de dados coletados traz para as organizações mais responsabilidade quanto a segurança e cuidado no processamento de dados. Essa responsabilidade cresce à medida que surgem novos regulamentos estaduais, federais e internacionais, que inicialmente eram desenvolvidos de forma isolada ou independente, mas que ao longo dos últimos anos, se consolidaram e deram origem a leis que em sua maioria visam a proteção dos interesses dos cidadãos.

CONTEXTUALIZAÇÃO

"O dado é o estado primitivo da informação" [DONEDA, Danilo. Da privacidade à proteção de dados. Rio de Janeiro: Renovar, 2066. p. 152], pois não é algo *per se* que acresce conhecimento. "Dados são simplesmente fatos brutos que, quando processados e organizados, se convertem em algo inteligível, podendo ser deles extraída uma informação". [BIONI, BRUNO RICARDO, 2019. p.36]

À medida que sistemas e tecnologia permitem revolucionárias maneiras e possibilidades de capturar e processar dados, vimos segundo Bioni [p.89], o nascimento de uma "biografia digital" a qual não deixa de ser um resultado lógico, mas que resulta na possiblidade de classificação e segmentação com bases nessas informações.

> "A conjunção dessas diversas variáveis, evidencia que a proteção dos dados pessoais tangencia o próprio rumo da vida das pessoas, perpassando, transversalmente, os seus mais variados contatos sociais. Desde a celebração de contratos e o ato de consumo à – até mesmo – busca pelo acesso à informação" [BRUNO, RICARDO BIONI, 2019. P.91]

Regulamento ou leis como o GPDR – Regulamento Geral de Proteção de Dados –, conjunto de regras aprovadas em 2016 e em vigor na comunidade europeia desde 2018 e a LGPD – Lei Geral de Proteção de Dados –, promulgada no Brasil pela lei n° 13.709/2018, trouxeram um contraponto a facilidade de busca e captura de dados e consigo, uma rigorosa regulamentação para a coleta e o processamento de dados, além de prever em certas circunstâncias, a obrigatoriedade do descarte dos dados.

PROBLEMA

As atuais leis de proteção de dados pessoais, buscam classificar e tipificar os dados coletados e para o contexto desse trabalho, destacamos a classificação dos dados do tipo "sensível".

O 5° artigo da LGPD classifica como dados pessoais sensíveis, aquele tipo de dado que possa identificar de forma única, ou seja, a individualidade de uma pessoa e busca que essa identificação não permita de alguma maneira, constranger ou discriminar e dessa forma atentar contra os direitos e liberdades fundamentais do indivíduo.

São definidos com dado pessoal sensível:

- Dado sobre origem racial ou étnica;
- Dado sobre convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político;
- Dado referente à saúde ou à vida sexual;
- Dado genético ou biométrico, quando vinculado a uma pessoa natural

Decorre que em sua maioria, os dados coletados no processo de atendimento assistencial a pacientes hospitalizados ou em regime ambulatorial, encaixam-se na definição de dado pessoal sensível.

Com essa constatação, resta recorrer a própria lei para estabelecermos se existem e quais são maneiras lícitas para a continuidade do processamento de dados coletados sob a circunstância de hospitalização e suas relações periféricas e correlatas.

Considerando que a massiva captura e o exaustivo processamento de dados de pessoais têm como principal finalidade o incentivo ao comércio e ao consumo, e que a legislação de proteção de dados de um modo geral procura proteger os interesses pessoais, objetivos de processamento que visem o interesse não apenas do cidadão, mas da sociedade, e ainda o processamento de dados que permitam o desenvolvimento de pesquisas na área de saúde, devem ser previstos, regulados e permitidos.

OBJETIVOS

No contexto do problema anteriormente apresentado, estabelecemos os objetivos geral e específico desse trabalho.

Objetivo geral

Analisar os aspectos mais diretamente relacionados ao processamento e tratamento de dados de saúde, quando sob o prisma da Ciência de Dados Aplicada.

Objetivo específico

Esse trabalho ter por objetivo analisar quais foram os impactos que a LGPD trouxe para a coleta e processamento de dados relativos à saúde, e de modo especial, quais foram os impactos para um sistema de gestão hospitalar informatizado, e baseando-se nessas possibilidades, apontar alternativas para a continuidade de coleta de dados que são imprescindíveis para o desenvolvimento do tratamento e pode beneficiar a pessoa e a sociedade como um todo.

2 FUNDAMENTAÇÃO TEÓRICA

O CONTEXTO HISTÓRICO DA PROTEÇÃO DE DADOS

Vinte anos após a aprovação da Declaração Universal de Direitos Humanos pela ONU em 1948, a qual tornou o direito à privacidade um direito fundamental, foi criada a primeira legislação a regular o tema de proteção de dados.

Em 1970, o ato Hessiches Datenschutzgesetz (Ato de Proteção de Dados de Hesse) no Estado de Hesse na Alemanha de Hesse surgiu como a primeira lei nacional de proteção de dados, que foi seguida pela lei sueca Sw. Datalagen (Ato de Dados Sueco), de 1973. Embora a lei sueca não tratasse da proteção de dados de maneira objetiva e pormenorizada, se omitindo, por exemplo, de regular em que situações os dados poderiam ser coletados[1].

Essa movimentação para a proteção de dados gerou um debate internacional, que possibilitou a diversas nações europeias em 1979, a criação de suas próprias leis de proteção de dados.

Entretanto, todas essas leis sofriam do mesmo tipo de problema, que era a forma genérica ou a omissão com que tratavam o problema das práticas específicas sobre o tema, mas serviram ao propósito de causar o debate sobre o assunto.

Em 1995 a Comunidade Europeia promulgou a Diretiva 95/46/CE que tratava a proteção do indivíduo em relação ao tratamento de seus dados pessoais e a livre circulação desses dados na comunidade.

Entre os regulamentos e leis recentemente promulgados ou modernizados, apresentamos destaque para a GPRD – Regulamento Geral de Proteção de Dados--, lei aplicada em 2018 na Comunidade Europeia, cuja base serviu de orientação para a LGPD Brasileira.

A IMPORTÂNCIA DA DIRETIVA 95/46 NA COMUNIDADE EUROPEIA

A União Europeia possui longa tradição na proteção de dados pessoais. A “Convenção 108” entrou em vigor em 1985, é considerado como o primeiro documento com relevância global que trata de questões relativas a proteção de dados.

[1] https://baptistaluz.com.br/espacostartup/28-01-dia-internacional-da-protecao-de-dados/ [acessado em 16/06/2021 as 22:30]

Tendo como base a Convenção 108, o conselho e o parlamento europeu aprovaram a Diretiva 95/46/CE, que viria a ser a base da atual legislação europeia sobre proteção de dados. Proposta em 1990 e aprovada em 1995, ela viria a ser um dos principais instrumentos sobre o tema de proteção de dados pessoais.

Entre outros temas, a diretiva lançou a ideia de que o processamento dos dados deve estar a serviço do Homem e não exclusivamente para atender aos interesses comerciais e de empresas, como pode ser percebido no trecho abaixo.

> "Os sistemas de tratamento de dados estão a serviço do Homem, (…) eles devem seja qual for a sua nacionalidade ou residência de pessoas singulares, respeitar os seus direitos e liberdades fundamentais, em particular o direito à privacidade, e contribuir para o progresso econômico e social, (…) e para o bem-estar dos indivíduos" [CARLA BARBOSA; DULCE LOPES, 2020].

A PROTEÇÃO DE DADOS NOS EUA

Diferentemente do pensamento europeu, nos EUA predomina um sentimento de que não deve haver uma legislação específica sobre a proteção de dados.

Não obstante, existem leis, regulamentos e normas específicas que abordam questões relativas à coleta, o processamento e a proteção de dados.

No tocante a coleta e processamento de dados no segmento de saúde o conjunto normativo mais significativo é a lei federal HIPAA (Health Insurance Portability and Accountability Act, de 1966; ou Lei de Portabilidade e Responsabilidade de Seguro de Saúde).

LEGISLAÇÃO HIPPA

Publicada em 1996, a HIPAA direciona e orienta todos os interessados e os agentes que atuam com dados médicos. Seu objetivo é evitar vazamento de informações e ameaças a conteúdos íntimos de pacientes e exige a criação de padrões nacionais para proteger as informações confidenciais de saúde do paciente contra divulgação sem seu consentimento ou conhecimento[2].

[2] https://www.cdc.gov/phlp/publications/topic/hipaa.html [acesso em 26/06/2021 as 21:30]

O Departamento de Saúde e Serviços Humanos (HHS) dos Estados Unidos emitiu a **Regra de Privacidade** para implementar os requisitos da HIPAA.

Os padrões da regra de privacidade tratam do uso e da divulgação de informações de saúde de indivíduos (conhecidas como "informações de saúde protegidas") por entidades sujeitas a essa regra. Os indivíduos e organizações sujeitos a essa regra são chamados de entidades cobertas.

A regra de privacidade contém padrões para que os indivíduos possam compreender e controlar como suas informações de saúde são usadas pelas entidades cobertas.

Um dos principais objetivos da regra de privacidade é garantir que as informações de saúde dos indivíduos sejam protegidas adequadamente, mas ao mesmo tempo permitir o fluxo de informações de saúde necessárias para fornecer e promover cuidados de saúde de alta qualidade e proteger a saúde e o bem-estar do público.

A regra de privacidade atinge um equilíbrio que permite usos de dados e de informações enquanto protege a privacidade das pessoas que buscam atendimento e cura.

Provedores de saúde

Todo provedor de saúde, independentemente do seu tamanho, mas que transmita eletronicamente informações de saúde em relação a certas transações estão sujeitas a regra de privacidade.

As transações eletrônicas reguladas incluem reivindicações, consultas de elegibilidade de benefícios, solicitações de autorização de referência e outras transações para as quais o HHS estabeleceu padrões da Regra de Transações HIPAA.

Planos de saúde

Entidades que fornecem ou pagam o custo dos cuidados médicos. Os planos de saúde incluem seguradoras de saúde, odontológica, oftalmológica e de medicamentos prescritos; organizações de manutenção da saúde, seguradoras de suplementos do "*Medicare*", "*Medicaid*"; e seguradoras de cuidados de longo prazo. Os planos de saúde também incluem planos de saúde em grupo patrocinado pelo empregador, pelo governo e pela igreja e ainda planos de saúde multiempregadores.

Usos e divulgações permitidos pela HIPPA

A uma entidade coberta é permitida, embora não seja obrigada, a usar e divulgar informações de saúde protegidas, mesmo sem a autorização de um indivíduo, para os seguintes fins ou situações:

- Divulgação ao indivíduo, entretanto, se a informação for necessária para o acesso ou contabilização das divulgações, a entidade é obrigada a divulgar ao indivíduo;
- Tratamento, pagamento e operações de saúde;
- Oportunidade de concordar ou contestar a divulgação PHI – Personal Health Information - (permissão informal que pode ser obtida perguntando diretamente ao indivíduo, ou por circunstâncias que claramente dão ao indivíduo a oportunidade de concordar ou contestar o fornecimento dos dados)

Incidente com uso e divulgação de outra forma permitidos

A regra de privacidade, no interesse público, permite o uso e divulgação de informações de saúde protegidas, sem a autorização ou permissão de um indivíduo, para algumas finalidades, notadamente visando o interesse e prioridade nacional, nas seguintes situações:

1. Quando exigido por lei;
2. Atividades de saúde pública;
3. Vítimas de abuso ou negligência ou violência doméstica;
4. Atividades de supervisão de saúde;
5. Processos judiciais e administrativos;
6. Aplicação da lei;
7. Funções relativas a pessoas falecidas (como identificação);
8. Doação de órgãos, olhos ou tecidos cadavéricos;
9. Pesquisa, sob certas condições;
10. Para prevenir ou diminuir uma ameaça séria à saúde ou segurança;
11. Funções essenciais do governo;
12. Compensação de trabalhadores.

Regra de segurança HIPAA

Enquanto a regra de privacidade da HIPAA protege as informações protegidas da saúde, a regra de segurança protege um subconjunto de informações abrangidas pela regra de privacidade.

Este subconjunto é composto por todas as informações de saúde individualmente identificáveis que uma entidade coberta cria, recebe, mantém ou transmite em formato eletrônico.

Essas informações são chamadas de "informações eletrônica de saúde protegida" (e-PHI). A regra de segurança não se aplica a uma PHI transmitidas oralmente ou por escrito.

Para cumprir a regra de segurança HIPAA, todas as entidades cobertas devem:

- Garantir a confidencialidade, integridade e disponibilidade de todas as informações eletrônicas de saúde protegidas
- Detectar e proteger contra ameaças antecipadas à segurança das informações
- Proteger contra usos ou divulgações inadmissíveis de forma antecipada
- Certificar a conformidade por sua força de trabalho

As entidades cobertas devem basear-se na ética profissional e no bom senso ao considerar as solicitações para esses usos e divulgações permissivos.

O Escritório de Direitos Civis do HHS aplica as regras da HIPAA e todas as reclamações referentes ao descumprimento desse conjunto de leis e regras, devem ser relatadas a esse escritório. As violações da HIPAA podem resultar em penalidades civis ou criminais.

PROTEÇÃO DE DADOS NO BRASIL

No Brasil o processo de criação de regulamentos, normas e leis que visem a proteção de dados tem início em 2010 quando o Ministério Público Federal apresentou um anteprojeto de Lei de Proteção de Dados e dessa forma, deu início a uma consulta pública sobre o assunto.

A consulta pública deu origem ao projeto de lei PL n° 4060/2012, que ficou parado até meados de 2013, quando o caso que envolveu o americano Edward Snowden[3], teve grande repercussão na mídia mundial.

[3] Edward Joseph Snowden é um analista de sistemas, ex-administrador de sistemas da CIA e ex-contratado da NSA que tornou públicos detalhes de vários programas que constituem o sistema de vigilância global da NSA americana [https://pt.wikipedia.org/wiki/Edward_Snowden acessado em 04/07/2021 as 11:25]

Snowden denunciou irregularidades quanto a práticas de violação de privacidade e vigilância praticadas pelos EUA, não apenas contra cidadãos ao redor do mundo, mas até mesmo contra chefes de Estados. Infelizmente o assunto perdeu força e a discussão e a consulta pública não avançaram.

Em 2015 o Ministério de Justiça voltou a promover nova consulta popular sobre o tema de proteção de dados, o que deu origem ao PL n° 5276/2016, dessa vez gerando um conteúdo mais robusto e consistente.

Com entrada em vigor da GPDR em 2018 na Comunidade Europeia, o tema ganhou nova força no Brasil, levando dessa forma, a promulgação da LGPD.

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 alterada pela Lei n° 13.853/2019, dispõem sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural[4].

A lei brasileira segue um alinhamento e esforço mundial na criação de leis e regulamentação que visam preservar o direito do cidadão, sua privacidade e maior segurança de seus dados e informações pessoais.

A necessidade de proteger a integridade do cidadão por meio de regulamentos e normas que evitem a sua exposição por meio de divulgação de dados e informações sigilosas, dando ao cidadão oportunidade de ter mais controle sobre seus dados, é um contraponto que surge e ganha força à medida que os sistemas digitais evoluem e permitem mais facilidade para a captura e o processamento de dados.

PRINCIPIOS DA LGPD

A LGPD foi concebida sob princípios fundamentais que são norteadores e perseguido pelo legislador. São dez os princípios declarados.

1. **Princípio da Adequação**

Está previsto no inciso II, do artigo 6.º da LGPD e prevê a "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento".

[4] https://www.gov.br/defesa/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dados-pessoais-lgpd [acesso em 25/06/2021 as 22h00]

Os dados devem ser tratados de acordo com a sua destinação. A coleta de dados deverá ser compatível com a atividade fim do tratamento.

2. Princípio da Necessidade

A coleta de dados deve ocorrer de forma restritiva, cuidando para que o tratamento dos dados pessoais esteja restrito à finalidade pretendida.

3. Princípio da Transparência

Visa garantir aos titulares, informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento dos dados.

4. Princípio do Livre Acesso

Possibilitar que o titular dos dados consulte livremente, de forma facilitada e gratuita, a forma e a duração do tratamento dos dados, bem como sobre a integralidade deles.

5. Princípio da Qualidade dos Dados

Este princípio busca garantir aos titulares dos dados a exatidão, a clareza, a relevância e a atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

6. Princípio da Segurança

Compreende medidas técnicas e administrativas para proteger os dados de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

7. Princípio da Prevenção

É um dos pilares da Segurança da Informação, buscando a antecipação de eventualidades, com a adoção de medidas para prevenir a ocorrência de danos em razão do tratamento de dados pessoais.

8. Princípio da Responsabilização e Prestação de Contas

Neste princípio espera-se que o controlador ou o operador demonstrem todas as medidas eficazes e capazes de comprovar o cumprimento da lei e a eficácia das medidas aplicadas.

9. Princípio da Não Discriminação

O tratamento dos dados não pode ser realizado para fins discriminatórios, ilícitos ou abusivos, ou seja, não se pode excluir de titulares de dados pessoais, no momento de seu tratamento, informações determinadas por características, sejam elas de origem racial ou étnica, opinião política, religião ou convicções, geolocalização, filiação sindical, estado genético ou de saúde ou orientação sexual.

10. Princípio da Finalidade

Previsto no inciso I do art. 6.º da LGPD, emprega-se como a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades", ou seja, o dado deverá, na coleta, ter a indicação clara e completa que a justifique.

DEFINIÇÃO DE DADOS PESSOAIS

Personalidade significa as características ou o conjunto de características que distingue uma pessoa da outra. [BIONI, BRUNO RICARDO, 2019, p.63]

Sendo assim, ao aceitarmos o fato de que dados são também atributos, eles podem então caracterizar uma pessoa e aceitamos assim que também podemos, a partir de seus dados, identificar uma única pessoa em meio centenas ou milhares de outras pessoas.

Ciente de tal fato o legislador brasileiro, foi bem claro e taxativo no conteúdo da LGPD, que definindo o que é considerado como dado pessoal e desses, quais são os considerados como sensíveis e quais as possiblidades e regras para seu tratamento.

Dados pessoais

De maneira muito simples e direta, dado pessoal é todo dado que possa identificar uma pessoa de um conjunto de outras pessoas. É a capacidade de distinção a partir do processamento de um conjunto de dados, que poderiam vir a ser caracterizados como informações dessa pessoa.

> O conceito de dado pessoal é bastante abrangente, sendo definido como a "informação relacionada a pessoa identificada ou identificável". Isso quer dizer que um dado é considerado pessoal quando ele permite a identificação, direta ou indireta, da pessoa natural por trás do dado, como por exemplo: nome, sobrenome, data de nascimento, documentos pessoais (como CPF, RG, CNH, Carteira de Trabalho, passaporte e título de eleitor), endereço residencial ou comercial, telefone, e-mail, cookies e endereço IP[5]. [SERASA EXPIRIAN]

Trata-se, aqui, de qualquer informação relacionada a pessoa natural identificada ou identificável (LGPD, Art. 5º, I). Informações abstratas e genéricas, portanto, estão fora da definição. (DALLARI: MONACO: COSTA, 2019, p.90).

Desse modo, dado pessoal é aquele que possibilita a identificação, direta ou indireta, da pessoa natural.

São exemplos de dados pessoais:

- Nome e sobrenome;
- Data e local de nascimento;
- RG;
- CPF;
- Retrato em fotografia;
- Endereço residencial;
- Endereço de e-mail;
- Número de cartão bancário;
- Renda;
- Histórico de pagamentos;
- Hábitos de consumo;
- Dados de localização, como por exemplo, a função de dados de localização no celular;
- Endereço de IP (protocolo de internet);
- Testemunhos de conexão (cookies);
- Número de telefone.

[5] https://www.serasaexperian.com.br/conteudos/protecao-de-dados/lgpd-e-a-definicao-de-dados-pessoais/ [acesso em 29/06/2021 as 21:51]

Dado pessoal sensível

Dentre os dados pessoais, existem alguns tipos que exigem maior atenção para o tratamento: são os relacionados a crianças e adolescentes e os “sensíveis”.

Dados sensíveis, segundo a classificação da LGP, são os que podem revelar origem racial ou étnica, convicções religiosas ou filosóficas, opiniões políticas, filiação sindical, questões genéticas, biométricas e sobre a saúde ou a vida sexual de uma pessoa.

CONCEITO DE TRATAMENTO DE DADOS

Conceitualmente podemos entender como tratamento de dados, todo o ciclo de vida do dado. A LGPD estabelece o ciclo de vida dos dados como sendo:

- **Coleta**; onde temos a colete e captura, a produção e a recepção;
- **Retenção**; onde temos o arquivamento e armazenamento
- **Processamento**; onde temos a classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e a modificação;
- **Compartilhamento**; onde temos a transmissão, distribuição, comunicação, transferência e difusão;
- **Eliminação**; onde temos a eliminação e o término do tratamento do dado.

A cobertura material da LGPD alcança o tratamento de dados pessoais, independentemente de quem a realize (LGPD, Art. 1º). [COSTA, JOSÉ AUGUSTO FONTOURA, 2019].

O artigo 5º da LGPD em seu X inciso conceitua como tratamento de dados:

> Toda operação realizada dom dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Desse modo, a compreensão das noções de tratamento de dados e de dados pessoais é muito amplo e fundamental para a delimitação do campo de incidência normativa, pois

basicamente o tratamento de dados representa todo o conjunto de operações com dados e estão sob a tutela da LGPD.

Requisitos para o tratamento de dados

As tecnologias atuais permitem uma impressionante capacidade de capturar e processar dados. Essa capacidade incrementa a eficiência em muitos processos.

Entretanto, é notório que essa capacidade exacerba o direito à privacidade e a intimidade das pessoas.

A LGPD em seu 7º artigo estabelece as hipóteses onde o tratamento de dados pessoais é permitido.

I - Mediante o fornecimento de consentimento pelo titular;

II - Para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

VII - Para a proteção da vida ou da incolumidade física do titular ou de terceiros;

VIII - Para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

VIII - Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019)

IX - Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Dessas hipóteses, destacamos que os itens: I, II, IV, VII e VIII, são condições recorrentes em atendimentos de atenção à saúde.

CONSENTIMENTO PARA USO

Os personagens envolvidos com atendimentos o setor de saúde sempre esteve preocupado com a questão de proteção de dados e da privacidade de seus pacientes, com exemplos, podemos citar trechos extraídos do Código de Ética Médica [CODIGO de ÉTICA MÉDICA: Resolução CFM nº 2.217], do Conselho Federal de Medicina. Quando deixa claro situações obrigatórias e condições para utilização de dados mediamente o atendimento de condições prévias.

> Artigo 22 - Deixar de obter consentimento do paciente ou de seu representante legal após esclarecê-lo sobre o procedimento a ser realizado salvo em caso de risco iminente de morte.
>
> Artigo 101 - Deixar de obter do paciente ou de seu representante legal o termo de consentimento livre e esclarecido para realização de pesquisa envolvendo seres humanos. Explicações sobre a natureza e as consequências da pesquisa.
>
> Art. 102 - Parágrafo único. A utilização de terapêutica experimental é permitida quando aceita pelos órgãos competentes e com o consentimento do paciente ou seu representante legal. Descido da situação e das possíveis consequências.

Quando a assistência médica e a coleta de dados acontecem para menores de idade, é imprescindível obter o consentimento específico, concedido por pelo menos um dos pais ou responsável legal e deve se limitar a apenas o conteúdo estritamente necessário, sem repasse a terceiros.

Poderão ser coletados dados pessoais de menores sem o consentimento, apenas, quando a coleta for necessária para contatar os pais ou o(a) responsável legal, podendo ser utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiros sem o consentimento dado por pelo menos um dos pais ou pelo(a) responsável legal.

Sobre os dados sensíveis, o tratamento depende do consentimento explícito do(a) titular dos dados e para um fim definido. Sem esse consentimento do(a) titular, a LGPD define que somente será possível, quando a informação for indispensável em situações relacionadas a uma obrigação legal; a políticas públicas; a estudos via órgão de pesquisa; ao exercício regular de direitos; à preservação da vida e da integridade física de uma pessoa; à tutela de procedimentos feitos por profissionais das áreas da saúde ou sanitária; à prevenção de fraudes contra o(a) titular.

INTERESSE LEGÍTIMO PARA TRATAMENTO DE DADOS

O caso da saúde é paradigmático por maioria das situações. Tem raízes no último reduto da vida privada de cada um de nós e que por este motivo se consideram dados sensíveis ou pessoalíssimos. [BARBOSA, CARLA: LOPES, DULCE, 2019, p. 56].

O tratamento de dados no âmbito hospitalar é fundamental para que evoluam as pesquisas científicas e diagnósticos.

> O certo é que em saúde no âmbito assistencial de investigação não existe dados pessoais. E por isso é necessário encontrar um equilíbrio entre os vários direitos, o direito à privacidade e o direito da autodeterminação, mas também o direito à investigação e o direito à proteção à saúde. [BARBOSA, CARLA: LOPES, DULCE, 2019, p. 57].

A LGPD oferece possibilidade de tratamento dos dados quando há claro "legitimo interesse para o tratamento".

> Previsto no inciso I do art. 6.º da LGPD, emprega-se como a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades", ou seja, o dado deverá, na coleta, ter a indicação clara e completa que a justifique[6].

Portanto entendemos clara a manifestação do 3º Tribunal de Justiça Brasileiro, de que havendo o legítimo interesse é permitido desde que no ato da coleta existam claro e lícito propósito.

---

[6] https://www.trf3.jus.br/lei-geral-de-protecao-de-dados-pessoais-lgpd/principios/ [acesso em 30/06/2021 as 20:55]

ANONIMIZAÇÃO E PSEUNDONONIMIZAÇÕ DE DADOS PESSOAIS

A ideia de anonimização é obter a partir dados pessoais identificáveis, uma condição tal que por meio de processamento desses dados não seja possível identificar a pessoa ao qual o dado pertence.

"Por definição a anonimização consiste na utilização de meios técnicos razoáveis e disponíveis no momento do tratamento por meio dos quais um dado perde a possibilidade de associação direta ou indireta a um indivíduo[7]".

> A irreversibilidade é o elemento principal do processo de anonimização e, diante da impossibilidade de garantir a irreversibilidade absoluta a LGPD estabelece determinados critérios, incluindo o custo, tempo, tecnologias disponíveis e utilização de meios próprios para a reversão, sem prejuízos de padrões e técnicas a serem eventualmente estabelecidos pela Autoridade Nacional de Proteção de Dados (ANPD) para a realização de processos de anonimização.[KUNG, ANGELA FAN CHI; AUN, NICOLE RECCHI, 2019, p. 107]

A anonimização é portanto, um processo que garante que uma vez que o conjunto de dados sejam anonimizados, não é mais possível reverter o processo e identificar uma pessoa.

A pseudoanonimização é um processo de tratamento dos dados que consiste em "disfarçar" os dados por meio da substituição de um atributo por outro, desse modo causando um embaralhamento que torna difícil identificação de uma pessoa.

Na pseudoanonimização são utilizadas técnicas como: criptografia com chave secreta, criação ou geração de *token*[8], aplicação de algoritmo de embaralhamento.

Em todas essas técnicas, o controlador dos dados possui mecanismos para reconstruir ou restaurar os atributos ocultos ou embaralhados, restaurando dessa forma a completude dos dados.

A diferença entre as técnicas é que na anonimização mesmo o controlador do dado, não é capaz refazer a identificação, mesmo que a "alto custo" enquanto na pseudoanonimização o dado é facilmente restituído, desde que se possua a "chave" utilizada para o embaralhamento.

---

[7] Artigo 5º, IX, da Lei nº 13.709/2018

[8] TOKEN é um recurso de segurança que gera um código identificador digital exclusivo, aleatório e temporário para proteger dados sensíveis. [https://www.mundodomarketing.com.br/artigos/geraldo-marques/38474/entenda-o-que-e-tokenizacao-e-por-que-o-mundo-esta-surfando-nessa-onda.html acesso em 03/07/2021 as 12h45]

GOVERNANÇA DE DADOS

A governança de dados consiste num conjunto de políticas e processos que uma empresa estrutura para apoiar o gerenciamento de dados. A governança de dados é essencial e complementar a estratégia de gestão de dados e deve ser aderente a práticas legais de processamento de dados.

Com o acúmulo exponencial de novos dados, as empresas precisam projetar uma arquitetura de dados para controlar essas fontes, integrá-las e disponibilizá-las aos fins a que os dados foram capturados.

A governança de dados deve ajudar a empresa a saber quais dados ela tem, onde estão e como e quando eles podem ser utilizados.

COMPARTILHAMENTO DE DADOS

A LGPD determina em seu 11º artigo, § 4º:

> É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes a saúde com o objetivo de obter vantagem econômica, exceto nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência a saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados e para permitir:
>
> I - A portabilidade de dados quando solicitada pelo titular ou?
>
> II - As transações financeiras e administrativas resultantes do uso e da prestação de serviços, de que trata este parágrafo.

O deputado Orlando Silva, relator de Medida Provisória MP 869, que deu forma ao texto atual da LGPD, assim expôs suas considerações acerca da possibilidade de compartilhamento de dados entre os agentes envolvidos no atendimento no âmbito da saúde[9].

[9] BRASIL. Congresso Nacional. Relatório Legislativo da Comissão Mista sobre a Medida Provisória nº 869, de 28 de setembro de 2018. 7 de maio de 2019. P. 69-70. Disponível em <https://legis.senado.leg.br/sdleg-getter/documento?dm=7945369&rts=1594019728155&disposition=inline>. Acesso em: 05 de julho de 2021.

“Tendo em vista todos os argumentos apresentados, estamos certos de que as chamadas “perfilizações” e a coleta de dados pelo comércio poderiam ser utilizadas em malefício do usuário, o que poderia resultar em negação de acesso a seguros médicos, planos de saúde e à saúde de maneira geral.

Por outro lado, a circulação, conexão e coordenação dos dados pelos diversos agentes envolvidos na contraprestação a serviço contratado são imprescindíveis ao atendimento médico moderno, rápido, eficiente e seguro.

Assim entendemos que a flexibilização proposta tanto pela MP quanto pelas emendas 96 e 121 são pertinentes no sentido de acatar a real necessidade de comunicação desse tipo de dados entre as empresas. Todavia, verificamos a necessidade de melhor precisar para que finalidades essa comunicação poderá ser feita, como forma de evitar abusos.

Com esse espírito, inspirados na citada Lei dos EUA e na legislação brasileira, notadamente na Lei Complementar nº 141/12 que estabelece critérios para os serviços públicos de saúde e nomenclatura consagrada pelo Ministério da Saúde, a exemplo da Portaria 403/07, determinamos que, nas “hipóteses relativas a prestação de serviços de saúde, incluídos os serviços auxiliares de diagnose e terapia”, poderá haver comunicação de dados referentes à saúde quando em benefício dos titulares e para “transações financeiras e administrativas resultantes do uso e prestação dos serviços contratados”.

TUTELA DE DADOS PARA USO EM SAÚDE

> Saúde e privacidade são temas congêneres que oferecem espaço para numerosos debates que invariavelmente convergem na busca pela conciliação entre a necessidade quotidiana de realizar o tratamento de dados pessoais do setor de saúde e as normas de proteção dos dados pessoais.

> São diversas as ocasiões em que os dados são tratados no setor de saúde dentre as quais destacam-se: as atividades de pesquisa e desenvolvimento de novos produtos tratamentos e tecnologias de saúde prática clínica e assistencial de pacientes por profissionais de organizações da área de saúde. Farmacologia fármaco vigilância e controle de qualidade em indústrias farmacêuticas dentre outras. [KUNG, ANGELA FAN CHI; AUN, NICOLE RECCHI, 2019, p. 101]

CONSENTIMENTO DE PAIS OU RESPONSÁVEIS

Na classificação dos tipos de dados e a forma de tratá-los, a LGPD apresenta preocupação e ainda mais detalhes quanto ao tipo de dados pessoal quando esse pertence a menores de idade.

O art. 14 da LGPD define com clareza:

"O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente. "

No tocante ao ambiente de saúde, interesse desse estudo, destacamos ainda pontos cruciais de mesmo artigo.

> § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.
>
> § 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.
>
> § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.
>
> § 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.
>
> § 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.
>
> § 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Ainda que observadas essas disposições, a coleta “deve obedecer ao princípio da finalidade e transparência” (PINHEIRO, PARICA PECK, 2018, P.75).

Pesa ainda sobre a necessidade dessa coleta o fato de que se deve “assegurar que o consentimento recebido realmente adveio dos responsáveis/pais do menor. Isso porque o ambiente digital possibilita inúmeros meios de fraude” (PINHEIRO, PARICA PECK, 2018, P.75).

3 METODOLOGIA

Para esse estudo avaliamos o caso de uma unidade hospitalar de Curitiba – PR, onde desde a efetivação da LGPD, foram estabelecidas ações para a reavaliação de documentos e dos fluxos operacionais que envolviam de alguma maneira a coleta de dados.

Foram avaliados os impactos nos processos de atendimento em emergência, as consultas do tipo eletiva e no fluxo das ações para a internação e das etapas subsequentes no processo de atendimento do paciente.

Entrevistas como gestores responsáveis por operações de atendimento, internação e pesquisas foram realizadas para colher detalhes e suas avaliações pessoais sobre o impacto da LGPD no cotidiano da unidade e do trabalho que essa desenvolve.

IMPACTOS DA LGPD NA CAPTURA E TRATAMENTO DE DADOS NO AMBIENTE HOSPITALAR

No cotidiano de uma unidade hospitalar, de clínicas assistenciais, nos ambulatórios e em consultórios médicos, os dados e informações que pudessem de alguma maneira expor o paciente sempre foram tratados com sigilo e cuidado, até porque esse sempre foi um setor com muita regulamentação contando com muita atenção não apenas de agências regulatórias de governo como a ANS, Secretarias de Saúde dos Governos Municipal e Estadual, mas também por muitas entidades de classe, tal como: CFM, CRM, COREN e outros.

O senso comum dos envolvidos na operação da assistência em saúde aceitava que a troca e o processamento de dados pessoais na cadeia operacional, entre as unidades ou departamentos internos, assim como com outras empresas, acontecia para viabilizar o atendimento médico, sendo, portanto, necessária e adequada.

A LGPD trouxe para o segmento da saúde, uma nova realidade de preocupações nos aspectos jurídicos e tecnológicos.

A unidade hospitalar avaliada por esse trabalho presta serviços especializados em várias áreas de saúde, possuindo muitas especialidades médicas, atuando desde atendimentos ambulatoriais, consultas eletivas, pronto atendimento, internações hospitalares e cirurgias.

Pelo nível de interações de processos nessa complexa cadeia de atendimento, é recorrente a captura de dados pessoais e por se tratar de assuntos relacionados a saúde, os dados capturados são caracterizados pela LGPD como dados pessoais sensíveis.

Sendo assim, a direção do hospital, em conjunto com gerentes e coordenadores setoriais considerou necessária a revisão dos processos e documentos utilizados durante o atendimento dos pacientes e clientes.

A revisão de processos e documentos foi baseada na LGPD, que no 7º artigo do seu IIº capítulo, estabeleceu as bases sob as quais a unidade hospitalar erigiu as linhas de atuação para a captura e processamento de dados necessários à sua operação.

O art. 7º estabelece possibilidades de tratamento de dados nas seguintes hipóteses:

> Inciso I - Mediante o fornecimento de consentimento pelo titular;
>
> Inciso II - Para o cumprimento de obrigação legal ou regulatória pelo controlador;
>
> Inciso VII - Para a proteção da vida ou da incolumidade física do titular ou de terceiros;
>
> Inciso VIII - Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
>
> Inciso IX - Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

No entendimento dos responsáveis pela unidade hospitalar, os cinco incisos citados, estabelecem condições para que os dados pessoais sensíveis possam ser capturados e processados no ciclo de atendimento dos pacientes, restando apenas questões relacionadas ao estudo epidemiológicos, pesquisas e estudos clínicos.

Para atender as exigências legais, no âmbito do atendimento hospitalar, o foco de atenção concentrou-se nos Termos de Consentimento Livre e Esclarecidos – TCLE, que passaram a conter informações sobre a coleta e o processamento de dados dos pacientes.

A cadeia de processamento e troca de dados com parceiros operacionais de serviços externos, como por exemplo laboratórios de exames especializados, tiveram seus contratos e processos revistos e modificados a medida do necessário, para permitir a troca de dados essenciais a execução das atividades.

Outra questão também tratada foram as autorizações para processamento de dados com finalidade de pesquisas clínicas. Para esse tipo de processamento foi necessário a utilização de TCLEs ou Termos de Consentimento – TC, específicos para cada finalidade de uso dos dados, uma vez que no entendimento do departamento jurídico do hospital, o uso de dados para a pesquisa clínica, não poderia ser caracterizado como uso com "interesse legítimo" na execução da atividade primária de assistência em saúde.

Para a utilização em pesquisa clínica, os dados passaram a ser tratados com técnicas de pseudoanonimização, suprimindo informações que pudessem levar a identificação do paciente, mas permitindo, se necessário, recuperar a informação original, uma vez que no entendimento dos pesquisadores, pouca validade teria pesquisas clínicas que não permitissem identificar o indivíduo objeto do estudo.

Mapear o ciclo ou caminho dos dados e documentos dos pacientes e clientes, dentro do hospital, foi outro processo necessário para permitir maior controle sobre quem tem acesso aos dados ou documentos, uma vez que muitos dados e informações estão em documentos e formulários de papel. Essa revisão permitiu uma análise mais detalhada oportunizou rever a decisão de permitir ou não o acesso aos dados e documentos.

No aspecto da segurança da informação, o hospital entendeu que para atender a legislação pertinente é necessária uma ampla revisão de regulamentos e normas internas, uma vez é necessário não apenas a validação dos sistemas informatizados que são utilizados para registro das informações de pacientes e clientes, mas até mesmo o nível de acesso dos colaboradores e esses sistemas.

Nesse quesito foram estabelecidos quatro pilares de fundamentação para a revisão de aderência a LGPD.

Os pilares estabelecidos foram: Identificação, Gerenciamento, Proteção e Monitoramento.

Cada pilar estabelece linhas de cuidados, como segue:

- A identificação garante que todos os acessos aos dados e documentos sejam corretamente registrados.
- O gerenciamento avalia o nível de acesso e o ciclo de vida dos dados e documentos

- A proteção avalia a classificação dos dados e dos documentos gerados por esse, avaliando o nível de criticidade, proteção de acesso e retenção.
- Monitoramento garante não apenas a disponibilidade dos dados, mas também cuida da validação do cumprimento das regras internas.

Os sistemas de informação do hospital também foram alvo de validação e adequações, que ficaram a cargo das empresas fornecedores, cabendo ao hospital, a validação das providencias tomadas para atendimento a legislação.

4 CONSIDERAÇÕES FINAIS

Após a apresentação dos entraves e dificuldades imposta as empresas no tocante a captura e o processamento de dados, certamente nos deparamos com uma pergunta que soaria como natural: - Porque existem as leis de proteção e de dados e em especial no Brasil, a LGPD?

Entendemos que a resposta é igualmente simples: - Essas leis surgiram como resposta a preocupação publica quanto a privacidade dos cidadãos e seus direitos básicos.

A resposta também traz consigo a reflexão de que em determinadas situações a proibição de processar os dados traria enorme prejuízo aos avanços em pesquisa e no desenvolvimento de novas tecnologias.

Felizmente essas condições também foram avaliadas e com as devidas salvaguardas, permitidas.

Impondo limites no processamento e troca de dados, a legislação inicialmente trouxe apreensão e certa desorganização em processos que já estavam estabilizados, mas a longo prazo, em nosso entendimento, a ciência de dados se beneficiará com as medidas de revisão e das restrições impostas ao processamento indiscriminado, pois as bases de dados tendem a tornar-se mais robustas e confiáveis e respeitando os direitos individuais.

Técnicas como a anonimização e pseudoanonimização serão mais praticadas e fortalecidas não apenas do ponto de vista técnico, mas também no âmbito organizacional.

Se o processamento de dados pessoais deve ser praticado com ética, considerando e assegurando a privacidade das pessoas, em se tratando de dados no segmento da saúde, os fatores éticos e de privacidade devem ser ainda mais rigorosos.

Dados são tratados no setor de saúde, em muitas atividades dentre as quais destacamos: tratamentos de saúde em clínicas e pronto atendimento emergencial, assistência continuada em tratamento específico e em pesquisa e desenvolvimento de novos produtos.

Em diversas ocasiões no atendimento de uma pessoa no segmento de saúde, surge a necessidade de processamento de seus dados, sendo essa necessidade fato inerente a atividade. A impossibilidade desse tratamento, causaria enorme impacto negativo, senão a inviabilidade de operação.

No segmento de saúde, fatores como a dificuldade em modificar processos e hábitos culturais, a dificuldade de compreensão por parte dos pacientes e clientes, quanto ao conteúdo dos documentos que eles devem assinar, autorizando a coleta e o processamento de dados, trouxeram maior dificuldade na operação cotidiana.

Entendemos que não devemos questionar a validade da LGPD, mas tratar a dificuldades de sua aplicabilidade, uma vez que entendemos que a médio e longo prazos, a existência de regulamentação na operacionalização da captura e tratamento de dados serão benéficos para a ciência de dados.

REFERÊNCIAS

FONTES, EDISON. Política e Normas para a Segurança da Informação: Como desenvolver; implantar e manter regulamento para a proteção da informação nas organizações. Rio de Janeiro: Brasport, 2012.

BIONI, BRUNO RICARDO. Proteção de dados pessoais: a função e os limites do consentimento. 1 ed. Rio de Janeiro: Forense, 2019.

LGPD na Saúde / coordenação Analluza Bolivar Dallari, Gustavo Ferraz de Campos Monaco. 1 ed. São Paulo: Thomson Reuters Brasil, 2021.

PINHEIRO, PATRCIA PECK. Proteção de Dados Pessoais: comentários a Lei nº 13.709/2018 (LGPD). 1 ed. São Paulo: Saraiva Educação, 2018.

Código de Ética Médica: Resolução CFM nº 2.217, de 27 de setembro de 2018, modificada pela Resoluções CFM nº 2.222/2018 e 2.226/2019 / Conselho Federal de Medicina – Brasília: Conselho Federal de Medicina.

Brasil. Lei nº 13.709, de 14 de agosto de 2018. Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Diário Oficial da República Federativa do Brasil, Brasília, DF, 15 ago., 2018, Seção 1.