A PROFISSÕES DA SAÚDE E O TRATAMENTO DOS DADOS PESSOAIS: BOAS PRÁTICAS E A CONFORMIDADE

THE HEALTH PROFESSIONS AND THE PROCESSING OF PERSONAL DATA: GOOD PRACTICES AND COMPLIANCE

Claudio Joel Brito Lóssio[1]

Resumo: Diante do transformar de nossa sociedade, novos padrões de segurança e privacidade deverão serem adotados, nesse caso, voltado ao espaço cibernético, onde os dados e as informações são de suma importância para sua existência. Cada vez mais as profissões se misturam com o direito e com a tecnologia, e na área da saúde não é diferente, inclusive quando se trata de lei de proteção de dados, pois essa não é uma tarefa para o TI, advogado, é para o DPO – Data Protection Officer, também conhecido como encarregado de proteção de dados. O profissional poderá alegar o desconhecimento do direito à proteção de dados dos titulares? Ambientes médicos, assim como os profissionais e seus auxiliares deverão com celeridade buscar aprimorar seus processos de segurança da informação e Compliance para que a proteção de dados seja garantida, visto que a privacidade é um Direito Fundamental. O aprimoramento não está relacionado exclusivamente a seara dos técnicos de informática, mas aos funcionários, aos profissionais da saúde, aos ambientes de saúde tanto públicos quanto privados, também não apenas na área digital, mas também no ambiente físico.

Palavras-Chave: Proteção de Dados; Saúde; Responsabilidade; LGPD; Médicos;

***Abstract**: In view of the transformation of our society, new standards of security and privacy must be adopted, in this case, aimed at cyber space, where data and information are of paramount importance for its existence. More and more professions are mixed with law and technology, and in the area of health is no different, even when it comes to data protection law, as this is not a task for IT, lawyer, it is for the DPO - Data Protection Officer, also known as data protection officer. Will the professional be able to claim ignorance of the data subjects' right to data protection? Medical environments, as well as professionals and their assistants should quickly seek to improve their information security and compliance processes so that data protection is guaranteed, since privacy is a fundamental right. The improvement is not related exclusively to the field of computer technicians, but to employees, health professionals, health environments, both public and private, also not only in the digital area, but also in the physical environment.*

***Keywords**: Data protection; Cheers; Responsibility; GDPR; Doctors;*

1- Professor, Palestrante, CEO SNR Sistemas Notariais e Registrais – empresa premiada pelo GPTW – *Great Place to Work* em 2019 e 2020, Sênior Software Dev, Doutorando em Ciências Jurídicas pela UAL - Portugal, Mestrando em Engenharia de Segurança Informática pelo IPBeja - Portugal. Advogado com Pós-Graduação em Direito Digital e Compliance, Direito Penal e Criminologia, Direito Notarial e Registral, MBA em Gestão de TI, Certificado DPO pela Universidade de Nebrija, Membro Pesquisador Lab UbiNET em Cloud Forensics e Segurança Ofensiva. Professor visitante na EJET-TJGM. Organizador e autor da obra Cibernética Jurídica: estudos sobre o direito digital pela EDUEPB, Autor de diversos artigos científicos e capítulos de livro. Email: claudiojoel@juscibernetica.com.br

INTRODUÇÃO

Diante do transformar de nossa sociedade, novos padrões de segurança e privacidade deverão serem adotados, nesse caso, voltado ao espaço cibernético, onde os dados e as informações são de suma importância para sua existência.

Cada vez mais as profissões se misturam com o direito e com a tecnologia, e na área da saúde não é diferente, inclusive quando se trata de lei de proteção de dados, pois essa não é uma tarefa para o TI, advogado, é para o DPO – Data Protection Officer, também conhecido como encarregado de proteção de dados.

O profissional poderá alegar o desconhecimento do direito à proteção de dados dos titulares? Ambientes médicos, assim como os profissionais e seus auxiliares deverão com celeridade buscar aprimorar seus processos de segurança da informação e Compliance para que a proteção de dados seja garantida, visto que a privacidade é um Direito Fundamental.

O aprimoramento não está relacionado exclusivamente a seara dos técnicos de informática, mas aos funcionários, aos profissionais da saúde, aos ambientes de saúde tanto públicos quanto privados, também não apenas na área digital, mas também no ambiente físico.

1. A SOCIEDADE DIGITAL

A indústria 4.0 é a qual estamos vivendo agora, vem transformando nossa atual sociedade criando um modelo social, a sociedade digital. Nesse novo cenário, o tempo é completamente diferente da sociedade real, ou é rápido demais, ou demora muito, ou é até mesmo, inesquecível.[2]

Um ato ou uma palavra tem muito mais força diante dos novos meios de comunicação do espaço cibernético. Muitos nasceram sem o contato com a tecnologia, e com o passar dos anos, foram se adequando, mesmo assim, as pessoas precisam se adequar cada vez mais ao espaço cibernético. Essas tecnologias proporcionadas pelo computador e a internet, institutos os quais são o berço desta nova revolução industrial.[3]

Esse novo modelo social condiciona as pessoas a uma permanente reabilitação, com base em treinamentos rotineiros para proporcionar uma maior cognição entre os usuários e essas novas tecnologias. Não diferente para os profissionais da saúde, sejam esses pessoas físicas como médicos, enfermeiros, farmacêuticos, operadores, técnicos, recepcionistas, sejam esses, pessoas jurídicas, como clínicas, hospitais, laboratórios, e empresas prestadoras de serviços na seara da tecnologia, sejam direcionados aos computadores, aos equipamentos, redes, cloud computing, etc. Sendo necessitando uma reinvenção do padrão operacional, com base no conhecimento não só nas legislações de proteção de dados, mas também no Direito Digital.

Diante deste cenário, a implementação da conformidade de tratamento dos dados pessoais nas profissões da saúde é fundamental para que sanções sejam mitigadas e os titulares dos dados tenha essa tutela assegurada.

2- SHWAB, Klaus – **A Quarta Revolução Industrial**. Ed. 1. São Paulo: Edipro, 2016. ISBN 978-85-7283-978-5.

3- CASTELLS, Manuel – **A Galáxia da Internet**: Reflexões sobre a Internet, os negócios e a sociedade; Tradução Maria Luiza X. de A. Borges. Rio de Janeiro: Zahar, 2003. ISBN: 978-85-7110-740-3.

2. OS DADOS NA SAÚDE

Os dados agora são o petróleo do mundo, em tempos de Big Data, todas as pessoas e empresas vivem buscando a segurança da informação, proteção dos dados e a privacidade com base em suas informações digitais, seja em seu computador, smartphone, servidores PACS, sistemas HIS / RIS, todo local onde possa armazenar dados pessoais, estejam esses em empresas privadas ou públicas.

Em busca de garantir a segurança e a privacidade das pessoas, a Lei 13.709, foi publicada em 14 de agosto de 2018, e entrará em vigor 18 meses de sua publicação. Pouco tempo que as empresas e pessoas se ajustem para tal legislação. O Regulamento Geral de Proteção de Dados da Europa foi publicado em 2016 entrando em vigor 2 anos depois, e mesmo a Europa tendo uma Directiva de proteção de dados desde 1995, ainda assim várias empresas e pessoas que tratam com dados pessoais estão irregulares pagando multas altíssimas devido a procrastinação.[4]

A falta de conformidade na busca ou aplicação de normas de segurança da informação, de leis de proteção de dados, de gestão de TI, e no Compliance digital pode determinar forte penalidades para os proprietários, sua equipe, assim como os prestadores de serviço nesta área. Sendo essa conformidade um fator determinante para os profissionais da saúde manterem seus empreendimentos e a proteção de sua profissão. O conhecimento nestas searas será não mais um conhecimento opcional para essa classe de profissionais, assim como para as demais profissões que manuseiam dados sensíveis.

Não só visando a regulação ou aplicação, mas focando também na busca pela conformidade digital diante dos profissionais e estabelecimentos voltados a saúde, tanto em pessoas físicas quanto jurídicas, poderá evitar um excesso de exposição e de insegurança na proteção dos equipamentos que guardam esses dados, sejam computadores, smartphones e equipamentos hospitalares, e consequentemente dificultando a perda, alteração ou roubo dessas informações digitais, devido a imperícia, imprudência ou negligência deste que nestas laboram.

O usuário, independentemente de função e titulação, é a principal ferramenta de proteção dos dados armazenados em seus dispositivos, sejam próprios ou da instituição onde presta serviço. As atitudes desses usuários, normalmente vem junto de pouco conhecimento de proteção no ambiente cibernético como também não vem seguindo as políticas de Compliance da instituição onde trabalha, sendo o principal quesito para aplicação de treinamentos de proteção de dados, *Compliance* Digital, HIPPA, segurança da informação e Direito Digital, promovendo assim, segurança e privacidade.

Os dispositivos cibernéticos com informações ficam expostos devido a práticas maliciosas de engenharia social, pelo uso inadequado das tecnologias e a outros métodos de invasão dos Crackers, assim fazendo com que dados privados caiam nas mãos de terceiros não autorizados. Apenas com uma nova modelagem de educação nas escolas e um novo padrão de gestão com base na conformidade e na evolução da responsabilidade, poderá reduzir para as futuras gerações esses métodos atuais de invasão, assim combatendo as violações e vazamento de dados, consequentemente, o Cibercrime.

Enquanto esse fator educativo *by Design* não ocorre, os treinamentos direcionados a instituição é o que poderá promover não só a segurança e privacidade no espaço laboral da saúde, mas também uma regulação e aplicação adequada do Direito Digital, visto que quanto maior a antecipação, maior o senso crítico dos profissionais da saúde.

4- **REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO**, de 27 de abril de 2016. [Em Linha]. Acessado em: 29 set. 2017. Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

3. A LEI DE PROTEÇÃO DE DADOS NA SAÚDE

A LINDB – Lei de Introdução ao Estudo do Direito[5], é um diploma legal norteador para todos, e traz em seu artigo 3º, "Ninguém se escusa de cumprir a lei, alegando que não a conhece.", com isso fica claro que ninguém pode alegar desconhecimento da lei, mesmo o nosso país possuindo várias leis e ainda sendo publicadas novas diariamente.

Ainda assim, a LGPD – Lei Geral de Proteção de Dados, Lei 13.709/2018, traz em seu texto a necessidade de adequação de toda pessoa física ou jurídica seja pública ou privada que efetuem tratamento de dados digitais ou físicos:[6]

> Art. 1º 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.

Assim o consultório, hospital ou clínica que possua sistema eletrônico ou fichas em papel deverão se adequar a tal normativo legal, seguindo o proposto pelo artigo 50, boas práticas de governança. Principalmente por se tratar de dados sensíveis segundo a lei, fato que torna a necessidade de segurança ainda maior, segundo o Artigo 5:[7]

> Art. 5º Para os fins desta Lei, considera-se:
>
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
>
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, 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; (grifo nosso)

Os agentes de tratamento, que são os controladores e os operadores, nesse caso, o proprietário da clínica, gestor, supervisor e todas as demais dessoas que efetuam o tratamento de dados, respectivamente. Mas o que é o tratamento de dados? Veja o que está presente no artigo 5º. X: [8]

> X - tratamento: toda operação realizada com 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;

Lembrando que a tarefa de adequação não é algo que deve ser direcionado ao TI, advogado ou gestor, deve ser direcionado ao DPO – *Data Protection Office*, também conhecido como encarregado de proteção de dados, o qual poderá executar toda a tarefa em conjunto ou não.

O que é necessário para a realização do tratamento de dados em conformidade com o diploma de proteção de dados, pode ser encontrado nos artigos 46, veja:

5- BRASIL. Declreto-Lei 4.657/1942, de 4 de setembro. **Lei de Introdução ao Estudo do Direito**. 1942. Acessado em: 12 de julho de 2020. Disponível em:<http://www.planalto.gov.br/ccivil_03/decreto-lei/del4657compilado.htm>

6- BRASIL. Lei 13.709/2018, de14 de agosto. **Lei Geral de Proteção de Dados Pessoais** (LGPD). 2018. Acessado em: 12 de julho de 2020. Disponível em:<http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>

7- Idem – Ibidem.

8- Idem – Ibidem.

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

O qual traz em seu caput, que os agentes de tratamento devem implementar políticas de conformidade, controles internos, reestruturação dos processos para que o acesso por terceiros não autorizados não ocorra, assim como qualquer outra forma ilícita relacionada aos dados. Já no Artigo 50:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Pode ser percebido que a busca pelas boas práticas de governança é um passo fundamental, e nesse artigo da Lei de proteção de dados, e essas boas práticas podem ser distribuídas em alguns tópicos:

- Formular Regras;
- Estabelecer condicionantes;
- Estabelecer regime de funcionamento;
- Estabelecer procedimentos;
- Canal de comunicação para as reclamações e petições de titulares;
- Implementar normas de segurança;
- Seguir padrões técnicos;
- Obrigações diversas aos envolvidos no tratamento;
- Treinamentos através de ações educativas;
- Monitoramento através de mecanismos internos de supervisão;
- Implementar gestão de riscos para que sejam mitigados;
- Entre outros;

Esses pontos foram elencados para que a Lei 13.787 possa ser apresentada, visto que para a conformidade dela, é necessária primeiramente a implementação da Lei 13.709, LGPD no estabelecimento.

Os artigos primeiro e segundo deste diploma que traz em seu preâmbulo: "Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente.":

> Art. 1º A digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente são regidas por esta Lei e pela **Lei nº 13.709, de 14 de agosto de 2018**.[9]
>
> Art. 2º O processo de digitalização de prontuário de paciente será realizado de forma **a assegurar a integridade, a autenticidade e a confidencialidade** do documento digital. (grifo nosso)

9- BRASIL. LEI Nº 13.787, DE 27 DE DEZEMBRO DE 2018. Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. 2018. Acessado em : 22 de fev. 2020. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13787.htm>

Assim, o prontuário digitalizado deverá estar em conformidade com a Lei de proteção de Dados pessoais, com a Lei 13.787, visto que contudo são complementares pois qualquer desses diplomas legais tutelam de forma geral a relação dos princípios da segurança informação diante das liberdades, direitos e garantias fundamentais individuais de seus titulares.

O conhecimento da lei pelos controladores e operadores é essencial para que seja mitigado ao máximo qualquer forma de vazamento e/ou violação de dados, seja intencional ou não. O processo de implementação ocorre através da alteração da cultura de todos gerando uma consciência protetiva quando se trata de dados. As sanções administrativas deste diploma legal estão elencadas no Artigo 52:[10]

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
>
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
>
> III - multa diária, observado o limite total a que se refere o inciso II;

A visão que o controlador deve ter nesse momento não é de medo das sanções legais, mas sim de mostrar que o seu empreendimento promove segurança aos dados dos pacientes, agregado valor e credibilidade social, até porque tais sanções poderão ser apenas advertências caso o estabelecimento comprove que possui toda adequação à LGPD mas ainda assim ocorreu o incidente de segurança da informação. Observe o texto da lei adiante do também artigo 52:[11]

> § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
>
> II - a boa-fé do infrator;
>
> IX - a adoção de política de boas práticas e governança;
>
> X - a pronta adoção de medidas corretivas; e

Segundo o exposto, a busca pelo controlador e seguida pelos operadores diante a implementação da conformidade à Lei de Proteção de Dados é um ato essencial para que exista uma minimização dos riscos diante do vazamento e/ou violação de dados.

4. CONSIDERAÇÕES FINAIS

Diante do transformar de nossa sociedade, novos padrões de segurança e privacidade deverão serem adotados, nesse caso, voltado ao espaço cibernético, onde os dados e as informações são de suma importância para sua existência.

Ambientes médicos, assim como também, os profissionais, técnicos, auxiliares, gestores e operadores deverão com celeridade buscar aprimorar seus processos de segurança da informação e Compliance Digital para que a proteção de dados seja garantida, visto que a privacidade é um Direito Fundamental, principalmente quando se trata de dados médicos, os quais são denominados dados sensíveis.

10- BRASIL. Lei 13.709/2018, de14 de agosto. **Lei Geral de Proteção de Dados Pessoais** (LGPD). – Ibidem.

11- Idem – Ibidem.

O aprimoramento não está relacionado exclusivamente a seara dos técnicos de informática ou jurídico, mas também a todos os colaboradores da saúde, independentemente de seu cargo, seja tanto em ambientes de saúde públicos quanto privados. Cabe perceber que a reinvenção dos processos com base na privacidade e proteção de dados não está relacionado apenas a área digital, mas também no ambiente físico e nas pessoas, com treinamentos voltados as boas práticas.

Diante de um cenário cada vez mais digital, o prontuário digitalizado deverá estar em conformidade com a Lei de proteção de Dados pessoais, com a Lei 13.787, visto que contudo são complementares pois qualquer desses diplomas legais tutelam de forma geral a relação dos princípios da segurança informação diante das liberdades, direitos e garantias fundamentais individuais de seus titulares.

Assim, fica transparente que a adequação é algo que deve ocorrer não só os estabelecimentos médicos, mas em todos que realizam o tratamento de dados. E é muito importante ver isso não como uma penalidade, mas como um investimento pela tutela dos titulares e credibilidade diante do valor agregado pela proteção dos dados dos pacientes.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Decreto-Lei 4.657/1942, de 4 de setembro. **Lei de Introdução ao Estudo do Direito**. 1942. Acessado em: 12 de julho de 2020. Disponível em:<http://www.planalto.gov.br/ccivil_03/decreto-lei/del4657compilado.htm>

BRASIL. Lei 13.709/2018, de14 de agosto. **Lei Geral de Proteção de Dados Pessoais** (LGPD). 2018. Acessado em: 12 de julho de 2020. Disponível em:<http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>

BRASIL. Lei Nº 13.787, De 27 De Dezembro De 2018. **Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente.** 2018. Acessado em : 22 de fev. 2020. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13787.htm>

CASTELLS, Manuel – **A Galáxia da Internet**: Reflexões sobre a Internet, os negócios e a sociedade; Tradução Maria Luiza X. de A. Borges. Rio de Janeiro: Zahar, 2003. ISBN: 978-85-7110-740-3.

NAÇÕES Unidas – **Carta das Nações Unidas**. 1945. [Em linha]. [Consult. 29 set. 2018]. Disponível em <https://nacoesunidas.org/wp-content/uploads/2017/11/A-Carta-das-Na%C3%A7%C3%B5es-Unidas.pdf>

REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO, de 27 de abril de 2016. [Em Linha]. Acessado em: 29 set. 2017. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>

SHWAB, Klaus. **A Quarta Revolução Industrial**. Ed. 1. São Paulo: Edipro, 2016.