SAÚDE, TELEMEDICINA, SAÚDE PÚBLICA E DIREITOS DIGITAIS[11]

Cláudia Ruiz Hespanha[12]

Resumo

O presente artigo discute a interseção entre saúde, telemedicina, saúde pública e direitos digitais, com ênfase na aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) no contexto dos serviços de saúde. Parte-se da compreensão constitucional do direito à privacidade e sua evolução normativa, passando pelo Marco Civil da Internet até a consolidação da LGPD, que estabelece regras específicas para o tratamento de dados pessoais. O texto analisa conceitos fundamentais da LGPD, destacando a centralidade do consentimento do titular e a necessidade de finalidade, adequação, necessidade e segurança no tratamento das informações. Na área da saúde, o vazamento de dados sensíveis pode gerar danos morais, reputacionais e discriminatórios, sendo considerado de alta gravidade pela legislação. Casos emblemáticos, como megavazamentos de dados e o uso indevido de informações por empresas e algoritmos, evidenciam os riscos de manipulação, discriminação e decisões automatizadas baseadas em dados imprecisos. O artigo também aborda a responsabilidade dos agentes de tratamento (titular, controlador, operador e encarregado), ressaltando a importância da governança, do *compliance* e da adoção de medidas técnicas e administrativas de segurança. No contexto da telemedicina e da telessaúde, regulamentadas por normas específicas, reforça-se a obrigatoriedade do Termo de Consentimento Livre e Esclarecido (TCLE), da proteção de prontuários físicos e digitais, da limitação temporal de armazenamento e da adequada eliminação de dados. Além disso, discute-se o impacto da LGPD na prática clínica, na gestão de recursos humanos, na pesquisa científica e na formação acadêmica em saúde, enfatizando a necessidade de anonimização em estudos e do consentimento específico para compartilhamento de informações. Conclui-se que a proteção de dados na saúde não é apenas uma exigência legal, mas um imperativo ético vinculado à dignidade da pessoa humana, à autonomia do paciente e à confiança na relação profissional.

Palavras-chave: LGPD; telemedicina; proteção de dados.

Estudar direito é matéria mandatória em todas as profissões. Hoje, mais do que nunca, na área da saúde, nós nos vimos forçados a ter determinadas condutas, pois nos

[11] Texto adaptado da palestra homônima, integrante da Semana de Responsabilidade Social de 2025, do Centro Universitário Padre Anchieta (UniAnchieta), cuja gravação em vídeo está disponível em: https://www.youtube.com/watch?v=nAcTXKeq5p0. A palestra foi mediada pelo prof. Humberto Moreira Spindola e pela aluna Mariana Fornazari de Lima.

[12] Docente do UniAnchieta. Possui MBA em Marketing pela Fundação Getúlio Vargas (FGV), pós-graduação em Direito Penal Econômico pela PUC, pós-graduação em Direito Digital pela Unyleya e pós-graduação em Direito Tributário e Aduaneiro. Graduada em Comunicação Social – Relações Públicas pela FIAM e em Direito pelo UniAnchieta.

vimos imersos pela Lei Geral de Proteção de Dados (LGPD) durante a pandemia, com novas regras e comportamentos.

Para começarmos a entender por que a LGPD existe, é necessário compreender por que precisamos proteger a nossa privacidade. Segundo o *Dicionário de Oxford*, privacidade significa "vida privada, vida particular, vida íntima". Mas o que é privacidade para mim pode não ser o mesmo que para o outro. Por exemplo, para uma pessoa famosa, tanto faz expor sua vida nas redes sociais, porque, para ela, a privacidade pouco importa. Já para uma pessoa mais recatada, privacidade é tudo. Então, a LGPD veio para trazer uma normativa, uma regra.

Se eu não quero que alguém tenha acesso a alguma informação minha, aquilo que considero privado, tenho que ter o direito de proteger aquela informação. A nossa Constituição de 1988 já falava em privacidade, afirmando que são invioláveis a intimidade e a vida privada, sendo que a casa é o asilo inviolável do indivíduo. Ela também diz que é inviolável o sigilo da correspondência. Já com essa ideia de privacidade e de confidencialidade, entramos no conhecimento de informação relativa à pessoa do impetrante. Nesse ponto, fala-se de *habeas data*, que é uma matéria específica da área jurídica. Além disso, a lei já fala em retificação de dados, em informações da pessoa, e é onde já começamos a ter um pequeno raciocínio sobre como isso se aplica hoje.

Em 2014, surgiu o Marco Civil da Internet (Lei nº 12.965), através de vários fatores que aconteceram no mundo, regulamentando como nossas condutas seriam consideradas em um ambiente virtual. Naquele momento, ele já previu a proteção da privacidade, mais uma vez, reforçando o texto constitucional, a inviolabilidade da intimidade e da vida privada, a inviolabilidade das comunicações privadas, a garantia de direito à privacidade, a inviolabilidade das comunicações e, por fim, a guarda e a disponibilização dos registros de conexão.

Assim, o Marco nos deu um norte de como nos comportaríamos em ambiente cibernético. Em seguida, veio a proteção dos dados com a LGPD. Os dados são o conhecimento que se tem sobre algo, usados para solucionar uma questão, fazer um julgamento, criar ou colocar em prática um pensamento, uma opinião ou uma informação. Existem dados identificados, dados identificáveis, titular do dado, dados sensíveis e dados anonimizados.

Um nome, por exemplo, é um dado identificado. O rosto e as digitais são dados que identificam alguém enquanto pessoa. Os dados identificáveis, portanto, são informações que, quando somadas, chegam a um indivíduo, como, por exemplo, o CPF, pois, se buscarmos um CPF e uma data de nascimento no portal da Receita Federal, chegamos a um indivíduo. O titular do dado é o dono daquela informação. São dados pessoais identificáveis: dados cadastrais, como nome, CPF, e-mail e telefone; dados de GPS; informações eletrônicas, como endereço de IP.

Com os dados sensíveis, entramos na área da saúde. Um dado sensível é aquele que é capaz de discriminar um indivíduo, partido político, religião ou um dado de saúde. Ele é considerado um dado sensível porque informa que aquele indivíduo é "diferente dos demais". Um exemplo é uma indústria que produz material cosmético para pessoas de pele negra, que, então, precisa ter essa informação no seu banco de dados, para poder se comunicar com determinada consumidora para vender seus produtos.

Essa informação de raça é considerada sensível porque pode vir a segregar, excluindo essa pessoa de um grupo social. A religião também pode ser considerada uma informação que pode segregar as pessoas, bem como um partido político. Atualmente, vivemos um cenário polarizado, então, todas essas informações são consideradas sensíveis. Assim, são dados pessoais sensíveis: filiação à organização religiosa, política ou filosófica; dados biométricos ou genéticos; dados de saúde ou vida sexual.

Em relação a um dado vazado de uma pessoa portadora de uma doença, há um exemplo que ocorreu na prefeitura de Barueri. Nessa ocasião, através do departamento pessoal, foi vazado que um funcionário da prefeitura era portador do vírus HIV. Como que um dado tão importante, tão sigiloso, que afastaria aquele indivíduo dos colegas no ambiente de trabalho, foi vazando? Qual é o prejuízo que causa para essa pessoa? Esse dado sensível e extremamente delicado não poderia ter vazado. E é isso que a lei protege. O direito do indivíduo, titular do dado, é que aquela informação seja tratada em caráter de sigilo. Aquela informação só pode ser passada adiante se o titular do dado autorizar.

Dados anonimizados é como devemos tratar esses dados, de uma forma que quem lê não entenda e não consiga identificar de quem se está falando. Um exemplo é divulgar as notas por meio do RA, para que os demais alunos não consigam identificar de quem são todas as notas. Isso se aplica a qualquer pessoa física ou jurídica de direito

público ou privado, sejam dados em caráter físico ou em caráter digital, a qualquer pessoa que detém, trata, manipula e está conectada a dados.

Todos que realizam tratamento devem ter seus dados protegidos, ou seja, há a responsabilidade de proteção de atividades em que se utiliza dado pessoal como coleta, armazenamento, compartilhamento e exclusão, inclusive nos meios digitais. Entretanto, quando eram documentos impressos, era mais fácil lidar com essas informações, podendo, por exemplo, passar em uma desfragmentadora, picar em milhares de pedacinhos, ou queimar, destruindo aquilo.

O problema é como eliminar um arquivo presente em uma esfera digital. Como se protege um sistema em uma esfera digital? É necessário criptografar, colocar senha ou proteger de alguma outra forma contra-ataques e vazamentos. E é aqui que mora, muitas vezes, a situação problema, pois as pessoas não sabem que elas facilmente, pelo próprio Windows, podem proteger as pastas e os arquivos.

As regras são mais rígidas, com maiores sanções e "punições", quando os dados sensíveis são vazados. A diferença entre ter um CPF vazado e um dado de saúde vazado é que o prejuízo, além de ser moral, é reputacional. Quando uma pessoa tem uma informação sensível vazada, principalmente na área de saúde, é como se ela tivesse a vida totalmente invadida; ela não consegue mais se encaixar no meio, sofrendo preconceito.

No caso do funcionário da Prefeitura de Barueri, que recebeu uma indenização muito pequena pelo tamanho do estrago que sofreu, é possível imaginar como é que ele vai conviver naquele ambiente e continuar trabalhando. Se estabelece uma situação muito delicada. Então, quando há um dado de saúde vazado, a pessoa recebe uma sanção muito maior do que se simplesmente o CPF tivesse sido vazado. Vazar um CPF tem uma gravidade, mas não tão grande quanto uma informação médica. São exemplos de dados sensíveis: relação entre usuários e serviços de internet; relação entre empresas e clientes; relações trabalhistas; relações entre médicos hospitais, laboratórios e pacientes. Dados sensíveis são negócios mesmo que off-line, quando preenchemos aquelas fichas cadastrais.

Quando vamos à farmácia, muitas vezes, ao passarmos no caixa, a primeira coisa que falam é sobre o CPF. Mas para quê? Para o desconto? Eles não querem saber se você quer o desconto, nem se quer fornecer o seu CPF. Eles também não informam o

que vão fazer com o seu CPF. Entretanto, as farmácias conectam o seu CPF ao medicamento que você está comprando, criando como se fosse um “avatar”, uma persona virtual, para saber que você está conectado àquela medicação, criando um registro sobre determinada doença.

Se você começa a comprar determinado medicamento com uma certa frequência, a farmácia cria um raciocínio de que você já tem aquela doença. Então, se a pessoa vai fazer 60 anos, seu convênio médico vai ficar mais caro. O convênio médico, de posse dessa informação, não quer saber se eu estou comprando para o meu pai no meu CPF; ele criou um rótulo e está dizendo que aquele medicamento implica que eu tenho aquela doença, logo, o convênio ficará mais caro.

Assim, eles vão criando personagens, fazendo conclusões sobre a pessoa com informações dadas, sendo que a empresa que está coletando não está dando nenhuma proteção sobre o dado coletado. Eu não sei o que eles estão fazendo com esses dados. Eu não sei por que eu estou dando esses dados. Eu não dei a permissão de que eles tenham posse desses dados.

A partir daí, já começamos a construir um raciocínio. Por que as empresas e as pessoas físicas precisam dos dados? Quando se fala de telemedicina, é necessário ter as informações básicas, para poder ter um atendimento de acordo. Dessa forma, a primeira palavra de ordem é consentimento. É preciso que o paciente dê um consentimento daquelas informações, para que, de posse dessas informações, possa ser feito o atendimento correto. Somente nessa relação de consentimento que se pode dar o atendimento.

Em seu TED Talk, Bruno Bioni explica que essa proteção dos dados é justamente porque deixamos rastros em tudo o que fazemos. E quando deixamos um rastro digital, fornecemos informações que podem não ser reais. Podem ser informações como, por exemplo, uma pessoa comprando um medicamento em seu CPF, mas para outra pessoa. E as empresas estão coletando dados que não são reais, criando uma informação que não é verídica sobre a pessoa.

A LGPD também prevê isso: a forma com que se tem o direito de ter os dados reais e verídicos gravados nos seus bancos de dados, ou seja, a realidade sobre a pessoa, assim como a revogação dos seus dados. Se eu não quero mais que você tenha informações sobre a minha pessoa, tenho o direito de remover essas informações do

seu banco de dados. Eu tenho o direito de não fornecer as informações, porque as informações são minhas. Tudo isso, a LGPD oferece, hoje, como um direito garantido.

O caso da *Cambridge Analytica* foi bem emblemático sobre o vazamento de informações pessoais, envolvendo aqueles testes bobinhos que se fazia no Facebook, como "Se você fosse um homem, com que ator você se pareceria?". Ao responder esses testes, o *Facebook* capturava os dados da pessoa e dos amigos dela. Aqueles dados foram vazados, e a *Cambridge Analytica* montou um banco de dados imenso. Esse foi um escândalo mundial, no qual houve uma deflagrada manipulação de eleições, principalmente das americanas.

A proteção de dados importa porque, quanto mais eu sei sobre você, mais eu posso te manipular. Se eu sei que você tem uma preferência pelo partido ou pela ideologia política X, eu vou favorecer publicações nas redes sociais e na internet de uma forma que você aprecie, deixando de lado publicações que você não aprecia. Por outro lado, deseja-se pegar o indeciso, para saber o que lhe preocupa e, assim, bombardeá-lo de informações que façam com que ele se decida em favor do meu candidato.

Então, os dados, principalmente nesse caso da *Cambridge Analytica*, são uma forma de manipulação. É por isso que proteger dados importa, e importa muito. Quanto mais eu sei sobre um indivíduo, mais eu consigo manipulá-lo e classificá-lo. Mas será que aquelas informações que eu tenho sobre aquele indivíduo são fidedignas? É uma dignidade humana ter uma informação real e adequada minha.

Houve um megavazamento de dados em 2021, com 223 milhões de brasileiros afetados, envolvendo fotos, *score* de créditos, dados de imposto de renda, escolaridade, volume de benefícios do INSS e informações do *LinkedIn*. Inclusive, o *LinkedIn* vem sofrendo vários vazamentos ao longo dos anos. Então, a responsabilidade de quem tem essas informações armazenadas em seus bancos de dados é enorme.

Outra razão da existência da LGPD é o caso das decisões automatizadas e o princípio da não discriminação. Um exemplo é o caso da Brisha Borden e do Vernon Prater. Brisha foi uma menor infratora que cometeu alguns crimes enquanto era adolescente, roubando uma bicicleta para circular pelo bairro. Já Vernon fez alguns assaltos à mão armada. Incluíram a foto dos dois em uma inteligência artificial e pediram para que fosse feita uma previsão sobre qual deles cometeria mais crimes no futuro. A resposta foi que Brisha voltaria a delinquir e Vernon não. Entretanto, essa conclusão da

inteligência artificial foi totalmente equivocada, porque Brisha nunca mais delinquiu, enquanto Vernon cometeu um crime muito maior anos depois. Vernon era branco; Brisha era negra.

A própria máquina aprendeu a discriminar com as informações equivocadas fornecidas do bairro onde Brisha morava, a raça dela e a escola onde ela estudava. Então, ela tirou uma conclusão baseada em informações falsas, não dignas. Ela tirou uma conclusão baseada num dado sem qualidade.

Toda operação realizada com dados pessoais envolve um ciclo completo que abrange desde a coleta, produção e recepção até a classificação, utilização, acesso, reprodução e transmissão. Isso inclui também a distribuição, o processamento, o arquivamento e o armazenamento das informações. No entanto, o ponto mais complexo de toda essa cadeia é a eliminação.

Muitos sabem como coletar dados, mas poucos compreendem o perigo de eliminá-los incorretamente, pois, muitas vezes, é possível resgatá-los. Um exemplo ocorre quando alguém decide trocar uma impressora antiga, que já não funciona bem, e opta por descartá-la no lixo ou doá-la para uma instituição de caridade. O que a maioria das pessoas ignora, por falta de conhecimento técnico, é que os dados permanecem no equipamento e podem ser recuperados. Além desses processos, a gestão de dados envolve a avaliação ou controle da informação, sua modificação, comunicação, transferência, difusão e extração.

Existem exceções, mas são poucas: fins jornalísticos, artísticos, acadêmicos, segurança pública, defesa nacional, segurança do Estado, atividade de investigação ou repressão de infrações penais, tratamentos realizados por pessoa natural para fins particulares e não comerciais. Para fins de pesquisa, a palavra-chave sempre é consentimento. É necessário ter de forma expressa a manifestação de consentimento da pessoa, seja por um documento escrito, físico ou digital.

Os envolvidos em todos esses processos são o titular dos dados, o controlador, o operador, o *data protection officer* (DPO) e a Autoridade Nacional de Proteção de Dados (ANPD). O titular dos dados é o dono das informações, dos dados. O controlador é quem toma as decisões sobre o tratamento dos dados. Então, em um consultório, o médico é o controlador, porque é ele quem vai tomar as decisões, informando o que fazer com aqueles dados.

Dessa forma, se o paciente entra em contato com o consultório para agendar uma consulta, a secretária vai coletar os dados básicos, como nome, se é convênio ou particular e telefone para contato, e agendar consulta. Quem terá acesso ao restante das informações, as sensíveis, será o médico, que as arquivará em um sistema. Se a secretária tiver acesso a essas informações, ela se tornará a operadora. O secretário é o responsável por buscar a ficha do paciente quando solicitado pelo titular ou pelo controlador. O operador é quem realiza o tratamento dos dados pessoais em nome do controlador. Logo, ele também se torna responsável, em algum momento, pelo processo. No caso de um vazamento de um dado médico, pouco importa se o dado é digital ou físico.

O DPO é o oficial de proteção de dados ou encarregado de proteção de dados. Ele é a pessoa indicada para atuar na interface, na comunicação entre o controlador e a ANPD. Essa autoridade é um organismo instituído justamente para controlar essa questão e a aplicabilidade da lei. O DPO muitas vezes é o próprio operador ou o próprio controlador, pois pode se tratar de um profissional liberal, que não tem vários personagens para colocar dentro de sua estrutura profissional. É o DPO quem notifica a autoridade. E ele é obrigado a notificar quando há um vazamento, além de informar o titular.

No ambiente de saúde, é preciso analisar qual é o fluxo da comunicação e dos dados. Quais são os dados que são coletados em primeiro lugar? Aonde vão ser armazenados esses dados? É o momento de encaminhar um termo de consentimento? É necessário haver documentação para consentimento e se precaver antes da realização da consulta, informando quem vai ter acesso ao conteúdo da consulta, como os dados serão protegidos e se é possível colocar senha.

De acordo com as bases legais, é preciso responder às seguintes perguntas: Quem? Quando? Como? Onde? Por quê? O quê? Quando? A lei aplica-se a qualquer operação de tratamento. Do lado profissional, cria-se um roteiro, um fluxo de informação. A prevenção sempre é a melhor coisa. Então, deve-se ter um momento de parar para pensar sobre qual é o fluxo dos dados, como esses dados entrarão no meu ambiente de trabalho e se é necessário proteger todo o caminho. É importante pensar também em como tudo isso será feito, instrumentalizar, documentar e criar um roteiro.

O roteiro pode ser feito no papel ou digitalmente, mas verbalmente não é algo indicado. É importante criar técnicas para isso, além de propostas e métodos para se proteger, pensando em onde colocar senha e quem terá acesso ao quê. Se um advogado, por exemplo, contrata um estagiário e deixa o computador logado, esse estagiário terá acesso a processos, fotos, dados, a tudo. Mas o cliente não deu a autorização de acesso para o estagiário, apenas para o advogado. É esse entendimento que é preciso ter ao lidar com dados.

Se um paciente deu acesso à informação para você, você não pode dar acesso àquela informação para terceiros. É permitido compartilhar uma informação com um colega para tirar uma dúvida, desde que não seja possível identificar quem é o paciente. "Você conta o milagre, mas não conta o santo". Assim, você não identifica quem é a pessoa, apenas qual é o caso. Você anonimiza o seu paciente.

O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses, de acordo com a LGPD (Brasil, 2019): mediante o fornecimento do consentimento do titular; "para a tutela da saúde, exclusivamente em procedimentos realizados por profissionais da saúde, serviços de saúde ou autoridade sanitária"; "o controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter o consentimento específico do titular para esse fim".

No caso hipotético citado anteriormente, caso não seja possível anonimizar o paciente, sendo realmente preciso atuar em conjunto com um colega, é necessário pedir autorização para poder compartilhar aquela informação. E se o titular dos dados não autorizar, você não pode compartilhar. O controlador é obrigado a comunicar tanto ao titular quanto à autoridade a ocorrência de incidente de segurança, quando houver vazamento de dados.

Não existe sistema 100% seguro, então é possível haver vazamentos. Além disso, muitas empresas não têm condições de pagar o que muitos sistemas cobram justamente para blindar plataformas e informações das empresas. É humanamente impossível, porque, enquanto eles estão criando sistemas para blindar, outros estão gastando o seu tempo para burlar.

O Serviço Federal de Processamento de Dados (Serpro) forneceu um mapa mental com as regras da LGPD:

Figura 1 – Mapa mental da LGPD

Fonte: Serpro, 2018.

Dessa forma, você pode ter que sofrer um processo administrativo, que é um termo de ajustamento de conduta usado quando se abre um prazo para que se corrija aquela falha. Então, é preciso se adaptar, corrigir aquela falha e demonstrar que a correção foi feita, ou poderá sofrer sanções mais graves, como multas das mais leves às mais severas.

A prefeitura é condenada por vazamentos de dados pessoais. O vazamento de informações médicas, prontuários, exames e afins, ou seja, dados que são considerados pessoais sensíveis pela LGPD, caracterizam a condenação do município, relacionando o dano experimentado pelo paciente à falha na prestação de serviço público. Essa é uma situação bem constrangedora.

Um outro exemplo de punição é o ocorrido no Procon de Minas Gerais, que multou uma rede de farmácias por exigir o CPF do consumidor. Mas não é simplesmente

pelo fato de exigir o CPF, mas por buscarem uma informação nossa e começarem a criar o nosso “avatar” digital com informações que não são dadas por nós. Assim, eles vão tirando conclusões sobre as pessoas, sem que elas tenham a opção de se defender. Na ocasião, a multa foi bem pesada, de R$ 8.497.500,00 sobre a Raia Drogasil S/A.

Assim, existem algumas questões a serem feitas: para que estou pegando aquele dado? Eu preciso daquele dado? Por quanto tempo eu tenho que armazenar aquele dado? Segundo o Código de Ética da Medicina, existem alguns dados que podem ser guardados por 20 anos, mas por quanto tempo eu preciso ficar com aquilo? Eu posso destruir? Quanto menos tempo eu ficar com aquela informação, melhor.

Se é um prontuário, pertence ao paciente. Se aquele paciente morrer, eu tenho que entregar para o representante legal, não para a família. E o representante legal é quem a família indicar, seja um advogado ou um inventariante. Muitas vezes, a família nem sabe disso, nem mesmo o que o paciente tinha. Tudo é extremamente sigiloso. Então, esse giro sobre a LGPD do Serpro fornece um roteiro para ser usado dentro dos escritórios e dos consultórios, para saber como lidar com os dados.

O Departamento de Recursos Humanos é o departamento que tem os dados mais sensíveis, pois geralmente detêm dados sobre saúde, quem é ex-detento, quem está de licença, quem foi operado, quem tem alguma deficiência, quem toma algum tipo de medicamento, quem paga pensão etc. Enfim, é um departamento pessoal, que tem informações muito sensíveis. Assim, é importante saber quais dados serão coletados, que tipo de informação é necessária, qual informação tem que ser registrada, o que é importante coletar e por que, onde os dados devem ser armazenados, qual é a finalidade do armazenamento, se vale o risco armazenar determinado dado, se será necessário compartilhá-lo; enfim, o que pode ou não ser feito e por quê.

Assim, se a autorização foi dada para um médico, ele não pode anotar à mão e pedir para a secretária digitar, apenas se o paciente autorizar previamente e oficialmente que isso seja feito. Após Para os casos de demissão, ou seja, quando o paciente não está mais sob os cuidados do mesmo médico, deve-se criar um regimento interno sobre como trabalhar com essas questões. Além disso, deve-se elaborar um modelo de termo de consentimento para variadas situações e um manual de condutas sobre o que se pode ou não fazer dentro da instituição. Isso porque muitas vezes não é

só a LGPD. O direito não é fragmentado; é uma coisa só. A LGPD pode implicar diversas áreas do direito, mas o direito é uma coisa só.

Em razão das infrações, caso haja um vazamento, pode haver uma sanção administrativa, com um Termo de Ajustamento de Conduta. Assim, informam que houve vazamento e enviam um Termo de Ajustamento de Conduta, pedindo para que se corrija esse vazamento. A vida segue após a demonstração de que o vazamento foi corrigido. Ou ainda podem haver sanções mais sérias, de até 50 milhões de reais por infração.

O governo irá mensurar qual é o tamanho do estrago e qual é o conteúdo da informação vazada, aplicando sanções à altura, como multa diária, publicização da infração (quando a empresa infratora deve divulgar publicamente a violação cometida) e até bloqueio e eliminação dos dados pessoais. Este último provavelmente seja o mais grave: você perder completamente todo o seu banco de dados.

Portanto, é por meio do Termo de Ajustamento de Conduta que se analisa a gravidade e a natureza das infrações e os direitos pessoais afetados. Aí fica um alerta: um dado na área da saúde é um dado gravíssimo para vazar. Então, a prevenção nessa área é o melhor caminho. Obviamente, ninguém quer vazar nada de graça, mas segundo o volume e a qualidade das informações que forem vazadas, pode ser que já ocorra direto uma multa ou uma penalidade maior. Dessa forma, a prevenção realmente é o melhor remédio.

A multa pode considerar o faturamento total da empresa, então o *compliance* é o melhor remédio. O *compliance* é olhar de fora e colocar a empresa em conformidade com a legislação específica da profissão. É colocar tudo em ordem, deixando tudo alinhado e fazendo tudo aquilo que a lei manda, para não ter problemas. Para qualquer um que se demitir ou admitir, haverá um manual com as regras.

É importante não perder tempo e fornecer um treinamento para a equipe, esclarecendo todas as dúvidas. E com o tempo, apenas ir atualizando esse manual, porque as leis mudam toda hora. Então, é preciso sempre reavaliar a política de privacidade e o contrato com o colaborador. Os colaboradores geralmente têm acesso às informações, aos bancos de dados.

Como forma de prevenção, é necessário conhecer múltiplos departamentos, obtendo múltiplos conhecimentos. É como “brincar de polvo”, porque deve-se ter um

conhecimento jurídico, ainda que mínimo, para se proteger enquanto profissional e criar as próprias regras dentro da profissão.

No portal da Autoridade Nacional de Proteção de Dados (ANPD), encontra-se muita informação e apostilas que orientam a base da LGPD, porque não basta proteger, é preciso ter programas para conscientizar e criar as novas regras, para que se adeque aos procedimentos internos de cada empresa. Mas não basta proteger; é preciso tomar muito cuidado principalmente com o descarte, políticas da empresa e acordos de confidencialidade.

O decálogo do Serpro é um catálogo muito interessante, com dez regras sobre o que observar na hora de tratar dados pessoais: finalidade, adequação, necessidade, acesso livre, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização. Por meio dessas dez perguntas, é possível saber o porquê de se pedir determinado dado para o paciente. Se uma dessas perguntas não estiver respondida, é melhor nem solicitar aquele dado.

Algumas matérias recentes trazem um panorama sobre o vazamento de dados: "Setor de Saúde é o segundo maior alvo de vazamentos de dados" (Medicina S/A[13], junho de 2025); "Setor de saúde lidera violações de dados, aponta IBM" (Meio e Mensagem[14], julho de 2025); "Brasil está entre os países com maior vazamento de informações médicas" (Saúde Digital News[15], junho de 2024); "Brasil lidera em vazamento de dados com alta de 250%" (Folha[16], junho de 2025). Vemos que o dano é reputacional com fins econômicos.

É preciso estudar isso, porque dados de saúde valem mais que informações financeiras na *dark web*. Matéria da *Forbes* fala sobre o tema:

> Para o consultor, a enorme cadeia de negócios envolvidos na saúde, desde rede farmacêutica até hospitais, torna o setor ainda mais frágil. "Já existem casos de hackers conseguirem o contato de fornecedores de saúde de medicamento do hospital, por exemplo, fraudar a compra desse medicamento e vender como droga no mercado negro. Há muito espaço para novos crimes cibernéticos no mercado da saúde, pois é algo muito recente", conta Sgarbi, complementando que

[13] Disponível em: https://medicinasa.com.br/vazamentos-dados/. Acesso em: 15 dez. 2025.
[14] Disponível em: https://www.meioemensagem.com.br/proxxima/setor-de-saude-lidera-violacoes-de-dados-aponta-ibm. Acesso em: 15 dez. 2025.
[15] Disponível em: https://saudedigitalnews.com.br/19/06/2024/brasil-esta-entre-os-paises-com-maior-vazamento-de-informacoes-medicas/. Acesso em: 15 dez. 2025.
[16] Disponível em: https://www1.folha.uol.com.br/colunas/painelsa/2025/06/brasil-lidera-em-vazamento-de-dados-com-alta-de-250.shtml. Acesso em: 15 dez. 2025.

> ataques a equipamentos de saúde podm prejudicar o tratamento de pacientes e colocar a vida deles em risco (Pacete, 2022).

Sabemos que a indústria farmacêutica é uma das que manda no mundo, sendo uma das potências econômicas. E saber que dados da saúde valem mais do que muita coisa nos preocupa ainda mais, principalmente para profissionais que operam na área da saúde. Porque será necessário ter um cuidado a mais com os dados coletados das pessoas com as quais se lida.

A Lei nº 14.510, de 2022, autoriza e regula a telessaúde, falando explicitamente sobre a questão do consentimento e da independência profissional. Já o Conselho Federal de Medicina, com a Resolução nº 2.299, de 2021, e a Resolução nº 2.314, de 2022, regula a telemedicina. Profissionais de saúde devem adotar medidas como documentos eletrônicos criptografados e armazenados em nuvem. Além disso, os dados têm que ter proteção, ambientes seguros (contra vazamentos e violação de dados) e controlados.

O fator humano é o elo mais fraco da segurança. Anita Allen (Franco, 2023) classifica a privacidade em quatro sistemas: informacional, que é o acesso à informação pessoal; física, que é o acesso a pessoas e espaços privados; decisória, que é a interferência em escolhas pessoais; proprietária, que é a apropriação de interesses sobre a personalidade humana.

Temos a questão de sigilo médico e princípio ético desde O Juramento de Hipócrates. Com relação às leis, há o Código Penal, o Código de Processo Penal, a Constituição, o Código de Ética Médica, o Marco Civil da Internet e, por fim, a LGPD. Além disso, existem as emendas constitucionais e as resoluções de telemedicina e registros eletrônicos. Assim, a tecnologia deve ampliar o acesso à saúde sem violar a privacidade, o sigilo, a honra e a autonomia do paciente.

Quando falamos em consentimento, o paciente concorda com o atendimento de forma digital, assim como o profissional da área da saúde concorda em dar aquele atendimento de forma remota. Isso é autonomia; é estabelecida uma troca. A Resolução nº 2.299 fala do teleatendimento; a Resolução nº 2.314 fala sobre a telemedicina. Entretanto, “os dados pessoais e clínicos do teleatendimento devem seguir as definições da LGPD” (Brasil, Resolução CFM nº 2.314, 2022). Por fim, a Resolução RDC nº 727, de julho de 2022, fala: “É obrigatório também garantir a preservação dos dados dos

pacientes, obedecendo às normas legais pertinentes, como a Lei Geral de Proteção de Dados".

O Termo de Consentimento Livre e Esclarecido (TCLE) é livre quando falamos da autonomia, porque o paciente está concordando com aquela modalidade de atendimento; é esclarecido porque tem que ter o conhecimento de que se está coletando dados sensíveis, tendo a consciência do que será feito com aquelas informações. Então, é um termo de concordância e autorização. O paciente deve estar consciente de que suas informações pessoais podem ser compartilhadas e tem o direito de negar permissão para isso, salvo em situação de emergência médica.

Ao dar uma busca na internet, é possível encontrar diversos modelos de TCLE, mas não tem segredo. O mais importante é colocar o máximo de informações, porque o paciente precisa ler tudo, para se prevenir. Se ele não lê e autoriza, o problema é dele. Porém, cabe ao profissional fornecer a orientação adequada. Se ele não teve a obrigação de ler, mas assinou, ele concordou.

Mas qual é a diferença entre tratamento de dados e compartilhamento de dados? O tratamento é quando aquele dado vai ficar com você; você irá armazená-lo. São informações que vão ficar sob o seu controle, então, por isso, você é o controlador. Já o compartilhamento é passar o dado para frente.

Os documentos de autorização devem ser passados sempre por e-mail, nunca pelo WhatsApp. É necessário documentar e formalizar tudo por e-mail. Inclusive, um formulário preenchido pelo *Google Docs* também tem validade, mas deve passar pelo e-mail. O paciente baixa, salva e envia por e-mail. Ou então ele preenche um PDF e passa por e-mail.

Em caso de vazamento de dados em atendimentos via telemedicina, a responsabilização, conforme a LGPD, depende da estrutura da operação. Para profissionais liberais que trabalham sozinhos, o controlador e o operador de dados, geralmente são uma só pessoa. No entanto, se houver uma secretária ou outro colaborador, o profissional responde como controlador. Em estruturas empresariais, a análise de onde ocorreu o incidente é mais complexa, mas a responsabilidade recai prioritariamente sobre o controlador, que é quem detém o poder de decisão sobre os dados e realizou a coleta, enquanto o operador apenas manipula as informações seguindo ordens.

Nesse contexto, destaca-se a importância do encarregado de dados, do DPO, que atua como o elo de comunicação entre a empresa, os titulares dos dados e a autoridade nacional, sendo o responsável por informar quando ocorre algum incidente de segurança.

Sobre o armazenamento, a recomendação é seguir estritamente o tempo exigido pela legislação de cada profissão da área da saúde, lembrando que alguns prontuários médicos devem ser guardados por 20 anos. É fundamental não correr riscos desnecessários, então, se um documento já pode ser descartado conforme a lei, ele deve ser eliminado. No entanto, o descarte digital exige cautela, pois *softwares* como o *Recuva*, por exemplo, podem recuperar arquivos apagados acidentalmente. Por isso, é aconselhável utilizar programas que realmente eliminem e "pulverizem" o dado do computador.

Deve-se, portanto, realizar uma limpeza periódica nas informações físicas e digitais a cada virada de ano, respeitando os prazos legais de guarda. Existem diversos manuais e sites úteis para aprofundar o estudo sobre o tema, fugindo do "jurisdiquês" e focando no que é essencial para o cotidiano do profissional.

A preocupação dos alunos na área da saúde, seja no estágio ou nas práticas clínicas, deve ser tratar o manuseio de dados com a mesma seriedade exigida de um profissional. Ao lidar com prontuários e informações de pacientes, é fundamental já começar a se ambientar, entendendo que é preciso proteger esses dados ao longo de toda a carreira. O ideal é que já se vejam como profissionais nesse momento. Na prática, isso implica adotar medidas de segurança simples, porém fundamentais: se houver dados no computador, é possível armazená-los em uma pasta protegida por uma senha que ninguém mais conheça.

A LGPD influencia o ensino e o uso de casos clínicos em sala de aula principalmente no que diz respeito à identificação. O estudo em si é tranquilo, desde que se anonimize o indivíduo. A ideia é subtrair a pessoa do contexto, não identificando de quem é aquele caso para que não haja conexão entre os dados e a identidade do paciente. É mais ou menos como contar uma história de vida inteira sem revelar de quem ela é; se você não sabe de quem se trata, a conexão deixa de existir e o uso pedagógico do material fica seguro perante a lei.

A dúvida sobre a correção de fornecer o CPF em troca de descontos, prática comum das farmácias, é relevante, especialmente para os mais jovens. O perigo está no fato de que o valor do convênio médico particular pode aumentar significativamente, por exemplo, ao atingir uma idade mais avançada, por volta dos 54 anos. Isso acontece porque as operadoras têm a capacidade de cruzar informações e afirmar que o usuário utiliza um determinado medicamento há anos, com base em uma condição de saúde pré-existente, por exemplo.

Se eu passo em uma consulta e meus dados vazam, como posso descobrir? Só pelas redes sociais? Trata-se de uma questão ética, uma vez que o controlador tem a obrigação de informar que os dados foram comprometidos. A triste verdade é que só tomamos conhecimento quando acontece um megavazamento que acaba sendo noticiado. É bastante frequente que ocorram vazamentos em empresas como LinkedIn e outras plataformas, porém a informação nem sempre é transmitida ao usuário de maneira clara.

Quando os dados vazam, eles são vendidos. Uma empresa que sabe tudo sobre você consegue te expor a produtos e ideias de forma muito precisa. Um exemplo que todos já viveram é quando estamos falando sobre um produto x, por exemplo, e de repente, começa a aparecer no *Instagram* várias propagandas sobre o produto x. Isso acontece porque os sistemas vão mapeando seus interesses, percebendo até quando você fica com os olhos parados por mais tempo em um anúncio. Com isso, eles vão criando um perfil comportamental completo, para saber exatamente o que te oferecer e como te influenciar. Esses algoritmos ensinam a máquina a mostrar a você um anúncio específico. Para a empresa, isso representa uma oportunidade valiosa, pois quanto mais informações eu tiver sobre você, maiores serão as possibilidades de vender para você.

Quando trabalhamos com pesquisa, uma das maiores preocupações é justamente a proteção de dados na pesquisa clínica. Para realizar esse tipo de estudo, é necessário submeter o projeto a um Comitê de Ética em Pesquisa (CEP) antes de extrair qualquer dado. Se pararmos para pensar, os consultórios na área da saúde são grandes produtores desses mesmos tipos de dados.

Na pesquisa, o TCLE precisa ser super detalhado. Por exemplo, se eu pedir autorização para analisar 50 prontuários e transformar isso em um artigo científico, preciso seguir regras rigorosas. A dúvida que surge é: no atendimento clínico de rotina,

poderíamos ter um termo de consentimento um pouco mais abrangente para evitar problemas éticos futuros?

Poderia o profissional incluir no termo de consentimento que, além de os dados estarem sob sua responsabilidade para o tratamento, o paciente já autoriza o uso dessas informações para uma eventual pesquisa futura? Assim, caso o profissional decida transformar aqueles dados em um projeto de pesquisa mais adiante, ele já teria uma autorização prévia do paciente para apresentar ao Comitê de Ética.

O problema surge quando queremos trabalhar com dados pregressos, como uma avaliação de prontuários que já existem. O comitê vai cobrar o TCLE, mas como acessar cada um desses pacientes antigos? Seria necessário ligar para o João da Silva de cinco anos atrás e perguntar se ele concorda com a pesquisa. É um processo complicado.

Uma sugestão estratégica seria fazer dois termos no mesmo ato, mas em documentos distintos. Isso porque o consentimento é revogável, o dado pertence à pessoa e ela pode mudar de ideia a qualquer momento. Se você cria um termo único, o paciente pode se sentir “preso” e a chance de ele negar a participação na pesquisa é muito maior. Fazendo dois documentos, você separa as finalidades: o termo da consulta se encerra naquele ato específico do atendimento, enquanto o termo da pesquisa tem vida própria e acompanha o projeto científico. Isso dá clareza ao paciente e segurança jurídica e ética para o profissional.

Para quem está iniciando, a principal orientação sobre a manutenção dos dados dos pacientes é adotar o que for mais confortável e possível para a sua realidade. Se for mais viável manter em papel, mantenha em papel; se preferir o digital, utilize o digital. O ponto fundamental, contudo, é o consentimento. Você deve criar um termo de consentimento, seja físico ou digital, questionando quais informações o cliente autoriza que você possua.

Nesse termo de esclarecimento, é essencial que o profissional explique a finalidade da coleta, para que servirá o dado e o que será feito com ele. Além disso, deve ficar explícito que o paciente pode desautorizar o uso ou pedir a atualização das informações a qualquer momento. Não se trata apenas de pedir uma assinatura, mas de garantir que a pessoa foi devidamente orientada.

Quanto ao armazenamento, o formato digital é mais prático, porém exige o uso de senhas em pastas para restringir o acesso. Já o formato físico, embora seja mais difícil

de vazar do que o digital, exige cuidado no arquivamento, como o uso de envelopes e gavetas trancadas.

Para a destruição de documentos físicos, caso não haja uma fragmentadora elétrica, a recomendação é realizar o descarte manual de forma estratégica. Nunca rasgue o papel apenas na horizontal; rasgue sempre na vertical, em tiras bem finas, para impossibilitar que as informações sejam reconstituídas. O objetivo é desfragmentar o conteúdo de modo que ninguém consiga juntar os pedaços e ler o que estava escrito.

Referências

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Organizado por Cláudio Brandão de Oliveira. Rio de Janeiro: Roma Victor, 2002. 320 p.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Redação dada pela Lei nº 13.853, de 2019. Brasília, DF: Diário Oficial da União, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 dez. 2025.

BRASIL. Serviço Federal de Processamento de Dados. O que muda com a LGPD. **Serpro**, 2018. Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd. Acesso em: 21 dez. 2025.

BRASIL. Conselho Federal de Medicina. **Resolução CFM nº 2.314, de 20 de abril de 2022**. Define e regulamenta a telemedicina no Brasil. Brasília, DF: CFM, 2022. Disponível em: https://sistemas.cfm.org.br/normas/arquivos/resolucoes/BR/2022/2314_2022.pdf. Acesso em: 21 dez. 2025.

BRASIL. Agência Nacional de Vigilância Sanitária. **Resolução nº 727, de 1º de julho de 2022**. Brasília, DF: Anvisa, 2022. Disponível em: https://ses.sp.bvs.br/wp-content/uploads/2022/10/U_RS-MS-ANVISA-727-REP_010722.pdf. Acesso em: 25 fev. 2025.

FRANCO, S. **A LGPD na prática da telemedicina**. São Paulo: Sociedade Brasileira de Genética Médica e Genoma, 2023. Disponível em: https://www.sbgm.org.br/ebook_lgpd.pdf. Acesso em: 21 dez. 2025.

PACETE, L. G. Dados de saúde valem mais que informações financeiras na dark web. **Forbes**, 2022. Disponível em: https://forbes.com.br/forbes-tech/2022/06/dados-de-saude-chegam-a-valer-mais-que-informacoes-financeiras-na-dark-web/. Acesso em: 21 dez. 2025.