DOI: 10.32385/rpmgf.v38i2.12751

Privacidade e confidencialidade em medicina: o que diz o Regulamento Geral de Proteção de Dados sobre o acesso a informação de saúde

Rodrigo Miguel Loureiro[1], Daniela Alves de Azevedo[2], Tiago Correia[2]

RESUMO

A revolução digital nos serviços de saúde veio disponibilizar novas oportunidades para o desenvolvimento da qualidade da prestação de cuidados, investigação de novos tratamentos e uma melhor utilização dos recursos. A maioria da informação que presentemente é partilhada digitalmente, anteriormente era partilhada em papel, suscitando, assim, novos desafios e ameaças digitais ao nível da segurança e privacidade.

Existiam cerca de 28 leis de proteção de dados diferentes baseados na *EU Data Protection Directive* de 1995, a qual foi desenhada há 20 anos atrás, antes da introdução generalizada da Internet e do crescimento das preocupações com a privacidade. Apesar dos avanços tecnológicos, a regulamentação existente permaneceu estagnada e cada vez mais inadequada para proteger os dados dos indivíduos ou das organizações. Dada esta necessidade foi desenvolvido e aprovado o Regulamento 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

O Regulamento Geral sobre a Proteção de Dados veio introduzir alterações significativas ao enquadramento legal da proteção de dados pessoais dentro da União Europeia, estabelecendo regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Estas alterações devem influenciar o modo de tratamento dos dados de saúde pelas entidades prestadoras de cuidados de saúde, quer no âmbito da prestação de cuidados de saúde quer para efeitos de investigação.

Palavras-chave: Privacidade; Confidencialidade; Regulamento Geral de Proteção de Dados; Acesso a informação de saúde.

INTRODUÇÃO

A revolução digital nos serviços de saúde veio disponibilizar novas oportunidades para o desenvolvimento da qualidade da prestação de cuidados, investigação de novos tratamentos e uma melhor utilização dos recursos. No entanto, na maioria dos países o sistema de saúde está fortemente pressionado por vários fatores. O efeito conjugado de uma maior esperança de vida e a prevalência de doenças crónicas tem sido responsável pelo crescimento dos custos dos cuidados de saúde e ameaçam a sustentabilidade do modelo tradicional de prestação de cuidados de saúde em muitos países. Assim, novos modelos de atendimento suportados por novas tecnologias e pela digitalização têm vindo a aparecer como solução para este cenário.

A utilização digital da informação tornou-se uma componente essencial de um novo setor de saúde orientado para a qualidade dos serviços prestados e para a eficiência dos recursos. Trata-se de uma transformação, desencadeada e suportada por novas tecnologias e partilha de informação, mas também pelas exigências das novas gerações para que o sistema público

1. USF Novo Norte. Arouca, Portugal.
2. USF Famílias. Lourosa, Portugal.

de saúde corresponda ao estilo de vida cada vez mais digital. A maioria da informação que presentemente é partilhada digitalmente era anteriormente partilhada em papel, suscitando, assim, novos desafios e ameaças digitais ao nível da segurança e privacidade, nomeadamente em relação à proteção dos dados pessoais numa sociedade cada vez mais digital.

Existiam cerca de 28 leis de proteção de dados diferentes baseados na *EU Data Protection Directive* de 1995, a qual foi desenhada há 20 anos atrás, antes da introdução generalizada da Internet e do crescimento das preocupações com a privacidade. Apesar dos avanços tecnológicos, a regulamentação existente permaneceu estagnada e cada vez mais inadequada para proteger os dados dos indivíduos ou das organizações, até 2016.[1] Dada esta necessidade, foi desenvolvido e aprovado o Regulamento 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados).[2]

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

O Regulamento Geral sobre a Proteção de Dados (RGPD) veio introduzir alterações significativas ao enquadramento legal da proteção de dados pessoais dentro da União Europeia (UE), estabelecendo regras relativas à proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Estas alterações devem influenciar o modo de tratamento dos dados de saúde pelas entidades prestadoras de cuidados de saúde, quer no âmbito da prestação de cuidados de saúde quer para efeitos de investigação.[2]

São considerados dados pessoais todos os dados que contêm informação que permite identificar ou tornar identificável (ou seja, que exista a possibilidade de vir a ser identificada) uma pessoa singular e titular dos dados (utente, cidadão, colaborador). Pode fazer parte deste conceito, o nome, um número de identificação, dados de localização, identificadores por via eletrónica, bem como um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular. Estão também abrangidos os dados genéticos e os dados biométricos.[2-6]

O RGPD aplica-se ao tratamento de dados pessoais de cidadãos residentes no território da UE, independentemente de o tratamento ocorrer dentro ou fora da UE. Este tratamento pode ser efetuado por meios total ou parcialmente automatizados e também por meios não automatizados. O tratamento de dados é uma operação ou um conjunto de operações efetuadas sobre dados pessoais, como: a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.[2]

CICLO DE RELAÇÃO DE PROTEÇÃO DE DADOS

O RGPD pressupõe uma relação de proteção de dados, que é constituída por três entidades fundamentais (Figura 1):[2]

- O responsável pelo tratamento dos dados é uma pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento dos dados pessoais. O responsável deverá aplicar as medidas técnicas e organizativas adequadas para assegurar, e poder comprovar, que o tratamento está em conformidade com o disposto no Regulamento. No caso dos estabelecimentos prestadores de cuidados de saúde, que tratam dados de saúde, o responsável pelo tratamento de dados deve manter um registo de todas as atividades de tratamento sob a sua responsabilidade.
- O subcontratante é uma pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que trata dos dados pessoais por conta do responsável pelo tratamento destes. Dever-se-á celebrar um contrato que estabelece o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e categorias dos titulares dos dados, e as obrigações e direitos do responsável pelo tratamento.
- A autoridade de controlo controla a aplicação das disposições do regulamento a fim de proteger as pessoas singulares/utentes relativamente ao tratamento dos seus dados pessoais e a fim de facilitar a livre circulação desses dados na EU. As autoridades de controlo agem com total independência no segui-

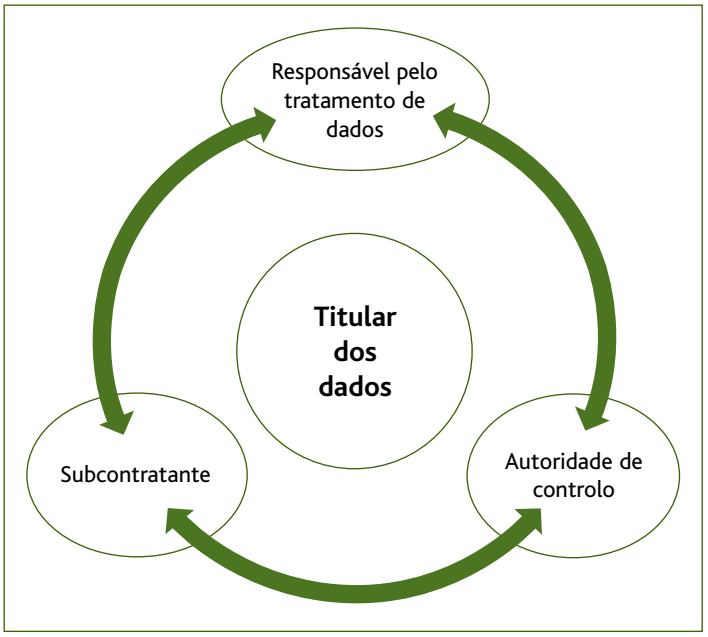

Figura 1. Ciclo de relação de proteção de dados.

mento das suas atribuições e no exercício dos poderes que lhe são atribuídos.

Para além das obrigações gerais que decorrem da Lei de proteção de dados pessoais, as entidades integrantes do Sistema Nacional de Saúde (SNS) deverão ainda assegurar o cumprimento das demais regras previstas na legislação e/ou disposições regulamentares específicas do setor da saúde, as quais regulam a propriedade, o acesso e a legitimidade do tratamento da informação de saúde dos utentes.

Assumindo-se como responsáveis pelo tratamento, incumbe às entidades integrantes do SNS, em termos genéricos, assegurar que:[2]

- Os dados pessoais são recolhidos para finalidades determinadas, explícitas e legítimas e não sejam posteriormente tratados de forma incompatível com as finalidades da recolha;
- Apenas são recolhidos os dados pessoais adequados, pertinentes e não excessivos relativamente às finalidades da recolha – princípio de minimização;
- Os dados pessoais recolhidos são exatos e atualizados;
- Os dados pessoais apenas são conservados durante o período necessário para a prossecução das finalidades da recolha/tratamento (garantindo o cumprimento das deliberações da Comissão Nacional de Proteção de Dados (CNPD) aplicáveis);
- São disponibilizadas ao titular dos dados todas as informações relacionadas com o tratamento efetuado, concedendo-lhe o direito de acesso e retificação dos seus dados;
- É obtido o consentimento do titular para o tratamento dos seus dados, exceto nos casos em que tal consentimento é dispensado nos termos da lei, como é o caso do tratamento de dados para a finalidade de proteção de interesses vitais do seu titular;
- São postas em prática as medidas técnicas e organizativas adequadas para proteger os dados pessoais, designadamente contra a sua destruição acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizado (nomeadamente quando o tratamento implicar a sua transmissão por rede) e qualquer outra forma de tratamento ilícito;
- O tratamento dos dados encontra-se devidamente notificado à CNPD e, quando legalmente exigido, é obtida a respetiva autorização prévia.

A CNDP é uma entidade administrativa independente com poderes de autoridade, que funciona junto da Assembleia da República (autoridade nacional de controlo de dados pessoais). Tem como atribuição genérica controlar e fiscalizar o processamento de dados pessoais, em rigoroso respeito pelos direitos do Homem e pelas liberdades e garantias consagradas na Constituição e na lei.

A lei estabelece que, para deter e tratar dados pessoais, qualquer entidade integrante do SNS terá que notificar previamente a CNPD. Existem, porém, certos casos em que não basta a notificação da CNPD, sendo necessário obter uma autorização antes de recolher, conservar e/ou tratar determinado tipo de informação relativa a pessoas singulares, como o caso dos «dados sensíveis». Nesta categoria incluem-se, entre outros, os dados de saúde, dados genéticos, dados de vida privada, origem racial ou étnica.[2]

No caso de tratamento de dados de saúde, incluindo dados genéticos, e não obstante constituírem dados sensíveis, o seu tratamento está sujeito a mera notificação à CNPD, na medida em que tal tratamento será necessário para efeitos de medicina preventiva, de

diagnóstico médico, de prestação de cuidados ou tratamentos médicos ou ainda de gestão de serviços de saúde. Além disso, o tratamento desses dados terá que ser efetuado por um profissional de saúde ou por outra pessoa sujeita a sigilo profissional.[2-6]

Contudo, se houver tratamento de outros dados (e.g., raça, fé religiosa ou outros dados da vida privada – toxicodependência, comportamento de risco, hábitos alcoólicos, problemas sociais de integração, etc.), se os dados de saúde, da vida sexual ou genéticos forem utilizados para finalidades diversas (e.g., para fins de investigação científica) ou forem tratados em circunstâncias distintas das referidas, as entidades integrantes do SNS devem submeter esse tratamento a controlo prévio, submetendo um pedido de autorização à CNPD.[2-6]

ACESSO A INFORMAÇÃO DE SAÚDE

A informação de saúde abrange todo o tipo de informação direta ou indiretamente ligada à saúde, presente ou futura, incluindo os dados clínicos registados nas unidades de saúde (e.g., o processo clínico ou quaisquer fichas clínicas), história clínica e familiar, resultados de análises e de outros exames auxiliares de diagnóstico, intervenções, diagnósticos e tratamentos. A informação de saúde pertence à pessoa a quem diz respeito.[2]

Atendendo à legislação aplicável em matéria de acesso à informação de saúde (Lei n.º 12/2005, de 26 de janeiro; Lei n.º 81/2009, de 21 de agosto; e Lei n.º 58/2019, de 8 de agosto), está claro que o utente tem o direito de tomar conhecimento de toda a informação de saúde que lhe diga respeito, salvo em circunstâncias excecionais, em que seja inequivocamente demonstrado que o acesso a essa informação pode prejudicar gravemente a sua saúde.[2-6]

O profissional de saúde ou a unidade de saúde não podem recusar o acesso do utente à sua informação de saúde. As unidades de saúde são meras depositárias da informação de saúde, devendo permitir ao utente o acesso à sua informação de saúde, A possibilidade de acesso à informação de saúde por parte do titular decorre do respeito pela respetiva autonomia e é condição para o exercício do consentimento informado, livre e esclarecido.[2]

O ato de consultar a informação de saúde não é o mesmo que obter cópia dessa informação, isto é, a mera consulta da informação é gratuita; no entanto, a sua reprodução (e.g., fotocópias, emissão de certidões ou gravação de informação em CD) ou a emissão de relatórios clínicos podem ter um custo associado, tanto nas unidades de saúde públicas como nas privadas.[2]

O acesso à informação de saúde deverá ser efetuado pelo próprio utente ou, alternativamente, o utente poderá indicar o médico que pretende que consulte essa informação de saúde. Por outro lado, o utente poderá emitir uma autorização escrita para que uma terceira pessoa aceda à mesma, se se demonstrar fundamentadamente que tem interesse direto, pessoal e legítimo que justifique o acesso à informação, nos termos da lei. Essa autorização deverá ser assinada e datada pelo utente, devendo constar a sua identificação completa (nome, número do cartão de cidadão e morada) e da terceira pessoa, bem como qual a informação a consultar.[2]

No caso de falecimento do utente, a respetiva família só pode aceder à sua informação de saúde, se demonstrar fundamentadamente ser titular de um interesse direto, pessoal, legítimo e suficientemente relevante que justifique tal acesso, nomeadamente quando pretende apresentar uma reclamação ou recorrer à via judicial para o exercício de um qualquer direito ou interesse.[2]

Nos casos em que a informação obtida possa ser considerada de natureza sensível, por poder afetar terceiros (familiares ou outros), ela deverá merecer proteção especial. É o caso, por exemplo, da informação genética, aliás alvo de legislação própria (Lei n.º 12/2005, de 26 janeiro), e a informação sobre doenças infeciosas transmissíveis.[2-6]

Relativamente ao acesso a informação de saúde para fins de investigação, a lei refere que os princípios da proteção de dados deverão aplicar-se a qualquer informação relativa a uma pessoa singular identificada ou identificável; e que os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. E, portanto, o presente regulamento não diz respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação. Adicionalmente acrescentam que os titulares dos dados deverão poder dar o seu consentimento para determinadas áreas de

investigação científica, desde que estejam de acordo com padrões éticos reconhecidos para a investigação científica. Os titulares dos dados deverão ter a possibilidade de dar o seu consentimento unicamente para determinados domínios de investigação ou partes de projetos de investigação, na medida permitida pela finalidade pretendida.[2-6]

SEGURANÇA E VIOLAÇÃO DOS DADOS PESSOAIS

No que diz respeito aos dados de saúde deve ser assegurada a implementação de medidas destinadas a impedir o acesso indevido de terceiros aos processos clínicos e aos sistemas informáticos que contenham informação de saúde, incluindo as respetivas cópias de segurança, assim como a separação lógica entre dados de saúde e dados administrativos.

As medidas de segurança deverão assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado aos riscos que o tratamento apresenta e à natureza dos dados a proteger.[2]

Como tal, será necessária a identificação das potenciais vulnerabilidades do sistema, bem como uma previsão do impacto que essas falhas de segurança possam causar, de modo a proceder a uma análise e avaliação de riscos correta e realista que conduza a uma definição eficaz das medidas de segurança que melhor poderão responder às necessidades da instituição.[2]

Tendo em vista garantir um nível de segurança adequado ao risco que existe no tratamento dos dados, o responsável pelo tratamento e o subcontratante devem aplicar as medidas técnicas e organizativas necessárias consoante o caso, como: [2]

- O tratamento dos dados de modo que deixem de poder identificar o seu titular sem recorrer a informações suplementares (pseudonimização) e a codificação dos dados pessoais;
- A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
- A capacidade de repor a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um imprevisto/acontecimento físico ou técnico;
- Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

Pode acontecer que haja uma violação dos dados pessoais, ou seja, uma violação da informação pessoal que provoque, de modo acidental ou mesmo ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento. E neste sentido, logo que o responsável pelo tratamento tenha conhecimento de uma violação de dados pessoais deverá participar à CNPD, sem demora injustificada, e sempre que possível até 72 horas após ter tido conhecimento do sucedido, a menos que seja capaz de demonstrar que da violação não resultará um risco para os direitos e liberdades das pessoas singulares. Se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas é acompanhada dos motivos do atraso.[2-6]

O desrespeito por algumas das regras constantes da lei de proteção de dados pessoais constitui uma contraordenação, punível com coima que poderá atingir os €29.927,88 (sendo as sanções aplicadas às contraordenações cumuladas materialmente).[2]

A lei de proteção de dados pessoais prevê ainda a possibilidade de aplicação, pela CNPD, de sanções acessórias, como o bloqueamento ou destruição de dados, a proibição, temporária ou definitiva, do tratamento de dados pessoais (o que na prática é suscetível de impedir o desenvolvimento da atividade) ou ainda a publicidade da sentença condenatória. O responsável pelo tratamento poderá ainda incorrer em responsabilidade civil ou criminal. Por exemplo, a utilização intencional de dados pessoais, de forma incompatível com a finalidade determinante da recolha, constitui crime punível com pena de prisão até um ano ou multa até 120 dias. No caso de dados sensíveis, a pena é agravada para o dobro.[2-6]

Para além dos custos jurídicos e financeiros, o incumprimento da lei tem ainda outros custos associados que podem ter um impacto negativo muito significativo para as entidades integrantes do SNS: os custos de imagem e de reputação.[2]

REFERÊNCIAS BIBLIOGRÁFICAS

1. Diretiva 95/46/EC do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. JO CE. 1995;L(281):31-50.
2. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho,

de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). JO CE. 2016;L(119):1-88.
3. Lei n.º 12/2005, de 26 de janeiro. Diário da República. I Série A;(18).
4. Decreto-Lei n.º 81/2009, de 2 de abril. Diário da República. I Série;(65).
5. Decreto-Lei n.º 58/2019, de 8 de agosto. Diário da República. I Série;(151).
6. Portaria n.º 248/2013, de 5 de agosto. Diário da República. I Série;(149).

CONTRIBUIÇÃO DOS AUTORES

Rodrigo Miguel Loureiro – Conceptualização, Metodologia, Validação, Investigação, Gestão de dados, Redação – manuscrito original, Redação – revisão e edição, Supervisão, Administração do projeto.
Daniela Alves de Azevedo – Conceptualização, Investigação, Gestão de dados, Redação – manuscrito original, Redação – revisão e edição.
Tiago Alpoim Correia – Conceptualização, Investigação, Gestão de dados, Redação – manuscrito original.

CONFLITO DE INTERESSES

Os autores declaram não possuir quaisquer conflitos de interesse.

ENDEREÇO PARA CORRESPONDÊNCIA

Rodrigo Miguel Loureiro
E-mail: rodrigo.mrsp.loureiro@gmail.com
https://orcid.org/0000-0001-7619-4604

Recebido em 10-11-2019
Aceite para publicação em 01-12-2021

ABSTRACT

PRIVACY AND CONFIDENTIALITY IN MEDICINE: WHAT DOES THE GENERAL DATA PROTECTION REGULATION SAY ABOUT HEALTH INFORMATION ACCESS

The digital revolution in health services has provided new opportunities for the development of quality care, research of new treatments, and better usage of resources. Most of the information that is currently digitally shared was previously shared on paper, thus raising new security and privacy challenges and digital threats.

There were about 28 different data protection laws based on the 1995 EU Data Protection Directive, which was drawn up 20 years ago, before the widespread introduction of the Internet and growing privacy concerns. Despite technological advances, the existing regulation has remained stagnant and increasingly inadequate to protect individual or organizational data. Given this need, the Regulation 2016/679 of the European Parliament and Council of 27 April 2016 was elaborated and approved.

The General Data Protection Regulation introduced significant changes to the legal framework for the protection of personal data within the European Union, laying down rules on the protection of individuals regarding the processing of personal data and its free movement. These changes should influence the way health care providers handle health data, both in the provision of healthcare and for research purposes.

Keywords: Privacy; Confidentiality; General Data Protection Regulation; Health information access.