ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

Proteção de dados e segurança informática no setor da saúde: o papel dos responsáveis pela proteção de dados no Direito da União Europeia

Data protection and computer security in the health sector: the role of data controllers under European Union Law

Protección de datos y seguridad informática en el sector sanitario: el papel de los responsables del tratamiento de datos en el marco de la legislación de la Unión Europea

Alexandre Libório Dias Pereira[1]

Resumo
A proteção de dados pessoais e a segurança informática são matérias sensíveis no setor da saúde. Este texto passa em revista o papel do responsável pelo tratamento de dados (*data controller*) segundo o Regulamento Geral de Proteção de Dados (RGPD). Estão em causa os princípios relativos ao tratamento e os direitos dos titulares de dados pessoais, os deveres de aplicar medidas técnicas e organizativas adequadas, de registar os tratamentos, de avaliar o impacto dos tratamentos ou, consoante os casos, de designar um encarregado de proteção de dados. São ainda analisadas as obrigações em matéria de segurança informática à luz do quadro legal aplicável, com destaque para a Diretiva europeia da cibersegurança.
Palavras-chave
Dados de Saúde Gerados pelo Paciente. União Europeia. Privacidade.

Abstract
Personal data protection and computer security are sensitive issues in the health sector. This work reviews the role of data controllers according to the General Data Protection Regulation (GDPR). At stake are the principles of data processing and the rights of holders of personal data, the duty to apply organized technical and organizational measures, to register treatments, to assess the impact of treatments or, as the case may be, to designate a data protection officer. Computer security obligations are also analysed under the applicable legal framework, in particular the EU Directive on Cybersecurity.
Keywords
Patient Generated Health Data. European Union. Privacy.

Resumen
La protección de los datos personales y la seguridad informática son cuestiones delicadas en el sector sanitario. Este trabajo revisa el rol del controlador de datos de acuerdo con el Reglamento General de Protección de Datos (RGPD). Em causa estão os princípios relativos ao tratamento e os direitos dos titulares de dados pessoais, os deveres de aplicar medidas técnicas e organizativas adequadas, de registar os tratamentos, de avaliar o impacto dos tratamentos ou, consoante os casos, de designar um encarregado de proteção de dados. Las obligaciones y materias de seguridad informática también se analizan a la luz del marco legal aplicable, en particular la Directiva de Ciberseguridad de la Unión Europea.

[1] Doutor em Direito; Professor Associado, Faculdade de Direito e Instituto Jurídico, Universidade de Coimbra, Coimbra, Portugal. https://orcid.org/0000-0003-4356-9195. E-mail: aldp@fd.uc.pt

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

Palabras clave
Datos de Salud Generados por el Paciente. Unión Europea. Privacidad.

Introdução

A proteção de dados pessoais e a cibersegurança são matérias de crescente importância prática, em especial no setor da saúde e no contexto da pandemia. Interessa, por isso, compreender a razão de ser da proteção dos dados pessoais e identificar as principais obrigações legais que impendem sobre quem realiza tratamentos de dados pessoais, sejam entidades públicas ou empresas privadas. O mesmo vale para a segurança informática, matéria estreitamente relacionada com a proteção de dados.

Para saber as principais obrigações neste domínio é estudada a legislação aplicável e cuja fonte é, no essencial, a União Europeia (UE). De todo o modo, a proteção jurídica dos dados pessoais funda-se no direito ao respeito pela vida privada proclamado na Declaração Universal dos Direitos Humanos de 1948 (art. 12) e consagrado com força normativa na Convenção Europeia do Direitos do Homem e das Liberdades Fundamentais de 1950 (art. 8), e no Pacto Internacional dos Direitos Civis e Políticos de 1966 (art. 17). Portugal aderiu à Convenção Europeia dos Direitos Humanos em 1978, na lei interna o Código Civil já consagrava, como direito de personalidade, a reserva sobre a intimidade da vida privada (art. 80), tal como sucederia com a Constituição da República Portuguesa (CRP) de 1976 (arts. 33 – posteriormente inserido no art. sobre direitos pessoais – e 26), a qual dedicou um artigo à inviolabilidade do domicílio e da correspondência (art. 34), e proibiu a utilização da informática para tratar dados da vida privada das pessoas (art. 35). Posteriormente, no virar de milénio, a Carta de Direitos Fundamentais da União também consagraria, autonomamente, o direito ao respeito pela vida privada e familiar e a proteção dos dados (arts. 7 e 8, respetivamente). Por seu turno, no direito internacional da saúde, a Convenção sobre os Direitos do Homem e a Biomedicina (Convenção para a Proteção dos Direitos do Homem e da Dignidade do Ser Humano face às Aplicações da Biologia e da Medicina), feita em Oviedo em abril de 1997, consagrou, além do direito ao respeito pela vida privada relativamente a informações relacionadas com a saúde, o direito de cada pessoa conhecer toda a informação recolhida sobre a sua saúde, salvo vontade expressa da pessoa ou exceção legal justificada no seu interesse do paciente (art. 10).

Embora gerada no seio do *direito à privacidade*, como é conhecido no EUA o direito à reserva da vida privada, a proteção dos dados pessoais desenvolveu-se e adquiriu uma

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

vida própria, com fundamento no direito fundamental à *autodeterminação informativa*, segundo a designação dada pelo Tribunal Constitucional Federal Germânico no seu acórdão de 15 dezembro de 1983, no âmbito de um processo relativo a informações pessoais coletadas durante o censo de 1983, em que o *Bundesgerichtshof* (BGH) considerou que, no contexto do processamento moderno de dados, a proteção do indivíduo contra a recolha, armazenamento, uso e divulgação ilimitados de seus dados pessoais é abrangida pelo direito fundamental de cada pessoa determinar, em princípio, a divulgação e o uso dos seus dados pessoais, sujeitando esta autodeterminação informacional apenas a limitações justificadas por razões de interesse público primordial (1-4).

Esse "produto da doutrina alemã tão exportado, quanto mal conhecido na sua origem" (5) seria recebido pela doutrina constitucional portuguesa, ao abrigo do art. 35 da CRP, no sentido de o "direito à autodeterminação informativa" atribuir "a cada pessoa o direito de controlar a informação disponível a seu respeito" e se impedir a redução da pessoa a mero "objeto de informação" (6). Assim, a autodeterminação informativa confere à pessoa, por um lado, um *"direito ao segredo* (à intromissão dos outros na esfera privada, com tomada de conhecimento de aspetos a ela referentes)" e, por outro, "um *direito à reserva* (proibição de revelação)" (7).

Na jurisprudência, o direito à autodeterminação informativa foi consagrado em diversos acórdãos do Tribunal Constitucional (8-10). O Supremo Tribunal de Justiça consagrou igualmente este direito à *autodeterminação informativa* em diversos casos (11). De igual modo, o Tribunal Europeu dos Direitos do Homem (TEDH) acolheu o direito à autodeterminação informacional. No acórdão *Satakunnan Markkinapörssi Oy and Satamedia Oy c. Finlândia*, o TEDH considerou que o art. 8.º da Convenção estabelece "o direito a uma forma de autodeterminação informacional" contra ingerência no exercício do seu direito à vida privada resultantes de recolha, processamento e disseminação coletiva dos seus dados pessoais (12).

A afirmação do direito à *autodeterminação informativa* contra a redução da pessoa a mero objeto de informação não impede, todavia, o reconhecimento do valor económico dos dados pessoais e que considerados bens transacionáveis, por ex. como forma de pagamento de serviços digitais (13, 14), defendendo-se, por isso, que deveriam ser objeto de um acordo internacional entre os EUA e a UE com vista a promover o seu fluxo transatlântico (15), e ainda que os dados pessoais, enquanto valores de exploração, não

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

podem ser excluídos do direito da concorrência, designadamente do abuso de posição dominante, na medida em que podem constituir recursos essenciais da economia digital (16).

De referir ainda que no direito britânico os tribunais elaboraram um novo ilícito para a violação de dados pessoais, o chamado *tort of misuse of personal information*, por ex. no caso *Naomi Campbell* c. *The Mirror*, e o critério da "expetativa razoável de privacidade" (17).

O responsável pelo tratamento de dados segundo o Regulamento Geral de Proteção de Dados

O Regulamento Geral de Proteção de Dados (RGPD) (18-20) regula a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, garantindo a liberdade de circulação de dados pessoais no interior da União Europeia (arts. 1/1 e 3). Por dados pessoais entende-se, para efeitos do RGPD, "informação relativa a uma pessoa singular identificada ou identificável [titular dos dados]" (18), sendo

> considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular (art. 4/1).[2] (18)

O titular dos dados pessoais é o sujeito principal da proteção de dados e o responsável pelo tratamento de dados (doravante RTD) é o sujeito principal de deveres e obrigações, incluindo as coimas e outras sanções previstas no RGDP para o não cumprimento das suas disposições e que são sensivelmente gravosas (arts. 83-84): o não cumprimento de uma ordem emitida pela autoridade de controlo a (por ex. em Portugal, a Comissão Nacional de Proteção de Dados) fica sujeito a coimas até vinte milhões de euros ou, no caso de uma empresa, até 4 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante mais elevado (art. 83/6) (21). Para além da responsabilidade pelo cumprimento dos princípios do tratamento de dados e do respeito pelos direitos dos seus titulares, o RGPD dedica especificamente o capítulo IV ao responsável pelo tratamento e subcontratante.

[2] Para efeitos do RGPD, são ainda definidas certas categorias de dados, nomeadamente os dados genéticos, os dados biométricos e os dados relativos à saúde – *vide infra*. O considerando 26 esclarece que "Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica." (18)

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

Noção de responsável pelo tratamento de dados

A noção de RTD é muito ampla, definindo-o o RGPD como "a 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 de dados pessoais" (art. 4/7, *itálico nosso*) (18). Assim, o RTD pode ser uma pessoa de direito privado, singular ou coletiva (por ex. associação, fundação, sociedade civil ou comercial, cooperativa), ou uma autoridade pública, agência ou outro organismo (por ex. uma câmara municipal, uma universidade pública, uma agência de regulação, uma entidade pública empresarial). A natureza pública ou privada da entidade é irrelevante. O que conta é saber se a entidade em causa, isolada ou conjuntamente com outras, determina as *finalidades* e os *meios* de tratamento de dados, i.e., o *para quê* e o *como*.

Ao RTD junta-se o subcontratante, entendido como qualquer pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do RTD (art. 4/8). Ambos realizam, por conseguinte, tratamento de dados, igualmente definido em termos amplos como

> uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais 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 (art. 4/2). (18)

Âmbito territorial de aplicação do RGPD para efeitos de determinação do RTD

O RGPD delimita o seu âmbito de aplicação territorial (art. 3) no sentido de abranger o tratamento de dados pessoais:

1. efetuado no contexto das atividades de um estabelecimento de um RTD ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União; ou

2. de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com: a) a oferta de bens ou serviços a esses titulares de dados na União - vd. considerando 23 -, independentemente da exigência de os titulares dos dados procederem a um pagamento; ou b) o controlo do seu comportamento, desde que esse comportamento tenha lugar na União – vd. considerando 16; ou

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

3. por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público, por ex. no âmbito de uma missão diplomática ou num posto consular de um Estado-Membro, como refere o considerando 25 (22, 23).[3]

Exclusão de atividades pessoais ou domésticas

As atividades pessoais ou domésticas, como a troca de correspondência ou a atividade nas redes sociais, não são abrangidas pelo RGPD, mas já são abrangidos os "responsáveis pelo tratamento e aos subcontratantes que forneçam os meios para o tratamento dos dados pessoais dessas atividades pessoais ou domésticas" (18) – vd. considerando 18.

Deveres do RTD

O dever de respeitar os princípios de tratamento de dados pessoais

No leque de deveres a cargo do RTD surge à cabeça o de respeitar os princípios relativos ao tratamento de dados pessoais estabelecidos no RGPD, a saber: a licitude, lealdade e transparência, a limitação das finalidades, a minimização dos dados, a exatidão, a limitação da conservação, e a integridade e confidencialidade (art. 5/1). Aliás, a responsabilidade do RTD pelo cumprimento dos princípios do tratamento de dados pessoais é, também, um desses princípios, o da responsabilidade, fazendo recair sobre o RTD o ónus da prova do cumprimento dos referidos princípios (art. 5/2). Ao contrário da regra geral da responsabilidade extracontratual, o RTD quem terá que "provar que de modo algum é responsável pelo evento que deu causa aos danos" (art. 82/3) (18).

A licitude do tratamento pode resultar de consentimento do titular de dados ou da sua necessidade em sede contratual, cumprimento de obrigação jurídica do responsável, defesa de interesses vitais do titular ou de terceiro, exercício de funções públicas ou autoridade pública do responsável, ou interesses legítimos do responsável ou de terceiro (art. 6). Nos termos do considerando 46:

> Alguns tipos de tratamento podem servir tanto importantes interesses públicos como interesses vitais do titular dos dados, por exemplo, se o tratamento for necessário para fins humanitários, incluindo a monitorização de epidemias e da sua propagação ou em situações de emergência

[3] O recurso à computação em nuvem para o tratamento de dados não prejudica o âmbito de aplicação do RGPD.

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

> humanitária, em especial em situações de catástrofes naturais e de origem humana. (18)

O consentimento para o tratamento de dados pessoais

O consentimento deve ser demonstrável, específico, livre e livremente revogável (art. 7). Para ser livre, o consentimento não deve ser condição *sine qua non* de prestação de um serviço, se o tratamento de dados pessoais não for necessário para o efeito (vd. considerando 42 e 43). Por outro lado, na oferta direta de serviços da sociedade da informação a crianças, o tratamento de dados pessoais de crianças é lícito se elas tiverem pelo menos 16 anos, embora os Estados-Membros possam reduzir até 13 anos a idade para consentir (art. 8), como sucedeu com a lei portuguesa (art. 16 da Lei de Proteção de Dados Pessoais [LPDP]). Cabe ao RTD implementar medidas técnicas de controlo da idade do menor, operação que envolverá, só por si, o tratamento de dados pessoais do menor – vd. considerando 51.

O tratamento de categorias especiais de dados[4] está sujeito a uma proibição geral, pelo que apenas é admitido excecionalmente verificados determinados requisitos específicos, por ex. a proteção de interesses vitais só justifica o tratamento de dados se o titular estiver incapaz de consentir. Por outro lado, é reservada aos Estados-Membros a possibilidade de manterem ou imporem novas condições, incluindo limitações, no que respeita ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde (art. 9/4). Os primeiros (*genéticos*) são definidos como

> os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa (art. 4/13). (18)

Os segundos (biométricos) consistem em

> dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos (art. 4/15). (18)

[4] Tais como os que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

Por último, os dados relativos à saúde, são “os dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde” (art. 4/15) (24).

O dever de respeitar os direitos do titular dos dados

O RTD deve respeitar os direitos do titular de dados. Desde logo o direito à *transparência* das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados. Para o efeito deve prestar informações por escrito ou por outros meios, incluindo, se for caso disso, por meios eletrónicos, de forma concisa, transparente, inteligível e de fácil acesso, gratuita, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças. O RGPD especifica as informações a facultar consoante os dados pessoais sejam ou não recolhidos junto do titular (arts. 13 e 14).

Depois, no exercício do direito de acesso, o titular dos dados deve poder saber que dados, para que fins, durante quanto tempo, de que modo, é feito o tratamento e a quem se destinam os dados (art. 15).

São ainda direitos do titular de dados o direito de retificação e de apagamento (ou direito a ser esquecido) (25-28) (art. 16), o direito à limitação do tratamento (arts. 17 e 18), o direito de portabilidade dos dados (art. 20) e o direito de oposição ao tratamento e a decisões individuais automatizadas (art. 21) (29).

O exercício destes direitos pelo titular gera obrigações para o RTD, nomeadamente, no que respeita à retificação ou ao apagamento, o dever de comunicar

> a cada destinatário a quem os dados pessoais tenham sido transmitidos qualquer retificação ou apagamento dos dados pessoais […], salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado (art. 19). (18)

Todavia, o interesse público, nomeadamente a prevenção e o combate da fraude e da evasão fiscais, justificam restrições aos direitos do titular de dados pessoais.

Dever de aplicar medidas técnicas e organizativas adequadas

O RTD de aplicar *medidas técnicas e organizativas adequadas* (consoante a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares) para assegurar e comprovar a

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

conformidade do tratamento com o RGPD, devendo rever e atualizá-las consoante as necessidades (art. 24). Para demonstrar o cumprimento das suas obrigações o RTD pode utilizar o cumprimento de códigos de conduta ou de procedimentos de certificação aprovados nos termos do RGPD (arts. 41 e 42).

Depois, o RTD deve adotar medidas técnicas e organizativas adequadas, como a *pseudonimização*, no sentido da proteção de dados *desde a conceção e por defeito*. Por exemplo, essas medidas devem assegurar que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares (art. 25/1-2). O cumprimento desta obrigação pode fazer-se através de um procedimento de certificação aprovado nos termos do RGPD (art. 42).

No caso de as finalidades e os meios de tratamento serem determinados conjuntamente por dois ou mais responsáveis, dá-se uma situação de *responsáveis conjuntos* pelo tratamento, respondendo todos solidariamente sem prejuízo do acordo de divisão interna de responsabilidades (art. 26).

Dever de designação de representante na União

Os responsáveis pelo tratamento ou dos subcontratantes não estabelecidos na União devem *designar por escrito um representante* [5] na União, salvo se forem atividades ocasionais e que não envolvam o tratamento em larga escala de dados sensíveis, ou realizadas por autoridades ou organismos públicos (art. 27; vd. considerando 80). O RTD só pode recorrer a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas a cumprir o RGPD e respeite os direitos do titular dos dados (art. 28).

Dever de manter um registo dos tratamentos

O RTD tem o dever de manter um registo por escrito de todas as atividades de tratamentos efetuados, especificando as informações como o seu nome e contactos, e do seu representante e EPD, as finalidades do tratamento, as categorias de titulares de dados, dados pessoais, e destinatários, as transferências, prazos de apagamento dos dados, e descrição das medidas técnicas e organizativas de segurança (art. 30). Ficam isentos os

[5] Por *representante* entende-se "uma pessoa singular ou coletiva estabelecida na União que, designada por escrito pelo responsável pelo tratamento ou subcontratante, nos termos do art. 27º, representa o responsável pelo tratamento ou o subcontratante no que se refere às suas obrigações respetivas nos termos do presente regulamento" (art. 4/17). (18)

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

RTD com menos de 250 trabalhadores, a menos que tratem *dados sensíveis* ou relativos a condenações penais (art. 30/5).

Dever de assegurar um nível de segurança adequado ao risco

O RTD tem o dever de aplicar medidas técnicas e organizativas para assegurar um nível de segurança adequado ao risco, incluindo a pseudonomização e a cifragem de dados, a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento, e um processo para testar, apreciar e avaliar regularmente a eficácia dessas medidas (art. 32). A prova do cumprimento desta obrigação pode ser feita pelo cumprimento de um código de conduta ou de um procedimento de certificação aprovados conforme o RGPD (arts. 40 e 42).[6]

Dever de cooperar com a autoridade de controlo, incluindo o dever de notificação

O RTD tem o dever de cooperação com a autoridade de controlo (art. 31). Desde logo, o RTD deve notificar, em princípio no máximo de 72 horas, uma violação de dados pessoais à autoridade de controlo (art. 33). Se a violação de dados pessoais implicar um elevado risco para os direitos e liberdades das pessoas singulares, o RTD deve comunicar esse facto ao titular dos dados, a menos que tenha usado técnicas como a cifragem (art. 34). Como informa o considerando 85,

> Se não forem adotadas medidas adequadas e oportunas, a violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas singulares, como a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social significativa das pessoas singulares. (18)

Dever de avaliação de impacto

O RTD deve avaliar o impacto sobre a proteção de dados por ex. em caso de tratamento sistemático de dados sensíveis em larga escala (art. 35). De acordo com o considerando 91:

[6] O regime jurídico da cibersegurança foi aprovado pela Lei n.º 46/2018, de 13 de agosto, que transpõe a Diretiva (UE) n.º 2016/1148, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

> O tratamento de dados pessoais não deverá ser considerado de grande escala se disser respeito aos dados pessoais de pacientes ou clientes de um determinado médico, profissional de cuidados de saúde, hospital ou advogado. Nesses casos, a realização de uma avaliação de impacto sobre a proteção de dados não deverá ser obrigatória. (18)

A referência ao hospital juntamente com os profissionais de saúde isentos do dever de avaliação de impacto resulta manifestamente de um lapso de redação da versão portuguesa do RGPD, como se constata comparando-a com as versões inglesa, francesa ou castelhana.

Se se concluir que o tratamento envolve um elevado risco para os direitos e liberdades das pessoas singulares, o RTD tem o dever de proceder a consulta prévia à autoridade de controlo (art. 36).

O RGPD ressalva ainda que a lei interna de cada Estado-Membro pode inclusivamente sujeitar a autorização prévia da autoridade de controlo o tratamento por um responsável no exercício de uma missão de interesse público, incluindo o tratamento por motivos de proteção social e de saúde pública (art. 36/6) (30, 31).

Dever de designar um Encarregado da Proteção de dados (EPD/DPO)

O RTD deve designar um encarregado de proteção de dados (EPD) se for autoridade ou organismo público (podendo ser comum a vários organismos ou autoridades, tendo em conta a respetiva estrutura organizacional e dimensão), ou exercer atividade que exija o controlo de titulares de dados ou o tratamento de dados em grande escala (art. 37). Segundo as Orientações do Grupo de Trabalho do art. 29 (32), consideram-se de grande escala:

> o tratamento de dados de doentes no exercício normal das atividades de um hospital; tratamento de dados de viagem das pessoas que utilizam o sistema de transportes públicos de uma cidade (p. ex., através de passes de viagem); o tratamento em tempo real de dados de geolocalização de clientes de uma cadeia de restauração rápida internacional para fins estatísticos por parte de um subcontratante especializado na prestação desses serviços; o tratamento de dados de clientes no exercício normal das atividades de uma companhia de seguros ou de um banco; o tratamento de dados pessoais para fins de publicidade comportamental por um motor de busca; o tratamento de dados (conteúdo, tráfego, localização) por operadoras telefónicas ou por fornecedores de serviços de internet. (32)

Pela negativa, não são de grande escala os tratamentos de dados de doentes pacientes por um médico e os de dados pessoais relacionados com condenações penais e infrações por um advogado.

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

Sendo um grupo empresarial, o RTD pode designar um único EPD se houver um EPD facilmente acessível a partir de cada estabelecimento (art. 37/2). O RTD deve publicar os contactos do EPD e comunicá-los à autoridade de controlo. O RTD deve apoiar o EPD e respeitar a sua autonomia, no desempenho das suas funções de zelar pelo cumprimento do RGPD; funções essas que pode cumular com outras funções e atribuições que não resultem num conflito de interesses, o que cabe ao RTD assegurar (art. 38/8) (33).

Adoção de código de conduta e obtenção de certificação de proteção de dados (facultativo)

As associações de RTD elaboram códigos de conduta (art. 40). A supervisão destes códigos pode ser efetuada por um organismo que tenha um nível adequado de competência relativamente ao objeto do código e esteja acreditado para o efeito pela autoridade de controlo competente (art. 41). O organismo de *supervisão acreditado* pode suspender ou excluir um RTD que não cumpra o código de conduta.

Os RTD podem cumprir *procedimentos de certificação* em matéria de proteção de dados, bem como adotar selos e marcas de proteção de dados, para efeitos de comprovação da conformidade dos tratamentos com o RGPD (art. 42). A certificação, válida em princípio por três anos, é efetuada por organismo de certificação acreditado pela autoridade de controlo ou diretamente por esta (art. 43).

Transferências de dados para fora da União Europeia

O RTD pode transferir dados pessoais para países terceiros ou organizações internacionais, se atuar em conformidade com o RGPD (art. 44). Para o efeito, o RTD pode fazer transferências com base numa decisão da Comissão de adequação do nível de proteção do país terceiro (art. 45) (34).

Na falta de uma tal decisão de adequação, a transferência pode ocorrer se o RTD apresentar garantias adequadas e os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes (art. 46). Essas garantias adequadas podem resultar, por exemplo, de *regras vinculativas aplicáveis às empresas* (art. 47), de cláusulas-tipo de proteção de dados adotadas ou aprovadas pela Comissão, de código de conduta ou procedimento de certificação, acompanhados de compromissos vinculativos e com força executiva – cf. considerando 108.

Além disso, mesmo na ausência de uma decisão de adequação ou de garantias adequadas (por ex. regras vinculativas aplicáveis às empresas), as transferências para

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

países terceiros podem ser efetuadas para situações específicas, nomeadamente se houver consentimento explícito e informado do titular dos dados, se a transferência for necessária em sede contratual ou por razões de interesse público ou para proteger interesses vitais de pessoa incapaz de consentir, para além de outras derrogações para situações específicas previstas no art. 49.

Derrogações: liberdade de expressão e informação, acesso aos documentos da Administração Pública, em contexto laboral

A liberdade de expressão e de informação, incluindo o tratamento para fins jornalísticos e para fins de expressão académica, artística ou literária, justifica derrogações específicas ao regime geral de tratamento de dados (art. 85), tal como sucede com o tratamento e acesso do público aos documentos oficiais (art. 86), o tratamento do número de identificação nacional (art. 87) e o tratamento no contexto laboral (art. 88). Além disso, são previstas garantias e derrogações relativas ao tratamento para fins de arquivo de interesse público ou para fins de investigação científica ou histórica ou para fins estatísticos (art. 89). Por exemplo a pseudonimização só é obrigatória se os referidos fins puderem ser alcançados desse modo.

De igual modo, podem ser estabelecidas derrogações aos direitos de acesso, retificação, limitação e oposição na medida em que esses direitos possam tornar impossível ou prejudicar gravemente a realização dos fins específicos de investigação científica ou histórica ou fins estatísticos e que tais derrogações sejam necessárias para a prossecução desses fins (art. 89/2).

Obrigação de sigilo

O RGPD não prejudica a obrigação de sigilo a que o RTD esteja sujeito, por lei interna do Estado-membro, relativamente aos dados pessoais que tenha recebido no âmbito de uma atividade abrangida por essa obrigação de sigilo ou em resultado da mesma (art. 90). Por ex., o Regulamento de Deontologia Médica (35) encarrega os responsáveis pelo tratamento da informação de saúde de tomarem as

> providências adequadas à proteção da sua confidencialidade, garantindo a segurança das instalações e equipamentos, o controlo no acesso à informação, bem como o reforço do dever de sigilo e da educação deontológica de todos os profissionais (art. 37). (35)

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

O dever de confidencialidade da informação de saúde é reiterado no capítulo VII do Regulamento sobre a telemedicina (arts. 46 a 49) (36).

Segurança informática (Diretiva 2016/1148)

O regime jurídico da segurança do ciberespaço foi estabelecido pela Lei n.º 46/2018, de 13 de agosto (19), que transpõe a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. Analisamos primeiro os deveres de segurança informática segundo a Diretiva 2016/1148.

A Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, estabeleceu obrigações de segurança face ao *papel vital* das redes e da informação na sociedade e na economia e ao potencial lesivo dos incidentes de segurança, em termos de disponibilidade, autenticidade, integridade ou confidencialidade dos dados armazenados, transmitidos ou tratados, e dos serviços utilizados. Por outro lado, a Diretiva criou uma rede de equipas de resposta a incidentes de segurança informática (rede de CSIRT) e um Grupo de Cooperação, incluindo os Estados-Membros, a agência europeia ENISA e a Comissão Europeia.

Destinatários das normas de segurança informática da Diretiva 2016/1148

Os deveres de segurança recaem sobre os operadores de serviços essenciais (energia, transportes, banca e bolsas, hospitais e clínicas privadas, fornecedores de água potável, e infraestruturas digitais - anexo II) e os prestadores de serviços digitais (mercados em linha, motores de pesquisa em linha, e serviços de computação em nuvem - anexo III). São excluídas deste regime as empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público, na aceção da Diretiva 2002/21/CE, e os prestadores de serviços de confiança na aceção do Regulamento 910/2014 (eIDAS), uma vez que tanto estes como aquelas ficam sujeitos aos requisitos de segurança estabelecidos nos respetivos diplomas. Por exemplo, o Regulamento eIDAS estabelece como requisitos de segurança aplicáveis aos prestadores de serviços de confiança (i) a adoção de medidas para impedir ou reduzir ao mínimo o impacto dos incidentes de segurança e informar as partes interessadas dos efeitos adversos dos eventuais incidentes, e (ii) o dever de notificação da autoridade nacional de segurança e da

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

autoridade de proteção de dados de todas as violações da segurança ou perdas de integridade que tenham um impacto significativo sobre o serviço de confiança prestado ou sobre os dados pessoais por ele conservados. Por seu turno, as medidas de controlo de segurança e gestão dos riscos de segurança na moeda eletrónica, em especial a notificação de incidentes, estão previstas na Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 relativa aos serviços de pagamento no mercado interno (altera as Diretivas 2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) 1093/2010, e revoga a Diretiva 2007/64/CE).

Na noção de serviço digital pode incluir-se o *software* considerado dispositivo médico. Com efeito, um domínio cada vez mais importante de aplicação das normas de segurança informática no setor da saúde diz respeito aos dispositivos médicos, que atualmente podem consistir em software nos termos do Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho de 5 de abril de 2017 relativo aos dispositivos médicos. Nos termos do art. deste regulamento, por dispositivo médico entende-se

> qualquer instrumento, aparelho, equipamento, software, implante, reagente, material ou outro art., destinado pelo fabricante a ser utilizado, isolada ou conjuntamente, em seres humanos, para um ou mais dos seguintes fins médicos específicos: (a) diagnóstico, prevenção, monitorização, previsão, prognóstico, tratamento ou atenuação de uma doença, lesão ou deficiência, (b) estudo, substituição ou alteração da anatomia ou de um processo ou estado fisiológico ou patológico, (c) fornecimento de informações por meio de exame in vitro de amostras provenientes do corpo humano, incluindo dádivas de órgãos, sangue e tecidos, e cujo principal efeito pretendido no corpo humano não seja alcançado por meios farmacológicos, imunológicos ou metabólicos, embora a sua função possa ser apoiada por esses meios. (37)

O considerando 19 do Regulamento clarifica que

> o software, por si só, é qualificado como dispositivo médico quando especificamente destinado pelo fabricante a ser utilizado para um ou vários fins médicos indicados na definição de dispositivo médico, ao passo que o software de uso geral, mesmo quando utilizado num contexto de saúde, ou o software previsto para fins relacionados com o estilo de vida e o bem-estar, não são um dispositivo médico. A qualificação de um software, quer como dispositivo quer como acessório, deverá ser independente da localização do software ou do tipo de interconexão entre este e um dispositivo. (37)

Deveres dos operadores de serviços essenciais

O operador de serviços essenciais fica sujeito aos deveres de segurança apenas no que respeita à prestação desses serviços e que podem não corresponder a toda a atividade

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

da empresa. Como se lê no preâmbulo da Diretiva 2016/1148 (cons. 22), a propósito do transporte aéreo, "os aeroportos prestam serviços que podem ser considerados essenciais por um Estado-Membro, tais como a gestão das pistas, mas também uma série de serviços que podem ser considerados não essenciais, como a disponibilização de áreas comerciais." (38)

Cabe aos Estados-Membros identificar os *operadores de serviços essenciais* nos setores da *energia* (eletricidade, petróleo, gás, incluindo empresas de comercialização, de distribuição, de transporte, operadores de rede, operadores de instalações de refinamento, tratamento ou armazenamento), *dos transportes* (aéreo, ferroviário, marítimo e fluvial, rodoviário – por ex., entidades gestoras aeroportuárias, aeroportos, operadores de controlo da gestão do tráfego aéreo, gestores de infraestruturas e empresas rodoviárias, empresas de transporte e entidades gestores dos portos, operadores de serviços de tráfego marítimo, autoridades rodoviárias e operadores de sistemas de transporte inteligentes), no *setor bancário* (instituições de crédito e infraestruturas do mercado financeiro, incluindo operadores de plataformas de negociação (bolsas) e contrapartes centrais), no *setor da saúde* (incluindo instalações de prestação de saúde, nomeadamente hospitais e clínicas privadas), no *setor do fornecimento e distribuição de água potável para consumo humano*, e *no setor das infraestruturas digitais* (incluindo pontos de troca de tráfego, prestadores de serviços e registos de DNS).

A identificação dos operadores de serviços essenciais faz-se segundo determinados critérios, tais como, por exemplo, saber se a entidade presta um serviço essencial para a manutenção de atividades societais e/ou económicas cruciais, se a prestação desse serviço depende de redes e sistemas de informação, e se um incidente pode ter efeitos perturbadores importantes na prestação desse serviço, tendo em conta: a) o número de utilizadores que dependem dos serviços prestados pela entidade em causa; b) a dependência de outros setores essenciais em relação ao serviço prestado por essa entidade; c) o possível impacto dos incidentes, em termos de intensidade e duração, sobre as atividades económicas e societais ou a segurança pública; d) a quota de mercado dessa entidade; e) a distribuição geográfica, no que se refere à zona que pode ser afetada por um incidente; f) A importância da entidade para a manutenção de um nível suficiente do serviço, tendo em conta a disponibilidade de meios alternativos para a prestação desse serviço (art. 6 da Diretiva 2016/1148). São ainda previstos fatores específicos por setor tais como a quantidade ou a percentagem de energia nacional gerada, para os fornecedores de energia,

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

o volume diário, para os fornecedores de petróleo, e a sua importância sistémica com base nos ativos totais ou no rácio ativos totais/PIB, para os serviços bancários ou as infraestruturas do mercado financeiro.

Obrigação de adotar medidas técnicas e organizativas adequadas

Os operadores de serviços essenciais devem adotar *medidas técnicas e organizativas* adequadas e proporcionadas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam nas suas operações e para reduzir ao mínimo o seu impacto, a fim de assegurar a continuidade desses serviços (39). As políticas de segurança dos operadores de serviços essenciais estão sujeitas a avaliação devendo para o efeito apresentar a respetiva documentação e provas da sua aplicação efetiva, tais como os resultados de uma *auditoria de segurança* efetuada pela autoridade competente ou por um auditor qualificado e que, no último caso, facultem os resultados dessa auditoria, incluindo os elementos de prova subjacentes, à autoridade competente. Se detetarem deficiências nas políticas de segurança ou na sua implementação, as autoridades competentes podem emitir instruções vinculativas dirigidas aos operadores de serviços essenciais, para que estes corrijam as deficiências detetadas (art. 15 da Diretiva 2016/1148).

Prestadores de serviços digitais

Por seu turno, os *prestadores de serviços digitais* são obrigados a garantir um nível de segurança proporcional ao grau de risco para a segurança dos serviços digitais que fornecem, dada a importância dos seus serviços para as operações de outras empresas na União. Entende-se que os requisitos de segurança aplicáveis aos prestadores de serviços digitais podem ser menos exigentes já que, na prática, o seu grau de risco é inferior ao grau de risco a que estão sujeitos os operadores de serviços essenciais. Assim, por exemplo, a autoridade competente não tem uma obrigação geral de supervisionar os prestadores de serviços digitais (considerandos 49 e 60 da Diretiva 2016/1148).

Isenção das micro e pequenas empresas

As microempresas e as pequenas empresas, tal como definidas na Recomendação 2003/361/CE da Comissão, de 6 de maio de 2003, estão isentas dos referidos deveres de segurança, de modo a não a ficarem sujeitas a encargos financeiros e administrativos desproporcionados (art. 16/11 da Diretiva 2016/1148 e cons. 53).

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

Dever de notificação dos incidentes de segurança

As entidades sujeitas a deveres de segurança têm um dever de notificar incidentes, i.e., *eventos com um efeito adverso real* na segurança das redes e da informação (art. 14/3 da Diretiva 2016/1148). As notificações de incidentes devem ser recebidas pelas autoridades competentes ou pelas equipas de resposta a incidentes de segurança informática (*Computer Security Incident Response Team* [CSIRT]). Para determinar a importância do impacto de um incidente são estabelecidos alguns parâmetros como (i) o número de utilizadores afetados pela perturbação do serviço essencial, (ii) a duração do incidente, e (iii) a distribuição geográfica, no que se refere à zona afetada pelo incidente (art. 14/4 da Diretiva 2016/1148).

Conclusões

A proteção de dados e a segurança informática são matérias da maior importância no domínio das comunicações eletrónicas em rede, com acentuado relevo no contexto pandémico. Este texto analisou o papel do responsável pelo tratamento de dados segundo o RGPD, passando em revista os princípios relativos ao tratamento de dados pessoais e os direitos dos respetivos titulares. Entre os vários deveres específicos do responsável pelo tratamento de dados sobressaem os de aplicar medidas técnicas e organizativas adequadas, de registar os tratamentos, de avaliar o impacto dos tratamentos e, consoante os casos, de designar um encarregado de proteção de dados.

A proteção de dados está intimamente ligada à segurança informática, sendo esta um pressuposto daquela. Por essa razão, foi igualmente importante conhecer as obrigações legais em matéria de segurança informática à luz da Diretiva da União Europeia sobre a segurança dos sistemas e das redes de informação, que reconhece expressamente o “papel vital” destas redes e da informação na sociedade e na economia e o potencial lesivo dos incidentes de segurança, em termos de disponibilidade, autenticidade, integridade ou confidencialidade dos dados armazenados, transmitidos ou tratados, e dos serviços utilizados.

Referências

1. Rouvroy A. Poullet Y. The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In Gutwirth, ed. Reinventing Data Protection? Dordrecht: Springer; 2009. p. 45-76.

2. Pinto PM. O direito à reserva sobre a intimidade da vida privada. Boletim da Faculdade de Direito de Coimbra. 1993;64:479-586.

3. Marques G, Martins L. Direito da Informática. 2.ª ed. Coimbra: Almedina; 2006. p. 129-313, 422-442, 330-391.

4. Gonçalves ME. Direito da Informação. Novos Direitos e Formas de Regulação na Sociedade da Informação. 2.ª ed. Coimbra: Almedina; 2003. p. 82-111, 173-183.

5. Pinheiro AS. Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional. Lisboa: AAFDL; 2015. p. 825

6. Canotilho JJG, Moreira V. Constituição da República Portuguesa Anotada. 4.ª ed. Coimbra: Coimbra Editora; 2007. p. 551.

7. Ribeiro JS. A tutela de bens da personalidade na Constituição e na jurisprudência constitucional portuguesas. In: Alves FA, ed. Estudos de Homenagem ao Prof. Doutor José Joaquim Gomes Canotilho. Vol. III. Coimbra: Coimbra Editora; 2013. p. 853-859.

8. Portugal. Tribunal Constitucional. Acórdão n.º 442/2007, de 14 agosto de 2007. Processo n.º 815/2007 (considerando que o sigilo bancário não integra a esfera íntima da vida privada). Disponível em: https://www.tribunalconstitucional.pt/tc/acordaos/20070442.html

9. Portugal. Tribunal Constitucional. Acórdão n.º 403/2015. Processo n.º 773/15, de 17 de setembro de 2015 (considerando o direito à autodeterminação informativa como manifestação, juntamente com o direito à solidão e o direito ao anonimato, do direito ao livre desenvolvimento da personalidade previsto no art. 26 da CRP). Disponível em: https://www.tribunalconstitucional.pt/tc/acordaos/20150403.html

10. Portugal. Supremo Tribunal de Justiça. Acórdão do Supremo Tribunal de Justiça n.º 2/2008, de 13 de fevereiro de 2008. Publicação: Diário da República n.º 63/2008, Série I de 2008-03-31. Disponível em: https://dre.pt/home/-/dre/246534/details/maximized

11. Portugal. Tribunal Constitucional. Acórdão n.º 437/05, de 12 de setembro de 2005. Processo n.º 679/05. Disponível em: https://www.tribunalconstitucional.pt/tc/acordaos/20050437.html

12. Tribunal Europeu dos Direitos Humanos. Acórdão Satakunnan Markkinapörssi Oy and Satamedia Oy c. Finlândia [GC], de 27 de junho de 2017, § 137. Disponível em: https://www.echr.coe.int/

13. Sloot B, Borgesius FZ. Google and Personal Data Protection. In: A. Lopez-Tarruela A ed. Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models. The Hague: Asser/Springer; 2012. p. 75-111.

14. Franceschi A, Lehmann M. Data as tradeable commodity and new measures for their protection. The Italian Law Journal. 2015;1(1):51-72.

15. Sedgewick MB. Transborder data privacy as trade. California Law Review. 2017;105(5):1513-1542.

16. Bishnoi V. Data protection law: An inhibition in enforcement and promotion of competition law. European Competition Law Review. 2019;40(1):34-4.

17. Cram I. The right to respect for private life: digital challenges, a comparative-law perspective – The United Kingdom. Brussels: European Parliamentary Research Service; 2018. p. 14-20.

18. União Europeia. 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.

19. Portugal. Lei n.º 46/2018, de 13 de Agosto de 2019. Estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. Emissor: Assembleia da República. Publicação: Diário da República n.º 155/2018, Série I de 2018-08-13, p. 4037 1 – 4037.

20. Portugal. Lei n.º 58/2019, de 8 de Agosto de 2019. Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento 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. Emissor: Assembleia da República. Publicação: Diário da República n.º 151/2019, Série I de 2019-08-08, p. 3 – 40.

21. Clement J. Google, Amazon, Facebook, Apple, and Microsoft (GAFAM) - statistics & facts. Statista [Internet]. 4 fev. 2021. Disponível em: https://www.statista.com/topics/4213/google-apple-facebook-and-amazon-gafa/

22. Blume P. Data Protection in the Cloud. Computer Law Review International. 2011;3:76-80.

23. Hon WK, Hörnle J, Millard C. Data protection jurisdiction and Cloud Computing – when are cloud users and providers subject to EU Data protection law? The Cloud of Unknowing. International Review of Law, Computers & Technology. 2012;26(2-3):129-164.

24. Matos FA. O Regulamento de Protecção de Dados Pessoais (2016/679) no contexto dos desafios da actividade seguradora — o caso particular dos seguros de saúde. Revista Bolsa, Banca e Seguros. 2018;3:51-122.

25. União Europeia. Tribunal de Justiça. Acórdão do Tribunal de Justiça (Grande Secção) de 13 de maio de 2014. Google Spain SL e Google Inc. contra Agencia Española de Protección de Datos (AEPD) e Mario Costeja González. Processo C-131/12.

26. União Europeia. Tribunal de Justiça. Acórdão do Tribunal de Justiça (Grande Secção) de 24 de setembro de 2019 (pedido de decisão prejudicial apresentado pelo Conseil d'État – França) – Google LLC, sucessora da Google Inc./Commission nationale de l'informatique et des libertés (CNIL). Processo C-507/17.

27. Casimiro SV. O direito a ser esquecido pelos motores de busca: o Acórdão Costeja. Revista de Direito Intelectual. 2014;2:307-353.

28. Calvão F. A protecção de dados pessoais na internet: desenvolvimentos recentes. Revista de Direito Intelectual. 2015;2:67-84

29. Gregorio G. From Constitutional Freedoms to the Power of the Platforms: Protecting Fundamental Rights Online in the Algorithmic Society. European Journal of Legal Studies. 2019;11(2):65-103.

30. Grupo de Trabalho do Artigo 29.º para a Proteção de Dados. Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é "suscetível de resultar num elevado risco" para efeitos do Regulamento (UE) 2016/679 (adotadas em 4 de abril de 2017, revistas e adotadas pela última vez em 4 de outubro de 2017). WP 248 rev.01.

31. Portugal. Regulamento n.º 798/2018, de 14 de novembro. Lista de tratamentos de dados pessoais sujeitos a avaliação de impacto sobre a proteção de dados. Emissor: Comissão Nacional de Proteção de Dados (CNPD). Publicação: Diário da República n.º 231/2018, Série II de 2018-11-30, p. 32031 – 32032.

32. Grupo do Artigo 29.º para a Proteção de Dados. Orientações sobre os encarregados da proteção de dados (EPD) (adotadas em 13 de dezembro de 2016, com a última redação revista e adotada em 5 de abril de 2017). WP 243 rev.01.

33. Cordeiro ABM. A Autonomia da Função de Encarregado de Proteção de Dados e a Independência do Exercício da Advocacia. Revista da Ordem dos Advogados. 2018;78(I-II):17-38.

34. União Europeia. Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho [notificada com o número C(2016) 4176]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32016D1250

35. Portugal. Regulamento n.º 707/2016, de 21 de julho de 2016. Regulamento de Deontologia Médica. Emissor: Ordem dos Médicos. Publicação: Diário da República n.º 139/2016, Série II de 2016-07-21, p. 22575 – 22588.

36. Pereira ALD. A proteção dos dados pessoais no direito português, em especial no setor da saúde. In: Caletrio AB, Vaquero JPA, eds. Algunos desafios en la proteccion de datos personales. Madrid: Comares; 2018.

37. União Europeia. Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos, que altera a Diretiva 2001/83/CE, o Regulamento (CE) n.° 178/2002 e o Regulamento (CE) n.° 1223/2009 e que revoga as Diretivas 90/385/CEE e 93/42/CEE do Conselho.

38. União Europeia. Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

39. ISO 27001. O que é a norma ISO 27001? Integrity [Internet]. [s.d.] Disponível em: https://www.27001.pt/

Submetido em: 28/02/21
Aprovado em: 09/04/21

Como citar este artigo

Dias Pereira AL. Proteção de dados e segurança informática no setor da saúde: o papel dos responsáveis pela proteção de dados no Direito da União Europeia. Cadernos Ibero-Americanos de Direito Sanitário. 2021 abr./jun.;10(2):211-232.

https://doi.org/10.17566/ciads.v10i2.772