Centro de Direito Biomédico

PROTECÇÃO DE DADOS PESSOAIS EM SAÚDE

ARMINDO GIDEÃO K. JELEMBI

PROTECÇÃO DE DADOS PESSOAIS EM SAÚDE

Conforme a Lei de Protecção de Dados Pessoais de Angola, e tendo presentes o Regulamento Geral de Protecção de Dados da União Europeia e a Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais

ARMINDO GIDEÃO K. JELEMBI

Centro de Direito Biomédico
Universidade de Coimbra

FICHA TÉCNICA

PROTECÇÃO DE DADOS PESSOAIS EM SAÚDE

Conforme a Lei de Protecção de Dados Pessoais de Angola, e tendo presentes o Regulamento Geral de Protecção de Dados da União Europeia e a Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais

Autor
Armindo Gideão K. Jelembi

Editor
Centro de Direito Biomédico
Faculdade de Direito da Universidade de Coimbra
Pátio das Escolas · 3004-528 Coimbra
Telef./Fax: 239 821 043 · cdb@fd.uc.pt
www.centrodedireitobiomedico.org

Execução Gráfica
Ana Paula Silva
apsilva.design@gmail.com

ISBN
978-989-36320-2-4 · Impresso
978-989-36320-1-7 · Ebook

O Centro de Direito Biomédico, fundado em 1988, é uma associação privada sem fins lucrativos, com sede na Faculdade de Direito da Universidade de Coimbra, que se dedica à promoção do direito da saúde entendido num sentido amplo, que abrange designadamente, o direito da medicina e o direito da farmácia e do medicamento. Para satisfazer este propósito, desenvolve acções de formação pós-graduada e profissional; promove reuniões científicas; estimula a investigação e a publicação de textos; organiza uma biblioteca especializada; e colabora com outras instituições portuguesas e estrangeiras.

ABREVIATURAS E MODO DE CITAR

Adoptamos a forma de citar da seguinte forma: indicação da identidade do autor, título da obra, editora, local da publicação, ano, seguindo-se o número da página. Sempre que a citação já tiver ocorrido, será referido apenas o nome do autor, o título da obra abreviada e o número da página.

Relativamente à lei, sempre que a indicação do artigo não se fizer acompanhar da fonte é porque se trata da lei de protecção de dados pessoais em vigor em Angola. Pode ocorrer que, estando a discorrer sobre a explicação ou entendimento de questões relativas a um diploma legal específico e indicarmos na sequência várias normas, seja bastante a referência do diploma na primeira norma, porque quando houver mudança de diploma a referência será feita à primeira norma correspondente ao novo diploma.

Como a nossa escrita não corresponde às regras do acordo ortográfico da CPLP de 1990, sempre que citarmos um autor cujo país aderiu ao referido acordo, respeitaremos a escrita original da fonte citada, garantindo assim o rigor científico.

AAFDL	Associação Académica da Faculdade de Direito de Lisboa
al.	alínea
art.	artigo
APD	Agência de Protecção de Dados
BFD	*Boletim da Faculdade de Direito* (Universidade de Coimbra)

CC	Código Civil
CEDIS	Centro de I&D sobre Direito e Sociedade
cfr.	conferir
CJ	Coletânea de Jurisprudência
CNPD	Conselho Nacional de Protecção de Dados (Portugal)
CPA	Código de Procedimento Administrativo
CPC	Código de Processo Civil
CRA	Constituição da República de Angola
CUACPDP	Convenção da União Africana de Cibersegurança e Protecção de Dados Pessoais
ed.	edição
LPDP	Lei de Protecção de Dados Pessoais
n.º	número
RDC	*Revista de Direito Civil*
RJLB	*Revista Jurídica Luso-Brasileira*
RGPD	Regime Geral de Protecção de Dados
RRDDIS	*Revista Rede de Direito Digital, Intelectual & Sociedade*
seg.	seguinte(s)
TJUE	Tribunal de Justiça Europeu
UC	Universidade de Coimbra

ÍNDICE

1. GENERALIDADES

A protecção de dados pessoais é hoje uma preocupação permanente. O reforço dessa protecção e a sua consciencialização tiveram início com o desenvolvimento da sociedade de informação, que veio delimitar a esfera de garantia: o objecto de tutela não são os dados em si, mas a pessoa titular dos dados pessoais. É um instrumento de prevenção contra potenciais riscos que o tratamento de dados possa causar contra a esfera jurídica da pessoa, e oferece medidas de responsabilização civil, administrativa e criminal pelos danos causados ao titular dos dados e contra o responsável pelo tratamento indevido e pela inobservância das leis e regulamentos do sistema de protecção de dados.

As nossas relações com pessoas e instituições, de forma presencial ou remota, deixam sempre rastos dos nossos dados. Num primeiro momento a preocupação estava simplesmente colocada do lado da privacidade. Agora os dados pessoais são verdadeiros bens transaccionáveis nos diversos segmentos do mercado, de tal maneira que a nova preocupação é a de que os proventos económicos de quem faz o processamento dos dados não deixe de fora o titular dos mesmos,

proporcionando-lhe determinados benefícios[1]. Daí que a protecção vá além da privacidade, e que exista o direito, por exemplo, à oposição, ao tratamento ou à revogação do consentimento[2].

A privacidade está a ceder a determinadas exigências manifestadas em reclamações colectivista. Os transumanistas representam a vanguarda desta reivindicação em nome de um "bem-estar do homem"[3]. Os vários sistemas de videovigilância em nome da segurança pública, a recolha de dados quando se abre uma conta bancária, quando realizamos uma compra *online*, quando efectuamos uma consulta *online*, quando é executada uma telecirurgia, enfim, estamos expostos de tal forma à tecnologia e a interesses de terceiros que a nossa privacidade fica à mercê de ataques. Vivemos numa sociedade de risco, sob a sensação de que temos todos um "telhado de

---

[1] Alan F. WESTIN, *Privacy and Freedom*, New York: Atheneum, 1967, 324. Apesar do facto de este autor ter manifestado as suas ideias no início da segunda metade do século passado, já indicava uma doutrina que defendia um certo tipo de propriedade ou apropriação das informações pessoais. Neste sentido, o indivíduo seria o titular de direito de propriedade sobre as suas informações, podendo, neste sentido, e não violando valores ínsitos nos direitos de personalidade, comercializar os seus dados, não ficando os mesmo ao dispor de quem realiza o seu processamento.

[2] Inês Camarinha LOPES, *Os Dados Sensíveis dos Menores à Luz do RGPD*, Coimbra: GestLegal, 2021, 72.

[3] Adriano Martelo GODINHO, *Transhumanismo e Pós-Humanismo: a Humanidade em seu Limiar*, nº 2, Edição Instituto Jurídico / Faculdade de Direito da Universidade de Coimbra, 2024, 48. O autor afirma que o "transhumanismo vislumbra, em essência, o ultrapassar os limites impostas à condição humana". Citando Max More, define transhumanismo como sendo "a filosofia baseada na razão e um movimento cultural que afirma a possibilidade e o desejo de aperfeiçoar fundamentalmente a condição humana pelos meios da ciência e da tecnologia. Transhumanistas buscam a continuação e a aceleração da vida inteligente para além da sua forma humana corrente e das limitações humanas por via da ciência e da tecnologia, guiados por princípios e valores promotores da vida".

vidro", onde a protecção é frágil. Afinal, a fragilidade humana, tantas vezes invocada para justificar determinados deveres de protecção, vai-se tornando mais efémera. Por natureza, na nossa peregrinação terrena nascemos e morremos imbuídos de uma fragilidade, "fragilidade que – conforme ensina JOÃO CARLOS LOUREIRO – se revela, desde logo, no ser 'animal incompleto', carente ou defectivo, condicionado, mas não determinado, pelos instintos, aberto ao mundo, ou, melhor, tendo a mundanidade como nota constitutiva, um ser 'ex-cêntrico'"[4]. Vivemos sempre incompletos, sendo a nossa intersubjectividade dialógica na comunidade um instrumento de contínua acção de completude. Manifesta-se em nós uma constante vulnerabilidade, carecendo da força protectora do Direito para colmatá-la[5].

A protecção de dados visa fundamentalmente evitar que a disponibilidade dos dados pessoais do seu titular para o responsável pelo tratamento abra uma janela da sua privacidade e intimidade e seja conhecida por terceiros; por exemplo, os produtos da actividade imagiológica, ou aqueles que permitem identificar os elementos genéticos dos pacientes submetidos a vários exames de diagnóstico, tornarem-se do domínio de conhecimento que ultrapassa o estritamente necessário para a actividade médica.

Como acabamos de deixar expresso, os dados ganharam uma importância para os processos económicos e para o processo de *marketing*. As empresas necessitam cada vez mais de conhecer os seus clientes, o que não tem escapado à actividade médica, com a

---

[4] *Constituição e Biomedicina: Contributo para uma teoria dos deveres bioconstitucionais na esfera da genética humana*, vol. I, Faculdade de Direito da Universidade de Coimbra, 2003, Tese de doutoramento, 38.

[5] António Menezes CORDEIRO, "Vulnerabilidades e Direito Civil", *Revista da Faculdade de Direito da Universidade de Lisboa*, Número Temático: Vulnerabilidade(s) e Direito, 62/ 1 (2021) 21-58.

participação dos particulares nos sistemas nacionais de saúde e da actividade seguradora no ramo da saúde. Esta realidade tornou a informação sobre nós tão importante que o conteúdo ganhou um valor económico inexorável. Vai-se assim esfumando a tradicional ideia de considerar o aspecto económico como secundário, pois, na verdade, os efeitos económicos associados aos dados pessoais não podem ser menosprezados. A informação sobre a saúde das pessoas passou a ser objecto de acrescido interesse por parte das instituições de saúde, e não só (as seguradoras e os bancos também utilizam tais informações). Os dados têm também importância para a planificação e definição pelos governos de políticas públicas, utilizando para o efeito censos populacionais. Para uma cada vez maior prestação de cuidados de saúde às pessoas, os dados revelaram-se igualmente importantes, desde logo, para identificar e determinar grupos de pessoas com determinado tipo de doenças, o tipo de doenças que afecta determinado tipo de pessoas, identificação de endemias, epidemias e pandemias, o controlo da deslocação de massa populacional em áreas com pandemias (como acontece em África com a cólera, febre amarela, o ébola e, a nível global, com a Covid-19).

Para o que interessa neste estudo, devemos esclarecer que o objecto de estudo é a protecção jurídica dos dados pessoais em saúde. O termo "saúde" é aqui tomado na sua forma mais ampla. Assim, iremos abordar este agudo problema analisando a especificidade dos dados pessoais em saúde, enquanto aquele conjunto de informações de natureza pessoal relativo ao bem-estar físico e psíquico, incluindo também informações genéticas e da vida sexual, e visando um contributo dogmático para a sua compreensão.

Importa também referir que o estudo abordará, de forma mais genérica, referindo onde for necessário, a ligação do tratamento de dados pessoais nos cuidados de saúde e na saúde pública. A ambos faz referência a LPDP, no nº 2 do art. 14º, cuja epígrafe é "Requisitos específicos para o tratamento de dados sensíveis de saúde e da vida sexual", acrescentando-lhe os dados genéticos e biométricos,

pelo que doravante a referência a dados de saúde engobará os demais itens. Justifica-se que assim seja, pois, sendo os dados relativos à saúde considerados legalmente como dados sensíveis, por estarem ligados ao mais restrito reduto ético da pessoa, impõe uma especialidade no seu tratamento. Tomando de empréstimo as palavras de Paulo Mota Pinto e concordando com o Professor coimbrão, "(…) os dados pessoais sobre o estado de saúde do titular" constituem "parte integrante da esfera da vida privada"[6].

A Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais (CUACPDP), adoptada pela 23.ª sessão ordinária da Cimeira realizada em Malabo, Guiné Equatorial, aos 27 de Junho de 2014, ratificada por Angola através da Resolução da Assembleia Nacional n.º 33/19, de 9 de Julho, determina no art. 4.º, al. *a)* que "o processamento de dados pessoais envolvendo informação genéticas e a investigação na área da saúde", deve ser implementado por meio de acções, depois de autorização da autoridade nacional de protecção, abrangendo-se também o "processamento de dados pessoais relativos a informações biométricas" – al. *d)*.

A referência à CUACPDP é relevante por ser regulamentação resultante da competência territorial e material da União Africana, espaço continental onde estamos inseridos com compromissos políticos, económicos e culturais muitos fortes. Aliás, os objectivos traçados pela União Africana (UA) e constantes do seu Acto Constitutivo, referem explicitamente no art. 3º que a coordenação e harmonização das políticas entre Comunidades Económicas Regionais, existentes e futuras, devem assentar: *a)* uma África unida e forte; *b)* integração política e sócio-económica; *c)* estabelecimento de condições que habilitem África a desempenhar o seu legítimo

---

[6] "Protecção da Vida Privada e a Constituição", in *Direitos de Personalidade e Direitos Fundamentais. Estudos*, Coimbra, GestLegal, 2018,599.

papel na economia global e; *d)* desenvolvimento sustentável ao nível económico, social e cultural. Para alcançar estes objectivos, os *dados* constituem um factor imprescindível. Como parte de um dos objectivos de maior integração regional, a Assembleia da União, na sua 27ª Sessão Ordinária, de Julho de 2016 realizada em Kigali, no Ruanda, deliberou implementar um protocolo para a livre circulação de pessoas no continente. Esta deliberação tem implicações no intercâmbio de dados de identificação dos cidadãos, tendo em atenção a tutela da privacidade normalizada e segura, no contexto do cruzamento das fronteiras e do intercâmbio subsequente de dados pessoais através das fronteiras, como nos casos em que um cidadão trabalha, reside ou faz transacções fora do seu país de origem. A circulação de pessoas, bens e serviços, como um elemento de integração e unidade mais profunda, implica também ela a transacção de dados pessoais. Significa que devem ser adoptadas políticas e obrigações entre Estados para que o intercâmbio de dados seja seguro, transparente, robusto e respeitador da privacidade das pessoas.

Ao nível europeu, estas questões vêm previstas no Regulamento Geral de Protecção de Dados (RGPD), no art. 9º, nº 2, al. *h)* e al. *i)*. A al. *h)* preceito visa englobar a "medicina preventiva ou de trabalho; o diagnóstico médico; a prestação de cuidados ou tratamentos de saúde ou de acção social; e a gestão de sistemas e serviços de saúde, e de acção social, incluindo o tratamento por parte da administração e das autoridades centrais nacionais desses dados para efeitos de controlo da qualidade, informação de gestão e supervisão geral a nível nacional e local do sistema de saúde ou acção social, assegurando a continuidade dos cuidados de saúde ou de acção social". A al. *i)* atende "a protecção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos"[7].

[7] A. Barreto Menezes CORDEIRO, *Direito da Proteção de Dados à Luz do RGPD e da Lei nº 58/2019*, reimpressão, Coimbra: Almedina, 2022, 249-251.

1.1 O que é protecção de dados pessoais?

O desenvolvimento da ciência e da tecnologia está a quebrar dogmas e tabus. Não vivemos num mundo idealizado por "boas vontades". Vivemos num mundo problemático, em permanente transformação (transformações essas algumas vezes más e rápidas), com excesso de utilização de tecnologia da chamada nova revolução industrial, ou simplesmente revolução digital, em que o risco de desumanização das pessoas e das instituições está patente. Por isso, são cobradas respostas dinâmicas e à altura dos referidos problemas e transformações. Não temos registo de que os tribunais angolanos tenham tratado do tema, e também não há literatura abundante sobre a questão central da recolha, tratamento, registo e transferência de dados pessoais.

Num campo de acção humana muito problematizante, é importante ter atenção à forma como alguns direitos, princípios e valores apresentam profundas diferenças de significação normativa, ainda que sejam abordados na mesma época. Os princípios, por exemplo, não surgem nem são estruturados com a predisposição para um fim concreto; apesar de estarem limitados, esses limites não são estanques, e comunicam com outros vectores do sistema jurídico, sofrendo o seu conteúdo influências endógenas e exógenas de vária ordem. Por isso, a ideia de protecção jurídica deve atender às características e à natureza dos direitos a proteger, bem como ao campo da vida, da actividade ou da zona social em que estão inseridos.

O direito à protecção de dados começou por se afirmar enquanto instituto orientado para a defesa dos indivíduos perante o Estado e outros poderes públicos. Na verdade, um dos marcos para firmar a regulação do tratamento de informação relativas a pessoas singulares foi o *hesseische Datenschutzgesetz*, de 07 de Maio de 1970, cujo

âmbito de aplicação estava restrito às pessoas colectivas públicas do Estado Federado alemão de Hesse, que procediam ao tratamento automatizado de dados. Na Suécia foi implementada a *Datalag,* de 11 de Maio de 1973, com um âmbito de aplicação mais alargado do que a lei de Hesse, pois abrangia qualquer entidade, desde que se procedesse ao tratamento de dados pessoais, cuja técnica de procedimento era mecânica[8].

Sendo certo que estas leis vieram assinalar um momento histórico na protecção de dados, também é verdade que os referidos instrumentos legais visaram mais a tomada de "medidas técnicas destinadas a proteger os dados pessoais". Para melhor reforçar a protecção das pessoas, urgiu estabelecer a distinção entre protecção técnica (*Datensicherung*) da protecção jurídica que o sistema pode oferecer aos titulares de dados (*Datenschutz*). A partir daqui, iniciou-se o processo de consolidação de um Direito da Protecção de Dados[9].

---

[8] Joel A. ALVES, "A regulação europeia de proteção de dados e a sua aplicação à administração pública", in Isabel Celeste M. FONSECA, coord., *Estudos de E-Governação, Transparência e Proteção de Dados*, Coimbra: Almedina, 2021, 35 seg. O autor explica que a preocupação das primeiras leis era de ordem "histórico-política. É que, como não resulta árduo de intuir, todos os referidos diplomas – como, de resto, a maioria dos que lhe sucederiam, um pouco por toda a Europa, na década subsequente – forjaram-se sob um contexto fortemente marcado pelas memórias do autoritarismo do totalitarismo. Donde, o receio de que, tal e qual sucedera com tecnologias como as escutas telefónicas ou as máquinas de cartões perfurados, num passado recente, também as potencialidades introduzidas pelo computador e pelas bases de dados informatizados pudessem vir a ser exploradas pelos detentores da autoridade pública com vista à construção de novas e cada vez mais sofisticadas formas de 'domínio total' sobre os indivíduos".

[9] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 31-32. O autor indica uma lista de bibliografia indicativa do percurso histórico deste direito.

O direito à protecção de dados pessoais veio expresso no Texto Constitucional angolano como *Habeas Data*, do latim "que tenhas os dados", atribuindo a qualquer pessoa o direito à protecção aos seus dados pessoais. Tal protecção funciona, primeiro, para garantir que o indivíduo possa obter as informações sobre si que estejam no banco de dados de uma entidade autorizada por lei. Em segundo lugar, como garantia fundamental, vem possibilitar que o indivíduo possa rectificar ou modificar os seus dados armazenados pelo responsável pelo tratamento, caso os considere inexatos. Assim está expresso no art. 69º da CRA. É, em síntese, uma acção constitucional sumária e especial que visa a tutela dos cidadãos perante os bancos de dados dos responsáveis públicos ou privados que exerçam tais funções, a fim de permitir o fornecimento e o acesso das informações registadas numa base de dados, bem como a sua rectificação, em caso de não estarem conformes, sejam susceptíveis de atingir negativamente a privacidade ou intimidade do titular dos dados.

A lei nº 22/11 de 17 de Junho, sobre a protecção de dados pessoais, estabelece no art. 5º um conjunto de definições e na al. *c)* define dados pessoais como "qualquer informação, seja qual for a sua natureza ou suporte, incluindo imagem e som, relativa a uma pessoa singular identificada ou identificável (titular de dados). É considerada identificável a pessoa que possa ser identificada, directa ou indirectamente, designadamente por referência a um número de identificação ou à combinação de elementos específicos da sua identificação física, fisiológica, psíquica, económica, cultural ou social".

No âmbito da União Africana, a CUACPDP determina no art. 1º (Definições) o conceito de dados como sendo: "qualquer informação relativa a uma pessoa singular identificada ou identificável, através da qual esta pessoa pode ser identificada, directa ou indirectamente, em particular através de referência a um número de identificação ou a um ou vários factores específicos à sua identidade física, fisiológica, mental, económica, cultural ou social". No essencial, esta definição é semelhante àquela constante na nossa lei de protecção de dados.

O Regulamento Geral de Protecção de Dados na Europa, no art. 4º, sobre definições, oferece-nos o conceito de dados pessoais como a "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, directa ou indirectamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via electrónica ou a um ou mais elementos específicos de identidade física, fisiológica, genérica, mental, económica, cultural ou social dessa pessoa singular".

1.2 Dados pessoais e sua especificidade em saúde

A lei de protecção de dados não traz uma definição específica sobre protecção de dados de saúde, pelo que ao trazermos esta terminologia queremos clarificar já qual o caminho a seguir. Numa dimensão mais lata falaremos, como não poderia deixar de ser, da protecção de dados pessoais e – noutra dimensão mais restrita, talvez uma subcategoria – os dados de saúde.

Apesar de a actividade de um estabelecimento hospitalar ser a prestação de cuidados de saúde (a cura, como muitas vezes se afirma), considera-se praticamente impossível que essa actividade esteja dissociada do tratamento de dados pessoais dos utentes, para uma adequada prestação de cuidados. Como afirmou SÉRGIO DEODATO[10], a intervenção para encontrar as soluções dos problemas dos utentes implica "um conhecimento do passado histórico de cada pessoa, que muitas vezes obriga a um conhecimento familiar, naquilo a que se denomina pela «historia pessoal e familiar de saúde». Ou

[10] *Proteção de Dados Pessoais de Saúde*, Universidade Católica Editora, 2017.

seja, a intervenção de saúde necessita aprofundar significativamente o conhecimento sobre a pessoa e a sua família, para que se possa diagnosticar e intervir de forma eficaz". Temos assim um primeiro elemento: os dados pessoais de saúde contêm uma condicionante, a de que o seu tratamento deve ser realizado por profissionais de saúde.

Os dados de saúde são os dados pessoais relativos à saúde física ou mental de uma pessoa, bem como as informações reveladas sobre o estado de saúde de uma pessoa constantes no sistema de prestação de serviços de saúde e que normalmente são recolhidos, registados e usados pelos profissionais de saúde para fins diversos. Estes dados são, como referido, considerados dados sensíveis pois, devido ao seu conteúdo, revelam uma situação de especial vulnerabilidade. A sua natureza sensível de dados de saúde não significa abertura à sua utilização descontrolada, já que, se assim acontecer, podem ocorrer danos na esfera de direitos fundamentais do seu titular, designadamente na sua dignidade, revelados no ataque à intimidade, privacidade e igualdade (racial, de oportunidade, de acesso, ou seja, discriminação e desigualdade[11]).

---

[11] Cfr. Sérgio Marços Carvalho de ÀVILA NEGRI / Maria Regina Detoni Calvacanti Rigolon KORKMAZ, "A normatividade dos dados sensíveis na lei geral de proteção de dados: ampliação conceitual e protecção da pessoa humana", *Revista de Direito, Governança e Novas Tecnologias*, Goiânia, 5/1 (2019) 63-85. Estes autores entendem que os dados sensíveis "são aqueles associados às opções e características basilares da *persona* e, portanto, aptos a gerar situações de discriminação e desigualdade". Para chegarem a esta conclusão, apresentam o seguinte exemplo real: "No ano de 2002, um estudo do King's College de Londres identificou um determinado gene em seres humanos responsável pela actividade da enzima MAOA. As conclusões da pesquisa indicaram que quanto menor fosse a produção dessa enzima, maior a probabilidade de o indivíduo desenvolver comportamentos antissociais, como crimes violentos, casos sofressem abusos. Um dos autores do estudo, o Professor Terrie Moffitti, observou, a partir dos resultados, a existência de uma relação de influência da constituição genética de uma pessoa sobre a sua sensibilidade a fatores ambientais, notadamente com relação ao comportamento de agressividade. De acordo com o

Os dados relativos à saúde podem ter por fonte, exemplificativamente, o seguinte:

a) Recolha de informações por um prestador de cuidados de saúde na ficha clínica, onde consta a "história clínica";
b) Informações que são convertidas em dados de saúde pelo cruzamento com outros dados, revelando o estado de saúde da pessoa ou os riscos de saúde;
c) Informações que se convertem em dados de saúde devido à sua utilização num contexto específico, como por exemplo informações relativas, no âmbito da Covid-19, a viagens para uma zona afectada, processada por um profissional de saúde para fazer um diagnóstico;
d) Informações provenientes de um inquérito de "autoverificação", em que os titulares dos dados respondem a perguntas relacionadas com a sua saúde, *v.g.*, indicação de sintomas.
e) Informações resultantes de processos de investigação científica (testes de vacinas ou outros fármacos, bem como de dispositivos médicos).

A Declaração Internacional sobre os Dados Genéticos Humanos, aprovada por unanimidade e aclamação, no dia 16 de Outubro de 2003, pela 32ª sessão da Conferência Geral da UNESCO, determinou no seu preâmbulo que "*reconhecendo ainda* que os dados

relato do jornal BBC, à época, em vista ao então chamado 'gene do crime', foi manifestado receio pela sociedade civil em vista de potenciais rotulagens dos portadores daquela condição genética, além de temores no sentido de que os governos passassem a apostar em medicamentos para combater o crime, ao invés de enfrentar os problemas sociais ligados à violência. Diante desta pesquisa, Stephen Post, especialista em bioética, destacou que a pessoa poderia ter a suscetibilidade genética e, no entanto, não manifestar ditos comportamento antissociais, não se podendo falar em determinismo. O potencial de vigilância pelo Estado dos indivíduos com essa condição resvalaria em nítida discriminação da pessoa a partir de um dado sensível".

genéticos têm uma especificidade resultante do seu caracter sensível e podem indicar predisposições genéticas dos indivíduos e que essa capacidade indicada pode ser mais ampla do que sugerem as avaliações feitas no momento em que os dados são recolhidos"; e que "esses dados podem ter um impacto significativo sobre a família, incluindo a descendência, ao longo de várias gerações, e em certos casos sobre todo o grupo envolvido"; além disso, "podem conter informações cuja importância não é necessariamente conhecida no momento em que são recolhidas as amostras biológicas e que podem assumir importância cultural para pessoas e grupos". Adianta ainda: "*sublinhando* que todos os dados médicos, incluindo os dados genéticos e os dados proteómicos, independentemente do seu conteúdo aparente, devem ser tratados com o mesmo grau de confidencialidade" e "*considerando* que a recolha, o tratamento, a utilização e a conservação dos dados genéticos humanos se revestem de uma importância capital para os progressos das ciências da vida e da medicina, para as suas aplicações e para a utilização desses dados para fins não médicos". A Declaração dispunha, para além do que deixamos referido *supra*, que "os princípios consagrados pela Declaração Universal sobre o Genoma Humano e os Direitos Humanos e bem assim os princípios de igualdade, justiça, solidariedade e responsabilidade, de respeito da igualdade humana, dos direitos humanos e das liberdades fundamentais, em particular da liberdade de pensamento e de expressão, incluindo a liberdade de investigação, assim como a protecção da vida privada e da segurança da pessoa, em que devem basear-se a recolha, o tratamento, a utilização e a conservação dos dados genéticos humanos", devem estar consagrados nas ordens jurídicas internas dos países que vierem a adoptar a Declaração.

A nível europeu, o RGPD no Considerando 35 dispõe que "deverão ser considerados dados pessoais relativos à saúde de um titular

de dados que revelam informações relativas ao seu estado de saúde física e mental no passado, no presente e no futuro"[12].

Neste sentido, tem-se entendido que a elaboração de um conceito de dados em saúde deveria abarcar todos os dados de carácter médico e também os que têm uma conexão com finalidades de saúde, os tratados no âmbito da saúde pública, seguros de doenças ou actividades científicas e estatísticas, incorporando toda a informação relativa ao corpo humano, incluindo a sexualidade, raça e código genético, os antecedentes familiares, hábitos de vida e consumo, enfermidades passadas e presentes ou previsíveis, assim como os dados psicológicos e referentes à saúde mental. Os dados psicológicos e mentais devem derivar expressamente de historial médico (de um determinado tratamento psicológico ou psiquiátrico), bem como os que provenham de pesquisas; nestes últimos há que levar em consideração que se trata de dados referentes à saúde das pessoas, diretamente à sua saúde mental ou com esta estreitamente relacionados [13]. Por sua vez, o art. 4º, nº 15 do RGPD define dados de saúde 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".

---

[12] Advirta-se que faremos muitas referências a instrumentos normativos europeus, aonde o desenvolvimento legislativo, dogmático e jurisprudencial está a um nível superior ao nosso. Os Considerandos e as Orientações serão muitas vezes citados, apesar de reconhecermos que não têm valor de lei. O seu objectivo é apenas o de "clarificar o sentido de uma norma ou de explicar as suas fundamentações, mas em caso algum poderão ser invocados para sustentar uma interpretação que não encontre correspondência na letra da lei. Neste sentido, e enquanto se reconheça a possibilidade de o responsável dirigir um pedido de esclarecimentos ao titular dos dados (…)", cfr. A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 264.

[13] J. SÁNCHEZ-CARO / F. ABELLÁN, *Telemedicina y Protección de Datos Sanitários, Aspectos Legales y Éticos*, Granada: Comores, 2002, 45.

A CUACPDP refere no art. 1º a definição de "dados no domínio da saúde" como "qualquer informação sobre o estado físico e mental de uma pessoa titular dos dados, incluindo as informações genéticas acima mencionadas". Este instrumento jurídico oferece também o conceito de dados sensíveis: "todos os dados pessoais relativos às opiniões ou actividades religiosas, filosóficas, políticas, sindicais, bem como relacionadas à *vida sexual* ou raça, *saúde*, medidas sociais, processos judiciais, sanções penais ou administrativas"[14].

Do conjunto de elementos que preenchem o "conceito" de dados pessoais de saúde retirados da legislação angolana, europeia e africana, são identificados em comum: *(i)* saúde física ou mental; *(ii)* informações genéticas; e *(iii)* dados sobre a prestação de serviços de saúde.

1.3 Protecção de dados como protecção de direitos fundamentais

Do ponto de vista constitucional, os deveres de protecção são deveres do Estado compreendidos como deveres de abstenção, de prestação *stricto sensu* e deveres de protecção. No plano da protecção de dados pessoais, aos particulares também incumbe o dever de abstenção, de não violação da vida privada dos outros, o que significa, ao nível jurídico, estarmos perante um exercício de revalorização desta categoria, elevando-a ao nível de deveres fundamentais *stricto sensu*. Novamente nos socorrendo de JOÃO CARLOS LOUREIRO, entende o Professor de Coimbra[15] que "os deveres fundamentais em sentido amplo compreendem não apenas os designados deveres fundamentais (*stricto sensu*), i. é., numa primeira aproximação,

---

[14] Itálico nosso.

[15] *Constituição e Biomedicina,* 1131.

os deveres dos cidadãos e também dos homens para com o Estado/comunidade, mas também os deveres destes para com os outros homens, os deveres do Estado para com os seus cidadãos e, no caso de direitos de todos, também para com os estrangeiros e apátridas residentes nessa comunidade estatal. Discutível é a possibilidade de individualizarmos deveres para consigo mesmo, por exemplo, um dever de viver, uma categoria recorrente na ética".

A CRA estabelece no art. 69º o *Habeas Data*, como ficou expresso *supra*. O âmbito de protecção desta norma é largo, mas não abrange toda a problemática envolvida na protecção de dados pessoais. Por exemplo, não responde a esta simples pergunta: o que podem os titulares dos dados exigir ao Estado quanto à protecção e ao gozo efectivo dos seus direitos? Apesar de o art. 28º da CRA estabelecer a força jurídica dos preceitos constitucionais respeitantes aos direitos, liberdades e garantias fundamentais, podendo serem aplicados directamente, a verdade é que o art. 69º não é suficientemente irradiador de normatividade tutelar dos direitos subjacentes ao direito à tutela do titular dos direitos de dados pessoais; daí a extensa regulamentação existente sobre a matéria. Ainda assim, reconhece-se o papel (obrigação) que o Estado tem de proteger e assegurar o direito fundamental relativo aos dados pessoais, e de impor o respeito dos direitos fundamentais como instrumentos de garantia da segurança jurídica, pois define o objecto real da exigência garantística com que o titular do direito de dados pessoais está coberto. Nestes termos, o núcleo essencial do direito fundamental de *Habeas Data* traduz, conforme ensinamento de VIEIRA DE ANDRADE, "as faculdades típicas que integram o direito, tal como é definido na hipótese normativa, e que correspondem à protecção da ideia de dignidade humana individual na respectiva esfera da realidade – abrangem aquelas dimensões dos valores pessoais que

a Constituição visa em primeira linha proteger e que caracterizam e justificam a existência autónoma daquele direito fundamental"[16].

A noção germânica de protecção de dados (*Datenschutz*), anunciada na década de setenta do século passado, rapidamente se generalizou como uma nova extensão da protecção dos direitos de personalidade, situação já referida *supra*. Como em muitas matérias jurídicas, a Alemanha tem estado na vanguarda do oferecimento legislativo, jurisprudencial e doutrinário de soluções aos problemas que a ciência e a tecnologia apresentam. Numa decisão do Tribunal Constitucional Federal, resultado de um conflito havido no âmbito de um censo realizado no ano de 1980, vários cidadãos organizados em grupos impugnaram a lei federal de recenseamento, tendo estabelecido um *Grundrecht auf informationelle Selbstbestimmung* (direito fundamental à autodeterminação). Noutra recente decisão, de 27 de Fevereiro de 2008, o mesmo tribunal reconheceu a existência do *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* (direito à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais), que era *ein neues Grundrecht* (novo direito fundamental) por força de um desdobramento da *informationelle Selbstbestimmung*[17]. Constitui um marco para o que veio a desenvolver-se na Europa e, por esta via (com intermediação lusa), chegou ao nosso ordenamento jurídico.

---

[16] *Os Direitos Fundamentais na Constituição Portuguesa de 1976*, 5.ª ed., Coimbra: Almedina, 2012, 165.

[17] Fabiano MENKE, "A proteção de dados e o direito fundamental à garantia da confidencialidade e da Integridade dos Sistemas Técnico-Informacionais do Direito Alemão", *RJLB* 5/1 (2019) 781-809, em particular, 782.

No espaço lusófono, a dogmática sobre direitos fundamentais está amplamente desenvolvida. GOMES CANOTILHO[18], por exemplo, entende que os direitos fundamentais exercem quatro funções. Vamos enumerá-las e, ao fazê-lo, tentaremos um enquadramento com a protecção de dados pessoais, designadamente dos dados de saúde: *(i)* uma função de defesa: os direitos fundamentais desempenham sua função de defesa, mormente, "a defesa da pessoa humana e da sua dignidade perante os poderes do Estado". Esta função é manifestada em duplo sentido: no sentido objectivo constitui normas de competência negativa para os poderes públicos, já que proíbem intromissões na esfera jurídica das pessoas, designadamente com a recolha e tratamento de dados pessoais sem o seu consentimento e sem observância do princípio da licitude; em sentido subjectivo, o poder de exercer de forma positiva direitos fundamentais e exigir dos poderes públicos posicionamento omisso por forma a evitar agressões lesivas. Quer dizer, o exercício do direito de acesso à informação sobre os seus dados recolhidos e tratados e o direito ao esquecimento, e ainda o princípio da duração do período de conservação dos dados; *(ii)* função de prestação, que concebeu o Estado Social de Direito em detrimento do Estado liberal, oferecendo-se o Estado para garantir aos cidadãos a realização das suas necessidades. O Estado deve actuar no sentido de satisfazer os bens sociais por meio da prestação de serviços ou da disponibilização de bens; (iii) função de protecção perante terceiros: o Estado está obrigado a proteger o titular de determinado direito contra actos de terceiros, inclusive adoptando as medidas necessárias para o livre exercício dos direitos. Quanto à protecção de dados pessoas, a LPDP tipificou a tutela administrativa e jurisdicional, bem como estabeleceu as con-

[18] *Direito Constitucional e Teoria da Constituição*, 7.ª ed., Coimbra, Almedina, 2003, 407 seg.

travenções e multas; *(iv)* função de não discriminação: o Estado tem o dever de tratar os seus cidadãos de forma igual e de garantir os direitos de igualdade consagrados na CRA. Esta função é deveras importante, pois a noção de dados sensíveis inclui os dados referentes à saúde e vida sexual, e os dados genéticos não podem servir fins discriminatórios, como bem determina o art. 23º da CRA, em que "ninguém pode ser prejudicado, privilegiado, privado de qualquer direito ou isento de qualquer dever" em razão do seu estado de saúde e da sua vida sexual, ou condição da pessoa resultante dos dados genéticos. Neste último ponto, sabemos que o genoma é o material genético de todos os seres vivos, cada qual com suas particularidades, e composto pelo DNA de cada espécie. O estudo dos genes e a informação genética estão organizados dentro do genoma, e como essa organização determina a sua função, o resultado da análise do genoma permite a compreensão de diversas doenças genéticas humanas. Este estudo, além de apresentar novos desafios jurídicos e éticos, torna complexa a questão da privacidade de dados, não apenas na definição da titularidade, mas especialmente no uso e tratamento dos dados em investigação, análises clínicas preventivas ou de tratamento, e até na sua comercialização[19]. A LPDP, no art. 13º, nº 3 dispõe que "o tratamento de dados sensíveis deve ser efectuado com garantias de não discriminação e mediante adopção das especiais medidas de segurança".

Na sociedade de informação a que estamos sujeitos, os dados pessoais estão intimamente ligados ao direito de se informar e de ser informado sobre os vários aspectos da vida. O chamado direito geral à autodeterminação informacional visa garantir e salvaguardar os direitos fundamentais relativos à defesa dos cidadãos perante o tratamento

[19] I. BERIAN, "Legal issues regarding gene editing at the beginning of live: an EU perspective". *Regenerative Medicine* 12/2 (2017) 669-679.

informático dos dados pessoais, particularmente os dados sensíveis, pois facilita o estabelecimento da diferenciação entre a esfera privada e a esfera do domínio [20]. Este direito geral é, a par do princípio da dignidade da pessoa humana, projecção jurídica, com a devida normatividade axiológica, para outros direitos, nomeadamente o direito de acesso, de rectificação, actualização e cancelamento, o direito de sigilo e a proibição do tratamento de dados sem consentimento.

A presença contínua da tecnologia nos nossos afazeres, do acordar até ao dormir – até durante o sono (vejam-se os instrumentos tecnológicos que registam a actividade de diversos órgãos, principalmente os batimentos cardíacos, enquanto dormimos) –, vai gerando nas pessoas uma admiração e curiosidade, levando a generalidade das pessoas a aceitarem as suas potencialidades na promoção do bem-estar das pessoas. Esta aceitação estende-se à evolução que impulsiona a tecnologia como factor decisivo da inovação. Este lado que entusiasma deve levar o jurista a escrutinar os possíveis efeitos da tecnologia na comunidade e na vida das pessoas. Deve-se atender a que a progressiva digitalização dos serviços de saúde e a utilização da IA nas relações entre médico (e demais profissionais da saúde) e doentes, nos procedimentos para o diagnóstico e na produção de medicamentos e dispositivos médicos tem vindo a suscitar problemas, perplexidades e dilemas que interrogam o Direito, entre os quais a sua influência na forma tradicional da protecção dos direitos fundamentais.

---

[20] Cristina QUEIROZ, "A protecção constitucional de recolha e tratamento de dados pessoais automatizados", in *Homenagem da Faculdade de Direito de Lisboa ao Professor Doutor Inocêncio Galvão Telles* – 90 Anos, Coimbra: Almedina, 2007, 291 seg. Veja-se ainda Alexandre Libório Dias PEREIRA, que entende que a protecção de dados pode ser vista como uma "projecção do direito à autodeterminação informativa". "Big data, e-health e «autodeterminação informativa»: A lei 67/98, a jurisprudência e o regulamento 2016/679 (GDPR), *Lex Medicinae: Revista Portuguesa de Direito da Saúde* 29 (2018) 53.

A protecção dos dados pessoais, nos termos colocados pela LPDP, configura um direito fundamental. No preâmbulo da referida lei o legislador justifica o direito à protecção das pessoas singulares porque "a consagração, na Constituição da República de Angola, do direito à reserva da vida privada e da possibilidade do recurso à providência «habeas data» representa manifestamente um grande passo na adopção de um quadro legislativo nesta matéria". O fundamento último do direito de se poder controlar o tratamento, a divulgação e a utilização de dados pessoais, tido como corolário do direito à autodeterminação informativa assenta na tutela da dignidade da pessoa humana e no livre desenvolvimento da personalidade. Nesta linha de pensamento andou também o nosso legislador ordinário, ao dispor no art. 1º da LPDP que a lei tem por objecto o estabelecimento das regras jurídicas aplicáveis "ao tratamento de dados pessoais com o objectivo de garantir o respeito pelas liberdades públicas e dos direitos e garantias fundamentais das pessoas singulares". Pode-se assim dizer que os dados pessoais são também direitos de personalidade e, nesta perspectiva, os dados pessoais constituem um dado normativo que é extensão da personalidade humana, uma vez que os referidos dados são elementos caracterizadores da individualização de uma pessoa. Daí a possibilidade de, após recolhidos os dados, serem feitas suposições e ser identificado o seu titular. Como direito de personalidade, o direito à titularidade dos dados pessoais segue a linha caracterizadora geral, designadamente a oponibilidade *erga omnes*, a intransmissibilidade, a indisponibilidade (com limitações), a imprescritibilidade, a extrapatrimonialidade e a inderrogabilidade[21]. Como é do domínio geral, com o desenvolvimento da ciência jurídica e dos posicionamentos da jurisprudência, estes requisitos

[21] Sobre as características dos direitos de personalidade, veja-se Rabindranath V. A. Capelo de SOUSA, *O Direito Geral de Personalidade*, Coimbra: Coimbra

não são de cumprimento absoluto, havendo, principalmente na indisponibilidade e na extrapatrimonialidade, uma clara relativização, e observando-se aqui a importância do instituto do consentimento, que o CC o previu no art. 340º, estando mais desenvolvido no contexto do sistema legal de protecção de dados. O consentimento constitui um meio através do qual o titular do direito de personalidade permite que as informações constitutivas dos seus dados pessoais possam tornar-se públicas e ser objecto de tratamento ao de indicarem especificadamente a finalidade da recolha dos dados.

A CUACPDP, no seu preâmbulo, para justificar o instrumento internacional, considerou que "a criação de um quadro normativo sobre a cibersegurança e protecção de dados pessoais leva em consideração as exigências do respeito dos direitos dos cidadãos, garantidos pelos textos fundamentais do direito interno e protegidos pelas Convenções e Tratados Internacionais sobre os Direitos Humanos, em particular a Carta Africana dos Direitos do Homem e dos Povos".

O direito à intimidade apresentou-se sempre como o poder ou faculdade do titular de exigir a não interferência de terceiros na sua vida privada. Mas ao apreciar-se a necessidade da sua protecção perante o rápido desenvolvimento dos meios e procedimentos de captação, divulgação e difusão da pessoa e dos seus dados, passou a conceber-se como um bem jurídico que se relaciona com a liberdade de acção do sujeito, com as faculdades positivas de actuação para controlar a informação relativa à sua pessoa e à sua família no âmbito público, dando forma ao que se vem chamando "segunda dimensão da intimidade", conhecida também como liberdade informática ou *habeas data*, que encontra suporte constitucional na CRA, já referida acima.

Editora, 1995, 401 seg. Também, Mafalda Miranda BARBOSA, *Lições de Teoria Geral do Direito Civil*, 2ª ed., Coimbra, GesTelegal, 2022,319-324.

A protecção de dados pessoais visa também outros dois aspectos importantes: a patrimonialidade deste direito, ou seja, a mercantilização dos dados ancorada na ideia da liberdade económica do mercado (*data-driven economy*), com a compatibilização do direito à privacidade e intimidade; e o desenvolvimento da actuação algorítmica na gestão de múltiplos assuntos que representam fortes riscos às liberdades individuais e às organizações, impondo uma regulamentação apertada, sob pena de o valor por detrás dos direitos de personalidade desvirtuar a dignidade humana.

A privacidade e intimidade, objecto da protecção de dados pessoas, estão inseridas no catálogo dos direitos e garantias fundamentais. Expressamente previstas no art. 32º da CRA, a privacidade e intimidade vêm caracterizadas como direito de personalidade que tutela, em especial, a integridade psíquica do sujeito, mediante o resguardo de aspectos íntimos e privados, as amizades, as relações amorosas e as convicções políticas, religiosas e sexuais. Incompreensivelmente, em pleno século XXI, altura da proclamação da CRA, esta não contém uma norma que aborde directamente a protecção de dados pessoais. Todavia, através de uma interpretação conforme à Constituição[22], pode ser considerada um direito fundamental.

O direito à informação e o uso de dados pessoais na produção de conhecimento (ou de informações) transformaram-se numa arma muito poderosa. Como veremos *infra*, a saúde pública, com a actuação dos seus profissionais, conta com uma larga experiência na produção de informação a partir de dados pessoais dos usuários do sistema de saúde, mas infelizmente o sector não conta com uma regulamentação robusta sobre o assunto, e a que existe é frágil, fragmentada e, por isso, instável. Conforme explicam duas inves-

---

[22] J. J. Gomes CANOTILHO, *Direito Constitucional e Teoria da Constituição*, 7.ª ed., Coimbra: Almedina, 2003, 1195 seg.

tigadoras, "identificam-se na discussão acerca da regulamentação e governança dos dados pessoais pelo menos duas dificuldades. Uma conceitual, em torno da noção de público e privado, para definir bens e interesses objecto da regulamentação. Outra relacionada à operacionalização desses conceitos na formulação de um modelo normativo de regulamentação e de governança em relação aos dados pessoais, que abrange, inclusive, a cessão e seu tratamento"[23].

Na verdade, sendo direitos fundamentais, não faz sentido que a dicotomia público *vs* privado ganhe importância. Mas para se elevar crítico-problematicamente a elevação do "privado" à importância do "público" (sem qualquer visão ideológica), será necessário preservar (ou harmonizar) proporcionalmente os interesses individuais com os legítimos interesses colectivos em relação à vida privada e à saúde. Afinal, é a valorização conceitual e operativa do princípio da dignidade da pessoa humana que, com o seu conteúdo de clara intenção ético-axiológica, exige uma formulação de um tipo de tutela colectiva à protecção da privacidade mais efectiva na protecção e garantia do uso dos dados pessoais para fins de interesse público.

A protecção dos dados pessoais, apesar de ter tutela constitucional, não é um direito absoluto. Primeiro, porque ao lado dos direitos estão, a montante, obrigações legais dos responsáveis pelo tratamento dos dados, nomeadamente na segurança dos dados pessoais, nas garantias de acesso e portabilidade dos dados pelos seus titulares, na obrigação de prestar informação para a obtenção do consentimento do titular dos dados, na gestão de riscos e outras obrigações que em especial a lei determinar. Em segundo lugar, o interesse legítimo de entidades públicas e o seu exercício do tratamento de dados muitas

---

[23] Miriam VENTURA / Cláudia Medina COELI, "Para além da privacidade: direito à informação na saúde, proteção de dados pessoais e governação", *CSP Cadernos de Saúde Pública* 34/7 (2018).

vezes fogem ao controlo do titular dos mesmos. Também a transferência de dados para fins de interesse público – como o caso da medicina preventiva e a investigação e estatística em saúde – fogem ao controlo do titular dos dados. Ultimamente os dados pessoais tornaram-se um activo económico de grande valor, surgindo no mercado entidades de intermediação para os transacionar. Passou a discutir-se com afinco a necessidade de melhorar os mecanismos de atribuição aos titulares de maior controlo sobre os seus dados. Com as situações acabadas de serem descritas, aqui e acolá vai surgindo um potencial de enfraquecimento a garantia do titular de dados pessoais em alcançar as ferramentas que lhe permitam o controlo efectivo sobre os seus dados. O risco torna-se mais presente quando se sucumbe à ideia (frágil nos argumentos) de que as instituições (o responsável) usarão os dados pessoais sob a sua responsabilidade apenas para "as finalidades" acordadas com que "realizarão o bem". Na realidade, o risco é aqui o de poderem transacionar os dados com entidades que consideram de inestimável valor económico (incluindo financeiro, tecnológico e científico). O mesmo vale para o responsável enquanto pessoa colectiva pública, visto que lhe está associada a ideia de "interesse público" e, assim, uma concepção de "supremacia moral do Estado e de outras entidades públicas", que são "pessoa de bem", mas esquecendo que estamos sob o manto de uma apertada vigilância em que os nossos dados são utilizados para fins que muitas vezes são de interesses de grupos, e não do Estado Democrático e de Direito. Os argumentos de prevenção de risco colectivo incluem riscos no âmbito laboral, riscos no âmbito da saúde, riscos no âmbito da segurança colectiva, enfim, legítimos fundamentos, mas muitas vezes fins ilícitos. Por isso, a tutela dos dados pessoais deve ser um *continuum*, um dever-ser, jurisprudencial e reconstitutivamente intencionada, não bastando a existência de normas preordenadas positivamente.

1.4 Protecção de dados, digitalização e inteligência artificial

O apoio da informática nas actividades burocráticas (e não só) veio torná-las mais eficazes. Facilitou a criação de muitos arquivos numa única base e o manuseamento dos diversos documentos sem necessidade de desfazer o arquivo.

A inteligência artificial (IA) está na ardem do dia. A utilização de algoritmos no processo de recolha, tratamento e armazenamento de dados pessoais dos utentes dos serviços e de outros serviços conectados com a IA, vem demonstrando grandes vantagens, mas suscita também agudas preocupações. No campo das vantagens podemos indicar a eficiência, a celeridade e a desmaterialização na gestão de processos. No entanto, a IA oferece neste campo problemas alarmantes de ética, desde logo devido à pouca falta de transparência no seu domínio. No actual nível de desenvolvimento, que coloca o algoritmo a gerar novo algoritmo, vão-se criando verdadeiras *black boxes*, impossibilitando, muitas vezes, que os seus criadores ou programadores identifiquem como foi processada a análise de dados assim como a determinação da forma como se obteve determinado resultado. Com a capacidade de processar grande volumes de dados em tempo real, a IA facilita a detecção de padrões e anomalias que poderiam indicar uma violação de dados, o que representa uma enorme vantagem. Ferramentas conduzidas pela IA podem inclusive identificar e neutralizar ameaças cibernéticas com uma precisão e velocidade que seriam impossíveis de alcançar com métodos tradicionais.

Apesar das vantagens anunciadas, a utilização da IA apresenta questões éticas e de privacidade. A capacidade da IA de recolher e analisar dados em larga escala pode levar à vigilância em massa e à invasão da privacidade, se não forem tomadas medidas de segurança adequada. É muito importante, por isso, estabelecer um equilíbrio

entre o uso da IA para proteger dados e, em simultâneo, garantir que os direitos de privacidade dos indivíduos sejam respeitados.

A área do diagnóstico foi, no campo da saúde, a pioneira a usar a IA. Por meio de *expert systems* já é possível realizar diagnósticos com muita precisão (dados laboratoriais, electrodiagnóstico, diagnóstico genético), fornecer dados clínicos (sobre registos de doenças e doentes, sobre investigações médicas; por exemplo, o reaproveitamento de medicamentos ou a adequação de um medicamento ao perfil de determinados pacientes) e registos de operações (a IA não elimina as necessidades cirúrgicas, mas pode reduzi-las, ao mesmo tempo que melhora os resultados para pacientes e médicos; aliás, a utilização de robots cirúrgicos é cada vez mais comum), registos electrónicos de saúde e registos de dispositivos vestíveis (os algoritmos da *machine learning* são utilizados em grandes conjuntos de dados de saúde pública para diversos fins, como por exemplo controlo de pandemias), e relatórios diversos (por exemplo, a utilização de algoritmos para determinar se os pacientes são de alto risco o suficiente para precisarem de cuidados na unidade de cuidados intensivos ou para serem submetidos a experiências de eventos relacionados com um determinado código ou àquelas que requerem equipas de resposta rápida. Na verdade, os algoritmos avaliam a probabilidade de esses eventos ocorrerem dentro de uma janela de seis a dezoito horas, ajudando os médicos a tomar decisões mais confiantes)[24].

---

[24] Luís CAMPOS, em *A Relação Médico-Doente*, um contributo da Ordem dos Médicos de Portugal, na parte dedicada à tecnologia no contexto do relacionamento médico-doente, explica, sobre o "impacto das TICs", que "a introdução progressiva das Tecnologias de Informação e Comunicação (TICs) nos cuidados de Saúde veio introduzir mudanças avassaladoras. Os sistemas de informação vieram permitir o acesso a bases de dados de conhecimento médico, à introdução de sistemas de apoio à decisão, a recolha e partilha de informação clínica e administrativa através dos Registos de Saúde Electrónicos e Pessoais, de-

A utilização de algoritmos de aprendizagem automática na saúde implica o armazenamento e o tratamento de dados pessoais, o que implica a introdução de mecanismos jurídicos para uma eficaz segurança no processamento e protecção dos direitos do titular dos dados, também porque a tomada de decisão automatizada assenta na determinação do perfil dos titulares de dados[25]. Uma das formas para que a utilização da IA na saúde seja eficaz é, efectivamente, a criação de perfis dos pacientes. As tecnologias de perfilamento processam a partir do conhecimento de grandes bases de dados, que estão ligadas ao tratamento de dados comportamentais dos doentes (ou pessoas submetidas a diagnósticos), ou seja, o conjunto de informação em causa implica uma acção voluntária ou comportamento fisiológico da pessoa (os dados relativos às funções vitais, às perturbações funcionais do corpo ou de um órgão que seja ou não patológico) para definir determinadas doenças ou doentes e a organização de um tratamento adequado e dos medicamentos próprios para doentes com aquele perfil[26].

---

cisões automatizadas e sistemas de alerta, monitorização de indicadores e apoio à facturação dos serviços prestados ou da venda de medicamentos. Vieram também possibilitar o acesso online ao conhecimento por parte do doente, diversificar as formas de comunicação não presencial com os profissionais de saúde e a integração em redes virtuais de interajuda". Lisboa: By the Book, 285.

[25] Diego MACHADO, *Algoritmos e Proteção de Dados Pessoas. Tutela de Direitos na Era dos Perfis*, São Paulo: Almedina, 2023, 238 seg.

[26] No contexto do comércio electrónico, *v.g.*, pode pensar-se na inferência de perfil de consumidor com base em dados fornecidos para abertura de conta em sítio electrónico (dados fornecidos), no histórico de navegação e de compras de produtos e/ou serviços (dados de observação). Cfr. Bogdan MANOELA, "E-commerce and profiling in Romania: what is going on and who cares about privacy?", In Niklas CREEMERS, *et al.*, *Profiling Technologies in Practice*: *Applications and Impact on Fundamental Rights and Values*, Oiterwijk: Wolf Legal Publishers, 2017, 49.

Vamos indicar dois tipos de perfil que podem ser utilizados no tratamento de dados e com influência nos dados de saúde, na base de dois critérios diferenciadores, nomeadamente, o tipo de perfil a ser aplicado e a existência de decisão automatizada. Nos termos do primeiro critério, são dois os tipos de perfis aplicados: *a)* um perfil personalizado ou específico e *b)* um perfil de grupo ou abstracto. No primeiro, a aplicação envolve o tratamento de dados pessoais e a inferência de novos dados a partir do modelo em que o indivíduo é representado. Por exemplo, um robot assistente, integrado num amplo sistema inteligente, infere, a partir do timbre da voz, reacções faciais e movimentos corporais de pessoa idosa com histórico de doença cardiovascular, a ocorrência de infarto agudo do miocárdio, com base no qual acciona o serviço médico de atendimento de urgência do serviço de saúde de que o doente é beneficiário[27].

---

[27] Diego MACHADO, *Algoritmos e Protecção de Dados Pessoais,* 239. O autor oferece-nos um exemplo ocorrido na Holanda, em que o Tribunal do Distrito de Haia, no conhecido *caso SyRI*, em 2020, analisou a conformação entre a "CEDH com a legislação dos *systeem Risico Indicatie* (SyRI), sistema criado pela acção colaborativa de órgãos governamentais holandeses, que usou a aplicação de perfilamento automatizado baseado em aprendizado de máquina a fim de identificar os cidadãos com maior probabilidade de fraudar benefícios sociais. A aplicação do modelo com perfis de risco se subdividia em duas fases: o processamento (fase 1) e análise (fase 2). Na primeira fase, certa entidade (operador) trata os registos e os pseudónimos. Nomes pessoais e nomes de empresas, números de atendimento ao cidadão e endereços eram pseudonomizados, isto é, substituídos por um código (cifragem). O operador executava, então, a primeira fase na selecção do risco aos dados pseudonomizados: os dados eram processados e o modelo de risco aplicado de maneira automatizada. Isto gerava a sinalização de potencial caso, ou seja, inferia-se um alto risco de fraude. Sendo assim, as pessoas naturais, jurídicas ou endereços sinalizados como alto risco, seriam novamente identificados directamente (decifragem). Todos os dados relativos a pessoas enquadradas como de alto risco de fraude eram então remetidos à segunda fase de análise de risco pela unidade administrativa competente", 240.

No caso de na aplicação de perfilamento automatizado estar em causa perfil de grupo ou abstracto, a aplicação envolve (i) o tratamento de dados pessoais e a inferência de novos dados pessoais a partir da identificação e representação do perfil de grupo (categoria ou comunidade) como adequado ao indivíduo, ou (ii) o tratamento de dados de agrupamento (dados não pessoais) e a inferência de novas informações (não pessoais) a partir da identificação e representação do perfil de grupo (categoria ou comunidade) como adequado ao ente colectivo[28].

Socorrendo-nos do estabelecido no RGPD, o art. 4º (definições), nº 4, dispõe que perfil é "qualquer forma de tratamento automatizado de dados pessoais que consiste em utilizar esses dados pessoais para avaliar certos aspectos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspectos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses fiabilidade, comportamento, localização ou deslocações". A nossa LPDP não atende à figura de "perfil", mas o art. 29º, nº 1 pode indicar que houve da parte do legislador angolano a intenção teleológica de abranger, pois "qualquer pessoa tem o direito de não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afecte de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspectos da sua personalidade, designadamente, a sua capacidade profissional, o seu crédito, a confiança de que é merecedora ou o seu comportamento". O preceito nada diz relativamente à saúde, mas como a norma faz alusão a "com-

[28] Bart CUSTERS, "Profiling as Inferred Data. Amplifier Effects and Positive Feedback Loops", in Emre BAYAMILIOĞLU, *et al.,* org., *Being profiled: cogitas ergo sum 10 Years of "Profiling the European citizen"*, Amsterdam: Amsterdam University Press, 2019, 114.

portamento", pensamos que podemos estender o seu significado a abranger sintomas avaliadores do estado de saúde de uma pessoa. Neste sentido a Recomendação CM/Rec (2010)13 do Conselho Europeu, sobre a protecção dos indivíduos perante o processamento automatizado de dados pessoais, define *profiling* como sendo uma "técnica de processamento de dados automatizados que consiste na aplicação de uma definição de perfil individual para tomar decisões concernentes a preferências pessoais dela ou dele, *comportamentos ou atitudes*"[29]. Esta compreensão (de perfil) é tanto mais clara se conjugarmos com a leitura da Opinião nº 216/679, revista em 2018, do Grupo de Trabalho do art. 29º, hoje chamado de Comité Europeu para a Protecção de Dados (CEPD), que aponta três elementos integradores do conceito de *profiling*[30]:

a) A automatização: corresponde à forma de processamento;
b) O processamento: que é realizado por intermédio dos dados pessoais recolhidos;
c) Finalidade: a avaliação dos aspectos pessoais.

Por forma a mitigar os riscos de criação de perfil, que pode oferecer discriminações de vária ordem, deve ser respeitado o dever de obter dos titulares dos dados pessoais o consentimento, acompanhado do dever de informação de maneira clara, adequada à finalidade específica da construção de perfis e à forma de tratamento de dados. Igualmente deve ser respeitado o princípio da transparência algorítmica, captado a partir da LPDP, art. 6º, que deve ser entendido

---

[29] Itálico nosso.

[30] Cfr. Rafael Meira SILVA / Cristina Godoy Bernardo de OLIVEIRA, "Inteligência Artificial e Proteção de Dados: Definição de Perfil e Desafios", in <https://www.migalhas.com.br/coluna/migalhas-de-proteçao-de-dados-/339300/ia-e-proteçao-de-dados-definiçao-de-perfil-e-desafios>, consultado a 05 de Novembro de 2024.

como aquele segundo o qual os procedimentos técnicos que orientam o tratamento automatizado de dados susceptíveis de afectarem aspectos da vida dos seus titulares devem ser públicos.

No nosso ordenamento jurídico é identificável a existência de uma permanente intenção axiológica que é constitucionalmente imposta a todas as áreas de actuação, sendo mais importante quando nos referimos aos direitos, liberdades e garantias dos particulares, baseados na dignidade da pessoa humana, fazendo de cada ser humano e concreto a razão fundante do Direito e das instituições, conforme o art. 1º da CRA. Este princípio constitui a base a partir da qual se estruturam e funcionam os princípios da igualdade, da liberdade, da autodeterminação e do desenvolvimento da personalidade. Daí ser premente o estudo da ética na tecnologia, da consideração e aplicação do sentido axiológico imanente à ordem jurídica e, também, os cuidados a ter com os referidos riscos que podem potenciar dificuldades para uma utilização da IA mais conformes com o bem-estar do indivíduo e da humanidade[31].

---

[31] O Órgão Consultivo de Alto Nível sobre a Inteligência Artificial (IA) estabelecido pelo Secretário-Geral das Nações Unidas em Outubro de 2023, apresentou o relatório final sobre "Governança da Inteligência Artificial para Humanidade" no dia 17 de Novembro de 2024. O relatório identifica um défice de regulação, normas e instituições globais capazes de gerir o uso da inteligência artificial, colocando em risco o aproveitamento dos benefícios para o bem da humanidade. Defende-se no relatório a utilização de uma abordagem globalmente interligada, ágil e flexível para governar a IA, pois, pela natureza da própria tecnologia, que é transfronteiriça em estrutura e aplicação, requer-se uma abordagem global. Para mais elementos sobre o relatório, consultar <https://www.un.org/en/ai.advisory-body>, aos 24 de Dezembro, 2024. Nesta linha, a revista *Science* publicou a opinião de 25 cientistas, identificando haver um "risco catastrófico" para a humanidade. Entendem os especialistas que a "cibercriminalidade em grande escala, a manipulação social e outros danos podem aumentar rapidamente", admitindo-se uma "possibilidade real de que o avanço descontrolado da IA possa

Uma possível noção de "ética-digital"[32] conduz a uma discussão técnico-jurídica e dogmático-normativa, mas, devido ao interesse na protecção da pessoa, podemos ser conduzidos a concluir com ARTUR FLAMÍNIO DA SILVA[33] "pela existência de uma parametrização ética – concretizada normativamente – no âmbito do Direito (…) que permite apurar qual o sentido axiológico que deve guiar a utilização de tecnologia na actividade (…)" de tratamento de dados pessoais em saúde. Significa que devemos ultrapassar a barreira de uma inexistência legal e doutrinária (até jurisprudencial) do conceito em causa, para utilizar uma linguagem simples. Devemos sim identificar um conceito de "ética-digital" que seja vinculativo para todos, o que significa impor limites aos desafios contra a *dignitas* das pessoas. Assim, ainda que os robôs dotados de IA e a IA sem interface física de autoaprendizagem esteja dotada de uma determinada autonomia e adaptação ao meio ambiente, não lhes podemos atribuir consciência e liberdade humanas, que ditam a liberdade de escolha e de acção, o livre arbítrio que apenas aos homens é reconhecido. Se assim for traçado o caminho, a "consciência jurídica geral" permitirá o entendimento segundo o qual a dignidade humana bem como os demais direitos fundamentais são fontes originárias e conformadoras da ética no domínio da IA.

---

culminar numa perda de vidas e da biosfera em grande escala e na marginalização ou extinção da humanidade", in <https://www.science.org/doi/101126/science.adn0117>, consultado a 24 de Novembro.

[32] Deborah B. JOHNSON, *Computer Ethics,* 4.ª ed., New Jersey: Pearson, 2008, 174 seg.

[33] "Ética e Inteligência Artificial no Direito Administrativo", in Isabel Celeste M. FONSECA, coord., *Estudos de E-Governação, Transparência e Proteção de Dados*, Coimbra: Almedina, 2021, 251 seg. neste mesmo sentido, mas sem grande desenvolvimento, João A. FRANCISCO, *Manual de Direito da Informática*, Luanda: Editora das Letras, 2019, 165 e seg.

Se o tratamento de dados pessoais através da IA não respeitar os valores que garantam o respeito da liberdade e da autonomia da pessoa humana, então, deve garantir-se, através de medidas adequadas de segurança, que a autodeterminação plena e efectiva das pessoas não seja afectada negativamente. Sem rejeitar a IA, a sua utilização deve ser maximizada para aumentar, complementar e capacitar as competências cognitivas das pessoas. Se assim não for, corremos o risco de desumanizar as pessoas e as instituições[34].

A LPDP dispõe no art. 29º (Decisões individuais automatizadas), nº 1, que "qualquer pessoa tem o direito de não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afecte de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspectos da sua personalidade, designadamente, a sua capacidade profissional, o seu crédito, a confiança de que é merecedora ou o seu comportamento". Uma primeira observação a ser feita é respeitante ao facto de que estamos a fazer um estudo no campo da protecção de dados pessoais da saúde. Logo, os aspectos da personalidade do titular dos dados devem ser ligados ao seu estado de saúde física e mental. Ademais, a capacidade profissional do titular pode ser avaliada através de exames médicos, cuja informação resultante é considerada como *dados pessoais*, merecedores de confidencialidade e, por isso, objecto de tutela da LPDP.

A digitalização das nossas actividades vem influenciando a organização das instituições. Nos estabelecimentos de saúde[35], por exemplo, a organização do trabalho implica um controlo que inevitavelmente

---

[34] Artur Flamínio da SILVA, "Ética e Inteligência Artificial no Direito Administrativo", 259.

[35] Estabelecimento de saúde tido no seu conceito mais amplo, incluindo não só os estabelecimentos hospitalares, como centros laboratoriais, serviços burocrá-

vai determinar, através da recolha de dados (gerais e, em particular, da saúde), o tipo de organização, o perfil dos profissionais e dos utentes, a adopção de uma estratégia de segurança e de prevenção de risco laboral e do tratamento dos dados, tudo porque a entidade patronal tem conhecimento dos dados pessoais dos seus profissionais e das pessoais que entram em contacto com os estabelecimentos de saúde. Sabe-se, inclusive, a disposição física, e muitas vezes intelectual, dos seus colaboradores, o que permite algumas vezes manipular os contratos de trabalho e a forma de funcionamento dos serviços[36].

No campo da informática e da utilização da IA, o risco de invasão dos dados pessoais apresenta características muito particulares. Por isso, as medidas de segurança devem ser também muito particulares, sem desprimor do enunciado em legislação, designadamente, os deveres de segurança – arts. 30º e 31º da LPDP –, onde se estabelece o dever de adopção de medidas apropriadas para proteger os ficheiros contra perigos naturais, como a perda ou destruição acidental, e perigos humanos, como o acesso não autorizado, o uso fraudulento dos dados ou a contaminação por vírus informáticos.

Na actualidade, quanto mais se desenvolvem os mecanismos de segurança das redes das tecnologias de informação e comunicação, mais são aprimorados os meios de intromissão nas mesmas. Um dos processos que mais se tem destacado, apesar de ter nascido nos sistemas bancários, tendo sido utilizado onde há redes informáticas, é o *phishing* e

ticos (secretaria, arquivos, etc.), serviços de emergências e outros que integram as relações de prestação de saúde.

[36] Javier FERNÁNDEZ-COSTAS MUÑIZ, "El tratamiento y protección de los datos de salud de los trabajadores en el ordenamiento español", in Francisco Pereira COUTINHO / Graça Conto MONIZ, *Anuário da Proteção de dados*, Centro de I&D sobre Direito e Sociedade, Faculdade de Direito da Universidade Nova de Lisboa, 2023, 11 seg.

pharming[37]. A técnica de *phishing* (do inglês 'fishing', pesca) consiste no envio de mensagens de correio electrónico procurando obter palavras-passe de serviços electrónicos ou PINs de cartões de acesso a ficheiros informáticos ou informações que permitam o acesso a contas de emails, a bases de dados ou ao "conjunto dos sistemas tecnológicos e infra-estruturas de redes telemáticas, bem como ao conjunto de informações e serviços da internet", ou ainda a "qualquer dispositivo ou conjunto de dispositivos que procedem ao armazenamento, tratamento, recuperação ou transmissão de dados informáticos em execução de um programa de computador"[38]. Já o *pharming* é uma técnica relativamente mais sofisticada, e por isso de maior perigosidade para a segurança da recolha, processamento e, principalmente, armazenamento de dados pessoais, na medida em que é alterado fraudulentamente o próprio nome de domínio (*domain name*) de uma instituição financeira, redirecionando o utilizador para um *sítio* falso – muito similar ao verdadeiro – sempre que digita no teclado a morada correcta do banco de dados ou outro sítio. Uma vez na página falsa, o utilizador indica as suas passes secretas

[37] Cfr. Maria Raquel GUIMARÃES, "O *phishing* de dados bancários e o *pharming* de contas. Análise jurisprudencial", in Luís Miguel Pestana VASCONCELOS, coord., *III Congresso de Direito Bancário*, Coimbra: Almedina, 2018, 405-432. Neste estudo a autora assenta a sua investigação na banca. *Ibidem,* 418-419. Por isso, os conceitos foram por nós adaptados para a área dos dados pessoais.

[38] Estes são os conceitos de *ciberespaço* e de *sistema informático* que a Lei nº 7/17, de 16 de Fevereiro – Lei de Protecção das Redes e Sistemas Informáticos.

de acesso que posteriormente são utilizadas na página verdadeira para aceder, transferir ou adulterar os dados pessoais[39].

1.5 Fontes da Protecção de Dados Pessoais

A temática da protecção de dados pessoais assenta num sistema jurídico amplo. Por isso, as fontes da ordem jurídica tutelar dos dados das pessoas são, não apenas as que constituem a legislação angolana, mas também a regional e a internacional. E justifica-se. A já muito referenciada em todas as ciências como justificação de teses, é

---

[39] Estes conceitos tiveram aceitação na jurisprudência portuguesa. Em acórdão do Supremo Tribunal de Justiça de 18 de Dezembro de 2013, ficou escrito que "O phishing (do inglês fishing 'pesca') pressupõe uma fraude electrónica caracterizada por tentativas de adquirir dados pessoais, através do envio de e-mails com uma pretensa proveniência da entidade bancária do receptor, por exemplo, a pedir determinaos elementos confidenciais (número de conta, número de contrato, número de cartão de contribuinte ou qualquer outra informação pessoal), por forma a que este ao abri-los e ao fornecer as informações solicitadas e/ou ao clicar em links para outras páginas ou imagens, ou ao descarregar eventuais arquivos ali contidos, poderá estar a proporcionar o fruto de informações bancárias e a sua utilização subsequente"; "A outras modalidade de fraude online é o pharming a qual consiste em suplantar o sistema de resolução dos nomes de domínio para conduzir o usuário a uma página Web falsa, clonada da página real, baseando-se o processo, sumariamente, em alterar o IP numérico de uma direcção no próprio navegador, através de programas que captam os códigos de pulsação do teclado (os ditos keyloggers), o que pode ser feito através da difusão de vírus via spam, o que leva o usuário a pensar que está a aceder a um determinado site – por exemplo o do seu banco – e está a entrar no IP de uma página Web falsa, sendo que ao indicar as suas chaves de acesso, estas serão depois utilizadas pelos crackers, para acederem à verdadeira página da instituição bancária e aí poderem efectuar as operações que entenderem, destinando-se ambas as técnicas (phishing e pharming) à obtenção fraudulenta de fundos",*apud* Maria Raquel GUIMARÃES, "O *phishing* de dados bancários e o *pharming* de contas", 418-419.

também aqui designada realidade justificante: a globalização. Vivemos num mundo muito mais partilhado e compartilhado. A ciência e a tecnologia colocam-nos como vizinhos físicos e virtuais. Esta situação, faz da presente geração aquela que mais produz dados pessoais. Desde o nosso nascimento com o registo de nascimento (para não dizer, antes do nascimento, com os registos de consultas de ginecologia da progenitora), registos escolares, registos de casamento e divórcios, registos de mortes, registos militares e paramilitares (no seu sentido mais amplo), registos sobre o emprego (no sector público e privado), registos dos serviços de saúde, registos bancários e do sector de seguros, registos financeiros, registos dos diversos serviços de tecnologias de informação, dos utentes dos serviços de transportes públicos – só para citar alguns, pois há outros tipos de registos[40].

Assim, o sistema de protecção de dados pessoas começa pelo topo da pirâmide da nossa ordem jurídica, a Constituição da República de Angola, onde encontramos um conjunto de normas, em que algumas constituem princípios normativos e outras normas pragmáticas, carecendo de concretizações. Indicamos como o núcleo do sistema de protecção de dados pessoais o princípio da dignidade da pessoa humana, já referido *supra*. Depois, o princípio *habeas data*, instituto que serve para "assegurar o conhecimento das informações sobre si constante de ficheiros, arquivos ou registos informáticos, de ser informados sobre o fim a que se destinam, bem como de exigir a rectificação ou actualização dos mesmos" constante no art. 69º, e o direito à identidade, à privacidade e à intimidade, conforme o art. 32º, cujo nº 1 dispõe que "a todos são reconhecidos os direitos os direitos à identidade pessoal, à capacidade civil, à nacionalidade, ao bom nome e reputação, à imagem, à palavra e à reserva de intimidade da vida privada e familiar".

---

[40] Alan WESTIN, *Privacy and Freedom*, 158-159.

Mesmo que a CRA não refira directamente a protecção de dados pessoais, ela é suficientemente protectora, pois apresenta uma vitalidade e continuidade devido à sua capacidade de se adaptar às novas transformações sociais, históricas, técnicas e tecnológicas, possibilitando ser o guardião de um sistema de protecção que abarque os dados pessoais contra novas possibilidades de ataques.

Outra legislação que pode ser apontada como fonte: a Lei nº 22/11, de 17 de Junho (LPDP), o principal instrumento que estabelece "as regras aplicáveis ao tratamento de dados pessoais com o objectivo de garantir o respeito pelas liberdades públicas e os direitos e garantias fundamentais das pessoas singulares" (art. 1º), que será o principal instrumento da presente monografia. A Lei nº 23/11, de 20 de Junho, Lei das Comunicações Electrónicas e dos Serviços da Sociedade de Informação (LCESSI), estabelece as suas bases disciplinares e regulamentares, destacando-se, dentro dos objectivos gerais da lei, garantir o acesso universal à informação e ao conhecimento, assim como proteger a privacidade e os dados pessoais dos utilizadores[41]; a Lei nº 7/17, de 16 de Fevereiro, Lei de Protecção

---

[41] Sobre esta situação, cf. Silvia Menezes da CARVALHO, *Manual de Direito das Comunicações Electrónicas. Mercado e Regulação*, Luanda: Literacia-Editora, 2021, 123. A autora defende a ideia de que "a recolha e tratamento dos dados pessoais e das empresas públicas, privadas e cooperativas enquanto assinantes ou utilizadores finais encontra acolhimento normativo no regime da privacidade da comunicações electrónicas, que visa salvaguardar a garantia da intimidade das comunicações, enquanto serviço público de interesse geral, sendo que a protecção dos dados pessoais nas comunicações electrónicas recai sobre os seguintes serviços: a) dados de tráfego; b) dados de localização; c) factura detalhada; d) guias electrónicas; e) comunicações electrónicas comerciais não solicitadas".

Para a autora, "o tratamento dos dados de tráfego pelos operadores de comunicações electrónicas acessíveis ao público tem como finalidade a identificação e transmissão da comunicação com o objectivo de, por um lado, permitir à emissão da factura e, por outro, identificar os dados pessoais necessários para a efectivação

das Redes e Sistemas Informáticos (LPRSI). Esta lei tem por finalidade fundamental "responder de forma eficaz e eficiente, aos novos desafios da sociedade de informação, à protecção do espaço cibernético angolano contra os riscos a eles associados e promover a inclusão digital"; Lei nº 2/20, de 22 de Janeiro, Lei da Videovigilância – atendendo a que esta lei autoriza a captação de imagens de cidadãos de forma "indiscriminada", no sentido de proteger os direitos fundamentais, estabeleceu alguns princípios, nomeadamente, o da legalidade, da finalidade, da proporcionalidade, da transparência e da Conservação –; Decreto Presidencial nº 214/16, de 10 de Outubro, que aprova o Estatuto Orgânico da Agência de Protecção de Dados (APD); Decreto Presidencial nº 60/21, de 10 de Março, que aprova o regulamento das taxas a cobrar pela APD; Decreto Presidencial nº 275/20, de 21 de Outubro, que aprova o regulamento da actividade das centrais privadas de informação de crédito; Decreto Presidencial nº 308/21, de 19 de Março, que aprova as taxas a cobrar pela APD, para a autorização do exercício da actividade das CPIC; Decreto Presidencial nº 108/16, de 25 de Maio, que aprova o Regulamento Geral das Comunicações Electrónicas; Decreto Presidencial nº 202/11, de 22 de Junho, que aprova o Regulamento das Tecnologias e dos Serviços da Sociedade da Informação; e, por fim, o Decreto

da comunicação que, por imperativo legal, deverão ser eliminados ou tornados anónimos quando estiverem cumpridos os pressupostos que originaram a recolha desses mesmos dados pessoais. O tratamento dos dados de tráfego, para efeitos de facturação dos usuários ou utilizadores finais, deverá apresentar de modo taxativo os seguintes elementos: a) número ou identificação, endereço e tipo de posto de assinante e do utilizador; b) número total de unidades a cobrar para o período de contagem, bem como o tipo, hora de início e duração das chamadas efectuadas ou o volume de dados transmitidos; c) data da chamada ou serviço e número chamado; d) outras informações relativas a pagamentos, tais como pagamentos adiados, pagamentos a prestações, cortes de ligações e avisos", *ibid.,* 124.

Presidencial nº 166/14, de 10 de Julho, que aprova o Regulamento de Partilha de Infraestruturas de Comunicações Electrónicas.

Ao nível de África temos a Resolução da Assembleia Nacional nº 33/19, de 9 de Julho, que aprova, para ratificação, a Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais. Conforme o preâmbulo desta Convenção, "Considerando que a criação de um quadro normativo sobre Cibersegurança e Protecção de dados Pessoais leva em consideração as exigências do respeito dos direitos dos cidadãos, garantidos pelos textos fundamentais do direito interno e protegidos pelas Convenções e Tratados Internacionais sobre os Direitos Humanos, em particular a Carta Africana dos Direitos do Homem e dos Povos" (…), "Considerando que o objectivo da presente Convenção é responder à necessidade de uma legislação harmonizada no domínio da segurança cibernética nos Estados-Membros da União Africana e criar, em cada Estado Parte, um mecanismo que permita lutar contra violações da privacidade através da recolha, tratamento, transmissão, armazenamento e uso de dados pessoais; que ao propor o tipo da base institucional, a Convenção garante que qualquer forma de processamento que for utilizada respeite as liberdades fundamentais e os direitos das pessoas, ao mesmo tempo que se toma em consideração as prerrogativas dos Estados-Membros, os direitos das comunidades locais e os interesses das empresas, e ter em conta as melhores práticas reconhecidas a nível internacional". Este exercício de procurar harmonizar legislação num contexto de diversidade de culturas e de influência religiosa, como é o contexto africano, exige algumas cautelas. Significa que a diversidade cultural e jurídica representativa do nosso continente oferece conceituações e entendimento diferente; por exemplo, a pri-

vacidade há-de ter significações e perspectivas diferentes[42]. Regista-se um gritante desnivelamento entre o desenvolvimento tecnológico no seio os Estados-Membros, diferenciando o acesso à tecnologia,

---

[42] Nos países de base cristã, o Direito tem como fundamento a dignidade da pessoa humana, com diferenciações sobre a conceituação da pessoa. Desde a influência da filosofia antiga até ao posicionamento da teologia, o homem passou a ser o centro do Direito. É "de salientar ainda que a origem teológica do conceito e a sua aplicação na antropologia cristã dotaram o termo *persona* de profundos conteúdos valorativos e ético-jurídicos que, não obstante a evolução dogmática posterior, permanecem até aos dias de hoje". Cfr. entendimento de Diogo Costa GONÇALVES, *Lições de Direitos de Personalidade. Dogmática Geral e Tutela Nuclear*, Cascais: Principia, 2022, 164. Nos países muçulmanos, pelo contrário, "a ciência religiosa é, em primeiro lugar, assunto de juristas e *fuqahā* (especialista em *fiqh*, i.é, jurisprudência), tanto mais que o Islão desenvolveu entre os seus eruditos um verdadeiro amor pelo Direito. Sendo a Revelação divina apreendida primeiro como uma Lei, como a concessão de injunções destinadas a fazer viver os homens no bom caminho, constituíram-se escolas que se esforçaram por «aplicar o Direito» com base na mensagem divina e no testemunho do Profeta". Cfr. Henri TINCQ *et al., As Grandes Religiões do Mundo. Judaísmo, Cristianismo, Islão*. Vol. I, coord. Henri Tincq, Lisboa: Edições Texto&Grafia, 2016, 333 seg. Com essas diferenças, os conteúdos dos conceitos hão-de ter significações diferentes. De modo mais específico, poderíamos indicar, na perspectiva de Ali Mazrui, a indicação de cinco tradições do pensamento político em África, com influência no Direito, nomeadamente, *a)* conservadora, ou solidariedade tribal, assente na continuidade (da tradição) em detrimento da mudança. Esta engoba três subtradições: *the elder tradition* (o respeito pelos mais velos), *the warrior tradition* (a tradição dos guerreiros) e *the sage tradition* (a sabedoria); *b)* nacionalista, que surge parcialmente como resposta à arrogância da colonização branca, podendo assumir diferentes dimensões, nomeadamente, racionalismo linguístico, religioso, rácico, pan-africanismo, etnicidade (unidade tribal), racionalismo civilizacional; *c)* liberal-capitalista, com ênfase no individualismo económico, na iniciativa privada, assim como na liberdade civil; *d)* socialista, *e)* internacional ou não alinhamento – estas duas últimas não relacionadas com o tema desta investigação. Cfr. Silvia OLIVEIRA, "Pensamento africano em perspectiva comparada", in *História Unisinos*, Universidade do Vale do Rio dos Sinos, 23/3 (2019) 475-477.

o que pode perturbar o intercâmbio informativo. Há grandes riscos decorrentes da elevada dependência de fabricantes e de fornecedores de serviços não africanos.

Angola é membro da Comunidade dos Países de Língua Portuguesa e, sendo um espaço geográfico e político-económico onde se regista circulação de pessoas e bens de forma considerável, foi decidido instituir uma organização cujos membros componentes são as Autoridades de protecção de dados através da Declaração das Autoridades Lusófonas de Protecção de Dados (RLPD), assinada em Lisboa a 25 de Junho de 2024. Este instrumento contém sete objectivos: *(i)* reforçar a cooperação internacional entre as autoridades de protecção de dados que compartilhem a mesma língua; *(ii)* impulsionar o desenvolvimento de mecanismos de cooperação internacional entre as autoridades da Rede, as autoridades de protecção de dados não pertencentes a esta comunidade e outras entidades internacionais com competência na matéria; *(iii)* disponibilizar um fórum permanente de intercâmbio de conhecimento em matéria de protecção de dados e outras matérias conexas; *(iv)* criar um espaço de partilha de informação que possibilite o envolvimento dos sectores público, privado e social, da sociedade civil, com o fim de fomentar o desenvolvimento de instrumentos normativos que garantam o direito de protecção dos dados pessoais num contexto democrático e global; *(v)* incentivar a adesão a instrumentos internacionais que possibilitem transferências internacionais de dados pessoais com total respeito dos direitos fundamentais; *(vi)* incentivar e apoiar todos os países lusófonos a criar legislação de protecção de dados e entidades que garantam, de modo efectivo, o direito à protecção de dados pessoais; *(vii)* salientar a relevância da existência de entidades que, com independência, tutelem a protecção de dados.

Ao nível da Organização para a Cooperação e Desenvolvimento Económico (OCDE), encontramos as Linhas Directrizes que regem a Protecção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais. Este instrumento data de 1980 e foi uma resposta à intro-

dução da tecnologia de informação em várias áreas da vida económica e social, e a importância e poder crescentes do processamento automatizado de dados. Estas Directrizes foram adoptadas enquanto Recomendação do Conselho da OCDE em apoio aos três princípios comuns aos países membros, designadamente a democracia pluralista, respeito pelos direitos humanos e economias de mercado abertas. O instrumento está estruturado em V Partes, sendo a primeira relativa a "Generalidades", a segunda diz respeito aos "Princípios básicos de aplicação nacional", a terceira é atinente aos "Princípios básicos de aplicação nacional: livre fluxo e restrições legais", a quarta está relacionada com a "Implementação nacional" e, por fim, a quinta sobre "Cooperação internacional". Importa aqui referir que os princípios são: da limitação da colecta; da qualidade dos dados; da definição da finalidade; da limitação de utilização; do *back-up* de segurança; da abertura; da participação do indivíduo; e da responsabilidade.

No quadro da Organização das Nações Unidas encontramos as Directrizes para a Regulação de Ficheiros Informáticos de Dados de Carácter Pessoal, adoptadas pela Resolução nº 45/95 da Assembleia Geral das Nações Unidas, de 14 de Dezembro de 1990. Existem princípios que devem ser observados dentro da liberdade que os Estados têm para a regulamentação dos ficheiros informatizados de dados de carácter pessoal. São os seguintes: princípio da legalidade e equidade; princípio da exactidão; princípio da finalidade específica; princípio do acesso da pessoa interessada; princípio da não discriminação; princípio da faculdade de estabelecer excepções; princípio da segurança; princípio da supervisão e sanções; princípio do fluxo transfronteiriço. Os princípios enunciados devem ser aplicáveis, em primeira instância, a todos os ficheiros informatizados públicos e privados, bem como, mediante uma extensão facultativa e sem prejuízo de adaptações adequadas, aos ficheiros manuais: Podem ser tomadas providências especiais, também facultativas, para que todos ou alguns dos princípios abranjam também ficheiros relativos a pessoas colectivas, em particular caso os mesmos contenham alguma informação relativa a pessoas singulares.

1.6 Modelos Estrangeiros de Protecção de Dados Pessoais

Ainda que brevemente, realizar uma incursão em alguns sistemas de protecção de dados mais importantes no estrangeiro resulta sempre em avaliar como estamos, o que de importante foi feito e, depois, o que é possível realizar para melhorar o nosso sistema de protecção de dados, respondendo aos desafios da actualidade.

Cada um dos modelos indicados regista uma forte tutela dos titulares dos dados pessoais, quer por via constitucional quer por via de lei material, com posições jurisprudenciais muito protectoras. Há claramente a imposição ao Estado de um dever de intervir legislativamente, de forma regulatória, e de supervisão do processo de tratamento de dados. As particularidades de cada Estado, as características de cada processo político ditam a abrangência e o seu âmbito de aplicação, respondendo assim às idiossincrasias de cada realidade social.

A Constituição da África do Sul contém uma norma – art. 14º – que protege o direito à privacidade. Em Janeiro de 2020 aprovou e entrou em vigor em Julho de 2021 a *Protection of Personal Information Act*. Esta lei foi influenciada pelo legislador europeu, até porque a lei sul-africana é contemporânea da RGPD. Mas há diferenças: o seu âmbito pode ser considerado restrito, pois abrange apenas as instituições "domiciliadas na República" ou as que não estando domiciliadas fazem uso de meios automatizados ou não automatizados para processar dados pessoais naquele país, desde que tais meios não sejam utilizados apenas para encaminhar informações pessoais através (*through*) daquele país[43]. Não há um prazo fixo para o titular

[43] No original está assim escrito (subsecção 3(1)): *"(1) This Act applies to the processing of personal information (a) entered in a record by or for a responsible party*

dos dados exercer o direito de informação, pois a lei fala em "prazo razoável", o qual na prática, atendendo a cada caso concreto, será o tribunal a avaliar e determinar[44]. É obrigatória a designação de *data protection officers*, se assim não ocorrer a responsabilidade será do CEO. Não há um praxo fixo para comunicar as violações aos titulares de dados[45]. A responsabilidade civil é a objectiva[46] para os casos

---

by making use of automated or non-automated means: Provided that when the record personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof; and (b) where the responsible party is (i) domiciled in the Republic; or (ii) not domiciled in the Republic, but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic".

[44] Subsecção 23(1) *"(1) A data subject having provided adequate proof of identity, has the right to (a) request a responsible party or confirm, free of charge, whether or not the responsible party holds personal information about the data subject; and (b) request from a responsible party the record or a description of the personal information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information (i) within a reasonable time; (ii) at a prescribed fee, if any; (iii) in a reasonable manner and format; and (vi) in a form that is generally understandable".*

[45] Subsecção 99(1): *"(…) whether or not there is intent or negligence on the part of the responsible party*".

[46] (1) *A data subject or, at the request of the data subject, the Regulatory, may institute a civil action for damages in a court having jurisdiction against a responsible party of breach of any provision of this Act as referred to in section 73, whether or not there is intent or negligence on the part of the responsible party. (2) In the event of a breach the responsible party may raise any of the following defense against an action for damages: (a) vis major, Consent of the plaintiff; (c) fault on the part of the plaintiff; (d) compliance was not reasonably practicable in the circumstances of the particular cases, or the Regulator has granted an exemption in terms of section 37. (2) A court hearing proceedings in terms of subsection (1) may award an amount that is just and equitable (a) payment of damages as compensation of patrimonial and non-patrimonial loss suffered by a data subject as a result of breach of the provisions of this Act; (b) aggravated damages, in a sum determined in the discretion of the Court; (c) interest; and*

de danos derivados do tratamento de dados, podendo ser excluída nos casos de força maior, consentimento do reclamante, 'culpa' do lesado, sendo que a indemnização judicial deve ser "justa e equitativa", considerando a existência de danos patrimoniais e não patrimoniais, bem como os "danos agravados" (*aggravated damages*) cujo valor é fixado segundo uma prudente discricionariedade do tribunal (*in the discretion of the Court*). Por fim, a existência de sanção administrativa pecuniária (multa) no valor equivalente a dez milhões de rands, sem prejuízo de eventual sanção penal, que pode chegar até doze anos de pena de prisão.

Como é característico dos sistemas da *common law*, o instrumento de tutela da protecção de dados pessoais sul-africana utiliza quarenta e quatro vezes a expressão *reasonable*, deixando para a jurisprudência dos tribunais a função de consolidar e actualizar o conteúdo

---

(d) costs of suit on such scale as may be determined by the Court; (4) Any amount awarded to the Regulator with an appropriate financial institution; (b) as a first charge against the amount, the Regulator may recover all reasonable expenses, incurred in bringing proceedings at the request of a data subject in terms of subsection (5); and in administering the distributions made to the data subject in terms of subsection (5); and (c) the balance, if any (in this section referred to as the 'distributable balance'), must be distributed by the Regulator to the data subject at whose request the proceedings were brought. (5) Any amount not distributed within three years from the date of the first distribution of payments in terms of subsection (4), accrue to the Regulator in the Regulator's official capacity. (6) The distributable balance must be distributed on a pro rata basis to the data subject it referred to in subsection (1). (7) A Court issuing any order under this section must order it to be published in the Gazzete and by such other appropriate public media announcement as the Court considers appropriate. (8) Any civil action instituted under this section may be withdrawn, abandoned or compromised must be made an order of Court. (9) If a civil action has not been instituted, any agreement or settlement, if any, may, on application to the Court by the Regulator after due notice to the other party, be made an order of Court and must be published in the Gazette and by such other public media announcement as the Court considers appropriate".

normativo dos conceitos, e dos parâmetros de tutela ao longo do tempo. Na *Protection of Personal Information Act* encontramos: *reasonable manner; reasonable conditions; reasonable in the circumstances; reasonable means; reasonable procedures*, etc.

A autoridade administrativa com funções de supervisão e fiscalização é o *Information Regulator*. É um órgão dotado de autonomia e está sujeito apenas à Constituição e à lei, exercendo as suas funções desprovidas de qualquer complexo de medo, favor ou preconceito, cuja jurisdição abrange todo o país[47]. A estrutura do *Information Regulator* compreende a existência de um comité de execução (*Enforcement Committee*), composto por entidades indicadas pela própria autoridade reguladora, por um juiz do Supremo Tribunal da África do Sul, no activo ou reformado, ou um magistrado com pelo menos dez anos de experiência e um advogado igualmente com pelo menos dez anos de experiência, que preside o comité. Responde perante a Assembleia Nacional.

A profunda ideia de livre mercado defendida pelo capitalismo e o intercâmbio de modelos de investigação levam a trocas constantes de dados pessoais. O exemplo mais significativo é o que a União Europeia decidiu: o estabelecimento de um mercado comum, na América do Norte, o Tratado Norte-Americano de Livre Mercado (*North American Free Trade Agreement* – NAFTA), na América do Sul, o MERCOSUL (Mercado Comum do Sul), na África Austral, a Conferência de Coordenação para o Desenvolvimento da África Austral (*Southern Africa Development Community* – SADC). Mais recentemente, foram aprovados o mercado livre entre a União Europeia e o Mercosul (que já está a ser objecto de manifestações de

---

[47] Subsecção 39(1) (a) "(…) *is subject only to the Constitution and to the law and must be imparcial and perform its functions and exercise its powers without fears, favours or prejudice*".

rejeição da parte de alguns sectores da economia europeia, principalmente a agropecuária). Estes agregados de países desenvolvem múltiplas actividades que reclamam trocas de dados pessoais. A partir da *Web*, os responsáveis pelo tratamento de dados passaram a recolher informação dos utilizadores daquele sistema de informações ligadas através de hiperligações em forma de textos, vídeos, som e outras animações digitais, ao ponto de se fazerem *classificações* individuais segundo as escolhas das pessoas, suas preferências e interesses, grupo sanguíneo, especificidades biométricas etc.

Começamos pela União Europeia.

Podemos identificar a Convenção de Estrasburgo como ponto de partida da regulamentação de protecção de dados pessoais no espaço da UE, que teve por fonte de inspiração as *Directrizes sobre Protecção da Privacidade e Circulação Transfronteiriça de Dados Pessoais da OCDE* de 1980. Daí foram surgindo várias Directivas, que assentavam na ideia de direito humano, materializado com a *Charter of Fundamental Rights of the European Union* – 2000/C 364/01 e a *Convention for the Protection of Human Rights and Fundamental Freedoms*, aprovada em Roma em 04 de Novembro de 1950. Estes instrumentos foram tratados como *soft law* e deram lugar ao que hoje constitui o sistema de protecção de dados da UE, cujos instrumentos fundamentais registados até 2018 são a Directiva 95/46/EC, chamada *Personal Data Protection Directive*, de 24 de Dezembro de 1995, do Parlamento e do Conselho Europeu, que disciplinou a protecção dos dados pessoais, cuja finalidade era a eliminação dos obstáculos na circulação de dados pessoais entre os Estados-membros e assegurar o fortalecimento do mercado interno. Por fim, a *General Data Protection Regulation* – 2016/679 – GDPR. Este regulamento será citado várias vezes ao longo deste escrito, pelo que não interessa alongar-nos na sua apresentação, bastando indicar os seus onze capítulos:

- Capítulo I, disposições gerais, dispondo o objecto e os objectivos do Regulamento, seu âmbito de aplicação material e espacial e alguns conceitos;
- Capítulo II, estabelece os princípios e condições do tratamento de dados pessoais;
- Capítulo III, prevê os direitos dos titulares dos dados;
- Capítulo IV, regula a actividade dos agentes responsáveis pelo tratamento, segurança e avaliação do impacto sobre a protecção de dados, os códigos de conduta e a certificação;
- Capítulo V, dispõe sobre a transferência de dados pessoais para países terceiros ou organizações internacionais;
- Capítulo VI, estabelece a independência, competência, atribuições e poderes das Autoridades de Controlo;
- Capítulo VII, regula o sistema de cooperação entre as Autoridades de Controlo;
- Capítulo VIII, dispõe sobre as vias de recurso, responsabilidade e sanções determinadas pelas Autoridades de Controlo;
- Capítulo IX, trata de disposições relativas a situações específicas de tratamento de dados:
- Capítulo X, regula os Actos delegados e os actos de execução conferidos à Comissão Europeia;
- Capítulo XI, contém as disposições finais.

O modelo do Canadá.

Estando organizado por Províncias que têm competência legislativa para regular sobre o tratamento de dados, foi necessário um procedimento de uniformização. A *Uniform Law Conference of Canada* (ULCC), estabeleceu projectos de lei modelo que poderiam ou não ser seguidos pelas Províncias, sem perderem a sua autonomia legislativa. As preocupações com a protecção de dados remonta à se-

gunda metade do século passado, pois em 1972, depois de uma década de estudos, foi elaborado e publicado o *Privacy and Computers*, relatório que recomendou a introdução na *Canadian Human Rights Act* da protecção de dados pessoais armazenados em bancos de dados do Governo, que tinha passado a fazer tratamento de dados com a introdução de tecnologia de informação. Na continuidade da actividade protectora de dados pessoais, o Governo Federal fez aprovar a *Privacy Act*, que estabeleceu a garantia do acesso dos cidadãos às suas informações pessoais armazenadas nas estruturas da administração pública. Estabelecia assim o art. 2º: *Purpose of the act. The purpose of this Act is to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and then provide individuals with a right of access to that information*.

Outra lei importante no sistema canadiano foi o *Access to Information Act*, que veio reconhecer o direito dos cidadãos de acesso às informações da administração pública, consolidando e reforçando o sistema[48]. Para o sector privado foi aprovada a *Personal Information Protection and Electronic Documents Act* – PIPEDA, de 13 de Abril de 2000, que veio unir duas anteriores leis, designadamente a lei sobre a protecção de dados pessoais (na presente lei, correspondem a 1ª parte, secções 05 a 30) e a lei sobre documentos electrónicos (na PIPEDA constitui a 2ª, 3ª, 4ª e 5ª parte e secções 31 a 71)[49].

Aos 20 de Dezembro de 2001, como consequência das fortes garantias do sistema de protecção de dados pessoais do Canadá, a Comissão Europeia, através da Decisão 2002/2/CE reconheceu que

---

[48] R.S.C., 1985, c. A-1. Disponível em <https://www.canlii.org/en/ca/laws/stat/rsc-1985-c-a-1/lastest/rsc-1985-c-a-1.html>, acessado a 21 de Outubro de 2024.

[49] Stephanie PERRIN *et al., The Personal Information and Electronic Documents Act*, Toronto: Irwin Law Inc, 2001, 125.

o modelo que se adequava à protecção de dados conforme o padrão previsto pela Directiva 95/46/CE:

> COMMISSION DECISION (2002/2/EC) of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C (2001) 4539)
>
> Article 1
>
> For the purposes of Article 25(2) of Directive 95/46/EC, Canada is considered as providing an adequate level of protection for personal data transferred from the Community to recipients' subject to the Personal Information Protection and Electronic Documents Act ('The Canadian Act').

O modelo dos Estados Unidos da América.

Em primeiro lugar, anotar que neste país existe uma grande autonomia legislativa dos Estados federados e uma forte autorregulação do sector privado. Não há, assim, ao contrário da Europa e do Canadá, um normativo para todo o país ou até para cada Estado, a protecção de dados é amplamente regulada por leis sectoriais, tornando mais eficaz o sistema protector quando identificam particularidades de cada sector ou empresa. O exemplo que pode ser aqui ilustrado é a protecção de dados em saúde, a *Health Insurance Portability and Accountability Act* de 1996 (HIPAA)[50], na área da educação com

[50] George D. POZGAR, *Legal and Ethical Essential of Health Care Administration*, 3.ª ed., Burlington: Jones Bartlett Learning, 2021, 221. Explica o autor que "The Health Insurance Portability and Acountability Act of 1996 (HIPAA) (Public Law 104-191) was enacted by Congress to protect the privacy, confidentiality, and security of patient information. According to the Centers for Medicare and Medicaid Services, Title of HIPAA protects health insurance coverage for workers and their families when they change of lose their jobs (…). The key privacy provisions

a *Family Educational Rights and Privacy Act* de 1974 (FERPA) e o *Children's Online Privacy Protection Act* (COPA)[51].

Dentro do *United States Code* (5U.S.C. § 552a) há uma referência que não é propriamente de legislação específica de protecção de dados, mas a manifestação da protecção da intimidade e da vida privada antes criada pelo *The Privacy Act of 1974*.

A grande diferença de regulamentação entre os EUA e a UE levou, por força da já citada Directiva 95/46/CE, a que o art. 25º determine que o fluxo transfronteiriço de informações para fora da União Europeia seja condicionado à garantia de que o país destinatário das informações contenha um sistema de protecção de dados de nível igual ou superior ao da UE, os EUA, através do qual o Departamento de Comércio celebrasse um acordo com a Comissão da União Europeia, que veio a chamar-se *Safe Harbor*. Tal acordo estabeleceu que determinadas empresas americanas devessem observar alguns princípios para se adequarem às regras do modelo europeu sobre protecção de dados pessoais, resumido no seguinte:

---

of HIPAA include the following: patients must be able to access their record and request correction of errors; patients must be informed of how their personal information will be used; patient information cannot be used for marketing purposes without the explicit consent of the involved patients; patients can ask their health insurers and providers to take reasonable steps to ensure that their communications with the patient are confidential (e.g., a patient can ask to be called at his or her work phone number instead of home or cell phone number)".

[51] Paul M. SCHWARTZ, "The EU-U.S. Privacy Collision: a turn to institution and procedures", *Harvard Law Review* 126 (2013) 1966-2009, em particular 1975. Veja-se também, Sónia MOREIRA, "O RGPD e a sua aplicação transfronteiriça: até aonde estão protegidos os nossos dados pessoais", *Revista do Centro de Estudos Judiciais* 2 (2023) 27 seg. A autora faz referência a "EU – U.S. Data Privacy Framework Principles", dos Princípios Suplementares emitidos pelo *Department of Commerce* (DoC) dos EUA, bem como o Anexo I da decisão de adequação.

> An uneasy compromise between the comprehensive legislative approach adopted by European nations and the self-regulatory approach preferred by the US. The Safe Harbor Framework has been the subject of ongoing criticism, including two previous reviews (2002 and 2004). Those reviews expressed serious concerns about the effectiveness of Safe Harbor as a privacy protection mechanism.

A execução do acordo teve altos e baixos, tendo sido considerada por um sector da doutrina como um acordo com um amplo campo de fragilidades[52]. Com a decisão 2000/520/CE, a Comissão Europeia reconheceu que as empresas americanas tinham adequado o modelo de protecção de dados, mas em 2015 invalidou a decisão[53], pois da lista das empresas americanas identificadas naquela altura muitas delas deixaram de existir, descredibilizando o sistema sustentado pela *Safe Harbor*[54]. Foi necessário que o Departamento de Comércio dos EUA passasse a credenciar, por meio de um selo (*Safe Harbor Certification Mark*), as empresas que observavam os princípios *Safe Harbor*. Para a certificação, anualmente era feita uma auditoria para verificar se a empresa cumpria com os sete princípios do acordo, designadamente, o *notice*, *choice* (que podem ser *opt out* ou *opt in*), *Onward Transfer*, *security*, *data integrity*, *access* e *enforcement*[55].

---

[52] Paul M. SCHWARTZ, "The EU-U.S. Privacy Collision", 2008.

[53] Veja-se o Diário Oficial da União Europeia – *Official Journal of the European Communities*, de 25 de Abril de 2001. Disponível em <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000D=520R(01)&-from=PT>, consultado a 20 de Setembro de 2024.

[54] Na altura do início de vigência do Safe Harbor havia 1109 empresas, e a dada altura 348 deixaram de existir. Cfr. Chris CONNOLLY, *US Safe Harbor: facto or fiction*? Disponível em <https://www.galexia.com/public/research/articles/research_articles-pa08.html>, acessado a 20 de Setembro de 2024.

[55] Traduzindo esses princípios: 1) princípio da informação; 2) princípio da escolha/consentimento. Quando as empresas devem dar oportunidades para que

os indivíduos possam fazer escolhas (*opt out*) e quando, tratando-se de dados sensíveis, o seu titular deve dar o seu consentimento de forma livre e expressa (*opt in*); 3) princípio da transferência de dados a terceiros; 4) princípio da segurança; 5) princípio da integridade dos dados; 6) princípio do acesso; e 7) princípio da vigência obrigatória.

2. PRINCÍPIOS GERAIS SOBRE O TRATAMENTO DE DADOS

A lei sobre protecção de dados pessoais estabelece na Secção I do Capítulo II os princípios gerais sobre o tratamento de dados pessoais, representando, no entender de PINHEIRO e GONÇALVES[56], a "Constituição da LPDP". É neste sentido que entendemos que, apesar de a lei utilizar a expressão "princípios gerais", pela sua importância preferimos denominá-los como "princípios fundamentais da protecção de dados pessoais". São, na verdade, e utilizando as expressivas palavras de MOTA PINTO, "a ossatura (…)" do sistema de protecção de dados pessoais, "sustentando as normas que os desenvolvem e dando-lhes um sentido e uma função"[57]. Entendemos também que, mesmo não estando dito pelo legislador e sendo os dados sensíveis o centro deste estudo, está na base dos princípios positivados na LPDP a dignidade da pessoa humana como princípio basilar, ponto de partida para a abordagem principiológica da protecção de dados sensíveis. Neste sentido, o princípio da dignidade da pessoa humana, enquanto princípio normativo, desempenha duas funções dogmáticas da

---

[56] Alexandre Sousa PINHEIRO, coord., *et al., Comentário ao Regulamento Geral de Proteção de Dados*, Coimbra, Almedina, 2018, 205.

[57] Carlos Alberto da Mota PINTO, *Teoria Geral do Direito Civil*, 4.ª ed., por António Pinto Monteiro e Paulo Mota Pinto, Coimbra: Coimbra Editora, 2005, 95.

maior importância, a saber[58]:

a) função interpretativa, ao apontar o caminho no processo interpretativo dos preceitos do sistema de protecção de dados sensíveis;

b) função normogenética, que permite que o intérprete/aplicador, a título subsidiário e excepcional, utilize o princípio para fundamentar as soluções jurídicas, sendo, neste sentido, "fusíveis de segurança" do sistema jurídico de garantia dos direitos e liberdades dos utentes dos serviços de saúde.

É um princípio ao qual é inerente o reconhecimento não só da qualidade humana da pessoa e da sua dignidade, como também da dignidade da humanidade. É assim pois resultante da natureza humana, da espécie humana, impondo-se o respeito pelo ser humano como indivíduo e como membro da espécie a que pertence[59]. É esta manifestação de consideração e respeito que nos coloca num patamar acima da 'dignidade' dos demais animais, já que partilhamos a mesma condição mundanal.

---

[58] João LOUREIRO, *Constituição e Biomedicina,* 565.

[59] João LOUREIRO, *Constituição e Biomedicina,* 564.

Pensamos que tem havido uma crescente manifestação de *manipulação* das consciências manifestada através de alterações legislativas no que diz respeito aos direitos dos animais. Filipe Albuquerque MATOS e Mafalda Miranda BARBOSA entendem que a atuação legislativa tem servido para introduzir "(…) uma ideologia pós-moderna de equiparação entre pessoas e os animais. Refira-se, em abono do rigor, que esta visão, encabeçada pelos ativistas da causa da libertação animal, não pode ser confundida, por antonomásia, com a totalidade das preocupações teriofílicas, algumas das quais ainda marcadas por um nítido cunho antropocêntrico e outras convocadoras de uma concepção do direito que esbarra com esta instrumentalização do jurídico" – *O Novo Estatuto Jurídico dos Animais*, Coimbra: GestLegal, 2017, 8.

A dignidade da pessoa humana é invocada como primeira, não por uma questão de ordenação sistemática, mas, pelo contrário, por convocar a permanência ética-axiológica do nosso ser no mundo e no encontro com os *outros*. Significa, por fim, que os direitos de personalidade objecto de protecção de dados, assentam na dignidade da pessoa humana, designadamente as convicções filosóficas e políticas da pessoa, a sua filiação partidária ou sindical, fé religiosa, vida privada, origem racial ou étnica, saúde e vida sexual, incluindo os dados genéticos.

Os princípios anunciados pela LPDP são uma mola amortecedora que equilibra os pesos, permitindo, de um lado, aceitar as novas realidades fácticas e os valores que a ordem jurídica possa tutelar e, do outro lado, manter (ou não perturbar) a harmonia do sistema. Quando entendidos como princípios normativos, juntamente com a realidade social, transcendem a norma legal, constituem o fundamento decisivo da resposta jurídica que validamente seja de dar aos problemas suscitados pela realidade que é o tratamento de dados.

Mas devemos prestar muita atenção ao facto de que não vivemos num mundo ideal: vivemos num mundo problemático, em transformação constante, que exige respostas dinâmicas e à altura dos problemas e das transformações. Assim, os princípios que iremos anunciar, não foram estruturados com a pré-disposição para um fim concreto. Apesar de estarem limitados, estes limites não são estanques; o seu conteúdo sofre influências endógenas e exógenas. Tudo passa, tudo evoluciona, tudo se transforma; apenas o sentido personalista do Direito deve estar sempre presente, não sendo o baluarte da humanidade a permanecer "insensível aos beijos do sol, às violências dos ventos, aos embates das tempestades"[60]. Em consequência,

---

[60] Palavras de Don Germano Rossi na sua obra *Discursos de Circunstâncias*, tradução de Adolfo M. Tarroso Gomes, Lisboa: União Gráfica, 1956,145.

a nossa forma social, cultural, religiosa, económica e político-ideológica dita, em cada momento histórico da nossa vivência, o nosso pensamento jurídico, estruturado na "consciência jurídica geral"[61].

Seguimos a sistemática da LPDP, cuja arrumação nos parece não significar qualquer hierarquia, pois, se assim fosse, de certeza que o princípio da licitude estaria em primeiro lugar, desde logo pela sua função teleológica e axiológica-normativa. Por isso, a arrumação sistemática constante do RGPD é mais conforme a ideia da prioridade da actuação conforme a ordem jurídica[62]. No art. 13º da CUA-CPDP estão previstos os princípios relativos à protecção de dados pessoais: não consta o princípio da licitude, mas faz referência à legitimidade[63]. Este princípio impõe que os actos não estejam com a ordem jurídica e devem obedecer a determinados requisitos jurídicos, o que por si só espelha a sua importância. Passamos agora a explicitar cada um dos princípios.

2.1 Princípio da transparência

A art. 6º da LPDP estatui o *princípio da transparência*. Diz o preceito que "o tratamento de dados pessoais deve processar-se de forma transparente, em estrito respeito pelo princípio da reserva da vida privada, bem como pelos direitos, liberdades e garantias públi-

---

[61] Fernando Pinto BRONZE, *Introdução ao Estudo do Direito*, 2.ª ed., Coimbra: Coimbra Editora, 2006, Reimpressão de 2010, 433.

[62] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 152 seg.

[63] O art. 13º indica os seguintes princípios: Consentimento e legitimidade; tratamento legítimo e justo; finalidade, relevância e conservação dos dados; exactidão dos dados ao longo do seu ciclo de vida; transparência do tratamento, e confidencialidade e segurança dos dados pessoais.

cas fundamentais previstas na Constituição da República de Angola e na presente lei" (nº 1). Este princípio deve ser articulado com um princípio que o nosso legislador omitiu, mas adoptado pela maioria das nações modernas: o princípio da lealdade, o qual, numa perspetiva ampla, representa um *plus* em relação ao princípio da licitude, que veremos de seguida, podendo ser invocável naquelas situações em que o tratamento é susceptível de contradizer a intenção teleológica e axiológica da LPDP[64]. A transparência como princípio é horizontalmente transversal a todo o processo de tratamento de dados, desde a formação, recolha, execução até ao final da relação.

A União Europeia ao aprovar o RGPD tratou de elencar um conjunto de Considerandos. O nº 39 determina:

> "Deverá ser transparente para as pessoas singulares que os dados pessoais que lhes dizem respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento e a medida em que os dados pessoais são ou virão a ser tratados. O princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formulados numa linguagem clara e simples. O acesso e compreensão exigem uma linguagem inteligível para uma pessoa cujo padrão seja de uma pessoa média no âmbito do público-alvo, o que implica da parte do responsável pelo tratamento um mínimo

---

[64] Cfr. A. Barreto Menezes CORDEIRO, *Comentários ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*, CIDP, Faculdade de Direito da Universidade de Lisboa, Coimbra: Almedina, 2021, 103. Diz o autor que "numa perspectiva concretizadora, o princípio da lealdade (i) impõe que os tratamentos realizados pelos responsáveis pelo tratamento se guiem por critérios equitativos – a expressão "tratamento equitativo" é utilizada ao longo do RGDP e dos seus considerandos para densificar o conceito de lealdade; e (ii) na relação que os responsáveis pelo tratamento estabeleçam individualmente com cada um dos titulares de dados: a lealdade impõe, aos primeiros, uma obrigação de atenderem a todo o tempo aos seus interesses e expectativas legítimas dos segundos".

> de conhecimento da população objecto do seu trabalho. Esse princípio diz respeito, em particular, às informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento dos mesmos e os fins a que o tratamento se destina, bem como as informações que se destinam a assegurar que seja efectuado com equidade e transparência para com as pessoas singulares em causa, bem como a salvaguardar o seu direito a obter a confirmação e a comunicação dos dados pessoais que lhes dizem respeito que estão a ser tratados. As pessoas singulares a quem os dados dizem respeito deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente a esse tratamento. Em especial, as finalidades específicas do tratamento dos dados pessoais deverão ser explicitas e legítimas e ser determinadas aquando da recolha dos dados pessoais. Para isso, é necessário assegurar que o prazo de conservação dos dados seja limitado ao mínimo. Os dados pessoais apenas deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios. A fim de assegurar que os dados pessoais sejam conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica. Deverão ser adoptadas todas as medidas razoáveis para que os dados pessoais inexatos sejam retificados ou apagados. Os dados pessoais deverão ser tratados de forma que garanta a devida segurança e confidencialidade, incluindo para evitar o acesso a dados pessoais e equipamento utilizado para o seu tratamento, ou a utilização dos mesmos, por pessoas não autorizadas".

O nº 2 do art. 6º da LPDP dispõe que "para efeitos do disposto no número anterior, os dados pessoais devem, nomeadamente serem conservados de forma a permitir o exercício aos seus titulares dos direitos de acesso, informação, rectificação, cancelamento e oposição (…)". Este preceito impõe a observância, quanto à interpretação e aplicação do princípio da transparência, dos direitos dos titulares dos dados previstos nos artigos 25º, 26º, 27º, 28º e 29º.

Em suma, são três as obrigações resultantes deste princípio: *(i)* a comunicação com os titulares dos dados; *(ii)* a prestação de infor-

mações aos titulares de dados; e *(iii)* a disponibilização de mecanismos para o exercício dos direitos dos titulares de dados. Estas obrigações concretizam-se na existência de uma relação qualitativa entre o responsável pelo tratamento e o titular dos dados minimamente transparente. No seu relacionamento, o responsável pelo tratamento dos dados deve demonstrar clareza, abertura e honestidade[65].

Dadas as especificidades do tratamento de dados por entidades públicas, o princípio da transparência exerce um papel muito importante, porquanto este princípio é estruturante da Administração Pública contemporânea, a mesma que os estabelecimentos hospitalares públicos devem, em princípio, seguir. Trata-se de um princípio da Governança Pública que, numa perspectiva axiológica, constitui uma directriz, orientando a conduta da administração pública para que funcione de forma aberta e igualitária, comprometida com os valores dos direitos, liberdades e garantias constitucionalmente previstos.

Uma das concretizações deste princípio no âmbito do sector público é a extensão da responsabilidade. O responsável do sector público, durante o procedimento do tratamento dos dados pessoais em saúde deve demonstrar abertura para a prestação de contas, permitindo que o titular dos dados, mas também em algumas circunstâncias todos os interessados, possam acompanhar e, de certa forma, controlar o tratamento. Podem, nestes termos, exigir um controlo jurídico e social sobre a eficácia, eficiência e efectividade do tratamento de dados – referimo-nos à *accountability*, enquanto responsabilidade democrática do sector público na gestão de dados pessoais que, interessando ao "público", têm um peso garantístico da sua "privacidade e intimidade", como valores corolários do primado da dignidade da pessoa humana.

---

[65] Graça Canto MONIZ, *Manual de Introdução à Protecção de Dados Pessoais*, Coimbra, Almedina, 2023,103.

2.2 Princípio da licitude

O art. 7º da LPDP estatui o *princípio da licitude*. O nº 1 dispõe que "o tratamento de dados pessoais deve ser efectuado de forma lícita e leal, com respeito pelo princípio da boa-fé". Nos termos gerais, licitude é estar conforme a ordem jurídica estabelecida. Em consequência, o tratamento de dados pressupõe o cumprimento da lei, não apenas a LPDP, mas o conjunto de legislação susceptível de concorrer para uma efectiva protecção dos dados pessoais. Apesar de a nossa lei vincular à licitude a lealdade e a boa-fé, em boa análise devemos também agregar-lhe os princípios da responsabilidade e da finalidade. Com o princípio da responsabilidade, o responsável pelo tratamento de dados deve traduzir em documento as condições de licitude e justificar as razões de escolha, ficando aqui reflectida a ideia da necessidade de um contrato, até porque é exigível o consentimento como garantia/fundamento da licitude.

No entanto, centralizar o consentimento para a exclusão da ilicitude no tratamento de dados pessoais sensíveis não tem merecido unanimidade da doutrina. Conforme BARRETO MENEZES CORDEIRO[66], os críticos consideram que o consentimento "é uma ficção:

---

[66] *Comentários ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*, CIDP, Faculdade de Direito da Universidade de Lisboa, Coimbra: Almedina, 2021, 111. Refere o autor que numa perspectiva prática "(i) a maioria dos sujeitos não se pode negar a consentir sem incorrer em pesados riscos – os dados são pedidos por um superior hierárquico ou por um sujeito que detenha uma enorme ascendência, p. ex.: área da saúde; ou (ii) o consentimento é necessário para aceder a bens e serviços indispensáveis – emprego, energia, comunicações ou contas bancárias".

traduz uma falsa ideia de controlo e representa, quando manifestado, uma chave para um acesso virtualmente ilimitado a um sem fim de informações pessoais". No entanto, o consentimento é um elemento sempre importante para o tratamento de dados pessoais e fundamento para a sua licitude, pelo que, devido à sua relevância, dedicaremos *infra* um espaço autónomo à sua abordagem.

Quanto à combinação com o princípio da limitação das finalidades, obriga o responsável pelo tratamento dos dados a identificar as finalidades e a avaliar a proporcionalidade entre o tratamento e a finalidade do mesmo, para depois escolher o fundamento da licitude[67].

A ligação que o artigo faz à lealdade e ao princípio da boa-fé resultam no facto de que, como já foi referido, a lealdade consubstancia um *plus* em relação ao princípio da licitude. Por força da tradição alemã, que influenciou o direito português, o qual veio influenciar o angolano, a colocação na norma da locução *boa-fé,* ao invés do termo *leal*, é resultado da escolha feito pelo legislador germânico[68]. Parece-nos que, apesar de serem termos diferentes, oferecem um significado idêntico, em atenção à intenção teleológica do preceito. Nada impede que elucidemos mais um pouco o que é que o princípio da lealdade empresta ao princípio da licitude. A medida da sua importância para o Direito no seu todo e, especialmente, no tratamento de dados pessoais, é assinalável. Tomando por referência o RGPD, e para reforçar o nosso posicionamento, descortinamos que ao longo do seu corpo se encontra esparsamente escrita a terminologia "tratamento equitativo", que "é utilizada para densificar o princípio da

---

[67] Graça Canto MONIZ, *Manual de Introdução à Protecção de Dados Pessoais*, 67.

[68] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 153.

lealdade"[69]. Agir com lealdade significa que o responsável pelo tratamento de dados actua com honestidade, correcção e retidão perante todo o processo, i.e. desde a identificação do titular dos dados, a informação a prestar para a obtenção do consentimento, na recolha e tratamento dos dados.[70]

Não existe na lei angolana uma referência de obrigatoriedade que concretize o conceito de lealdade referida no preceito em análise. Por isso, a lealdade deve ser encarada como um princípio amplo, com uma função de "guarda-chuva" (*umbrella function*)[71], que impede que os dados pessoais em saúde sejam tratados com a finalidade de prejudicar, ou tratados de forma discriminatória, dissimulada, ou com surpresa para o seu titular, ou que haja motivo para ser invocado quando o tratamento esteja em contradição com o espírito da LPDP. A lealdade obriga também os responsáveis pelo tratamento a que atendam permanentemente, enquanto for justificável, aos interesses e às legítimas expectativas dos titulares dos dados[72].

O nº 2 do art. 7º dispõe que "o tratamento de dados pessoais que conduza a uma discriminação arbitrária e ilícita em relação ao seu titular é considerando contrário ao princípio da boa-fé". A não discriminação deveria ser um princípio autónomo, pois no processo de tratamento de dados ganha contornos especiais, devido à natureza

---

[69] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 153.

[70] Ana Francisco Pinto DIAS, "A Dimensão Processual da Proteção de Dados – Uma breve referência à luz do regulamento geral de proteção de dados", *Revista de Direito da Responsabilidade*, Coimbra, 4 (2022) 7.

[71] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 153.

[72] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 153.

dos dados, que são qualificados como sensíveis, revelando um alargado espaço de riscos de estratificação e estigmatização das pessoas a partir de perfis desenhados pelo processamento de dados.

Para se evitar que o tratamento de dados pessoais sensíveis seja considerado ilícito, impõe-se que o seu titular dê o seu consentimento para uma ou mais finalidades específicas; não podendo consentir, o tratamento justifica-se por ser necessário para a defesa de interesses vitais do seu titular, ou de outra pessoa singular ou de interesses legítimos. Para o caso em apreço, e dado o facto de a locução *interesses vitais* revestir a forma de cláusula geral, o seu campo de aplicação deve ser tendencialmente limitado: o tratamento necessário para acautelar os interesses vitais do titular ou de interesses de terceiros que envolvam dados relativos à saúde e à vida sexual do titular dos dados, bem como aos dados genéticos (e biométricos). Afinal, quando fizermos alusão a interesses vitais como medidor da licitude do tratamento de dados, no preenchimento da materialidade do conteúdo da cláusula geral em causa, devem ter-se em atenção questões de significativa gravidade, como atentar contra a vida, a integridade física e a incolumidade do indivíduo. Já os interesses legítimos devem ser entendidos sob três perspectivas[73]: "*(i)* a prossecução de interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados; *(ii)* a necessidades do tratamento dos dados pessoais para a realização do interesse legítimo prosseguido e *(iii)* os direitos e liberdades fundamentais do titular dos dados não prevalecem".

Há que atender também a um interesse público ou da autoridade pública, designadamente quando está em causa *(i)* o exercício de

---

[73] Cfr. acórdão *Fashion ID* do Tribunal TJUE (Tribunal de Justiça da União Europeu), C-40/17, 29 de Junho de 2019, parágrafo 95, *apud* Graça Canto MONIZ, *Manual de Introdução à Proteção de Dados Pessoais*, Coimbra: Almedina, 2023, 91.

funções de interesse público ou *(ii)* o exercício de autoridade pública de que está investido o responsável pelo tratamento. O exemplo que a LPDP nos pode oferecer decorre do art. 14, nº 2, que isenta o consentimento para o tratamento de dados sensíveis de saúde, nomeadamente "(…) para efeitos de medicina preventiva, de diagnóstico médico, de assistência médica consentida, de gestão e estatística de serviços de saúde ou quando se trata de uma emergência médica ou justificada pelo interesse público". Outra exigência que se pode adicionar à legitimidade do exercício de funções de interesse público ou de autoridade pública é a existência de *poderes públicos* atribuídos por acto legislativo competente. A Agência de Protecção de Dados é dos órgãos com *poderes públicos* que intervêm sempre, quer para emitir a autorização para o tratamento, quer para tomar conhecimento do tratamento através de notificação.

2.3 Princípio da proporcionalidade

O art. 8º da LPDP dispõe o *princípio da proporcionalidade*. Anuncia assim o legislador: "os dados pessoais sujeitos a tratamento devem ser *pertinentes, adequados* e *não excessivos* relativamente às finalidades que legitimamente a sua recolha e tratamento." (itálico nosso). O que o responsável pelo tratamento dos dados deve fazer é sopesar a protecção da esfera jurídica do seu titular e a realização das finalidades que legitimam a recolha e o tratamento, ou seja, ponderados os interesses em causa, do responsável e dos titulares, o tratamento de dados deverá ser realizado através de meios adequados para o fim visado, salvaguardando, por um lado, o direito à protecção dos dados pessoais e outros direitos fundamentais, e por outro o interesse do responsável, o qual se consubstancia também num direito que não pode ser comprimido para além do necessário, devendo ser atingido num justo equilíbrio

que não afecte o conteúdo essencial dos direitos em presença[74].

Esta ponderação, exige a colocação em presença do direito à privacidade e à protecção dos dados pessoais de todas as pessoas, enquanto direito fundamental inscrito expressamente no catálogo de direitos, liberdades e garantias individuais, com o interesse público constitucionalmente consagrado no capítulo dos direitos e deveres culturais e que se consubstancia no incremento da protecção do direito à saúde e à investigação científica. Resulta assim a necessidade de ponderação dos valores em face dos casos concretos. Tal exercício exige ultrapassar uma simples obrigação de consideração, desprovida de efeitos normativos concretos. O direito convoca resultados e só por meios deles se efectiva, por isso, um princípio normativo, na qualidade de ponto de apoio do sistema, "sustentando as normas que os desenvolvem e dando-lhes um sentido e uma função"[75], não podendo impor uma simples contemplação de outros princípios – pelo contrário, a consideração de um princípio equivale à respectiva aplicação. Assim, o princípio da proporcionalidade, ou da proibição do excesso, equaciona a convocação dos meios para a realização dos

---

[74] Ana Raquel Gonçalves MONIZ, *Os Direitos Fundamentais e a sua Circunstância. Crise e Vinculação Axiológica entre o Estado, a Sociedade e a Comunidade Global*, Coimbra: Imprensa da Universidade de Coimbra, 2017, 158. A autora entende que "a matéria dos direitos fundamentais constitui terreno fértil para a mobilização do princípio da proporcionalidade. Constituindo um dos subprincípios do Estado de direito, a proporcionalidade conhece uma aplicação específica em matéria de direitos fundamentais, quer enquanto elemento coadjuvante da interpretação dos próprias normas que consagram os direitos, sem ignorar que estas podem colidir com outros bens jurídicos constitucionalmente protegidos, quer como padrão para a aferição da constitucionalidade das medidas dos poderes públicos, em especial naquelas que restringem direitos liberdades e garantias, assumindo-se como um dos «limites dos limites»".

[75] Carlos Alberto da Mota PINTO, *Teoria Geral do Direito Civil*, 95.

fins preconizados, "visando responder ao problema de saber se, depois de aferida a legitimidade dos últimos, a sua consecução se pode alcançar através das medidas selecionadas, que hão de ser idóneas e exigíveis, causando mais benefícios que prejuízos"[76].

O princípio da proporcionalidade estatuído na LPDP tem três elementos que conformam o seu conteúdo, designadamente a pertinência, a adequação e a não excessividade relativamente às finalidades do tratamento. Vamos fazer-lhes uma breve referência.

2.3.1 O tratamento deve ser *pertinente*

Quando o responsável pelo tratamento de dados decide avançar com o procedimento, deve avaliar se é o momento exacto para o fazer, e se as condições objectivas e subjectivas estão reunidas. A pertinência diz respeito também á conveniência e congruência do tratamento de dados. É importante que a ocasião se mostre oportuna para que a finalidade seja alcançada de forma lícita, e o tratamento deve responder às finalidades e ao momento da sua realização. Ou seja, o tratamento dos dados deve ser não apenas desejável, mas também necessário, e muitas vezes indispensável. A indispensabilidade é também entendida como necessidade, para revelar que os meios alternativos são todos adequados e constituem um "instrumento menos lesivo ou menos intrusivo, em consequência directa da força jurídica dos direitos"[77].

2.3.2 Deve ser *adequado*

---

[76] Ana Raquel Gonçalves MONIZ, *Os Direitos Fundamentais e a Sua Circunstância,* 158.

[77] Ana Raquel Gonçalves MONIZ, *Os Direitos Fundamentais e a Sua Circunstância,* 159.

É adequado na medida em que o tratamento deve ser oportuno, propício e conforme com os objectivos pré-definidos para o mesmo. A adequação não se confina às finalidades determinadas, mas deve atender também ao respeito pelos direitos fundamentais do titular dos dados, ainda que esteja em causa interesse público (recolha de dados para gestão e estatística de serviço de saúde, ou quando se trate de emergência médica) ou o exercício de autoridade pública de que esteja investido o responsável pelo tratamento (recolha de dados para efeitos de medicina preventiva ou de diagnóstico médico). O processo de tratamento está em conformidade com as finalidades definidas; logo, é possível a realização do propósito da recolha dos dados que é adequada e relevante.

A adequação reclama que os meios a serem usados para o tratamento possam ser alternativos (no sentido da escolha pelo responsável) daquele que seja menos invasivo da esfera jurídica do titular dos dados, como por exemplo a anonimização[78].

2.3.3 Deve ser *não excessivo*

A lei, ao determinar que o tratamento de dados não deve ser excessivo relativamente às finalidades que legitimam a sua recolha e tratamento, pretendeu que o responsável adoptasse as medidas menos restritivas para os direitos do titular dos dados, que haja *razoabilidade* entre o sacrifício imposto aos direitos do titular, mesmo que consentido, e a relevância dos motivos que justificam o tratamento dos dados. Por isso, o responsável deve tomar as providências de equilíbrio, não sendo desmedido ou demasiado o equilíbrio entre a quantidade e qualidade dos dados a recolher e as finalidades que se propuser, pro-

---

[78] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 159.

cedendo para o efeito através de juízos valorativos e de ponderação.

A razoabilidade, como categoria do princípio da proporcionalidade, deve ser também vista como uma forma individualizadora de apreciação: no âmbito do direito da saúde, podem ser tidas como excessivas as finalidades determinadas para o tratamento de dados, na medida em que os fundamentos que se impuseram possam ser considerados como razoáveis no contexto geral. Os dados pessoais em saúde são qualificados como sensíveis, resultando daí a exigência de determinabilidade, como dimensão da proibição do excesso. Com efeito, bastará que os fundamentos sobre os quais assentam as finalidades do tratamento dos dados em saúde manifestem determinabilidade, clareza e suficiente densidade. Assim se garante a supremacia da dignidade da pessoa humana, como também a garantia da protecção da confiança no tratamento em si, e no responsável pelo tratamento[79].

2.4 Princípio da finalidade

O art. 9º da LPDP prevê o *princípio da finalidade*, e o nº 1 determina que "os dados pessoais devem ser recolhidos e tratados para finalidades determinadas, explícitas e legítimas de acordo com o definido em diploma próprio". Este princípio está conexionado com o da licitude pois, como não deveria ser de outra forma, quando a identificação da finalidade do tratamento dos dados não for contra a dignidade da pessoa do seu titular acaba por legitimar e tornar o processo lícito. A finalidade do tratamento de dados, com maior incidência na área da saúde, impede que o responsável pelo tratamento execute o processo de forma livre, sem qualquer permissão específica e sob as condições que a lei estabelece.

---

[79] Jorge Reis NOVAIS, *Os Princípios Constitucionais Estruturantes da República Portuguesa*, Coimbra: Coimbra Editora, 2004, 178 seg.

A importância deste princípio no quadro do regime jurídico da protecção de dados pessoais em saúde pode ser exposta da seguinte forma: funciona como fundamento para a realização de tratamento dos dados, justificando a imposição do consentimento. Assim, o princípio é uma "razão-finalidade"[80] para legitimar o tratamento. O nº 2 deste artigo determina que "é proibido o tratamento de dados pessoais para fins distintos ou incompatíveis com aqueles que originam a sua recolha e tratamento, salvo se: *a)* o titular dos dados tiver dado o seu consentimento expresso; *b)* o tratamento tenha fins históricos ou estatísticos e os dados sejam anonimizados para este efeito; *c)* o tratamento tenha por objectivo a prevenção, investigação e repressão criminal, ou a segurança nacional, desde que não devam prevalecer os direitos, liberdades e garantias dos titulares dos dados".

Começando pela última alínea do preceito referido supra, cumpre notar que a CRA impede, de uma forma geral, a limitação ou suspensão dos direitos, liberdades e garantias, excepto (art. 58º) em caso de estado de guerra, de estado de sítio ou de estado de emergência, e estas situações anómalas só podem ser declaradas em todo ou em parte do território nacional, nos casos de agressão efectiva ou iminente por forças estrangeiras, de grave ameaça ou perturbação da ordem constitucional democrática ou de calamidade pública. Porque estamos a falar de protecção de dados pessoais em saúde, parece ser de se admitir que possa ocorrer alguma perturbação na sua garantia em casos de calamidade pública[81]. Mas a CRA é pobre

---

[80] Alexandre Sousa PINHEIRO, *Privacy e Protecção de Dados Pessoais: a Construção Dogmática do Direito à Identidade Informacional*, Lisboa: AAFDL, 2015, 826.

[81] Cfr. Raúl Carlos Vasques ARAÚJO / Elisa Rangel NUNES, *Constituição da República de Angola Anotada*, Tomo I, Luanda, 2014, 363. Entendem os autores que as restrições aos direitos, liberdades e garantias estão sujeitas a um conjunto de regras muito apertadas que são as seguintes: "*a*) proibição absoluta da suspensão de alguns direitos, liberdades e garantias. São chamados direitos invioláveis.

na sua regulamentação, pelo que se impõe a necessidade de nos socorrermos da lei da protecção civil – lei nº 28/03, de 7 de Novembro, que sofreu alterações aos artigos 12º e 29º, introduzidas pela lei nº 14/20, de 22 de Março. Esta lei veio proteger todo o sistema de saúde, nos casos de ocorrência de calamidade pública, determinando no art. 4º, nº 1 que "(…) o Titular do Poder Executivo pode adoptar medidas de natureza administrativa, que incidem sobre: *e)* a protecção de cidadãos em situação de vulnerabilidade; *g)* o funcionamento de creches, infantários, instituições de ensino, lares de terceira idade e lares de acolhimento; *i)* a prestação de serviços de saúde; *m)* a defesa e controlo sanitário das fronteiras; *o)* a definição de cordões sanitários". O nº 3 do artigo em referência determina a observância e respeito do princípio da proporcionalidade do agir público, devendo as medidas a serem tomadas serem *necessárias* e *adequadas* para pôr cobro à ameaça que visam combater ou evitar.

Por fim, as finalidades do tratamento de dados sensíveis estão circunscritas a determinadas limitações, designadamente, deverem ser:

Estes direitos são: a aplicação das regras constitucionais relativas à competência e ao funcionamento dos órgãos de soberania. Significa que em caso algum se podem alterar as competências próprias de cada órgão de soberania em restringir a sua actividade; *b)* os direitos e imunidades dos membros dos órgãos de soberania; c) o direito à vida, à integridade pessoal e à identidade pessoal; *d)* a capacidade civil e a cidadania; *e)* a não retroatividade da lei penal; *f)* o direito à defesa dos arguidos; e *g)* a liberdade de consciência e de religião".

O direito à vida e à integridade pessoal é uma expressão do direito à saúde, pelo que só em situação de calamidade, como foi o que ocorreu com a pandemia da Covid-19, se podem justificar determinadas limitações ao tratamento de dados pessoais, como por exemplo para efeitos de prevenção do alastramento do vírus e da investigação científica sobre o vírus, a doença e a sua transmissão, ou seja, quando está em causa a necessidade de os serviços de saúde tomarem medidas sobre prevenção ou controlo de doenças transmissíveis e outras ameaças para a saúde pública.

a) *determinadas*, no sentido de que a determinação deve ser declarada antes do processo de tratamento. Neste sentido, "a identificação das finalidades não pode ficar por realizar, não pode ser adiada ou condicionada a um evento futuro, certo ou incerto"[82];

b) *explícitas*, depois de determinadas as finalidades, o responsável pelo tratamento deve informar, para tomada de conhecimento, os titulares dos dados, as autoridades competentes e terceiros;

c) *legítimas*, pois não bastará o cumprimento das exigências constantes no art. 9º, mas o cumprimento de todas as obrigações legais que em concreto possam ser convocáveis; nestes termos, todas as finalidades eleitas em violação da lei (em sentido geral) devem ser consideradas ilegítimas.

As limitações às finalidades, no contexto da saúde, particularmente na investigação, em que há uma utilização primária e outra secundária de utilização de dados, pode perder fulgor. Neste domínio, o tratamento posterior para fins de investigação científica, histórica ou estatística, não deve ser considerado incompatível com as finalidades iniciais. No entanto, sem colocar em causa a compatibilidade expressa, o responsável pelo tratamento poderá vir a apresentar um novo fundamento legal para o tratamento de dados, quando o fundamento anterior (de investigação clínica) não se estende para a nova operação (*v.g.*, de estatística clínica)[83]. Justifica-se esta posição, pois o responsá-

---

[82] A. Barreto Menezes CORDEIRO, *Comentários ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*, 104.

[83] Elisabete CASTELA / Tiago Branco da COSTA, "A investigação clínica na era do altruísmo dos dados: algumas considerações em torno da proteção de dados pessoais", in *Anuário da Protecção de Dados*, Centro de I&D Sobre Direito e Sociedade, Faculdade de Direito da Universidade Nova de Lisboa, 2023, 267.

vel e os participantes no processo de investigação clínica não deverão alegar existência de "compatibilização" de fundamentos para fins de investigação científica ou de estatística com base em presunção, pois tal poderá facilitar que outras intenções que não as estritamente para fins de investigação clínica se achem encobertas[84].

2.5 Princípio da veracidade

O art. 10º da LPDP estabelece o *princípio da veracidade*. Determina o nº 1 que "os dados pessoais sujeitos a tratamento devem ser exactos". A exatidão aqui significa que os dados pessoais devem ser *correctos* e *actualizados* sempre que necessário, devendo ser adoptadas, conforme o nº 2, as medidas "para assegurar que dos dados total ou parcialmente inexactos ou incompletos sejam apagados ou rectificados, de forma que correspondam à situação actual e concreta do seu titular". "Correctos" significa que devem estar conforme foram autorizados pelo titular, ou a recolha dos dados está em conformidade com as características reais do seu titular. Em saúde e no âmbito do diagnóstico médico, "correctos" significa que a imagem de radiografia captada no tórax de um paciente deve representar fielmente os elementos constantes do tórax (por exemplo os pulmões) e pertencer àquela pessoa concreta. "Actualizados" significa que, no momento do tratamento, publicação ou transferência, devam ser como as informações adquiridas ou recolhidas através do estatuto real do seu titular, podendo ser alterados se ocorrer alteração nos seus dados de estado civil ou no estado de saúde do titular. Retomando o exemplo supra, quando o responsável estiver a realizar o tratamento de dados daquele paciente concreto, a informação deverá corresponder àquela

---

[84] Elisabete CASTELA / Tiago Branco da COSTA, "A investigação clínica na era do altruísmo dos dados", 267.

imagem e não a uma anterior. Quando no decorrer do processo dúvidas surgirem, deverá realizar-se nova captação de imagem; é neste sentido que deve ser entendido "actualizado". Só assim o participante no processo de investigação poderá exercer o seu direito, sejam os dados rectificados ou, *in extremis*, apagados.

O sentido teleológico do preceito em análise, exige do responsável pelo tratamento de dados pessoais uma acção movida pela correcção, actualizando os dados sempre que for necessário, através de medidas garantidoras de tal desiderato.

2.6 Princípio da duração do período de conservação

O art. 11º do LPDP estabelece o *princípio da duração do período de conservação*. Determina o nº 1 que "os dados pessoais devem ser conservados de forma a permitir a identificação dos seus titulares apenas durante o período necessário à prossecução das finalidades que originaram a sua recolha ou tratamento, devendo ser posteriormente eliminados ou tornados anónimos". Quando a finalidade da qual resultou o tratamento de dados pessoais for atingida, nada justifica a manutenção dos mesmos, a não ser que a conservação passe a estar sob anonimato. É um mecanismo para garantir que a finalidade do tratamento seja respeitada, e assim se evitar o risco de utilização ilegítima dos dados. A finalidade do tratamento configura assim o principal critério para determinar o prazo de conservação dos dados. Outro motivo para a conservação dos dados pode ser o fundamento para a demonstração de um ónus jurídico, como provar um facto decorrente de um tratamento médico (cirurgia, receita médica, diagnóstico, *v.g.*) de que resultou dano para obrigar o lesante a indemnizar, ou para efeitos de garantias para justificação de execução de um contrato de doação de órgãos, tecidos ou células, principalmente *post mortem*. Entretanto, nestas situações, a conservação de dados deve limitar-se a um prazo razoável para cumprimento daquela obrigação, sujeitando o seu acesso a um controlo.

O nº 2 do artigo em análise dispõe que "a conservação de dados pessoais para fins históricos, estatísticos, de investigação criminal e de segurança nacional pode ser autorizada pela APD por período superior mediante requerimento do responsável pelo tratamento". Para o que interesse ao presente escrito, nestas circunstâncias os dados de saúde para fins históricos e estatísticos conjugam-se para determinar, por exemplo, épocas de endemias e pandemias, períodos sazonais de aparecimento de determinados doentes ou vectores de transmissão de doenças, ou seja, dados para interesse e valor para a saúde pública, bem como o interesse para a segurança nacional. Vejamos o que pode acontecer se mais de metade da população de um determinado território nacional ficar afectada por um vírus mortífero como o ébola.

Na verdade, este princípio, também chamado princípio da limitação da conservação na Europa, determina que "volvido o período de tempo necessário para a prossecução dos fins determinados, os dados devem ser, o quanto antes, apagados"[85]. Assim, é dever de cada responsável pelo tratamento determinar os prazos para o apagamento ou para a revisão periódica da sua conservação, de forma a assegurar que os dados pessoais de saúde sejam mantidos apenas durante o período para a concretização da finalidade.

Se avaliarmos os instrumentos de protecção de dados sensíveis de países ou regiões modernas, verificaremos que a nossa lei de protecção de dados pessoais não regulou dois princípios importantes, nomeadamente o da integridade e confiabilidade, e o da responsabilidade.

---

[85] A. Barreto Menezes CORDEIRO, *Comentários ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019*, 106.

3. O CONSENTIMENTO

O consentimento constitui um elemento estruturante da protecção de dados pessoais. Não resulta apenas do facto de esta protecção ser uma categoria jurídica geral aplicável ao direito, mas também porque representa já uma expressão de autenticidade para a anuência ao seu tratamento por parte do titular dos dados pessoais, em atenção à sua finalidade[86]. Dado este duplo aspecto, o consentimento carrega consigo alguns problemas, dos quais importam, por serem objecto de contínuo estudo, os vícios de vontade e os vícios da forma de manifestação da vontade, de que falaremos *infra*.

O tema do consentimento não tem a sua sede exclusiva no tratamento de dados. O Código Civil faz inúmeras referências; aliás, é sua fonte, *v.g.*, o art. 340º. O Código Penal também trata do tema – artigos 34º, 35º e 165º – oferecendo tutela ao agente quando actua, excluindo a ilicitude do facto quando se referir a interesses livremente disponíveis e o acto não for contrário aos bons costumes e à dignidade da pessoa humana.

É no âmbito da bioética que o consentimento ganhou a intenção axiológica que hoje lhe é reconhecida, pois neste campo é que foi desenvolvido o termo *consentimento informado* e *consentimento li-*

---

[86] George D. POZGAR, *Legal and Ethical Essentials of Health Care Administration*, 233 e seg.

vre e esclarecido. No geral, este consiste no procedimento através do qual – exceptuadas as situações de risco iminente de morte, após elucidar o paciente, seus familiares ou pessoas próximas, no caso de impossibilidade ou risco de dano do paciente – se obtém o seu consentimento para a realização de actos médicos.

Sem pretender aqui embarcar na discussão sobre a natureza jurídica do consentimento, vamos apenas abordar as três linhas imprescindíveis para que o tema em questão tenha sustentabilidade dogmática. Em primeiro lugar, o consentimento deve ser visto como um processo, e não como um simples acto. Na verdade, as informações sobre terapêutica, sobre a finalidade do tratamento dos dados pessoais, devem ser levadas de forma esclarecida ao paciente ou titular dos dados de forma contínua para que ele forme voluntariamente a sua convicção. Não é, pois, qualquer documento que é levado ao paciente ou titular de dados que servirá de elemento para autorizar o profissional a realizar qualquer acto ou a isentá-lo de responsabilidade. Em segundo lugar, e relacionado com o que acabamos de referir, decorre do facto de o consentimento informado, livre e esclarecido ter uma dupla função: *jurídica*, porque excludente da ilicitude do acto, por isso, de defesa do profissional; *ética*, como processo contínuo de esclarecimento na relação entre médico/responsável pelo tratamento de dados e paciente/titular de dados pessoais, protegendo sempre a autodeterminação deste último. Em terceiro lugar, em muitas situações a questão do consentimento é colocada em relação a pessoas que se encontram em situação de vulnerabilidade, quer se trate de pessoa em situação crítica de saúde, quer se trate de pessoa com pouco ou nenhum conhecimento técnico (não sabendo, por exemplo, diferenciar quando está no campo do tratamento terapêutico ou na área da investigação científica, já que em ambas se exige tratamento de dados pessoais). A vulnerabilidade pode atingir a situação económica e, sendo os dados pessoais um produto económico de grande importância global, as pessoas podem oferecer os seus dados pessoais sensíveis sem terem o devido conhecimento dos

riscos que daí podem resultar, por entenderem que a contrapartida económica oferecida é, naquelas circunstâncias, vantajosa.

Com base nestes aspectos de vulnerabilidade, devemos atender aos limites que impõem a utilização do consentimento. Ou seja, o consentimento não deve ser usado pelo responsável pelo tratamento de dados pessoais se não estiver garantida a observância de alguns requisitos, designadamente, o respeito pela privacidade, inviolabilidade da intimidade, da honra, bom-nome e imagem, livre desenvolvimento da personalidade, dignidade e livre exercício da cidadania, enfim, dos direitos humanos. O respeito destes direitos serve de fundamento ao consentimento, pelo que consentir não é um acto por si só bastante, devendo ser exigida a observância destes requisitos/fundamentos. Veja-se, por exemplo, quando o tratamento de dados é realizado de forma digital, é comum encontrar em *sites* depararmo-nos com *boxes* ou caixas com a pergunta se o utilizador consente no tratamento dos seus dados. O mundo digital favorece a recolha de dados em grande escala, fornecida de forma voluntária ou involuntária pelas pessoas através da internet. Neste espaço da "sociedade de informação", predomina a *hiperinformação* e uma economia de dados interconectada por um sistema electrónico. Nestas situações, ainda que se assegure que o consentimento obedece à lei, ou seja, que se apresenta como livre, informado, inequívoco e com finalidade determinada, é importante que antes esteja em consonância com princípios e fundamentos que norteiam o sistema de protecção de dados, destacando-se os direitos dos titulares dos dados pessoais. Como entende POZGAR[87], "*informed consent is a legal doctrine that provides that a patient has the right to know the potential risks, benefits, and alternatives of a proposed procedure*". Citando o caso judicial

[87] George D. POZGAR, *Legal and Ethical Essentials of Health Care Administration*, 234 e seg.

Canterbury v. Spence de 1972, afirma que "*set the 'seasonable man' standard, which required informed consent for treatment*".

Dentro das definições oferecidas pela LPDP no art. 5º, al. *a)*, vem a de *consentimento do titular dos dados*, sendo "qualquer manifestação de vontade livre, específica, explícita e informada, independentemente do suporte, no qual o titular dos dados autoriza o seu tratamento". Desta definição é possível extrair os seus elementos, designadamente a manifestação de vontade, que seja livre, específica, explícita e informada. O conceito que o legislador europeu elaborou no RGPD, art. 4º, nº 1, é próximo do nosso, mas apresenta um pouco mais de detalhe na forma de manifestação da vontade. Aí, o consentimento é a "manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou acto positivo, que os dados pessoais que lhe dizem respeito sejam objecto de tratamento". Como verificaremos no desenvolvimento dogmático dos elementos constitutivos do conceito de consentimento conforme o legislador angolano, A. BARRETO MENEZES CORDEIRO[88] entende que a expressão "explícita" se encontra apenas na versão portuguesa do RGPD, resultando de um erro de tradução, pelo que não deve ser considerada. Efectivamente, o legislador angolano foi infeliz em colocar no preceito onde encontramos o conceito de "consentimento" a exigência de uma manifestação "específica" e "explícita", que parecem ter a mesma intenção teleológica, pelo que nos dispensaremos de abordar o elemento "explícita", para elegermos manifestação "inequívoca".

As premissas correspondentes aos elementos constitutivos do consentimento levam a deduzir que o direito à intimidade é vulnerável quando a intromissão no âmbito do próprio e reservado do

---

[88] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 171.

titular dos dados não seja de acordo com a LPDP, não seja eficazmente consentida ou, mesmo que autorizada, subverta os termos e alcance para o qual se manifestou o consentimento. Quebra-se a conexão entre a informação pessoal que se recolhe e o objectivo tolerado para o qual foi colhida. A lei impõe, portanto, não só a confidencialidade dos dados médicos recolhidos e analisados, como também o tratamento dos dados realizado com os meios técnicos robustos e deve seguir uma forma que não possibilita a intromissão no contexto da vida privada e íntima do paciente.

De uma forma geral, o consentimento em saúde, nos termos do nº 1, al. a) do art. 14º determina o consentimento inequívoco como condição de validade do tratamento de dados; em especial – convocada a legislação para o caso – o consentimento na investigação clínica não é condição de validade/legitimidade da participação do doente e, para a investigação científica é dispensável, bastando notificação à APD, conforme o nº 2 da mesma norma. É dado assente e unânime na doutrina que o tratamento de dados para fins de investigação clínica e científica, bem como estatística, tende a superar o consentimento como condição, bastando que a informação recolhida seja anonimizada, ou seja, tornando-a um dado não pessoal. Ainda assim, respeitar-se-á em primeira linha a autodeterminação informativa no contexto da saúde (incluindo o tratamento médico, medicina preventiva e investigação clínica/científica).

Uma exigência presente no consentimento em saúde é o seu aspecto ético. A lei que muita falta nos faz, mas que existe por exemplo na pátria de Camões e no Reino de Espanha, é a Lei da Investigação Clínica. A portuguesa dispõe no art. 2º, al. *l),* que o consentimento informado é "a decisão expressa de participar num estudo clínico, tomada livremente por pessoa dotada de capacidade de o prestar ou, na falta desta, pelo seu representante legal, após ter sido devidamente informada sobre a natureza, o alcance, as consequências e os riscos do estudo, bem como o direito de se retirar do mesmo a qualquer momento, sem quaisquer consequências, de acordo com as

orientações emitidas pela Comissão de Ética Competente, que deve ser escrito, sempre que aplicável".

Assim, o consentimento ético exigível no âmbito do tratamento de dados em saúde não se confunde nem é absorvido pelo consentimento estabelecido no âmbito da LPDP. É verdade que eles podem conviver, e é desejável que assim seja. Mas o consentimento ético para cá e para lá da norma positivada faz sobressair o primado da pessoa humana como seu ponto de partida, ou seja, a linha mestra do consentimento ético, por ser imperioso no tratamento de dados em saúde o respeito pela dignidade da pessoa humana, que deve nortear a actuação dos actores envolvidos na investigação clínica/científica.

3.1 Manifestação de vontade

A manifestação de vontade que a LPDP anuncia no preceito referido, não destaca uma especialidade, devendo remeter para o conceito tratado em sede dos negócios jurídicos.

A manifestação de vontade é a forma de actividade exercida com plena consciência. Uma atitude ou inibição precedida de reflexão. É a capacidade de poder tomar uma decisão de forma autónoma e responsável. Expressar uma vontade corresponde à soberania do eu sobre si mesmo. Kant veio emprestar um toque de evolução ao conceito de autonomia considerando como "fundamento da dignidade da pessoa humana"[89]. A autonomia é condição da realidade humana que lhe dá capacidade para ser e agir como sujeito, ultrapassando uma ideia, que vigorou durante muito tempo em saúde, de manipulação utilitária.

---

[89] Immanuel KANT, *Fundamentação da metafísica dos costumes*, Lisboa, Edições 70, 2008, 83.

3.2 Manifestação de vontade livre

Não há consentimento livre se o titular dos dados não se encontrar numa situação de completa liberdade, podendo fazer escolhas. A liberdade é o principal pressuposto da manifestação de vontade, pois só com ela o titular dos dados manifesta prioridades, decisões e renúncias. Não poderá existir manifestação livre da vontade de consentir se o titular dos dados for coagido ou sofrer consequências negativas. Ele deve decidir se presta o consentimento ou não.

Em saúde, a manifestação do consentimento para a recolha e tratamento de dados tem particularidades a ter em consideração. Há situação em que o titular de dados não se acha em condições de prestar o consentimento ou de prestá-lo manifestando de forma específica inequívoca ou informada. Muitas vezes o titular dos dados encontra-se numa unidade de tratamento intensivo (UTI), noutras vezes traumatizado, pode ser mudo/surdo, menor de idade ou com problemas do foro psíquico/psiquiátrico. Também tem acontecido, mais no âmbito da investigação clínica ou científica, que o titular, enquanto participante no processo, presta o consentimento por estar com ânsia de cura, ou simplesmente com razões do ego pessoal, como a fama, de ver-se envolvido num processo científico.

Muito menos será livre se, por exemplo, algo que se regista com muita frequência nos nossos estabelecimentos hospitalares, o consentimento for prestado em circunstâncias de ameaças de não vir a ser tratado, ou convenientemente tratado, se não aceitar a decisão médica. Deste modo, a regra a ser considerada será aquela em que, o consentimento será considerado inválido se o titular dos dados não puder exercer uma verdadeira escolha, se se sentir coagido a dar o consentimento.

3.3 Manifestação de vontade específica

Para que ocorra manifestação do consentimento de forma específica é necessário que o responsável pelo tratamento preste informação específica acerca das finalidades que se propõe, se para prestação de cuidados ou tratamento de saúde, se para investigação clínica/investigativa ou outra, mas no âmbito da saúde. Ora, a especificação em função da finalidade pressupõe que a finalidade deva ser determinável, explícita e legítima, pois só assim faz sentido que o titular dos dados emita o seu consentimento de forma específica.

Ademais, o responsável pelo tratamento deve colocar "em cima da mesa" a possibilidade de o titular optar, entre várias finalidades, separadamente, por forma a possibilitar o consentimento específico para cada finalidade. E para cada finalidade oferecida, o responsável pelo tratamento deve prestar informações específicas, por forma a que o consentimento livre seja igualmente informado.

Quando se está a lidar com um doente, a finalidade é a cura ou prestação de cuidados, havendo certamente opções de escolha: aquela que o médico elege como estando conforme com a doença e as características do doente, e outra, caso alguma anomalia possa registar-se. Por exemplo, a telecirurgia é um processo moderno e com alguma eficácia, mas o médico/responsável deverá sempre informar o paciente das vantagens e desvantagens daquele processo, e quais são as alternativas. Quanto à investigação clínica/investigação também haverá escolhas, o que leva a concluir da necessidade de o consentimento específico exigir granularidade nos pedidos de consentimento.

3.4 Manifestação de vontade inequívoca

O consentimento específico e explícito parece, como referido supra, convergir no mesmo objectivo. Assim, cumpre abordar a manifestação de vontade inequívoca, que impõe ao titular dos dados a prestação do consentimento de forma a não resultarem dúvidas,

devendo a manifestação ser feita por escrito ou oralmente, de forma expressa ou tácita. A lei angolana não a prevê dentro do conceito que o legislador elaborou; mas, dada a sua importância dogmático-normativa para uma melhor compreensão do consentimento, indicamos também como elemento constitutivo do conceito em causa, como veremos já a seguir.

A opção por abordar a manifestação da vontade de forma inequívoca prende-se também com o facto de que o art. 5º, al. *a)*, que nos oferece o conceito de *consentimento do titular dos dados*, não conter este elemento, mas encontramo-lo no art. 12º, nº 1, al. *a),* que dita "consentimento inequívoco (…)". O mesmo ocorre no art.º 13º, nº 1, al. *b)*, *ii)* última parte, art. 14º, nº 1, al. *a)*; art. 16º, nº 1, al. *a)*; art. 19º, nº 1, al. *a)*; art. 20º, nº 1, al. *a)*; art. 22º, nº 1, al. *a)*. São muitas as normas que fazem referência ao *consentimento inequívoco*, não se compreendendo que o legislador tenha elaborado o conceito de "consentimento" com a introdução dos seus elementos constitutivos, esquecendo-se do elemento "inequívoco" em sete artigos que estabelecem os requisitos das várias situações específicas de tratamento de dados.

A inequivocidade do consentimento traduz o facto de a sua manifestação dever ser feita pelo titular dos dados, de forma que não suscite dúvidas ou incertezas antes do tratamento pelo responsável. A manifestação não pode oferecer diversos entendimentos; pelo contrário, o consentimento deve ser claro, evidente, manifesto e óbvio. A decisão é reservada ao titular dos dados, havendo sempre a possibilidade de o consentimento ser transmitido por terceiro[90], bastando que resulte claro, sem dúvidas de que o titular deu o seu consentimento para o tratamento dos dados em questão.

---

[90] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 185, em especial a nota 722.

3.5 Manifestação de vontade informada

A decisão livre depende da informação prestada ao titular dos dados pelo responsável do tratamento. A prestação da informação deve atendar às circunstâncias e ao contexto em que o responsável e o titular dos dados se encontram, para facilitar a compreensão deste último. Importa qui convocar o princípio da transparência, o qual, exigindo clareza na linguagem ou na escrita, torna a informação de fácil acesso e perceptível para facilitar ao titular dos dados saber e ter consciência dos efeitos jurídicos da prestação do consentimento. É de capital importância que a clareza e acessibilidade exigidas para a prestação de informações se traduzam numa linguagem de fácil compreensão cujo critério de prova seja a do padrão de uma pessoa comum, por forma a poder-se fazer uma distinção clara do consentimento de outros elementos.

Olhando uma vez mais o Direito europeu, nas *Orientações Relativas ao Consentimento*, o GT 29[91] considera imprescindíveis as seguintes informações para a validade do consentimento: "(i) identidade do responsável pelo tratamento; (ii) a finalidade de cada uma das operações de tratamento em relação às quais se procura obter o consentimento; (iii) que dados serão recolhidos e utilizados; (iv) existência do direito de retirar o consentimento; (v) informações acerca da utilização dos dados para decisões automatizadas (…), e; (vi) sobre os possíveis riscos de transferência de dados devido à inexistência de uma decisão de adequação e de garantias adequadas (…)". Segundo A. BARRETO MENEZES CORDEIRO[92], não é admissível a limitação da "informação devida aos titulares dos dados, no

[91] Grupo de trabalho sobre o artigo 29º do RGPD.

[92] *Direito à Proteção de Dados à Luz do RGPD e da Lei nº 58/2019*, 182-183.

que aos seus direitos respeita" ao (iv) direito a retirar o consentimento, nem em circunscrever o dever de informar dos riscos ao disposto no ponto (vi)". Apresenta ainda dúvidas quanto à autonomização do ponto (v). Para o autor, as informações que devem ser disponibilizadas aos titulares dos dados são: "(i) os dados pessoais a serem objecto de tratamento; (ii) a identidade do responsável pelo tratamento; (iii) as finalidades a que o tratamento se destina; (iv) os direitos dos titulares dos dados; e (v) os riscos associados ao tratamento. A informação prestada, a propósito de cada um destes pontos, deve ser completa, verdadeira, actual, clara e objectiva".

O consentimento informado no domínio da prestação de cuidados de saúde, deve respeitar a dignidade individual, pois assim "afasta os riscos de fraude ou influência indevida, estimula a adopção de uma atitude racional (…) e se aproxima do ideal de uma aproximação plena". Por outro lado, "tal como outro precioso bem, a liberdade, a autonomia tem as suas limitações e será tanto mais respeitada quanto mais racional e ponderada for utilizada"[93].

3.6 O problema do interesse público

Outra questão relativa ao consentimento como elemento integrativo do conceito de licitude é a legitimidade atribuída à entidade/responsável pública e privada pelo tratamento de dados. O interesse público subjacente é marca de licitude no domínio do tratamento de dados em saúde. Assim, o lugar para tratar deste assunto seria quando falamos do princípio da licitude. Mas, como está em causa o afastamento do consentimento quando se elege o interesse público como fundamento do tratamento de dados, preferimos a sua discussão neste espaço.

---

[93] Walter OSSWALD, "Limites do consentimento informado", in *Estudos de Direito de Bioética*, Coimbra: Almedina, 2009, 151-160.

A dispensa do consentimento não torna os entes públicos dispensados do cumprimento das regras constantes da LPDP e legislação conexa; pelo contrário, as obrigações impostas à generalidade dos responsáveis pelo tratamento, são consequência do princípio da autorresponsabilidade baseada no risco em assentar o quadro normativo angolano e internacional a que Angola se vinculou em matéria de protecção de dados.

Não deve ser desvalorizado o papel do sector público numa realidade actual em que há novos riscos, novas ameaças à privacidade, identidade e liberdade pessoal com a utilização no tratamento de dados de novas tecnologias, como os *big data*, a inteligência artificial e a internet das coisas; os responsáveis do sector público estão, assim, juridicamente vinculados a defender, garantir e promover o interesse público. Há neste campo, sem margem para dúvidas, uma tensão de difícil conciliação entre a segurança do bem-estar colectivo (garantia da imparcialidade, objectividade das decisões, protecção da saúde pública, medicina preventiva, prevenção da fraude, etc.) e a defesa da dignidade da pessoa humana, considerando-a uma realidade ontológica viva, concreta e irrepetível. Apoiando-nos nas nossas posições, escutemos o TJUE, que num acórdão elucidou que "o direito à protecção de dados pessoais não é um direito absoluto, devendo ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade"[94].

Sobre o interesse legítimo há que analisar aquelas situações em que tal interesse se apresenta sobreposto aos direitos fundamentais, prin-

[94] Processo C-507/17, ECLI:EU:C:2019:772, Google LLC contra Commission National de L'informatique et des libertés (CNIL), de 24 de Setembro de 2019, §60, disponível em <https://curia.europa.eu/jcms/jcms/j_6/pe/>, consultado a 24 de Fevereiro de 2024.

cipalmente quando os dados se encontram na disponibilidade de terceiros, cujo escopo é mais o lucro do que o interesse público propriamente dito, apesar de o fim último de empresas no ramo da farmácia e do medicamento, e das fabricantes de dispositivos médicos, ser também um interesse público, sendo nesta medida portadoras de legítimo interesse. Assim, o que importa é saber se os meios, métodos e responsabilidade ética serão os mesmos usados no sector público e privado.

De um lado, o tratamento de dados pessoais no âmbito da investigação clínica/científica por cumprimento de uma obrigação legal, "pelas pessoas de direito privado, parece, em abstrato, consubstanciar uma ingerência eventualmente excessiva (…) na esfera jurídica das mesmas, colocando em causa a livre iniciativa económica e autonomia privada que as caracteriza"[95]. Por outro lado, ainda que as pessoas privadas não prossigam, em princípio, interesse público, teremos apenas as seguintes exigências a assinalar: o consentimento explícito do titular dos dados; a necessidade do tratamento de dados para o cumprimento de obrigações e para o exercício de direitos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, segurança social e de protecção social; que o tratamento seja realizado no âmbito das actividades legítimas e mediante garantias adequadas por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais; se o tratamento for necessário à declaração, exercício ou defesa de um direito num processo judicial. Num segundo plano, podem considerar-se também exigências para os privados, o tratamento de dados para efeitos de medicina preventiva ou do trabalho, para avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou trata-

---

[95] Elisabete CASTELA / Tiago Branco da COSTA, "A investigação clínica na era do altruísmo dos dados", 271.

mento de saúde ou de ação social ou a gestão de sistema e serviços de saúde ou de acção social; o tratamento é necessário por motivos de interesse público no domínio da saúde pública; se o tratamento é necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórico, ou para fins estatísticos[96].

No caso específico do sector público, a finalidade do tratamento de dados deve estar relacionada com a execução de políticas públicas de saúde e o cumprimento de obrigações legais ou regulatórias. Nestas duas situações, o consentimento do titular de dados é dispensado; no entanto, em hipóteses específicas, o consentimento do titular pode ser necessário para determinadas finalidades (por exemplo, apesar de a insuficiência renal ser um problema de saúde pública, ser *doador* requer o consentimento do mesmo para o tratamento dos seus dados pessoais).

3.7 Suporte da prestação do consentimento

O art. 5º al. *a),* onde consta a definição legal de consentimento, dispõe que a sua prestação deva ser feita "(…) independentemente do suporte, no qual o titular dos dados autoriza o seu tratamento". Parece que o legislador está a indicar um suporte físico ou digital, onde o titular pode deixar expressa a manifestação de vontade, escrita ou oral, sendo importante que no suporte transpareça o modo inequívoco do consentimento. O critério para aferir da inequivocidade da manifestação é o do declaratário normal, conforme art. 236º do CC. Contrariamente ao que ocorre com a regra geral, aqui o silêncio não produz qualquer efeito jurídico[97].

---

[96] A enumeração feita foi realizada com base na sistemática do artigo 6.º do RGPD.

[97] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 184. No Direito europeu, o RGPD no seu Considerando 32 dispõe que

Não será assim se o consentimento visar tratamento médico, naquelas situações em que o doente entra para as urgências do hospital sem capacidade de comunicar-se, presumir-se-á que ele consentiu o tratamento. Nestas circunstâncias é também de admitir o consentimento presumido de o diagnóstico obtido através de meios tecnológicos servir para investigação clínica a favor do doente titular dos dados pessoais. Há, no entanto, que atender ao que dispõe o art. 14º, nº 1, al. *a)*. Diz este preceito que o tratamento de dados pessoais referentes à saúde e à vida sexual, incluindo os dados genéticos, só pode ser efectuado verificadas as seguintes circunstâncias: "consentimento inequívoco, expresso e *escrito* do seu titular ou seu representante legal"[98]. Será que a determinação legal da forma escrita afasta a forma oral? Parece que para o tratamento de dados sensíveis, entre eles os relativos à saúde, vida privada e genéticos, obrigam à forma escrita, conforme a norma indicada supra, acrescentando o art. 13º, nº 1, al. *b)*, (i).

Questão duvidosa é a de saber se a manifestação oral do consentimento pode constar de um gravador. A escrita pode ser feita em papel físico ou de forma digital, devendo neste último seguir-se as regras de segurança legal e técnica. Há aqui um problema legal: Angola não tem aprovado regimes jurídicos para as plataformas digitais, para as assinaturas digitais e para validação de outros suportes electrónicos. Por outro lado, o formato onde assentar o consentimento deverá ser de fácil acesso e leitura.

"o silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento".

[98] Sublinhado nosso.

3.8 Revogação do consentimento

A LPDP não prevê a revogação do consentimento, contrariamente ao que dispõe o RGTP, no art. 7º, nº 3. Na CUACPDP, art. 13º, sobre os princípios de base que regem o processamento de dados pessoas, encontramos no primeiro princípio (Princípio de Consentimento e de Legitimidade do Processamento de Dados Pessoais) referência à revogação, mas pensamos ser erro de tradução, pois, tendo em conta a estrutura da referida norma, estabelece uma excepção ao consentimento[99]. No entanto, não podemos considerar que, no âmbito do consentimento para a recolha e tratamento de dados pessoais, excluídas as imposições legais, não funcione o princípio da autonomia da vontade. Sendo um princípio transversal ao nosso ordenamento jurídico, é de aceitar que a liberdade do titular dos dados possa revogar a declaração de consentimento prestada de modo informado, livre e esclarecido.

O regime jurídico da limitação voluntária dos direitos de personalidade que pode ser transponível para o sistema de protecção de dados pessoais encontra-se no art. 81º do CC, que constitui a excepção à regra

[99] Assim estabelece a norma: "O processamento de dados pessoais é considerado legítimo quando o titular dos dados der o seu consentimento. Todavia, este requisito pode ser revogado quando o processamento de dados for necessário para: *a)* cumprimento de uma obrigação legal à qual o controlador de dados se subordina; *b)* execução de uma missão de interesse público, no exercício de autoridade pública conferida ao controlador de dados ou a uma terceira parte, a que os dados serão submetidos; c) execução de um contrato no qual o titular dos dados é parte ou a fim de tomar medidas a pedido do titular dos dados, antes de celebrar um contrato; *d)* salvaguarda de interesses vitais ou dos direitos fundamentais e liberdades do titular dos dados". Como se pode verificar, o que está em causa é uma excepção no tratamento de dados sem a manifestação de consentimento e não uma revogação.

segunda a qual, nos negócios jurídicos, conforme o disposto no art. 406º do CC, deve imperar o mútuo consentimento como condição para a modificação ou extinção do contrato, com base no princípio *pacta sunt servanda*. Daí que o art. 81º CC disponha no nº 2 que "a limitação, quando legal, é sempre revogável, ainda que com obrigação de indemnizar os prejuízos causados às legítimas expectativas da outra parte". Ora, pelo tratamento indevido, o titular dos dados pessoais, considerado um direito de personalidade, tem o poder de fazer cessar, com eficácia *ex nunc*, o consentimento anteriormente prestado.

Num país como o nosso, em que a literacia sobre protecção de dados e evolução tecnológica é residual, o direito à revogação constitui um mecanismo de defesa para que, ocorrendo situações que ultrapassam o entendimento que o titular teve no momento de manifestar o consentimento, possa alterar ou retirar a autorização prestada[100].

3.9 Consentimento de incapazes

O consentimento informado a este nível é visto numa perspectiva da vontade, pois corresponde ao reconhecimento da autodeterminação da pessoa, que entretanto está em estado de incapacidade. É um claro problema de vulnerabilidade que o direito deve atender, pois diz respeito à protecção dos mais fracos no exercício da autonomia de uma franja de titulares de dados pessoais[101]. O fundamento

---

[100] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 188.

[101] António Menezes CORDEIRO, "Vulnerabilidades e Direito Civil", 21-58. Entende o autor que "a tutela da parte fraca ou do sujeito vulnerável preenche, na atualidade, numerosas intervenções, em artigos especializados e em manuais". Por isso, ao indicarmos o mestre de Lisboa foi exactamente no sentido de enquadrarmos o tema da vulnerabilidade conforme os seus ensinamentos. O artigo que estamos citando é abrangente do Direito Civil, de uma forma geral.

do consentimento está alicerçado no respeito pela liberdade, autonomia e autodeterminação do titular dos dados pessoais. Como já referido, a manifestação de consentir deve ser livre e informada, e tal só se alcança com o exercício da autonomia, que para além da liberdade e da independência, exige outro campo de capacidades, designadamente a compreensão das questões envolventes no tratamento dos seus dados, capacidade de julgamento dos riscos envolventes e das possíveis consequências no plano material e jurídico, e de gestão da informação que o responsável pelo tratamento lhe tenha transmitido[102].

A LPDP não contém um regime específico para o consentimento de incapazes. Encontramos nela algumas indicações: no art. 13º, nº 1, al. *b)* (i), ao referir "(…) seu representante legal"; (ii) "(…) e o titular dos dados estiver física ou legalmente incapaz de dar o seu consentimento"; art. 14º, nº 1, al. a) "(…) seu representante legal"; art. 26º, nº 7 "(…) representante legítimo"; art. 29º, "(…) direito de representação". Quando o legislador faz referência a representante legal, o que quer dizer? Não havendo no sistema tutelar de protecção de dados pessoais um regime próprio sobre a matéria, vamos apelar ao regime geral de incapacidade para deixarmos o nosso entendimento, começando pela situação dos menores, passando depois a outras incapacidades.

A Convenção Africana sobre a matéria destaca no art. 14º os princípios específicos relativos ao processamento de dados sensíveis, proibindo, no nº 1, "qualquer recolha e processamento de dados que revelem a origem racial, étnica ou regional, filiação, ideologia, política, crenças religiosas ou convicções filosóficas, filiação sindical, vida sexual, informação genética ou, de uma forma geral, as infor-

---

[102] Joaquim PINHEIRO, "A autonomia na pessoa com doença crónica", *Revista Portuguesa de Bioética* 9 (2009) 291-305.

mações relativas ao estado de saúde do titular dos dados". O nº 2 determina que a proibição constante do nº 1, "não se aplica para as categorias de processamento que se seguem, quando: (…), *c)* o processamento de dados pessoais for necessário para proteger os interesses vitais do titular dos dados ou *de uma outra pessoa, se o sujeito titular dos dados estiver física ou juridicamente incapacitado para dar o seu consentimento*"[103]. Este preceito é estranho à forma como a nossa ordem jurídica trata a incapacidade de exercício de direitos. Será que o legislador da União Africana quis encontrar uma diferenciação entre incapacidade física e incapacidade jurídica usando como critério uma decisão judicial? Possivelmente, a incapacidade física seria a resultante, por exemplo, de situações de doença em que o sujeito se encontra fisicamente impossibilitado de falar, ouvir e entender, ou quando se encontre completamente imobilizado. Já a incapacidade jurídica seria aquela resultante de decisão do órgão competente para declarar, que no caso de Angola seria o juiz.

3.9.1 Menores

O Código Civil dispõe no art. 122º que menor é aquele que ainda não completou dezoito anos de idade, não sendo, em consequência, sujeito com capacidade de exercício de direitos – art. 123º CC. Não significa que o menor não tenha personalidade ou capacidade de gozo de direito; está-lhe é vedada a capacidade de agir de forma autónoma. Sendo assim, como pode ser suprimida esta incapacidade? Determina o art. 124º CC que a forma de suprimento da incapacidade de exercício do menor é a representação legal. Significa que deve haver um terceiro que actua em nome do menor, repercutindo na sua esfera jurídica os actos praticados pelo representante. Mas é

[103] Itálico nosso.

bom observar que há actos que o menor pode praticar, e são legalmente três. Dispõe para o efeito o art. 127º CC, no nº 1, que *(i)* são válidos os actos de administração ou disposição de bens que o maior de dezasseis anos haja adquirido por seu trabalho; *(ii)* os negócios jurídicos próprios da vida corrente do menor que, estando ao alcance da sua capacidade natural, só implicam despesas ou disposições de bens de pequena importância; *(iii)* os negócios jurídicos relativos à profissão, arte ou ofício que o menor tenha sido autorizado a exercer, ou os praticados no exercício dessa profissão, arte ou ofício.

Temos de observar que há uma tendência progressiva de maioridade emancipativa (casos excepcionais de capacidade do menor), conforme dispõe o art. 132º CC. Este processo de autonomização da actuação dos menores pode ser encontrado noutras áreas do direito, como no Código Penal, que no art. 34º, nº 3, determina que o consentimento pode ser prestado por menor de 16 anos, desde que "tenham discernimento para avaliar o sentido e alcance do acto no momento em que é prestado o consentimento"[104]. Neste mesmo sentido, o Código da Família, no nº 2 do art. 24º abre uma excepção à idade núbil para o casamento. Diz assim o preceito: "Excepcionalmente, poderá ser autorizado a casar o homem que tenha completado 16 anos e a mulher que tenha completado 15 anos, quando ponderadas as circunstâncias do caso e tendo em conta o interesse dos menores, seja o casamento a melhor solução"[105]. Esta tendência

---

[104] Paula Távora VÍTOR, "Os dados de saúde de crianças e jovens: capacidade e competência decisória", *Revista de Centro de Estudos Judiciários* 2 (2023) 109-127.

[105] Este preceito tem uma história muito particular: em plena guerra, havia muitos soldados-criança que naqueles ambientes se tornaram pais. As opções em termos de política pública foram no sentido de proteger os filhos, evitando que se transformassem em filhos sem pais. O legislador seguiu-lhe o caminho. De outro lado, a grande maioria dos povos que constituem a diversidade cultural e étnico-linguístico de Angola, consagram como normal o casamento de menores, princi-

é compreensível se agregarmos o facto de se defender cada vez mais uma ideia de "desenvolvimento acelerado da adolescência" ou da "capacidade evolutiva e da maioridade antecipada"[106], mas que deve ser tomada com cautela, devendo assegurar que o menor compreendeu a finalidade do tratamento e o tipo de dados a ser processado, defendendo-se, assim, um consentimento informado do menor como um processo contínuo.

Pela natureza do consentimento em matéria de tratamento de dados pessoais, tendo em consideração que a *maturidade* do incapaz deve ser *vigiada,* pois é frágil a sua consciência sobre os riscos inerentes a toda a temática sobre protecção de dados. Por isso, não é um dado consagrado que o menor considerado maturo tenha completa liberdade para manifestar o seu consentimento, devendo, ainda que *a posteriori*, o seu representante legal ter conhecimento.

Sobre o assunto, o RGPD, no art. 8º, estabeleceu o regime específico para o consentimento dos menores[107]. Esta norma regula o consentimento de menores relativamente à oferta de serviços da sociedade da informação, por isso de âmbito muito limitado, sendo legítimo discutir se relativamente aos dados sensíveis de saúde dos menores a RGPD não teve esta preocupação[108]. Determina o artigo em questão que, se a criança tiver pelo menos 16 anos de idade, o

palmente adolescentes. É até aos nossos dias um fenómeno que existe, mas que as famílias encobrem. No sudeste de Angola têm ocorrido conflitos, entre as autoridades tradicionais e as autoridades judiciárias e judiciais, quando uma menor é engravidada e é protegida pela família através da realização do casamento tradicional.

[106] Paula Távora VÍTOR, "Os dados de saúde de crianças e jovens", 114.

[107] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 191.

[108] Inês Camarinha LOPES, *Os Dados Sensíveis dos Menores à Luz do RGPD*, 103. A autora refere nos méritos e as insuficiências do art. 8º da RGPD.

tratamento de dados é lícito. No caso de o menor ter menos de 16 anos de idade, "o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança"[109].

Importa dar nota da Recomendação nº 3/2022, do Conselho Nacional de Ética para as Ciências da Vida de Portugal, que trata do *Processo de Consentimento Informado em Menores de Idade: Requisitos Ético-jurídicos*. Relata que "o consentimento informado no caso dos menores de idade assume particular complexidade por ser prestado por terceiros, os titulares das responsabilidades parentais, regra geral os progenitores ou, na sua ausência ou impedimento, um tutor designado pelo tribunal. Não obstante, e tal como afirma a Convenção sobre os Direitos Humanos e a Biomedicina (nº 2 do artigo 6º), 'a opinião do menor é tomada em consideração como um factor cada vez mais determinante, em função da sua idade e do seu grau de maturidade'"[110]. Há aqui uma combinação entre a autoridade res-

---

[109] O Considerando da RGPD dispõe que "As crianças merecem protecção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências dos dados pessoais. Essa protecção específica deverá aplicar-se, nomeadamente, à utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidades ou de utilizador, bem como à recolha de dados pessoais em relação às crianças aquando da utilização de serviços disponibilizados directamente às crianças. O consentimento do titular das responsabilidades parentais não deverá ser necessário no contexto de serviços preventivos ou de aconselhamento oferecidos directamente e uma criança".

[110] Veja-se em <ww.cnecv.pt/deliberações/recomendações-sobre-processo--de-consentimento-informado-em-menores>, consultado a 15 de Novembro de 2024. A Recomendação em causa informa que "no contexto da tomada de decisões de saúde relativas a menores de idade, encontra-se hoje legalmente estabelecido que: *a)* as intervenções em menores carecem de consentimento informado, sendo este, em regra, exercido pelos representantes legais, normalmente os progenitores ou, na ausência ou impedimento destes, por um tutor designado pelo

ponsável pela representação do menor e um processo de audição do menor, tendo em atenção o seu nível de compreensão da informação que influencia a tomada de decisão com autonomia sobre a gestão dos seus interesses. É, novamente, a consagração da valoração do consentimento como manifestação da vontade individual, ou dito melhor,

---

tribunal; *b)* o menor de idade, em função da sua capacidade de discernimento e decisão deve também ser informado, de forma adequada ao seu nível de compreensão, e ter a oportunidade para expressar a sua opinião; *c)* o Código Penal prevê que o consentimento informado para a realização de intervenções ou actos médico-cirúrgicos seja eficaz quando prestado pelo menor a partir dos 16 anos de idade, que possua em concreto o discernimento necessário para avaliar o sentido e alcance da sua decisão. Abaixo deste limiar etário, ou caso não se comprove o grau de compreensão necessário, o consentimento dos representantes legais mantém-se como requisito obrigatório; *d)* excepções à exigência de obtenção de consentimento informado por parte dos representantes legais nas condições descritas no ponto anterior estão previstas na lei, verificando-se nas situações de doação e transplante de órgãos (o menor não pode consentir directamente ser dador, mas pode vetar, o mesmo se verificando relativamente à sua participação em estudos de investigação, em contexto de patologia mental (a idade mínima de consentimento são os 14 anos) e de recusa por objecção religiosa, por exemplo transfusão sanguínea (16 anos, comprovado o discernimento) e de interrupção voluntária da gravidez (IVG) (em que a idade mínima de consentimento são os 16 anos, sem outras condições). Particularmente na área da saúde sexual e reprodutiva ou noutras áreas de forte intimidade do adolescente e que não impliquem risco para a vida ou para a saúde do menor, deve também ser respeitada a relação terapêutica directa entre o profissional de saúde e o adolescente, com a devida privacidade e confidencialidade (educação sexual/planeamento familiar: jovens em idade fértil, sem limite de idade); *e)* no caso de investigação clínica, no âmbito dos benefícios esperados relativamente ao próprio, a legislação exige que um estudo clínico só possa ser realizado em menores quando, cumulativamente, for obtido o consentimento informado do menor com idade igual ou superior a 16 anos e do seu representante legal. No caso de o menor ter idade inferior à referida, o consentimento informado deve ser prestado pelos representantes legais, o qual deve refletir a vontade presumível do menor, podendo, em ambos os casos, o consentimento ser revogado a todo tempo, sem prejuízo para o menor".

como manifestação de concordância ou discordância do titular dos dados em relação ao posicionamento do seu representante legal[111].

3.9.2 Outros incapazes

Os sujeitos com incapacidade física ou mental têm um regime diferente do anunciado supra. Estamos a referir as pessoas doentes num estado em que não conseguem falar, ouvir ou entender, e as situações de inabilitação e de interdição[112]. Uma grande e primeira nota diz respeito ao facto de que, no primeiro caso, dispensa-se intervenção judicial; a segunda e terceira situação são decretadas por decisão judicativa.

O art. 138º, nº 1 CC dispõe que "podem ser interditos do exercício dos seus direitos todos aqueles que por anomalia psíquica, surdez-mudez ou cegueira se mostrem incapazes de governar suas pessoas e bens". Já o art. 152º CC determina que "podem ser inabilitados os indivíduos cuja anomalia psíquica, surdez-mudez ou cegueira, embora de carácter permanente, não seja de tal modo grave que justifique a sua interdição, assim como aqueles que, pela sua habitual prodigalida-

---

[111] Álvaro da Cunha Gomes RODRIGUES, "Consentimento Informado – Pedra Angular da Responsabilidade Criminal Médico", in *Direito da Medicina*, I, Centro de Direito Biomédico / UC, 2002, 5-52.

[112] Há que ter em consideração que, quando o titular dos dados é um doente, pode ter a sua liberdade ameaçada ou diminuída. "Perante situações de sofrimento físico, nomeadamente dor, por limitações cognitivas causadas por doença mental orgânica ou psiquiátrica, por medo e sensação de inferioridade provocada pela doença", podem mesmo anular a sua liberdade e, em consequência, resultar difícil manifestar o seu consentimento para recolha e tratamentos dos seus dados de saúde. Cfr. António SARMENTO, "Quando o doente está privado de liberdade", in *A Relação Médico-Doente, Um contributo da Ordem dos Médicos*, Lisboa: By the Book, 2019, 505.

de ou pelo uso de bebidas alcoólicas ou de estupefacientes, se mostrem incapazes de reger convenientemente o seu património". Vamos dispensar as "disputas" doutrinais sobre o entendimento do que deveria ser o conteúdo axiológico-normativo e até o sentido teleológico dos dois institutos[113], para nos fixarmos na lei, até porque o importante é considerar que os preceitos em causa são manifestação do princípio geral do direito de protecção dos mais fracos, dos vulneráveis ou dependentes, que é consequência da ideia de solidariedade humana[114]. Há, nos dois casos, uma limitação da liberdade apertando a capacidade de agir dos incapazes. Dado que a liberdade pressupõe renúncias, decisões e liberdades, não se pode deixar que a alguém com declarada inabilidade e interdição seja dada completa autonomia para consentir sobre a recolha, tratamento e armazenamento dos seus dados pessoais.

Nas situações em que há doente em estado de coma, que sofreu um acidente e entre para as urgências sem poder comunicar com

---

[113] Por exemplo, António Menezes CORDEIRO, entende que a surdez-mudez e a cegueira não deveriam conduzir à interdição e, pelo contrário, o consumo excessivo de bebidas alcoólicas e de estupefacientes poderiam, quando conduzissem à incapacidade de gerir a sua pessoa e o seu património, ser causa de interdição. *Tratado de Direito Civil Português,* I, Parte Geral, Tomo III, Coimbra: Almedina, 2004, 419 seg.

[114] Gabriela Páris FERNANDES, *Comentário ao Código Civil, Parte Geral*, Coord. Luís Carvalho FERNANDES / José Brandão PROENÇA, Faculdade de Direito: Universidade Católico Editora, 2014, 294-335. A autora entende que "os regimes da interdição (artigos 138 a 151 do CC) e da inabilitação (artigos 152 a 156 do CC) visam a proteção de quem, maior de idade, e conforme o caso, seja incapaz de reger a sua pessoa e bens ou inábil para reger os seus interesses. Legitimam-se no princípio constitucional e civil da proteção dos mais fracos, vulneráveis ou dependentes, que decorre da ideia de solidariedade humanas (cfr. artigos 63º, 64º, 71º e 72º da CRP) e as restrições aos direitos fundamentais à capacidade civil e ao desenvolvimento da personalidade que deles decorrem são admitidas nos termos do nº 4 do artigo 26º e do nº 1 do artigo 71º da CRP".

os profissionais de saúde, para além das situações de presunções de consentimento, haverá outras em que estão presentes representantes legais ou outros familiares. Estes poderão, em nome e no melhor interesse do incapaz, prestar o consentimento.

Nos casos de interdição e inabilitação, as situações são diferentes. As "deficiências físicas e mentais, e os hábitos de vida", como diz Luis A. Carvalho Fernandes[115], introduzem perturbações na capacidade cognitiva das pessoas, o que leva a que o indivíduo possa encontrar-se numa situação de incapacidade de gerir as situações do seu interesse. No primeiro caso, pensamos que é de atender apenas à anomalia psíquica, pois não nos parece para o caso relevante a deficiência física que não afecta a sua capacidade intelectual. Já a surdez-mudez e a cegueira não justificam a convocação do representante legal para ser ele a autorizar o tratamento de dados. Há hoje, e muito desenvolvidas, técnicas de comunicação que resolvem completamente as dificuldades para a comunicação de forma natural, por exemplo a linguagem gestual. A mesma situação se coloca com a cegueira: a leitura em *Braille* (que é um sistema de escrita táctil usado por pessoas cegas ou com baixa visão) é uma técnica em que os cegos conseguem ler perfeitamente, acrescendo o facto de que podem receber toda a informação sobre a finalidade do tratamento através da comunicação oral. Quanto à inabilitação, em alguns casos o regime da interdição pode ser aplicável à incapacidade de ordem física ou psíquica; já quanto à prodigalidade, alcoolismo e toxicomania, há um regime específico. Se enquadrarmos a incapacidade física e psíquica num contexto de saúde (doença) e vida sexual, bem como dados genéticos, estaremos perante o tratamento de dados sensíveis.

---

[115] *Teoria Geral do Direito Civil*, I, 5.ª ed., revista e actualizada, Lisboa: Universidade Católica Editora, 2009, 332.

Há duas situações sobre as quais recaem os efeitos da inabilitação: na capacidade de gozo e na capacidade de exercício e, em particular, nos actos de administração. É esta última incapacidade que nos interessa, se atendermos ao que dispõe o art. 153º, nº 1, última parte: para além dos actos de disposição, o juiz pode determinar a intervenção de assistente em "todos os [actos] que, em atenção às circunstâncias de cada caso, forem especificados na sentença". Por isso, a inabilitação é decretada por decisão judicial. A intervenção do representante legal ocorre porque ao inabilitado está vedado praticar actos equivalentes a actos de disposição, onde toma decisões, avaliando situações para fazer escolhas, cabendo aqui a capacidade de exercício[116].

Como se sabe, a inabilitação não tem um regime fixo, cabendo sempre ao juiz determinar quais os actos que estão vedados ao sujeito inabilitado. Assim, se no campo dos "actos proibidos" couber a prestação de consentimento para a recolha, registo e tratamento de dados pessoais, será convocado o representante legal (art. 153, nº 1, 154º CC *ex vi*, art. 954º CPC).

As situações do chamado analfabetismo funcional, que é a incapacidade que a pessoa apresenta em não compreender textos simples, também influi na liberdade de consentir[117]. Em pior situação estão,

---

[116] Luís A. Carvalho FERNANDES, *Teoria Geral do Direito Civil*, I, 354. O autor entende que "a expressão [referida na segunda parte do nº 1 do art. 153º] é suficientemente ampla para contemplar direitos não patrimoniais, se o juiz assim o considerar conveniente, em face do tipo e grau de gravidade da causa de que o inabilitado se mostra afectado". Ponderada a situação, o juiz avaliará da necessidade de se socorrer do representante legal ou de deixar que o inabilitado, por si mesmo, decida consentir na recolha e tratamento dos seus dados de saúde.

[117] Vera Masagão RIBEIRO, "Alfabetismo funcional: Referências conceituais e metodologia para a pesquisa", *Revista de Educação & Sociedade*, Pontifica Universidade Católica de São Paulo, 18/60 (1997) 144-158. Informa a autora que "o termo alfabetismo funcional foi cunhado nos Estados Unidos na década de 1930 e utiliza-

como é natural, o analfabeto absoluto, que nem sequer sabe ler e escrever. No analfabetismo funcional há alguma capacidade de ler, mas as pessoas com estas dificuldades, mesmo que apresentem capacidade para descodificar minimamente as letras, compreender textos simples e curtos, bem como números, não desenvolvem habilidades para interpretar os referidos textos e realizar operações matemáticas com os respectivos números. As dificuldades do uso da leitura e da escrita diminuem as habilidades de compreensão da pessoa, ou seja, os problemas com o "domínio pleno e versátil da leitura e da escrita ou um nível de habilidades restrito às tarefas mais rudimentares referentes"[118] para a interpretação de um conjunto de informação que circula à nossa volta, pode conduzir o titular de dados a uma situação de incapacidade para o exercício de direitos. Este é o ponto relacionado com o direito à autodeterminação informacional e da autonomia sem o qual é difícil falar-se de consentimento. Quem está com deficiente grau de habilidades relativas à sua capacidade de compreensão da informação que lhe é colocada para tomar a decisão que esteja em linha com os seus direitos e interesses terá também dificuldades no campo do consentimento, pois consentir pressupõe que o seu autor tenha a noção de que uma parte da sua esfera pessoal

---

do pelo exército norte-americano durante a Segunda Guerra, indicando a capacidade de entender instruções escritas necessárias para a realização de tarefas militares". Mais adiante afirma que, "em alguns casos, o termo analfabetismo funcional foi utilizado também para designar um meio termo entre o analfabetismo absoluto e do domínio pleno e versátil da leitura e da escrita ou um nível de habilidades restrito às tarefas mais rudimentares referentes à «sobrevivência» nas sociedades industriais. Há ainda um conjunto de fenómenos relacionados que podem ser associados ao termo analfabetismo funcional, por exemplo, o analfabetismo de regressão, que caracterizaria grupos que, tendo alguma vez aprendido a ler e escrever, devido ao não uso dessas habilidades, retornam à condição de analfabetos".

[118] Vera Masagão RIBEIRO, "Alfabetismo funcional: Referências conceituais e metodologia para a pesquisa", 145.

está a ser cedida, e a noção da finalidade para a qual o faz.

Para que o titular de dados possa manifestar o seu consentimento de forma livre e informada, o dever do responsável pelo tratamento a prestar informação tem de ser operacionalizado. No tocante às dificuldades relacionados com o analfabetismo funcional, a garantia de um consentimento informado e esclarecido pressupõe, conforme Eduardo Dantas[119], que a informação seja levada ao titular dos dados com "linguagem simples" (evitar linguagem carregada de terminologia técnica), "apresentação gradual", apresentando a informação de forma faseada, "começando pelo básico e avançando pelos detalhes", a possibilidade de fazer recurso a meios visuais, como "diagramas, modelos, gráficos ou ilustrações" que não piorem as dificuldades do titular dos dados que já sofre das consequências do analfabetismo funcional; o "ensino de retorno", que consiste no processo em que, depois de fornecer uma informação, se pede ao titular dos dados que "explique com suas próprias palavras o que ele entendeu". Por fim, o "suporte de terceiros" quando, com a anuência do titular dos dados, se possa incluir uma pessoa próxima a si nas conversas informativas para "ajudar na compreensão e retenção da informação".

---

[119] "Dilemas Bioéticos na Literacia em Saúde: Consentimento Informado, o Exercício da Autonomia e o Analfabetismo Funcional", *Lex Medicinae: Revista Portuguesa de Direito da Saúde* 21/4 (2024) 41-55.

4. TITULARIDADE DOS DADOS PESSOAIS EM SAÚDE

Os dados pessoais de saúde são as informações relativas à vida de cada pessoa ao longo de todo o ciclo de vida, as quais geralmente se encontram registadas nas organizações de saúde (hospitais, clínicas, laboratórios para análises clínicas, para ensaios clínicos, etc.) onde a pessoa nasceu, beneficiou de assistência médica e morreu. Mas os dados de saúde podem também ser encontrados nos registos fora do sistema de saúde, como por exemplo nos estabelecimentos de pessoas idosas, nas creches, nas empresas, nos estabelecimentos prisionais, nas equipas desportivas e noutras instituições.

O titular dos dados é a pessoa singular identificada ou identificável, portador da informação objecto de tratamento. É considerada "identificável a pessoa que possa ser identificada directa ou indirectamente, designadamente por preferência a um número de identificação ou à combinação de elementos específicos da sua identidade física, fisiológica, pesquisa, económica, cultural ou social" (art. 5º, al. *b)* da LPDP). Esta referência legal é também encontrada da CUACPDP, no art. 1º (Definições). O RGPD, no art. 4º, nº 1, igualmente estabelece esta conceituação, acrescentando alguns elementos de identificação, nomeadamente o "nome", "dados de localização" e "identificadores por via electrónica". Observe-se que a norma europeia indica a referência a um identificador como exemplo, e não como elementos taxativos. Pensamos que devemos realizar uma leitura do art. 5º, al. *b)* da LPDP com sentido meramente exemplificativo, evitando que, se falharem as referências legais, se

possam encontrar outras referências susceptíveis de identificar uma determinada e concreta pessoa singular.

Em saúde, incluindo a vida sexual e os dados genéticos, por serem dados sensíveis, o tratamento dos dados obedece a imposição legal de determinados requisitos específicos (art. 14º, nº 1, al. *a)*) exigindo-se por isso o consentimento inequívoco, expresso e escrito do seu titular ou do seu representante legal; e/ou *b)* a autorização da APD, garantindo-se duas situações: a legitimidade para o responsável realizar o tratamento de dados, e autorização do titular para que o responsável invada a sua esfera de privacidade.

O tratamento de dados referido tem uma excepção, conforme o nº 2 do art. 14º: é permitido sem o consentimento do titular dos dados, quando for necessário para efeitos de medicina preventiva, de diagnóstico médico, de assistência médica consentida, de gestão e estatística de serviços de saúde, ou quando se trate de emergência médica ou justificada pelo interesse público.

Nos termos do nº 3 do artigo acima referido, "o tratamento de dados da saúde e de vida sexual deve ser efectuado por um profissional de saúde com registo na ordem profissional correspondente, obrigado a cumprir o dever de sigilo profissional".

Como se sabe, os estabelecimentos hospitalares, enquanto processo interno de organização, constituem um processo clínico de cada paciente onde consta toda a informação da sua situação, designadamente os dados de identificação, dados genéticos, disgnósticos, doenças, exames realizados e tratamento a realizar ou que está em vias de realização.

Outra questão importante diz respeito à transferência internacional de dados, mais concretamente quando são dirigidos para países que não asseguram um nível de protecção adequado (art. 34º). Nestes casos, a transferência deve estar sujeita a autorização da APD, a qual só pode ser concedida se verificada uma das seguintes circunstâncias ou outras constantes de legislação específica (nº 1, al. g)): "se a transferência de dados for necessária para proteger os interesses

vitais do titular dos dados, ou para prevenção, diagnóstico ou tratamento médico e o titular estiver física ou legalmente incapaz de dar o seu consentimento".

O titular dos dados pessoais está presente em toda a relação jurídica de tratamento de dados, sendo a peça central. Como titular de dados (do conjunto de informações sobre o seu estado físico e mental, incluindo as informações genéticas), é sujeito de uma relação jurídica, logo, investido de um poder jurídico que o sistema de protecção de dados pessoais lhe reconhece para que de forma livre exija ou pretenda que o responsável (subcontratado, destinatário ou terceiro) adopte um comportamento positivo (acção) (cumprimento da lei, designadamente o reconhecimento dos direitos do titular, o cumprimento dos princípios gerais sobre tratamento de dados, cumprimento dos requisitos para o tratamento e transferência dos dados, medidas de segurança e organizativas), ou negativo (omissão) (abster-se de realizar tratamento indevido), ou por meio de um acto autónomo, só por si (revogação do consentimento, direito de rectificação, actualização ou eliminação) ou integrado por um acto de autoridade pública (poder da APD para "apreciar e decidir sobre as reclamações que lhe sejam dirigidas e garantir o exercício do direito de acesso, de rectificação, actualização e cancelamento de dados" (art. 44º, nº 1, al. *e)*), produzindo efeitos jurídicos queridos que, inelutavelmente, se venham a impor sobre o responsável[120].

---

[120] Leia-se Luís A. Carvalho FERNANDES, *Teoria Geral do Direito Civil*, I, 126, que aborda a posição das pessoas na relação jurídica, afirmando que "enquanto realidade intersubjectiva, a relação jurídica desenvolveu-se entre duas ou mais pessoas que nela ocupam posições diferentes. Numa análise puramente esquemática, uma dessas pessoas surge numa posição dominante e, *qua tale*, como titular de direitos subjectivos; em contrapartida, outra encontra-se adstrita às vinculações correspondentes. Reportando-se a esta análise, a doutrina clássica distingue o *lado* (ou sujeito) activo do *lado* (ou sujeito) passivo da relação jurídica.

A par do responsável pelo tratamento dos dados (e do subcontratado) e destinatário, o titular dos respectivos dados é um dos sujeitos da relação que se estabelece com o tratamento dos dados. Quer dizer, o titular dos dados é a pessoa singular com capacidade de adquirir direito e assumir obrigações através da sua participação no tráfico jurídico (relação jurídica), alicerçada no princípio da autonomia da vontade[121].

(…) Desde logo, a relação jurídica desenvolve-se, em concreto, em múltiplas situações jurídicas, da mais diversa natureza. Se, pelo que respeita ao lado passivo, a expressão *vinculação*, tomada num sentido muito amplo, poderia aspirar a cobrir essa diversidade, já quanto ao activo o mesmo não poderia pretender o *direito* (*subjectivo*) sem violentar gravemente o sentido técnico-jurídico deste conceito; ao lado deste, tem de se atender a outras posições activas, como direitos potestativos, poderes-deveres. Por isso, em termos genéricos, é mais adequado contrapor *poderes jurídicos a vinculações*.

Mas, para além disso, cada uma das pessoas entre as quais a relação se estabelece surge correntemente (para não dizer sempre) como portadora, a um tempo, de poderes e vinculações, que se entrelaçam numa teia complexa; também esta realidade não pode ser ignorada".

[121] Heinrich Ewald HÖRSTER, *A Parte Geral do Código Civil Português*, *Teoria Geral do Direito Civil,* 4.ª reimpressão da edição de 1992, Coimbra: Almedina, 2007, 310. Explicita este Professor que "a participação no trafico jurídico, de acordo com o princípio da autonomia privada, pressupõe que as pessoas estão em condições de agir com base na sua vontade, pressupõe, portanto, que elas possuem o discernimento necessário para querer e entender os negócios que praticam bem como os efeitos pretendidos por eles. Apenas as pessoas nestas condições têm capacidade negocial para participar no tráfico jurídico e adquirir assim o gozo de direitos".

5. ALGUMAS ÁREAS EM SAÚDE ABRANGIDAS PELA PROTECÇÃO DE DADOS

Quando falamos em saúde não estaremos a referir-nos apenas ao estado pessoal. Em causa está o lado organizatório, estrutural e funcional. A recolha, processamento e armazenamento de dados pessoais de saúde podem ser encontrados nas mais diversas áreas, como as laboratoriais, clínicas, ortopédicas, cirúrgicas, de prevenção, enfim, uma larga zona que lida com dados pessoais e que é merecedora de protecção. O que pretendemos é apenas relevar as áreas que elegemos, porque não pretendemos elaborar um tratado de dados de saúde.

5.1 No estabelecimento hospitalar. O processo clínico

O reconhecimento generalizado de que é inevitável resultar do tratamento de dados pessoais na prestação de cuidados de saúde a imputação da correspondente responsabilidade decorrente da segurança da informação sensível, com as consequentes imposições de sigilo e segredo profissional[122]. A protecção dos dados pessoais sensíveis do paciente e a garantia do segredo dos profissionais de saúde encontram novos desafios quando confrontados com o direito

[122] Miguel LAGOUTE, "O processo clínico enquanto documento administrativo: da transparência à intrusão", *@publica*, CJP-CIDP / Faculdade de Direito da Universidade de Lisboa, 6/1 (2019) 102-122.

à autodeterminação e a autonomização da protecção de dados como direito fundamental. O processo clínico é um instrumento para mitigar os riscos decorrentes destes desafios.

O Código Deontológico e de Ética Médica estatui, no art. 43º, o "arquivo clínico". Assim determina o preceito, nº 1: "todo o médico deve ter obrigatoriamente, no seu gabinete, o registo de todos os pacientes observados, bem como o registo do diagnóstico aplicado e os resultados obtidos". O nº 2 determina que "o médico pode utilizar a informação existente no arquivo de registo dos seus pacientes observados no exercício da sua actividade para elaboração de seus trabalhos científicos, mas em hipótese alguma deve mencionar o nome ou qualquer detalhe que permita identificar a pessoa visada". Por fim, o nº 3 estatui que "os médicos devem conservar o arquivo de registo dos pacientes no mínimo até 15 anos, devendo neles respeitar-se sempre o segredo profissional, mesmo quando tenham que ser destruídos".

O mais antigo registo de informações de saúde relativo a pacientes foi, conforme notícia veiculada por ANDRÉ PEREIRA[123], num hospital na capital iraquiana Bagdad, datado dos séculos IX, X e XI, o que só vem demonstrar a necessidade de haver um dever de documentação dos médicos[124].

---

[123] "Dever de Documentação, Acesso ao Processo Clínico e sua Propriedade. Uma Perspetiva Europeia", *Revista Portuguesa de Danos Corporal* 15/16 (2006) 9-24.

[124] Rui Miguel Prista Patrício CASCÃO, "O dever de documentação do prestador de cuidados de saúde e a responsabilidade civil", *Lex Medicinae: Revista Portuguesa de Direito da Saúde* 4/4 (2007) 27-35. O autor entende que "um prestador de cuidados de saúde está vinculado a um dever de documentação relativo às vicissitudes do tratamento médico prestado". Mais adiante afirma que "em traços largos, a entidade prestadora de cuidados de saúde, bem como os profissionais de saúde e outros agentes envolvidos no processo, tem o dever de *criar*, *manter*, actualizar e *conservar* em arquivo ficheiros adequados relativos ao processo clínico do paciente".

Um dos primeiros actos hospitalares é o registo do paciente, dando-se início ao processo clínico. Na linguagem clínica, este primeiro acto é chamado de rastreio, serve para identificar, num primeiro momento, o estado (gravidade) do paciente; com efeito, o que não está registado não existe. Aqui se dá início à intervenção do médico, que fica também adstrito ao dever de "proceder à documentação e registo da actividade clínica"[125]. Também chamado de "diagnóstico principal", é aquele acto em que, depois do estudo do doente, é considerado responsável pela sua admissão no hospital para tratamento[126]. A recolha de dados dos doentes vai para lá do primeiro contacto; há outros dados, como a história pessoal e familiar, o seu s*tatus* profissional, para definir a continuidade de cuidados dentro ou fora do hospital (o que implica codificar um conjunto de informação a partir das seguintes perguntas: o que aconteceu? como? onde? quando? haverá outros factores envolvidos?).

---

[125] André Gonçalo Dias PEREIRA, "Dever de documentação, acesso ao processo clínico e sua propriedade", 9-24.

[126] George D. POZGAR*, Legal and Ethical Essentials of Health Care Administration*, 218. Este autor entende que "*Medical records provide pertinent information regarding the daily care and treatment of each patient. The medical record is the principal means of communication between healthcare professionals in matters relating to patient care. The medical record provide documentation of a patient's illness, symptoms, diagnosis, and treatment; serve as a planning tool for patient care; protects the legal interests of patients, healthcare organizations, and healthcare providers; provides a database for use in statistical reporting, continuing education, and research; and provides information necessary for third-party billing and regulatory agencies. The medical record is an essential tool in the delivery of quality patient care. Therefore, providers and healthcare organizations must strive to maintain the integrity and accuracy of records*".

O processo clínico é o documento que contém informações completas, precisas e organizadas sobre o paciente[127]. Tais informações estão registadas para servir de estudo e tratamento dos doentes, servem para que a prática clínica siga escrupulosamente conforme registado, é um instrumento de comunicação interpares, interprofissionais e é uma base de dados para investigação e formação. Com interesse público, o processo clínico serve para o relato e registo de serviços prestados, colheita de dados sobre movimento assistencial, colheita de dados sobre mortalidade, gestão dos vários serviços hospitalares, planeamento em saúde e garantia da qualidade.

A recolha de dados dos doentes deve ser feita registando, além da descrição *supra*, os problemas surgidos fora e dentro do hospital. Os problemas surgidos durante o internamento não são comuns, preferindo agrupá-los: complicações de cuidados médico/cirúrgicos; *misadventures* e *never events*, outros acidentes não relacionados com cuidados médicos (quedas, *v.g.*); reacções alérgicas, úlceras de decúbito, etc.

Da parte dos estabelecimentos hospitalares há o dever legal da existência de informação e documentação. A recolha de informação do paciente é um instrumento da maior importância para os profissionais de saúde. Os objectivos mais importantes para existência do

---

[127] Rui Miguel Prista Patrício CASCÃO, "O dever de documentação do prestador de cuidados de saúde e a responsabilidade civil", 28, enumera os dados que um processo clínico deve conter, nomeadamente *a)* a identificação do paciente, *b)* a memória da anamnese (entrevista prévia ao paciente), *c)* diagnóstico (incluindo resultados de análises, exames, imagens, etc.), *d)*estado de saúde do paciente à altura da admissão, *e)* evolução do seu estado de saúde, *f)* informação prestada ao paciente (bem como o meio através do qual essa informação foi prestada), *g)* registo do consentimento informado por parte do paciente, *h)* correspondência com outros profissionais de saúde relativa ao paciente, *i)* métodos terapêuticos utilizados, *j)* monitorização do paciente, *k)* fármacos, produtos e materiais empregues (e respectiva dosagem, lote, marca e outros elementos relevantes) e, *l)* prognóstico.

processo clínico, conforme ANDRÉ PEREIRA[128], são:

a) Melhorar os cuidados de saúde prestados ao doente;
b) Partilhar informação clínica entre os profissionais de saúde;
c) Diminuir o erro;
d) Melhorar a forma como a informação é obtida, registada e disponibilizada;
e) Garantir a mobilidade e acesso remoto;
f) Melhorar o suporte à decisão clínica;
g) Acesso fácil a standards terapêuticos; e,
h) A racionalização de recursos.

Outro elemento muito importante no processo clínico é a sua codificação. Ela serve, em primeira linha, para criação de uma Base de Dados Nacional. A sua utilização visa a caracterização de produção de medicamentos e outros materiais de saúde, gestão interna, cálculo de indicadores hospitalares locais regionais e nacionais, investigação académica/clínica, facturação e distribuição de recursos, planificação provincial e municipal para ajustamento do risco (identificar as complicações intra-hospitalares e reconhecer a infecção intra-hospitalar), e avaliação da qualidade. A codificação ainda serve para a implementação de programas de educação de saúde no geral, avaliar medidas seguras nas escolas e noutros estabelecimentos com frequência de muitas pessoas (possibilitar estudos epidemiológicos na área dos cuidados de saúde), identificar causas mais comuns de lesões evitáveis, adaptar programas de saúde pública a tendências de consumo e de utilização de novas tecnologias, avaliar os efeitos adversos de medicamentos e avaliar complicações e acidentes ocorridos

[128] *Direitos dos Pacientes e Responsabilidade Médica*, Coimbra: Coimbra Editora, 2015, 602.

em meio hospitalar.

Toda esta informação deve estar disponibilizada para o paciente que a prestou. O direito de acesso ao processo clínico pode ser considerado uma manifestação do constante no art. 26º da LPDP, que no nº 7 determina o direito de acesso do titular dos dados à informação sobre os dados de saúde e vida sexual, incluindo os dados genéticos.

Existe também o processo clínico electrónico. A digitalização dos serviços é uma realidade em desenvolvimento em Angola. Não é a questão da introdução da inteligência artificial. Com a digitalização, o processo clínico deixa de ser materializado, apresentando várias vantagens. Desde logo, a facilidade de acesso para as pessoas com autorização, facilitando o processo colaborativo entre os profissionais de saúde (e até entre hospitais, ou dentro do sistema nacional de saúde); gestão mais eficiente, pois possibilita o acesso de forma remota, e facilita o acesso aos dados para fins de consulta e investigação; por fim, quanto à segurança, em regra são usadas senhas para aceder ao processo. Os dados constantes do processo clínico electrónico são abrangidos na previsão do art. 29º da LPDP, designadamente a proibição de sujeitar qualquer pessoa a uma decisão automatizada que produza efeitos na sua esfera jurídica ou que a afecte de modo significativo. Ainda assim não deixa de haver problemas. O processo clínico traz consigo questões quanto à garantia de confidencialidade (daí atentados contra a privacidade e intimidade da vida privada), de integridade e segurança das informações que aí são guardadas (o desenvolvimento da actividade dos piratas informáticos, *hackers*, é uma crescente preocupação), que se confrontam com os elementos materiais da *lex artis* na relação médico-paciente.

5.2 Na telemedicina

O termo telemedicina tem a sua origem na palavra grega "tele", que significa distância, e está na base da formação de palavras como telefone, televisão, e outras. Assim, a telemedicina abrange a prática

médica realizada a distância, independentemente do instrumento utilizado para essa relação, sendo hoje massivamente utilizada através da internet[129]. Relembrando o que a história registou, com o avanço dos meios de comunicação, o contacto entre profissionais de saúde e paciente tornou-se simples e prático. A relação e a troca de informação foram ampliadas com o telefone fixo, depois com os telemóveis, e tornou-se ainda mais rápida com a internet. Os computadores, os tablets e os smartphones facilitam as videoconferências, e o avanço da inteligência artificial leva a informação ao alcance do todos. Hoje, até a realização de cirurgias a distância é uma realidade. Na verdade, a telemedicina faz parte de um conceito mais amplo, conhecido no mundo como *eHealth* ou 'saúde digital'. Conforme definição da *Health Information and Management Systems Society* – HIMSS, *eHealth* é qualquer aplicação da internet utilizada em conjunto com outras tecnologias de informação, com a finalidade de oferecer melhores condições aos processos clínicos, ao tratamento dos pacientes e melhores condições dos custos no Sistema Nacional de Saúde.

Segundo a *US Veterans Administration*, a telemedicina está sendo tratada como telesaúde pois inclui "o uso de informações electrónicas e de tecnologias de comunicação para fornecer e apoiar cuidados de saúde quando a distância separa os participante"; já o *Office for the Advancement of Telehealth, US Health Resources and Services Ad-*

---

[129] Veja-se, por exemplo, o estudo realizado por Jorge Maciel Silva RODRIGUES, "Sistema de Vídeo Vigilância Digital e Gestão Remota. Análise da sua aplicação à Telemedicina", dissertação de mestrado em instrumentação e microelectrónica – especialidade em instrumentalização e controlo industrial, da Faculdade de Ciências e de Tecnologia (Departamento de Física) da Universidade de Coimbra, 2006. Colocando em atenção a distância temporal desta dissertação, já que hoje houve uma evolução significativa de tecnologias ligadas à telemedicina, o trabalho do autor foi constituído "por servidores baseados numa arquitectura PC operado através de uma aplicação Windows, através de dispositivos móveis ou da Internet", IX.

ministration consiste no "uso de informações electrónicas e tecnologias de telecomunicações para dar suporte aos cuidados clínicos de saúde pública a longa distância, a educação relacionada à saúde para profissionais e pacientes, a saúde pública e administração de saúde".

Este conceito abarca outras dimensões que vão desde o envio de informações clínicas aos parceiros do sistema de atendimento, e facilita a interacção entre os seus membros, informação que pode chegar aos mais distantes e difíceis lugares. Tal desempenho é possível através da web, e por seu intermédio podemos indicar algumas ferramentas, designadamente o prontuário electrónico (*ePaciente*), saúde móvel (*mHealth*), *Big Data*, *Cloud Computing*, Medicina Personalizada, Telemedicina, etc.

Estão a ser utilizados com frequência equipamentos electrónicos para se fazer acompanhamento de doentes. O GPS Indoor é uma ferramenta utilizada no sentido de calcular as rotas e identificar localizações. Funciona por satélite e permite o seu funcionamento nos ambientes cobertos, como interiores de edifícios. A prática de geolocalização permite monitorar doentes, admitindo-se vantagens para doentes mentais, como doentes com Alzheimer, e foi muito utilizada na época da pandemia da Covid-19. A geolocalização traz consigo um premente problema da protecção dos dados pessoais, pois tal tecnologia além de registar os elementos de informação pessoal, também regista a doença da pessoa, e acompanha a sua locomoção[130].

A inteligência artificial tem sido um instrumento que vem favorecendo a actividade médica. O cruzamento de dados entre diferentes sistemas permite que os médicos tenham uma ampla (múltipla) visão do paciente que permite um conhecimento oportuno e

---

[130] Guilherme Pereira PINHEIRO / Alexandre Pereira PINHEIRO, "Covid-19 e geolocalização: entre a saúde e a proteção de dados pessoais", *Revista Jurídica da Presidência*, Brasília, 24/132 (2020) 245-268.

certo da sua situação de saúde. Este facto tem sido utilizado pelos estabelecimentos hospitalares públicos e privados, bem como pelo poder público, permitindo tomar decisões com vista ao combate de doenças e ao combate de endemias e pandemias, ou seja, enfrentar problemas que podem colocar em perigo a saúde pública.

A pandemia da Covid-19 (muitas vezes citada pelas respostas inovadoras que proporcionou aos operadores da saúde) levou a que pessoas, profissionais de saúde e pacientes passassem a usar com mais frequência a telemedicina, sendo a teleconsulta a mais frequentada. Por meio da telemedicina, os especialistas conseguem ter acesso a exames de qualquer lugar e à distância, sendo possível consultar os doentes sem a possibilidade de contágio. O exercício da telemedicina tem por suporte técnico infraestruturas e serviços de telecomunicações. Por isso, os cuidados com a protecção de informação pessoal que é transacionada merece a atenção de duas entidades: os profissionais de saúde e os operadores de comunicações electrónicas (tratamento dos dados de tráfego[131]).

A inteligência artificial tem sido utilizada na área da saúde de forma muito expansiva. Na área do tratamento dos dados, principalmente na autonomia e definição de prioridades médicas ou casos de urgências, tem sido utilizado computadores capazes de armazenar e processar um considerável volume de dados, tornando possível cruzar informações e imagens captadas de forma digital. Desta forma, é possível formar um processo histórico de doentes, que é arma-

[131] A Lei das Comunicações Electrónicas e dos Serviços da Sociedade da Informação, na al. *l),* art. 3º, dispõe sobre a definição de *dados de tráfego* como sendo "quaisquer dados tratados para efeitos de encaminhamento e do envio de uma comunicação através de uma rede de comunicações electrónicas e acessíveis ao público, relativos à duração, ao tempo, ao volume, protocolo usado e ao formato da comunicação ou para facturamento da mesma".

zenado digitalmente, facilitando aos médicos e aos pacientes uma compreensão dos diagnósticos, cada vez mais precisos.

Em Angola, o serviço de telemedicina não regista um crescimento digno de referência; aliás, a fraca expansão da internet dificulta o desenvolvimento da telemedicina, só havendo em pouquíssimas áreas serviços de teleconsulta. Este mecanismo é realizado entre médicos, quando um clínico geral, por exemplo, procura de um especialista uma informação sobre um disgnóstico, um medicamento mais adequado ou orientação sobre um determinado procedimento. Pode também ocorrer a consulta *online*, realizada directamente entre médico e paciente. Há também a teleassistência, centrada na comunicação com o doente e no seu bem-estar. É uma técnica próxima da geolocalização. Por este intermédio, o paciente é monitorado, no seu domicílio ou num centro de saúde, por um profissional de saúde que se comunica com outros profissionais a distância. No sentido de aumentar a eficácia e eficiência do sistema, e garantir uma investigação médica rigorosa, são utilizados diversos equipamentos que avaliam parâmetros clínicos e enviam dados, geralmente por internet, para os especialistas a distância. Dentro da vasta área da telemedicina encontramos também a emissão de atestados e/ou certificados a distância. Por meio da tecnologia existente, alguns exames podem ser realizados em qualquer lugar e certificados por especialistas conectados à internet. Desta forma é possível ter acesso fácil aos melhores médicos, dentro ou fora do país. Em resumo, a telemedicina abrange[132]:

a) Consultas e troca de informações entre instituições de saúde; reduzir transferências, tempo e custos de transporte de pacientes;

---

[132] É importante observar que o termo telesaúde vai para além da telemedicina, pois abrange os cuidados prestados por outros profissionais da área, como técnicos de diagnósticos, enfermeiros, nutricionistas, etc.

b) Informação de resultados de exames laboratoriais e de imagens;

c) Discussão de casos clínicos, principalmente relacionados com doenças raras ou contagiosas; intensificar a cooperação e integração de investigadores com partilha de registos clínicos;

d) Cirurgia robótica;

e) Assistência a pacientes crónicos, gestantes de alto risco e idosos; aprimorar a gestão dos recursos de saúde através da avaliação e triagem feita por especialistas, diminuindo a pressão sobre os hospitais;

f) A e-farmácia, que é o fornecimento de medicamentos através da farmácia digital.

Não deixam de estar associados riscos às vantagens que acabamos de referir. A primeira é a intervenção de várias entidades, sendo importante para tornar eficiente a telemedicina que cada uma das entidades intervenientes faça a sua recolha de dados ou, pelo menos, a partilha dos mesmos com outras entidades. A recolha de dados pessoais tem sido uma realidade, pois sem esse processo a telemedicina estaria votada ao fracasso. Concorrem para potenciar os riscos apontados a intervenção das empresas de seguros bem como o desenvolvimento da inteligência artificial na saúde. As seguradoras prestam serviços que obrigam a cruzar informação dos seus clientes entre diversos estabelecimentos hospitalares, colocando tais dados sob risco. Além disto, não é fácil estabelecer confiança entre paciente e profissionais de saúde pois, por natureza, as pessoas hesitam em confiar em alguém que não tiveram oportunidade de conhecer pessoalmente. Em algumas ocasiões o paciente entra em contacto com o médico de forma remota, depois de ter estado pessoalmente com ele num consultório; ainda assim, não é necessariamente suficiente para garantir que o profissional tenha conhecimento técnico e seja confiável. O risco está sempre presente, e por isso o tratamento

de dados deve seguir o disposto nas diversas leis referidas, acrescendo que se deve atender constantemente ao *dever de cuidado do profissional de saúde*, incluindo os termos das suas *leges artis*, para a protecção da privacidade e intimidade dos doentes.

A confidencialidade na telemedicina é semelhante à do sector da saúde no seu todo, tendo apenas algumas especificidades. Os médicos e outros profissionais no âmbito da telesaúde (*eSaúde*) devem agir em conformidade com as regras sobre como recolher, tratar, registar e compartilhar as informações dos doentes. Quando o doente está a ser consultado pelo médico através de videoconferência, este não deverá divulgar o que aconteceu naquela sessão, a menos que o paciente lhe tenha dado autorização.

A ciência e a tecnologia têm desenvolvido *software* para telemedicina, em que utilizam autenticação e criptografia de dados para manter as transmissões seguras (de forma mais ampla, será a implementação de políticas de segurança cibernética), assim se mitigando os riscos de segurança associados ao uso de um dispositivo móvel em ambiente menos controlado do que o consultório médico. Em suma, as ferramentas escolhidas para a telemedicina devem ter uma infraestrutura que permita comunicações seguras entre médicos e pacientes. Tais infraestruturas seguras devem permitir a comunicação remota sem reduzir a segurança que os dados confidenciais recebem. A CUACPDP estabelece que cada Estado Parte, no âmbito do seu sistema nacional de cibersegurança, promova "cultura de cibersegurança" e que sejam criadas estruturas nacionais de acompanhamento da cibersegurança com um quadro institucional definido e medidas de gestão da cibersegurança ("a gestão da cibersegurança deve ser criada dentro de um quadro nacional capaz de responder aos desafios actuais como a quaisquer questões relativas à segurança da informação ao nível nacional, no maior número possível das áreas das cibersegurança" – al. c), nº 1 do art. 27º). Já a lei nº 23/11, de 20 de Junho (LCESSI), estabelece no art. 44º a "segurança das redes e infraestruturas básicas", atribuindo ao Titular do Poder Exe-

cutivo a competência para "adoptar e aplicar as regras necessárias de forma a garantir a segurança, inviolabilidade e disponibilidade da rede básica e dos serviços suportados nesta, em particular em situações de catástrofes, calamidades ou guerras" (nº 1). O Direito é um ordenamento que oferece sempre uma solução para os problemas. O sistema jurídico é uma unidade, que não significa "algo" fechado; pelo contrário, e parafraseando MAFALDA MIRANDA BARBOSA[133], os conceitos de flexibilidade e permeabilidade, enquanto conceitos indeterminados oferecem, no tocante à permeabilidade, garantia de "abertura a novas realidades e a contaminação do regime com as marcas valorativas que se projectam nos vários princípios normativos chamados à colação para concretizar os conceitos em causa". Já a flexibilidade "viabiliza a adaptação das soluções a que se chega, tendo em conta não só as exigências de sentido comunicadas pelo fundamento axiológico da disciplina jurídica em questão, mas também as especificidades do caso concreto". Assim, toda a regulamentação que no âmbito alargado da segurança dos meios de comunicação electrónica protege os dados pessoais permite justamente aspirar à resolução do hipotética caso.

Os anunciados riscos existentes na telesaúde quanto à protecção de dados dos pacientes são abordados com dificuldade, pois em Angola não existem regras ou directrizes próprias de privacidade da telemedicina, que deveria fornecer um roteiro seguro para a teleconsulta, a e-farmácia, a telecirurgia, por exemplo, o que não significa uma completa lacuna nesta área, pois pode socorrer-se da legislação acabada de ser anunciada, que é mais geral.

É fácil constatar o potencial perigo que derivaria de um inadequado uso de informações processadas por meios digitais, as quais, quando

---

[133] "Conceitos Indeterminados e Flexibilização do Sistema: Considerações a Propósito da Negligência", *Revista de Direito da Responsabilidade* 5 (2023) 206-245.

indevidamente tratadas e cruzadas, podem permitir que um determinado serviço de saúde, de farmácia ou de seguro consiga elaborar perfis extremamente precisos sobre os seus usuários, que incluam dados da sua mais estrita intimidade, circunstância que poderia dar lugar ao início de acções discriminatórias camufladas, e a informação como poder deixa desprotegido o seu caracter de tópico para se converter numa tangível realidade[134].

Assim, perante a agressividade que os meios digitais possuem frente aos direitos das pessoas, algo mais preocupante numa tele-relação, o importante será estabelecer pontos de equilíbrio no âmbito do poder que o responsável (*controller*) utilizador dos meios digitais, principalmente da IA, possui para usá-los de forma que tais tecnologias sirvam também para facilitar a preservação e o respeito dos direitos e liberdades fundamentais dos doentes.

5.3 No medicamento e na farmacologia

Neste ponto, é preciso distinguir duas situações: uma diz respeito à participação voluntária em testes clínicos de medicamentos, e outra é relativa aos dados recolhidos pelas farmácias com acesso às prescrições médicas. Aqui, em particular, cabe, em princípio, anotar que com a emissão de facturas nas farmácias há a identificação do utente, os fármacos comprados e outros dados. Como sabemos, há hoje uma preocupação de cada vez mais as várias áreas da saúde estarem integradas, o que implica uma comunicação (electrónica) entre tais áreas. A privacidade e protecção de dados nas comunicações electrónicas, adverte SILVIA MENEZES de CARVALHO[135],

---

[134] J. LUJÁN ALCARAZ, *Uso y controle en la empresa de los médios informáticos de comunicación*, Aranzi Social, Tomo III, 2005, 55.

[135] *Manual de Direito das Comunicações Electrónicas: Mercado e Regulação*, 129.

"abarca, de igual modo, o tratamento dos dados dos" utentes de farmácias "para efeito da emissão da factura detalhada e identificação da" farmácia ou outro local de aquisição dos medicamentos, sendo que aos utentes "é atribuído o direito de receber a respectiva factura detalhada ou não detalhada" com as informações que o sistema das comunicações electrónicas registou e conservou, bem "como todos os pressupostos que a privacidade exige". Na verdade, as exigências de tutela da privacidade dos utentes de farmácias pela emissão de factura devem ser estendidas a todos os serviços de saúde; do pagamento decorre o dever por parte dos respectivos serviços da emissão de uma factura ou de um documento equivalente. O dever de segurança, conforme a LPDP, é acrescido aos operadores da comunicação electrónica, os quais, além da protecção dos dados relativamente ao emitente da factura, devem proteger as infraestruturas de comunicações.

Cabe ao farmacêutico preparar o medicamento, a sua mistura, para ser ministrada ao paciente. A assistência farmacêutica engloba todo o ciclo do medicamento antes do uso pelo paciente. É por isso que a preocupação com a utilização pelo paciente, que é o consumidor final, se coloca em várias etapas anteriores, nomeadamente de investigação, desenvolvimento, produção, formulação, transporte, distribuição e selecção, difusão de informações, e educação continuada para os profissionais da saúde e pacientes. Quanto à atenção do farmacêutico, caracteriza-se pelo relacionamento directo entre farmacêutico e paciente, tendo em vista o acompanhamento e o uso racional da farmacoterapia, que inclui o atendimento farmacêutico (*maxime*, relação farmacêutico-paciente), fornecimento do medicamento, acompanhamento da farmacoterapia e a intervenção farmacoterapêutica[136]. Já ao farmacologista compete estudar como as

[136] Barbara G. WELLS *et al., Manual de Farmacoterapia*, 9.ª ed., McGraw Hill Education, 2016, 2026. Esta obra oferece informações importantes para a

substâncias químicas se integram com os sistemas biológicos. Se estas substâncias têm propriedades medicinais, elas são referidas como substâncias medicinais. Por isso, para compatibilizar as substâncias químicas com propriedades medicinais com os sistemas biológicos são necessárias experiências em humanos ou laboratoriais. Naquelas, cumpre o consentimento para a realização da investigação. Havendo consentimento e podendo (normalmente) participar do estudo mais do que uma pessoa, estas devem prestar informações relativas à sua pessoa para ser identificada ou identificável, designadamente o nome, um número de identificação, dados de localização, elementos específicos da identidade física, fisiológica, genética e mental, para se distinguir das demais pessoas participantes.

A identificação pessoal, para além de individualizar os participantes, visa obter separadamente dados para tratamento (cruzamento com os dados dos demais) sobre história, origem, propriedades físicas e químicas, associações, efeitos bioquímicos e fisiológicos, mecanismos de absorção, biotransformação e excreção dos fármacos para o seu uso terapêutico ou não. Estas descobertas levam a um conhecimento profundo da pessoa, o que justifica a protecção dos dados recolhidos.

Como os medicamentos visam servir as pessoas, fica justificada a ideia de que a protecção das pessoas singulares relativamente ao tratamento de dados pessoais constitui um direito fundamental. O processo de descoberta do medicamento implica, muitas vezes, a participação de pessoas, como já referido. Por isso, a concepção personalista do direito associada a uma matriz ética, estabelece que os princípios e regras que norteiam a protecção de dados pessoais devem sempre respeitar os seus direitos e liberdades fundamentais, com excepção daquelas situações que a lei permitir.

---

tomada de decisão em terapia farmacológica, incluindo as doenças e distúrbios encontrados com mais frequência no ambiente clínico.

Para melhor protecção dos doentes, estes podem organizar-se em associações, o que facilita o acesso a medicamentos e o controlo por parte dos serviços de saúde. Por exemplo, os membros de uma associação de doentes com diabetes têm os seus dados registados nesta organização associativa, e os seus registos nas farmácias onde adquirem os seus medicamentos; também os serviços de saúde têm os seus dados processados para efeitos de exercício de controlo no âmbito da saúde pública.

5.4 Nas experiências (investigações) clínicas

Quais os dados pessoais objecto da investigação científica? A investigação clínica é suportada por dados pessoais e, em especial, dados relativos à saúde e vida sexual, dados genéticos e biométricos. Tentemos defini-los. Os dados relativos à saúde e vida sexual já os definimos, mas nada obsta repetir que dizem respeito à saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde que revelem informações sobre o seu estado de saúde.

Os dados genéticos dizem respeito aos dados pessoais relativos às características genéticas, hereditárias ou adquiridas de uma pessoa singular que oferecem informações únicas sobre a fisiologia ou saúde dessa pessoa singular, e que resulta, designadamente, de análise de uma amostra biológica proveniente da pessoa em causa.

Os dados biométricos referem informação pessoal resultante de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentos de uma pessoa singular que permitem ou confirmam a identificação única dessa pessoa singular.

A abordagem desta matéria apresenta uma dificuldade significativa: Angola não tem legislação relacionada com a investigação científica em geral, e com investigação científica em saúde em particular, facilitadora de um diálogo dogmático esclarecedor. Não temos, por exemplo, uma lei que regule a investigação clínica, nem dispositivo legal que contenha o regime jurídico de "estudo clínico" que abran-

ge o "estudo clínico de regime alimentares" e o "estudo clínico de terapêutica não convencional", o "estudo multicêntrico", o "estudo clínico sem intervenção", o "estudo clínico com intervenção", o "estudo clínico de dispositivo médico" e o "estudo clínico de produtos cosméticos e de higiene corporal"[137]. O Ministério da Saúde deverá, como legislador material, propor uma Lei sobre a Informação Genética Pessoal e Informação de Saúde, Lei sobre os Dispositivos Médicos e outra legislação afim, todas elas tendo por fundamento axiológico o princípio de não ingerência na esfera da privacidade e o princípio da autodeterminação do indivíduo; devido a diversas finalidades da investigação clínica/científica, tais princípios devem assentar naqueloutro princípio fundamental de que irradia todo o sistema jurídico e que merece destaque neste contexto: o princípio da dignidade da pessoa humana.

O tratamento de dados pessoais para fins de investigação científica não está devidamente desenvolvido na lei sobre protecção de dados. A referência à investigação científica está no art. 26º, sobre o direito de acesso, no nº 6, onde está estabelecido que "a lei pode restringir o direito de acesso, verificadas as seguintes circunstâncias: *a)* os dados serem utilizados para tomar medidas ou decisões relativamente a pessoas determinadas, mas exclusivamente para fins de investigação científica ou conservados sob forma de dados pessoais durante um período que não exceda o necessário à finalidade exclusiva de elaborar estatísticas". O nº 7 dispõe, entretanto, que "o direito de acesso do titular dos dados à informação sobre os dados de saúde e vida sexual, incluindo os dados genéticos, é exercido por intermédio de médico escolhido pelo titular dos dados ou de seu representante legítimo". O investigador, na qualidade de responsável

[137] Elisabete CASTELA / Tiago Branco da COSTA, "A investigação clínica na era do altruísmo dos dados", 249 e seg.

pelo tratamento, está adstrito a um conjunto de deveres, como o de informar o participante no estudo, os seus contactos e identidade, contactos do encarregado da protecção de dados, as finalidades do tratamento a que os dados se destinam e o seu fundamento jurídico, interesse legítimo do responsável pelo tratamento e investigação ou de terceiro, entre outras que a lei especifique.

Somos um país novo relativamente aos materiais de regulamentação de protecção de dados, havendo por isso zonas onde a ausência de regulação e supervisão é notória; a relativa a dados pessoais na investigação científica/clínica é uma delas. Com mais experiência, referimos a realidade portuguesa, onde, por exemplo, o Conselho Nacional de Protecção de Dados, através das Deliberações nºs 227/2007 e 333/2007 estabeleceu, respectivamente, os princípios aplicáveis aos tratamentos de dados pessoais efectuados no âmbito de estudos de investigação científica na área da saúde, e os princípios aplicáveis aos tratamentos de dados pessoais, no âmbito de ensaios clínicos com medicamentos de uso humano. Estes instrumentos foram consequência da aprovação da lei nº 46/2004, de 19 de Agosto, que operou a transposição para a ordem jurídica portuguesa da Directiva 2001/20/CE, do Parlamento Europeu e do Conselho, de 4 de Abril, que estabelecia a regulamentação dos ensaios clínicos. Muito recentemente, o CNPD publicou a deliberação nº 1704/2015, aplicável ao tratamento de dados pessoais no âmbito de investigação clínica. Da mesma forma como ocorreu com as deliberações referidas *supra*, esta resultou da entrada em vigor da lei da investigação clínica – Lei nº 21/2014, de 26 de Abril, alterada pela lei nº 73/2015, de 27 de Julho –, em cujo art. 3º inequivocamente estabelece que os estudos clínicos são realizados no estrito respeito pelo princípio da dignidade da pessoa humana e dos seus direitos fundamentais, garantindo que os interesses dos participantes prevalecem sobre os interesses da ciência e da sociedade. O preceito em questão impõe às entidades que realizam a investigação o dever de tomar todas as precauções no sentido do respeito da privacidade e dos direitos de personalidade.

No âmbito europeu, o RGPD também não traz uma definição explícita da expressão "tratamento para efeitos de investigação científica". Para o seu melhor entendimento, socorre-se do considerando 159, que estabelece o seguinte: "o tratamento de dados pessoais para fins de investigação científica deverá ser entendido em sentido lato, abrangendo, por exemplo, o desenvolvimento tecnológico e a demonstração, a investigação fundamental, a investigação aplicada e a investigação financiada pelo sector privado. Deverá, além disso, ter em conta o objectivo da União mencionado no artigo 179º, nº 1, do TFUE, que consiste na realização de um espaço europeu de investigação. Os fins de investigação científica deverão também incluir os estudos de interesse público realizados do domínio da saúde pública".

Em África, a CUACPDP, no art. 10º (Formalidades prévias ao tratamento de dados pessoais), estabelece no nº 4 as acções que apenas podem ser implementadas depois da autorização da autoridade nacional de protecção: *a)* "o processamento de dados pessoais envolvendo informações genéticas e a investigação na área da saúde"; *d)* "o processamento de dados pessoais relativo a informações biométricas"; *e)* "o processamento de dados pessoais de interesse público, nomeadamente para fins históricos [estabelecer comparações ao longo do tempo sobre doenças sazonais, *v.g.*], estatísticos [para fins de fixação de endemias, pandemias, aumento ou diminuição de determinadas doenças, estabelecendo comparações com períodos homólogos] ou científicos [descobertas de viroses, de medicamentos, de novas formas de tratamento de determinadas doenças, *v.g.*]".

Há uma particularidade que deve ser realçada: quando envolva intervenção no ser humano, a investigação clínica implica a observância das regras clínicas e técnicas, mas também de exigências de natureza ética e jurídica. A investigação não é uma actividade em si mesma e pode assumir a forma de ensaios clínicos, estudos clínicos sem intervenção, estudos clínicos com intervenção, estudos clínicos de dispositivo médico, estudos clínicos de produtos cosméticos e de higiene corporal. Também podem ser ensaios de medicamentos para

uso humano ou para uso animal (aqueles que estão dentro da cadeia alimentar humana). Na ausência de instrumentos éticos e jurídicos (específicos sobre investigação que envolvam dados da saúde), pensamos que em Angola, em homenagem ao princípio da dignidade da pessoa humana, os direitos dos participantes na investigação prevalecem sobre os interesses da ciência e da sociedade. Quem promove a utilização de dados pessoais no contexto da investigação clínica deve assegurar que os participantes consentirão com os termos do tratamento dos dados para fins desta investigação. Nestes casos, e em atenção ao Considerando 33 do RGPD, sendo sempre possível identificar na totalidade a finalidade de dados pessoais para efeito de investigação científica no momento da recolha dos dados, os seus titulares poderão dar o seu consentimento para determinadas áreas específicas de investigação, desde que estejam de acordo com padrões éticos reconhecidos para a respectiva investigação científica.

Uma das áreas de investigação em saúde é a definição de perfis de ADN[138]. Para além das questões de protecção de dados, há problemas de ordem ético-legal, pois o ADN pode constituir a base

[138] O desenvolvimento tecnológico parece estar a romper barreiras que o conhecimento de há escassos dez anos parecia impossível de se alcançar. O DNA sintético vai substituir os discos rígidos de computadores num futuro muito próximo. O dispositivo inspirado no armazenamento do nosso código genético levará ao desenvolvimento de meios de comunicação muito menores, mas potentes e capazes de garantir a integridade das informações durante muito tempo. Actualmente, a forma de se armazenar dados são as arquiteturas remotas em nuvem. Estes locais remotos, os chamados *data centres*, já consomem 1% da energia eléctrica mundial, e o aumento da procura por armazenamento deve fazê-los passar a consumir 30% dentro de poucos anos, o que representa um problema energético grave. Preocupados com a iminente crise que esta situação pode vir a gerar, os cientistas estão a começar a estudar alternativas mais eficientes para o armazenamento de dados. Uma das mais promissoras envolve o uso de versões sintéticas do ADN para guardar informações digitais.

para a descoberta do que biologicamente seja considerado íntimo da pessoa ou, mais perigoso, desencadear processos defendidos pelos transhumanistas, que enveredam por esse caminho em vista de uma melhoria da nossa condição humana. O surgimento de bases de dados de perfis de ADN nos diversos países tem motivações diferentes: na Europa, a sua história é diferente da dos EUA[139]. Em Angola, não se faz recurso ao ADN para além da investigação criminal. Não temos notícia da existência de que uma instituição pública ou privada use dados pessoais extraídos do ADN como sua matéria de trabalho.

---

[139] No século passado, em 1984, Sir. Allec Jeffreys da Universidade de Leicester anunciava a descoberta de um método de identificação de indivíduos pelo ADN, tendo-a denominado de "DNA fingerprinting", e RFLP "restriction fragment length polymorphism". Este método baseava-se nos diferentes tamanhos de fragmentos que eram produzidos quando uma amostra de ADN era submetida à acção de uma enzima que procedia ao seu corte. Longe de ser a chave para a individualidade absoluta, aliado ao longo tempo necessário aos procedimentos e à quantidade de ADN preciso, revelou-se pouco vantajoso e foi progressivamente substituído. Em 1986, nos EUA, Karry Mullis, que trabalhava na Cetus Corporation, descobre o método de replicação de ADN chamado PCR, "polymerase chain reaction". Assim, com a possibilidade de replicar o ADN, conseguiu-se que não fosse necessária uma recolha de amostra tão ampla. Em 1991, começa a usar-se um outro método de identificação, baseado no uso da PCR e de STR "short tandem repeats", o qual compara o comprimento de secções altamente variáveis do ADN repetitivo, como microssatélites, em pessoas diferentes. O mote para a criação de bases de dados foi dado em 1988 quando os perfis de ADN foram usados pela primeira vez para a condenação de Colin Pichfork pelo assassinato de Narborough e de Enderby, em 1983 e 1986 no Reino Unido. Aparece, assim, a vontade de que exista uma compilação efectiva dos perfis de ADN, com o intuito de tornar as investigações mais eficientes, solucionando muitos casos criminais, especialmente os crimes de abuso sexual e homicídio.

5.5 Na transfusão de sangue e nos transplantes de órgãos

No processo de realização de um estudo notificado é necessário tratar várias categorias de dados: dados de saúde, dados genéticos, dados da vida sexual e dados da vida privada. A maioria são dados sensíveis, cujo tratamento está, em princípio, proibido. Os estudos podem ser prospectivos e retrospectivos, obrigar à recolha de dados identificados ou decorrer com dados não identificáveis.

Um investigador, no âmbito dos deveres éticos e jurídicos a que está obrigado, deve sempre optar, podendo, por um estudo sem o tratamento de dados pessoais, ou seja, sem dados identificados ou identificáveis. Se não puder, deve privilegiar a utilização de dados codificados. Mas há casos de imposição legal. Entre nós, a lei nº 20/19, de 20 de Setembro, sobre o transplante de células, tecidos e órgãos, prevê no art. 5º, o registo nacional de doadores, dispondo que "os doadores devem estar devidamente controlados, mediante a sua inscrição numa base de dados especialmente criada para o efeito, designada Registo Nacional de Doadores". Por sua vez, o art. 6º determina o registo nacional para candidatos a receptores para transplante. Sendo uma base de dados que contém dados pessoais dos doadores e dos receptores, a sua protecção é um imperativo. Assim, o art. 9º, estabelece a confidencialidade da identidade do doador e do receptor, salvo se houver consentimento de um dos sujeitos.

A transfusão de sangue é usada para tratar milhões de pessoas por ano. A transfusão não implica intervenção cirúrgica, como o transplante, nem implica a utilização de fármacos para inibir o sistema imunológico. Existe um sistema local de registo de doadores de sangue que, no geral, dispensa a identificação do nome, bastando apenas a identificação codificada do sangue.

Na área do transplante de órgãos, o tratamento de dados é considerado fundamental, desde logo porque o paciente que necessita de transplante, chamado de receptor, é levado a realizar um conjunto

de exames, não só com vista ao êxito do processo de transplante, como também visa determinar as necessidades de tratamento. Os dados como potencial receptor de órgãos ou tecidos são organizados num programa informático, sob responsabilidade da entidade gestora do serviço de transplantes. O sistema informático deve registar e disponibilizar os doadores de órgãos e os resultados dos exames do receptor. Os resultados processados ficam à disposição deste sistema para a classificação de receptores numa única lista. O sistema informático faz também o cruzamento entre os dados dos doadores e dos receptores e apresenta as opções mais compatíveis, ou seja, o sistema deve gerar uma única lista de receptores capaz de indicar a compatibilização com cada doador disponibilizado. Só laboratórios especificamente autorizados podem realizar os exames que comprovam a compatibilização para que o receptor tenha segurança de receber o órgão doado. Para tal, o pessoal técnico do laboratório está obrigado ao dever de sigilo. A complexidade deste processo e o número de pessoas envolvidas convoca a imperiosa necessidade de obediência à regulamentação atinente à protecção de dados pessoais.

Em 2016, na Austrália, uma instituição dedicada à colheita e doação de sangue, denominada *Red Cross Blood Service*, sofreu uma grave anomalia no seu sistema de segurança de dados e vazaram informações de mais de quinhentos mil doadores de sangue (nome, sexo, endereço, data de nascimento e o tipo de sangue). A grave falha ocorreu quando se realizava a transferência de um arquivo contendo informações dos doadores para um ambiente computacional não seguro, acessível a pessoas sem autorização para processar aqueles dados. A recolha dos dados foi realizada através de um questionário e num deles, cuja resposta era apenas "verdadeiro-falso", perguntava se o doador tinha tido, nos últimos 12 meses, actividade sexual de risco; em caso positivo, o resultado do tratamento dos dados considerava o doador como

"pessoa com comportamento sexual de risco"[140].

Em Angola, existe um formulário dirigido ao doador de sangue onde consta, na primeira página, informação geral sobre doação de sangue, e a segunda página está reservada a um questionário. As respostas ao questionário agregadas à informação levam o doador a prestar o seu consentimento para, em primeiro lugar, submeter-se a observação clínica e análises ao sangue colhido para, em segundo lugar, os dados daí resultantes estarem sujeitos a processamento e armazenamento electrónico que a instituição, para além de garantir a confidencialidade dos dados, assegura os direitos expressos na lei. Com o consentimento fica também garantido que o sangue do doador será sujeito a exames laboratoriais e que qualquer anomalia importante para a sua saúde lhe será comunicada confidencialmente.

Com os exames de sangue, obtém-se um conjunto de informação como, por exemplo, doenças transmissíveis, grupo sanguíneo, possibilidade de produção de outros componentes (como o plasma e plaquetas); a obtenção de concentrado de eritrócitos (CE) a partir do sangue total (ST) permite aplicar as seguintes regras específicas que se devem seguir na hora de realizar uma transfusão deste componente, o que amplia as possibilidades terapêuticos: o grupo O pode doar eritrócitos (glóbulos vermelhos) a qualquer outro tipo, mas receber unicamente do seu mesmo tipo; já o grupo A pode doar eritrócitos (glóbulos vermelhos) aos tipos A e AB, mas receber dos tipos O e A. O registo destas características dos doadores demonstra a importância dos registos e da protecção dos dados.

---

[140] Caitlin Sampaio MULHOLLAND, "Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (lei 13.709/18)", *Revista de Direito e Garantias Fundamentais*, Vitória, 19/3 (2018) 159-180.

5.6 Na procriação medicamente assistida

A lei angolana sobre a reprodução humana medicamente assistida – lei nº 29/21, de 9 de Novembro – dispõe no art. 21º, sob a epígrafe "Registo e conservação de dados", no nº 1, que "aos dados pessoais relativos aos processos de reprodução humana medicamente assistida, respectivos beneficiários, doadores e crianças nascidas é aplicável a legislação de protecção de dados". Portanto, a lei que vimos citando, lei nº 22/11, de 17 de Junho, serve para a tutela dos titulares de dados, embora o nº 2 da lei nº 29/21 determine que "em diploma próprio, de acordo com a especificidade dos dados relativos à reprodução humana medicamente assistida, é regulamentado, nomeadamente, o período de tempo durante o qual os dados devem ser conservados, quem pode ter acesso a eles e com que finalidade, bem como os casos em que podem ser eliminadas as informações constantes dos registos".

Infelizmente, Angola ainda não criou diploma próprio que estabeleça a disciplina jurídica sobre o período para a conservação dos dados nem das pessoas com legitimidade de acesso aos referidos dados e em que situações eles podem ser eliminados. Entendemos que, com a não criação de facto do Conselho de Ética em Reprodução Humana Medicamente Assistida (CERHUMA), que a lei já prevê (art. 11º), a protecção de dados pode considerar-se fragilizada, uma vez que as várias técnicas de reprodução devem ser realizadas apenas em centros públicos e privados expressamente autorizados pelo Ministério da Saúde, sob parecer do CERHUMA.

Outras questões éticas se colocam a este nível, como por exemplo a de saber a identidade do doador de gâmetas ou espermatozoides

ou da gestante na gestação de substituição.[141]

A lei em referência estabelece no art. 3º os princípios gerais sobre a reprodução humana medicamente assistida, e dela retiramos, pela importância para o presente estudo, o constante da al. *c)*: consentimento expresso, informado, esclarecido e livre. Este princípio vem desenvolvido nos arts. 6º e 19º, que em resumo dispõem da necessidade do consentimento prévio, informado e devidamente fundamentado do beneficiário das técnicas de reprodução humana medicamente assistida. Tais técnicas são, designadamente, conforme o art. 1º:

a) Inseminação artificial;
b) Fecundação laboratorial ou fertilização *in vitro*;
c) Diagnóstico genético pré-implantacional;
d) Injecção intracitoplasmática de espermatozoides;
e) Transferência de embriões, gâmetas ou zigotos;
f) Outras técnicas laboratoriais de manipulação de gâmetas ou embriões, equivalentes ou subsidiárias.

Em todas estas técnicas os dados constituem a matéria-prima. O chamado *diagnóstico genético pré-implantacional* (DGPI – art. 32º da lei nº 29/21), "consiste numa biópsia celular, realizada num embrião em desenvolvimento, com a finalidade de proceder à subsequente avaliação genética dessa amostra, para assim determinar a presença de desconformidades genéticas específicas que determinam doenças como a hemofilia ou a fibrose quiástica. Normalmente, o DGPI é efectuado em embriões com três dias de desenvolvimento, quando o embrião é composto por seis a dez blastómeros, sendo alguns recolhidos para realizar a análise, sem prejuízo para o embrião.

---

[141] Rafael Vale e REIS, *Procriação Medicamente Assistida: Gestação de substituição, anonimato do doador e outros problemas*, Coimbra: GestLegal, 2022, 392.

Com esta técnica, consegue, igualmente, descobrir-se o sexo do ser a que o embrião dará lugar. É, assim, uma alternativa muito importante ao diagnóstico pré-natal invasivo e ao aborto terapêutico. Em rigor técnico, o DGPI (que tem por finalidade diagnosticar doenças específicas), distingue-se, quanto aos objectivos, de uma técnica parecida, que pode definir-se como *rastreio genético pré-implantatório* (RGPI, ou *Preimplantation Genetic Screening*), e que procura descobrir no embrião qualquer tipo de aneuploidias (anomalias cromossómicas), ou seja, procura ajudar a saber qual é o melhor embrião para transferir"[142]. Todas estas técnicas precisam de codificação, que é feita por meio de informação de natureza específica relativa à natureza genética de quem poderá vir a ser identificado ou identificável. Esta informação deve ser protegida, não só para garantir a privacidade da pessoa que vier a nascer, como da gestante e do doador do espermatozoide. Neste sentido, a lei nº 29/21, de 9 de Novembro, no art. 20º dispõe sobre o "dever de confidencialidade e sigilo", determinando a todos "aqueles que, por alguma forma, tomarem conhecimento do recurso a técnicas de reprodução humana medicamente assistida ou da identidade de qualquer dos participantes nos respectivos processos estão obrigados a manter absoluto sigilo sobre a identidade dos mesmos e sobre o próprio acto da reprodução medicamente assistida" (nº 1), cuja violação é punida nos termos do disposto da LPDP.

5.7 Na saúde no trabalho

Muito pouco desenvolvida em Angola é a questão da protecção de dados pessoais de saúde e vida sexual dos trabalhadores, o que

---

[142] Rafael Vale e REIS, *Procriação Medicamente Assistida*, 113.

implica abordar também a relação do médico do trabalho[143]. Para além dos dados especialmente pessoais, como o nome, filiação, data e local de nascimento, endereço electrónico e telefónico, moradia, habilitações literárias e profissionais, aos trabalhadores são cobrados dados sensíveis da sua saúde física e psico-emocional.

Há uma área dentro do Direito do Trabalho que trata de um "direito da segurança e da saúde no trabalho"[144]. O primeiro elemento, aquele que trata da prevenção de acidentes de trabalho, o reconhecimento e controlo dos riscos associados aos componentes materiais do trabalho, não interessa desenvolvê-lo aqui. Já interessa o elemento saúde no trabalho, que é, segundo o Comité Misto da Organização Mundial da Saúde e da Organização Internacional do Trabalho, "a promoção e a manutenção do mais alto grau de bem--estar físico, mental e social dos trabalhadores em todas as profissões e, não apenas, a ausência de enfermidade ou doença". Ora, para haver bem-estar é necessário haver diagnósticos médicos que implicam a realização de exames médicos especializados, consoante o posto do trabalhador, resultando na recolha, tratamento, registo e conservação dos seus dados de saúde.

A LPDP não contém uma norma específica que aborda o tratamento de dados de saúde do trabalhador. No entanto, exercendo

---

[143] Já há escritos em Angola sobre Protecção de Dados Pessoais. Norberto Moisés Moma CAPEÇA*, Estudos de Direito Privado* II, Luanda: Editora Caneta de Estilo, 2022, 111-134, trata da "Privacidade e a Protecção de Dados Pessoais" e da135 a 170 fala da "Protecção de Dados e Responsabilidade Civil. Realidade Angolana". Ainda do mesmo autor, *A Privacidade do Trabalhador como Garantia Constitucional*, Coimbra: Almedina, 2021. Nas p. 145-160 trata da protecção dos dados pessoais dos trabalhadores e da160 a 171 aborda a questão dos testes e exames médicos e o contrato de trabalho.

[144] Paula QUINTA, *Manual de Direito da Segurança e Saúde no Trabalho*, 5.ª ed., Coimbra: Almedina, 2023, 11 seg.

uma actividade interpretativa assente num processo de desvelação do sentido normativo que o sistema jurídico oferece para que a norma seja um critério adequado para a resolução do problema espoletado pelo caso concreto, entendemos ser possível apoiarmo-nos na mobilidade e abertura sistema jurídico. Assim, a regra constante no art, 12º, sobre os requisitos gerais para o tratamento de dados pessoais (que exige o consentimento inequívoco e expresso do seu titular, o trabalhador, ou a notificação à APD), deverão ser combinados com os requisitos específicos sobre o tratamento de dados sensíveis de saúde, constantes no art. 14º (nomeadamente, aplicação das regras da medicina preventiva, para efeitos de disgnóstico médico e de assistência médica consentida).

A LPDP traz no art. 29º a questão das decisões automatizadas, e no nº 1 prevê que "qualquer pessoa (trabalhador) tem o direito de não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afecte de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspectos *da sua capacidade profissional* (…)". Por sua vez, a Lei Geral do Trabalho – lei nº 12/23, de 27 de Dezembro – estatui no art. 24º a protecção de dados pessoais. A entidade empregadora, determina o nº 1, "não pode exigir ao candidato a emprego ou a trabalhador que preste informações relativas: *a)* à sua vida privada, salvo quando estas sejam estritamente necessárias e relevantes para avaliar da respectiva aptidão no que respeita à execução do contrato de trabalho e seja fornecida por escrito a referida fundamentação; *b)* à sua saúde ou estado de gravidez, salvo quando particulares exigências inerentes à natureza da actividade profissional o justifiquem e seja fornecida por escrito a respectiva fundamentação". O candidato a emprego ou o trabalhador que haja fornecido informações de índole pessoal goza do direito ao controlo dos respectivos dados pessoais, podendo tomar conhecimento do seu teor e dos fins a que se destinam, bem como exigir a sua rectificação e actualização (nº 3). Os ficheiros e acessos informáticos (ou qualquer tecnologia de recolha, processamento e transferência) utilizados pela

entidade empregadora para tratamento de dados pessoais do candidato a emprego ou trabalhador ficam sujeitos à legislação em vigor relativa à protecção de dados pessoais (nº 4).

O instrumento jurídico que disciplina a saúde no trabalho é o Regulamento sobre o Licenciamento para o Exercício de Serviços de Segurança, Higiene e Saúde no Trabalho, aprovado pelo Decreto Presidencial nº 179/24, de 1 de Agosto. No art. 3º daquele regulamento constam as definições. Na al. *c)* está a definição de "saúde no trabalho" como o "conjunto de actividades relacionadas com a saúde dos trabalhadores que têm como objectivo garantir a qualidade de vida no trabalho, promovendo o bem-estar físico, mental e social dos trabalhadores"; a al. *i)* dá a definição de "vigilância da saúde" como sendo o "processo contínuo e sistemático de colecta, consolidação, análise de dados e disseminação de informações sobre eventos relacionados à saúde do trabalhador"; já a al. *j)* define "ficha clínica" como sendo o "documento que contém informações detalhadas sobre o estado de saúde do trabalhador". Este documento deve conter as informações clínicas relativas aos exames de saúde e está sujeita ao segredo profissional, podendo, no entanto, ser facultada às autoridades de saúde e aos médicos afectos a entidade com competência para promover a saúde no trabalho. Esta ficha não deve conter dados sobre a raça, a nacionalidade, a origem étnica ou a informação sobre hábitos pessoais do trabalhador, salvo quando estes estejam relacionados com patologias específicas ou com outros dados de saúde. O trabalhador tem direito ao acesso à ficha clínica e os registos clínicos são mantidos num período mínimo de 20 anos após a cessação da relação jurídico-laboral do trabalhador (art. 29º); por fim, al. *k)* "atestado de aptidão laboral", é o "documento emitido pelo médico do trabalho, que atesta a aptidão ou não do trabalhador para o exercício de determinada função". O resultado do exame médico é dado a conhecer ao trabalhador, devendo o médico emitir, em duplicado, o

atestado, sendo o original depositado na área dos recursos humanos e o duplicado entregue ao trabalhador (art. 30º)[145].

Os serviços detentores de postos de trabalho (o empregador) devem (*podem*, no dizer do regulamento) "adoptar o serviço interno de saúde no trabalho, desde que possuam no seu quadro de pessoal recursos humanos qualificados e equipamentos específicos" (art. 6º, nº 1). A organização deste serviço implica, em primeiro lugar, a existência do médico do trabalho (art. 25º) e, em segundo lugar, deve estar garantido o seu funcionamento, ainda que seja por apenas determinadas horas (art. 26º). Como aludimos *supra*, a LPDP interpretativamente admite o tratamento de dados pessoais dos trabalhadores, quando resultarem da actividade de medicina preventiva ou da realização de diagnósticos. O regulamento sobre o licenciamento para o exercício de serviços de segurança, higiene e saúde no trabalho estabelece, no art. 27º, as modalidades dos exames de saúde a que os trabalhadores estão sujeitos. Dispõe o nº 1 a obrigatoriedade de os trabalhadores se submeterem a exames médicos, por conta

[145] Coloca-se aqui o problema de aclarar a discussão à volta do papel e da influência do médico do trabalho. A nossa legislação não é clara sobre o tema, mas podemos afirmar que o médico, podendo determinar os exames e sendo competente para preencher a ficha médica, determinando o seu conteúdo em termos de dados da saúde, é porque o médico "é o responsável a decidir, de forma discricionária, *porquê* – finalidade – e como – *meios* – utilizar os dados pessoais. Por outro lado, "o responsável ocupa a posição única de garantir uma proteção efetiva do titular dos dados pessoais, de aplicar os princípios de proteção de dados pessoais (…)", e as obrigações, em especial sobre responsabilidades do responsável pelo tratamento e da protecção de dados desde a concepção e, por fim, sobre segurança do tratamento. Cfr. Diogo BRANDÃO / Graça Canto MONIZ, "O papel do médico do trabalho à luz do RGPD", *Privacidade e Dados Pessoais*: *Revista do Centro de Estudos Judiciários* 2 (2º Semestre, 2023) 129-152.

do empregador[146]. Esta obrigatoriedade, conforme dispõe o nº 2, decorre da "investigação clínica ou radiológica, a fim de investigar a capacidade ou aptidão física e mental do trabalhador, para a função que deve exercer ou exerce". A lei nº 26/22, de Agosto – lei de bases da função pública -, estabelece no art. 11º os requisitos gerais de ingresso e impõe na al. *c)* "sanidade mental" e na al. *d*) "capacidade física compatível com a actividade a exercer". A Lei Geral do Trabalho dispõe no art. 25º que a entidade empregadora não pode, para efeitos de admissão, exigir ao candidato a emprego ou ao trabalhador a realizar apresentação de testes ou exames médicos, a não ser naqueles casos em que a finalidade dos mesmos seja a protecção e segurança do trabalhador ou de terceiros, se exigências inerentes à actividade o justificam (nº 1). Os exames ou testes de gravidez são proibidos, quando se trata de pessoa candidata a emprego (nº 2). O profissional de saúde responsável pelos testes e exames médicos apenas deve comunicar à entidade empregadora se o trabalhador está ou não apto para desempenhar a actividade (nº 3).

O Regulamento sobre o Licenciamento para o Exercício de Serviços de Segurança, Higiene e Saúde no Trabalho enumera, no já

---

[146] Em Portugal houve uma polémica acerca da constitucionalidade da norma que torna os exames médicos obrigatórios, nomeadamente os artigos 13º, nº 2, al. e), 16º, 17º, 18º e 19º do Dec.-Lei nº 26/94, de 1 de Fevereiro, com as alterações introduzidas pela Lei nº 7/95, de 19 de Março. O Tribunal da Relação de Lisboa considerou que aquelas normas não estavam feridas de inconstitucionalidade – acórdão do Tribunal Constitucional nº 368/02. Esta decisão foi criticada por Carlos Lopes do Rego. Por sua vez, João Palla LIZARDO, posicionou-se em sentido contrário e, demonstrando a complexidade da interpretação da legislação relacionada e da controvérsia doutrinária, apresenta como exemplo a decisão do Tribunal da Relação de Lisboa, de 25 de Outubro de 2000, que é diferente do posicionamento do Dr. Carlos Rego. Cfr. "Exames médicos e direito de personalidade – acórdão do Tribunal da Relação de Lisboa de 25 de Outubro de 2000", *Questões Laborais* 11/25 (2004) 215-224.

citado art. 27º, os seguintes exames: exame médico de admissão; exame médico periódico; exame médico de retorno ao trabalho; exame médico de mudança de função; e exame médico de demissão. Qualquer exame médico transmite informações pessoais que devem ser tuteladas conforme o sistema de garantia da protecção dos dados pessoais, devendo convocar-se os *princípios da precaução* e da *proporcionalidade* no sentido de garantir que os empregadores não abusem do direito de realizar exames[147] a quem seja candidato a emprego ou trabalhador com a prevenção de riscos relativos à capacidade de o empregado responder às exigências da função e, de modo geral, da saúde no trabalho. Por exemplo, quem for portador de HIV/SIDA ou de tuberculose não poderá, em princípio, trabalhar na área de saúde, com excepção das áreas administrativas e utilizando as ferramentas do teletrabalho, por exemplo. Aí existe um risco previsível: a possibilidade de utilização de elementos condutores de transmissão do vírus (agulha ou instrumentos cirúrgicos, a libertação de partículas na saliva ao tossir).

Não há na Convenção da União Africana sobre a Protecção de Dados Pessoais norma que faça referência directa à protecção dos dados dos trabalhadores. O art. 1º, que oferece as definições no âmbito da Convenção, define "dados no domínio da saúde" como sendo "qualquer informação sobre o estado físico e mental de uma pessoa titular dos dados, incluindo as informações genéticas (…)".

---

[147] Afirma João Palla LIZARDO, a propósito do teor do art. 274º, nº 1, al. b) do Código de Trabalho luso, que a intenção axiológica tem enquadramento na nossa abordagem sobre o tema, e não se deve, a qualquer título, levantar a ideia de que "(…) a saúde do trabalhador é um 'bem' que pertence à empresa, cuja conservação e melhoramento constituem obrigações de quem trabalha por conta de outem" - "Exames Médicos e Direitos de Personalidade", 221. O valor da dignidade da pessoa humana nunca deve ser atacado, e deve ter como fonte de irradiação o conteúdo da liberdade, da autonomia e da tutela da privacidade.

Na Europa a RGPD também nada diz, mas é possível extrair do art. 4º, nº 15 os elementos da definição de dados relativos à saúde que podem ser atribuídos aos trabalhadores: são os "dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelam informações sobre o seu estado de saúde". As duas noções vão ao encontro da definição que o Comité Misto da Organização Mundial da Saúde e da Organização Internacional do Trabalho estabeleceram. Por isso, servem muito bem para cobrir os trabalhadores quando estiverem em causa os seus dados pessoais de saúde no contexto das relações laborais. O recurso ao sistema jurídico facilita encontrar soluções justas; aliás, o Direito não está talhado para não encontrar soluções, até porque o seu campo de actuação é a acção humana.

6. DIREITOS DOS TITULARES DOS DADOS PESSOAIS

A divulgação de dados pessoais em saúde apresenta determinadas particularidades, não só por serem dados sensíveis, mas também porque os danos daí advenientes podem representar discriminação em função da raça, etnia, portador de doença, etc. Neste contexto, a Agência de Protecção de Dados exerce uma função importante. Tal como ocorre para os estudos intervencionistas, o objectivo da avaliação e fiscalização por parte da entidade reguladora é o de garantir a protecção dos dados pessoais no que respeita à qualidade e quantidade dos mesmos, admissibilidade da recolha, registo, tratamento, conservação e transferência.

Nos termos do art. 44º, nº 1 da LPDP, compete, em geral, à APD a fiscalização da aplicação das disposições da lei de protecção dos dados pessoais. Podemos assinar sumariamente as demais competências, já que nos deteremos com maior acuidade quando falarmos das funções de supervisão e regulação da entidade angolana vocacionada para a supervisão e fiscalização de dados pessoais. São elas: a emissão de recomendações, orientações e instruções; a emissão de parecer sobre o acesso aos documentos nominativos; a emissão de parecer sobre o sistema de classificação de documentos; a apreciação e decisão sobre as reclamações e a garantia do exercício do direito de acesso, de rectificação, actualização e cancelamento de dados; garantir aos titulares dos dados pessoais a obtenção de informação precisa sobre os seus direitos no âmbito do tratamento dos seus dados; proceder a orientação sobre a aplicação das medidas

técnicas e de segurança necessárias e adequadas; e exercer a função sancionatória. Por outras palavras, a APD deve cuidar de exercer vigilância sobre as actividades dos responsáveis a quem a lei confere legitimidade para o tratamento de dados, e garantir que estes sejam pertinentes, adequados e não excessivos no que respeita à finalidade do tratamento dos mesmos. No que diz respeito à admissibilidade do tratamento, este deve ser levado a cabo de forma lícita, sustentado no princípio da boa-fé, garantindo que os dados apenas sejam utilizados para o fim a que inicialmente se destinam. A manutenção destes dados deve ser feita apenas durante o tempo necessário para permitir o cumprimento da sua finalidade.

6.1 O consentimento

Conforme ficou amplamente explicitado, o consentimento, para além de ser um conceito doutrinário, é também um conceito legal (art. 5º, al. *a)* da LPDP). Constitui um direito de personalidade, pois implica a autodeterminação do indivíduo e a sua privacidade. O seu exercício é exitoso se o direito à informação estiver garantido. Como sabemos, o uso de dados pessoais para a produção de informação pode ser mercantilizado ou ter um destino que pode atingir a dignidade do seu titular e vir a causar-lhe danos.

Por isso, terão de ser estabelecidas as regras de prova da prestação da informação e do consentimento informado, e realizar uma avaliação do alcance da informação para prestar o consentimento. O direito ao consentimento está estruturado na dignidade da pessoa humana, constituindo um direito fundamental (direito humano) radicado na liberdade do homem[148]. É graças à liberdade que

[148] Arthur KAUFMANN, *Filosofia do Direito*, trad. António Ulisses Cortês, 2.ª ed., Lisboa: Fundação Calouste Gulbenkian, 2007, 352.

o homem, através de uma razão prática, manifesta a sua vontade e que esta determina a sua acção. Desta forma, poderemos avaliar se o consentimento foi "manifestação de vontade livre", pois a liberdade (informada) na prestação do consentimento significa a aceitação dada ao responsável pelo tratamento de dados.

6.2 Direito à informação

O titular dos dados pessoais tem o direito de obter ou aceder à informação acerca dos seus dados recolhidos, tratados ou divulgados a terceiros no contexto da saúde, da sua vida sexual ou genética ou da investigação científica que abrange a sua identidade física, fisiológica e psíquica. Cabe ao responsável pelo tratamento o fornecimento ao titular de uma cópia dos dados pessoais em fase de tratamento. Está em causa o direito à autodeterminação informacional[149].

António SARMENTO, "Quando o doente está privado de liberdade", 504 seg. Este autor defende que a "influência da liberdade na natureza da relação do médico com o doente é fundamental". Entendendo o valor da liberdade para o médico e para o doente, afirma que "a primazia da beneficência, valor ético fundamental da Medicina, só pode ser plenamente alcançada em liberdade. Só em liberdade o médico consegue colocar o bem do doente acima do seu interesse próprio e de outros interesses que não sejam o bem do doente. Só em liberdade, o doente poderá decidir aceitar a ajuda que o médico pretende prestar-lhe". Ora, é no âmbito desta liberdade que assenta o consentimento do doente, que é o titular dos dados de saúde, para permitir a recolha e tratamento das suas informações médicas.

[149] A terminologia *autodeterminação informacional* não tem sido pacífica. Apesar da sua consagração, principalmente nos tribunais superiores lusos, Teresa Coelho Moreira, Libório Dias Pereira e Sousa Pinheiro entendem que a melhor seria *autodeterminação informativa*, seguida também pela jurisprudência brasileira. *Apud* A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 259. Para nós, e aproximando ao nosso estilo de expressão lin-

A obrigação de ser seguida como um dever legal prende-se com o facto de que o responsável deve informar os titulares sobre os fins para os quais recolhe e usa informações de saúde sobre eles, como contactar o responsável relativamente a qualquer questão ou queixa, os tipos de terceiros a quem os dados podem ser transferidos, e as escolhas e meios que oferece aos titulares para limitarem a utilização e divulgação dos seus dados pessoais. Esta informação deve ser dada em linguagem clara sempre que os titulares dos dados sejam convidados a fornecer informações pessoais ao responsável pelo tratamento dos dados. Se a finalidade do tratamento dos dados ou o fluxo de informação (por exemplo, com a inclusão de uma entidade terceira para processamento dos dados) for alterada, o responsável pelo tratamento dos dados deverá informar novamente os titulares dos mesmos e obter o seu consentimento.

No âmbito do direito à informação deve considerar-se o direito à escolha, ou seja, o responsável pelo tratamento dos dados não deve colocar obstáculos aos titulares dos dados quanto à oportunidade de escolherem (*opt out* – oportunidade de exclusão): *a)* serem expostos a uma entidade terceira; *b)* serem utilizados para um fim diferente do originalmente acordado. Os titulares dos dados devem ter acesso rápido, fácil e sem custos excessivos para poderem exercer o seu direito de escolha. Mas há que ter presente que este direito dos titulares não é absoluto; aliás, só é possível exercê-lo porque há uma obrigação legal do responsável na prestação da informação. É assim que o art. 25º, nº 1 da LPDP dispõe: "(…) o responsável pelo tratamento deve disponibilizar aos titulares dos dados" as informações constantes neste preceito, designadamente as alíneas *a)* até *g)*.

guística, apoiamos a adopção de *autodeterminação informativa*; a primeira opção não ganhou espaço consolidado.

No caso de dados pessoais sensíveis deve ser dado um consentimento explícito (*opt in* – oportunidade de inclusão) por parte do titular dos dados no caso de a informação vir a ser partilhada com uma entidade terceira ou utilizada para outro fim além do que estava inicialmente proposto.

Também ligado ao direito à informação está o princípio da transparência. Na verdade, o acesso à informação deve estar sempre ligado a este princípio da transparência, que exige que a informação acedida pelo titular dos dados deve ser realizada com base nos critérios de compreensibilidade, produzida em linguagem clara e simples[150]. Mas não é apenas este princípio que incide sobre o direito à informação. Ele é também objecto do impacto valorativo da concisão, inteligibilidade e fácil acesso.

Os direitos dos titulares dos dados pessoais entrecruzam-se e complementam-se, não havendo, por isso, algum direito completamente autónomo. São direitos que dialogam entre si, para melhor compreensão e aplicação. É assim com o princípio da informação, que em determinados momentos reclama o princípio da transparência, pois a informação deve ser clara (n. 4, art. 25º). Noutros momentos confunde-se com o direito de acesso, conforme dispõe o nº 1, al. *e)*, pois este direito visa obter informação sobre as finalidades do tratamento (al. *b)*, nº 1), sobre as categorias de dados, sobre a categoria de destinatários dos dados recolhidos (al. *c)*, nº 1), sobre o prazo de conservação dos dados, sobre os direitos do titular e sobre as origens dos dados, quando não forem recolhidos directamente

---

[150] Para mais desenvolvimentos ver, Alexandre Sousa PINHEIRO, coord., *et al., Comentário ao Regulamento Geral de Proteção de Dados*, Coimbra: Almedina, 2018, 341. Na mesma obra e mesma página, o autor cita Alexander Roßnagel, o qual entende que "sem transparência suficiente o titular dos dados é colocado numa situação de facto sem direitos".

dos seus titulares, conforme nº 3, art. 25º, estabelecendo um prazo de 30 dias para prestar[151].

6.3 Direito de acesso

Este direito vem previsto no art. 26º da LPDP. Estabelece o nº 1 que "o titular dos dados tem o direito de obter do responsável pelo tratamento, livremente, sem restrições, demoras ou custos excessivos, informação sobre se são ou não tratados dados que lhe digam respeito, as finalidades desse tratamento, as categorias de dados sobre que incide e os destinatários ou categorias de destinatários a quem são comunicados os dados". Como se pode observar, este direito encontra-se a montante dos outros direitos: mesmo que o não coloquemos em primeiro lugar na ordem da nossa exposição, não significa uma ordem da sua importância operacional. Na sistemática apresentada pela LPDP, o direito de acesso também não é o primeiro direito: está colocado depois do direito à informação; no entanto, o direito de acesso à informação é o que permite o exercício posterior dos demais direitos.

O direito de acesso desmembra-se em outros direitos, nomeadamente *a)* o direito de o titular aceder aos dados pessoais objecto de tratamento; *b)* o direito de obter um conjunto de informações acessórias a esse tratamento; *c)* o direito à informação das garantias adequadas, quando os dados pessoais forem transferidos para um terceiro destinatário, nacional ou estrangeiro, *d)* o direito à obtenção de cópias dos dados pessoais[152].

---

[151] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 265.

[152] Alexandre Sousa PINHEIRO, coord., *et al.*, *Comentários ao Regulamento Geral de Proteção de Dados,* 360.

6.4 Direito à rectificação

Quando quaisquer dados pessoais não se encontrarem exactos, o seu titular tem o direito de obter do responsável pelo tratamento a sua rectificação. Conforme dispõe o art. 28º da LPDP, cuja epígrafe é "direito de rectificação, actualização e eliminação", ao titular dos dados é assegurado o direito de rectificação, actualização ou eliminação dos seus dados quando o tratamento não cumpra as regras legais, nomeadamente a inobservância do carácter incompleto ou inexacto desses dados (nº 1 e 2). Quando as informações objecto de rectificação, actualização ou eliminação tiverem sido já comunicadas a destinatários, o responsável pelo tratamento fica na obrigação de lhe notificar a rectificação, actualização ou eliminação, salvo se isso for comprovadamente impossível, neste caso, e que o destinatário agiu na base da informação que lhe foi comunicada (nº 3). Quando assim ocorrer, o destinatário que tratar os dados para os seus próprios fins ou para terceiros pode não proceder à eliminação dos dados, devendo neste caso tal destinatário informar o titular dos dados desta situação e confirmar se este pretende também rectificar, actualizar ou eliminar os seus dados dos ficheiros respectivos (nº 4).

O responsável pelo tratamento deve, todavia, bloquear e/ou conservar os dados pessoais caso ocorra o seguinte (nº 5): *a)* disposição legal ou ordem de autoridade competente que obrigue o responsável pelo tratamento a bloquear e/ou conservar os dados por um determinado período de tempo (as autoridades legais são a APD e um juiz); *b)* se o bloqueamento e/ou conservação dos dados for necessário à prossecução de um interesse legítimo do responsável pelo tratamento, designadamente para o exercício de um direito ou para o cumprimento de obrigações legais; *c)* se os dados estiverem a ser utilizados para efeitos de investigação criminal; *d)* se se tratar de dados relativos ao crédito e à solvabilidade, enquanto a situação creditícia do titular não estiver regularizada.

6.5 Direito ao apagamento dos dados pessoais

O acesso aos dados pessoais sensíveis pelos pacientes tem levantado nos últimos tempos problemas éticos ligados à privacidade e segurança, o que nos remete para outro assunto, aquele relativo ao direito ao esquecimento, direito em que o titular dos dados tem o poder de exigir o apagamento/esquecimento ou remoção dos dados, pois o titular pode encontrar-se, exemplificativamente, numa destas situações: numa situação de prestação de cuidados primários ou intensivos de saúde, implicando a possibilidade de ofensa do direito à privacidade, ou num processo de investigação, que inclui os ensaios clínicos, investigações clínicas e pesquisa epidemiológica.

O titular dos dados tem o direito de obter do responsável pelo tratamento o apagamento dos dados, se tal for aplicável. O art. 28º da LPDP, já exposto no ponto anterior, inclui o direito à eliminação dos dados, valendo aqui tudo o que foi dito antes. Também designado como "direito a ser esquecido" ou "direito ao esquecimento", confere ao titular dos dados o direito de requerer que os seus dados pessoais sejam apagados, ficando os responsáveis na obrigação de o fazer, com a maior brevidade possível[153].

---

[153] Há quem entenda que o direito ao esquecimento não é um direito autónomo. Diz Graça Canto MONIZ, que "em bom rigor e verdade, este direito a ser esquecido é uma extensão do direito ao apagamento (…)". Não temos intenção de aumentar a polémica, mas muito sumariamente diremos que são vocábulos diferentes que seguem o mesmo caudal do "rio jurídico", têm ambos a mesma intencionalidade de valores e de fins. "Direito do titular dos dados pessoais: o direito à portabilidade", in Francisco Pereira Coutinho / Graça Canto Moniz, coord., *Anuário da Protecção de Dados*, CEDIS, 2018, 11 seg.

Entende Rui Mascarenhas Ataíde[154] que "o ideário que comanda o direito ao esquecimento não é criação recente, antes inspira diversas figuras normativas tradicionais como a prescrição, o indulto, a amnistia e ainda a própria duração das inscrições de condenações no registo criminal, visando impedir que estejam permanentemente em liça factos que já não têm relevância social". Nesta mesma linha, dá-nos notícia René Ariel Dotti[155] de que uma prostituta, que respondia pelo nome Gabrielle Darley, foi acusada do crime de homicídio, vindo a ser absolvida no longevo ano de 1918. Depois deste acontecimento, ela casou-se com Bernard Melvin, levando desde então uma vida honrada, acreditando o bom nome na sociedade em que convivia. Em 1925, um produtor de cinema lançou uma obra cinematográfica intitulada Red Kimono, que relatava a vida da então prostituta, mesmo estando em situação de caso julgado. Os efeitos negativos da publicidade do filme, motivaram o marido de Gabrielle a intentar uma acção judicial junto da Corte da Califórnia, a qual, mesmo sem fazer alusão doutrinária, reconheceu um direito ao esquecimento.

---

[154] "Direito ao Esquecimento", *RDC* 2/2 (2018) 281. O autor adianta que "a ideia central da figura do direito ao esquecimento reside na protecção da vida privada e intimidade das pessoas, bem como a reabilitação e ressocialização dos indivíduos, que seriam impedidas ou consideravelmente dificultadas pela lembrança indefinida dos factos cometidos. O direito ao esquecimento pode assim ser considerado como um desmembramento do direito à reserva de intimidade da vida privada (artigo 80º CC), como se revelou de forma sintomática no caso de uma apresentadora brasileira que, no passado, fez um determinado filme do qual mais tarde se arrependeu e que ela não mais desejava que seja exibido ou rememorado por lhe causar prejuízos profissionais e transtornos pessoais", 282.

[155] "É possível defender um direito ao esquecimento?", "É possível defender um direito ao esquecimento?", *Gazeta do Povo,* disponível em <https://gazetadopovo.com.br/colunista/rene-ariel-dotti/e-possivel-defender-direito-ao-esquecimento-i-238ckdlqguwr2djwoy59ggbm>, acedido a 01 de Março de 2024.

Não é um direito novo, como ficou dito. O que veio lhe dar ênfase foi a utilização da internet, apresentando-se agora de forma mais moderna a partir de posições nascidas da jurisprudência do Tribunal de Justiça Europeu, quando foi chamado a pronunciar-se sobre dois casos[156]. Primeiro, no chamado caso *Google Spain,* indagou o tribunal para saber se se poderia invocar um direito de apagamento e de oposição pelos tratamentos de dados realizados por este motor de busca. Ou seja, procurou-se saber se nestes direitos cabiam a faculdade de o titular requerer ao motor de busca impedir a indexação da informação referente a si publicada em páginas *web* de terceiros. Esta preocupação assentava numa distinção: "uma coisa são os tratamentos de dados realizados pelos operadores de motores de busca e outra são os tratamentos realizados por esses 'terceiros' que são os editores de sítios web ou das páginas-fonte"[157]. Como operava este tratamento? Fazendo constar os dados pessoais numa página *web*, sendo no entanto o tratamento realizado pelos motores de busca, o que acarreta muita complexidade para o caso. Na busca de informação de forma automatizada na internet, o "operador recolhe, recupera, regista e organiza essa informação no âmbito dos seus programas de indexação, conserva-a nos seus servidores, comunica e coloca-a à disposição dos internautas sob forma de uma lista de resultados"[158]. O tribunal, salvaguardando a tutela dos direitos fundamentais com o resultado da pesquisa num motor de busca, deu provimento ao pedido. Decidiu que "o operador de um motor de busca é obrigado a suprir da lista de resultados, exibida na sequência de uma pesquisa efectuada a partir do nome de uma pessoa, as ligações de outra página *web* publicadas por terceiros e que con-

---

[156] Graça Canto MONIZ, *Manual de Introdução à Protecção de Dados Pessoais*, 184.
[157] Graça Canto MONIZ, *Manual de Introdução à Protecção de Dados Pessoais*, 184.
[158] Graça Canto MONIZ, *Manual de Introdução à Protecção de Dados Pessoais*, 184.

tenham informações sobre essa pessoa, também na hipótese de esse nome ou de essas informações não serem prévia ou simultaneamente apagadas dessas páginas *web*, se for caso disso, mesmo quando a sua publicação nas referidas páginas seja, em si mesma, lícita"[159].

O segundo caso tratou-se já não de um caso de apagamento propriamente dito, mas de supressão. O tribunal foi chamado a pronunciar-se sobre se "o operador do motor de busca está ou não obrigado a modificar *globalmente* os resultados de pesquisas, isto é, em todas as suas versões"[160]. O tribunal decidiu, *in extremis*, que a decisão final seria tomada pelas autoridades de controlo e pelos tribunais. No entanto, considerou que a mesma decisão deveria orientar-se por critérios de garantia de elevado grau de protecção dos titulares e da liberdade dos utilizadores de internet.

Apesar de o Professor Carlos Burity[161] considerar que não existe, na nossa ordem jurídica, consagração específica de "protecção da intimidade privada contra os potenciais atentados tornados possíveis pelos meios electrónicos ao dispor da moderna informática", entendemos que a LPDP, ao consagrar o *direito ao esquecimento*, está a oferecer aos particulares um meio de tutela jurídica, bastando, para tal, um exercício metodológico adequado de interpretação normativa e integração de (possíveis) lacunas.

Dois especialistas lusos nestas matérias entendem que a "publicidade dos dados pelo responsável, que, quando for obrigado ao respectivo apagamento, face ao exercício deste direito, terá que adoptar as medidas que forem razoáveis, incluindo de carácter técnico, ten-

---

[159] Acórdão Google Spain, C-131/12, 13 de Maio de 2014, nº 99, *apud,* Graça Canto MONIZ, *Manual de Introdução à Protecção de Dados Pessoais*,185.

[160] Graça Canto MONIZ, *Manual de Introdução à Protecção de Dados Pessoais*, 186.

[161] *As Pessoas e o Direito. Reflexões sobre o Direito das Pessoas*, Colecção da Faculdade de Direito da Universidade Agostinho Neto, Luanda, 2022, 336.

do em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efectivo dos dados pessoais de que o titular dos dados lhe solicitou o apagamento das ligações para esses dados pessoais, bem como as cópias, réplicas ou reproduções dos mesmos". O preceito que estava a ser objecto de estudo, era tratado pelos autores como estando a referir-se ao "direito a ser esquecido em linha, que se consubstancia na adopção de medidas técnicas, por parte do responsável pelo tratamento, para informar outros sítios web de que determinado titular requereu o apagamento dos seus dados pessoais"[162].

Em que circunstâncias pode este direito ser invocado? Diz o art. 28º que a eliminação dos dados pessoais ocorre quando o "tratamento não cumpra o disposto" na LPDP, ou seja, "devido ao carácter incompleto ou inexato desses dados". Esta circunstância aproxima este direito a uma informação prestada de forma clara e específica para que os dados sejam exactos e completos. Igualmente é convocado o princípio da lealdade e da transparência. Outro motivo será o facto de os dados pessoais perderem a utilidade/finalidade que serviu de fundamento para a sua recolha. Mesmo que não conste da norma referida, pensamos fazer todo o sentido, e a sua motivação dogmática foi inspirada do art. 17º, nº 1, al. *a)* da RGPD.

Há dados que não permitem o seu apagamento, constituindo um limite ao seu exercício. A primeira é a existência de uma situação de impossibilidade comprovada (art. 28º, nº 3, última parte). Ainda que a lei nada diga, consideramos estarem aqui abrangidos, como limites ao apagamento, os pedidos excessivos ou infundados. A segunda será quando haja motivos de necessidade de "prossecução de um interesse legítimo do responsável pelo tratamento, designada-

---

[162] Alexandre Sousa PINHEIRO, coord., *et al.*, *Comentários ao Regulamento Geral de Proteção de Dados*, 368.

mente para o exercício de um direito ou para o cumprimento de obrigações legais" (art. 28º, nº 5, al. *b)*). Em homenagem ao princípio da unidade do sistema e da intenção teleológica ínsita no Direito de Protecção de Dados, entendemos caber no âmbito axiológico-normativo desta norma o interesse público no domínio da saúde pública, fins de investigação científica em saúde, interesse público de estatística e arquivo de informação de saúde.

6.6 Direito à limitação do tratamento

É o direito que o titular tem de, em determinadas circunstâncias, exigir do responsável a limitação do tratamento, ou seja, os seus dados poderão ser armazenados, mas não tratados ou tratados com uma limitação. Este direito pode ser exercido mediante o contacto com o médico de estudo ou com o encarregado da protecção de dados. A LPDP não prevê este direito; fomos buscá-lo ao Direito estrangeiro, e a sua abordagem agora prende-se com a importância doutrinária e de garantia que nos oferece. Por isso, apoiando-nos na função de intenção teleológica e normativo-axiológica do direito tutelar, e para não deixar de referir a exigência metódico-intencional da juridicidade da dogmática, faremos referência ao direito extra-pátrio. Por isso, a perspectiva de trazer para esta abordagem o Direito da União Europeia deve ser vista sob duas visões: em primeiro lugar, não havendo, no direito vigente angolano, regulamentação que preveja este princípio, nada obsta que doutrinalmente se convoque um princípio consagrado além-fronteiras, desde que não seja contrário à Constituição, de modo que assim reforça o acervo de valores do catálogo de direitos, garantias e liberdades ínsitas na nossa ordem jurídica. Em segundo lugar, o direito não deixa de ser considerado vigente, ou seja, a vigência como o seu específico modo-de-ser ou específica existência histórico-comunitária do normativo, não é ine-

xistente só porque não está formalmente declarado[163].

---

[163] A. Castanheira NEVES, "Fontes do Direito: Contributo para a Revisão do seu Problema", in *Digesta*, vol. 2, Coimbra: Coimbra Editora, 1995, 55. Além do posicionamento que assumimos na esteira dos ensinamentos deste Professor de Coimbra, seguimo-lo no seu magistério. Entendo o mestre coimbrão que a experiência jurídica constituinte é constituída por três momentos: momento material, momento de validade, e momento constituinte. O primeiro momento demonstra que "nenhum direito se constitui senão em referência condicionante à realização histórico-social (a uma determinada realidade histórico-social) que bem se poderá dizer o *pressuposto material* dessa sua constituição. (…) Por outras palavras, aquele momento que, pelos factores que lhe são próprios (factores naturais e sociais, culturais e espirituais, e cada um desses tipos de factores com a sua estrutura e as suas intenções influentes), será, simultaneamente, *condição de possibilidade e de emergência, condição de adequação e de justeza, condição de relevância e de co-determinação*, e afinal, por tudo, *condição de possibilidade e de vigência do direito*. O direito é exigido por, e constitui-se para uma certa realidade histórico-social, sendo, por isso, função constitutiva dessa mesma realidade histórico-social". Um segundo momento, o de *validade*, determina que o "direito não surge todavia por mero efeito ou como consequência necessária da realidade histórico-social que o solicita, o condiciona e mesmo o codetermina, constituiu-se porque a pressuposição intencional de uma *validade* (a implicar, qualquer que seja o seu grau de determinação ou de indeterminação, um *sentido de justiça e de injustiça*, um sentido do *axiológico-normativamente valioso ou desvalioso*, ou seja, um sentido do que deve ter-se por *normativo-materialmente justificado ou injustificado*) o não dispensa como resposta normativa a problema emergente de realidade histórico-social, e emergente com fundamento justamente naquela pressuposição de validade – aliás, um problema é sempre o perguntar algo a algo *com fundamento em algo*, (…)". Concluindo, "é que não são as fontes o *prius* prescritivo da validade, mas antes a validade o *prius* constitutivo das fontes". Por fim, o *momento constituinte*. "O momento de validade enquanto tal, e ainda que na explicação de todos os seus valores e princípios, não é em si mesmo. Manifestando um fundamento axiológico e intencionando uma normatividade, não constitui só por isso uma *vigência* – o que, como sabemos, o jusnaturalismo ou a compreensão jusnaturalista da validade jurídica não teve em devida atenção. Por um lado, não impõe como necessário um certo direito, em certo direito positivo. Quanto a este último

O RGPD previu este direito no art. 18º e estabelece que o titular

ponto, não só porque o regulativo da validade admite sempre várias determinações e o direito, no cumprimento da sua função de «ordem», não dispensa uma determinação, mas ainda porque o direito positivo é função da contingente realidade histórico-social, em resposta normativa à qual se constitui. Por estas razões sempre à validade haverá de seguir-se a positividade. E a relação entre validade e o direito positivo não é, já por isso, uma relação de necessidade, mas só uma relação de possibilidade: o direito positivo não se deduz da validade normativa, deve ser perante ela possível. Por outros termos, prescindir-se, como aliás é próprio de toda e qualquer positivação dogmática, de uma constituída instituição – de uma mediação constituinte como positivação. E decerto através de uma *auctoritas* poderá garantir à determinação constituída, e não a quaisquer outras determinações possíveis ou que se não poderiam excluir em absoluto, a preferência social susceptível de sustentar a essa determinação, e não também a qualquer outra, a sua vigência. (…) Nestes termos se haverá de considerar, no global processo constitutivo do direito como direito positivo, também um momento especificamente constituinte da sua positiva normatividade – *momento constituinte* que é assim chamado a conexionar, numa particular síntese assimiladora e síntese em que o próprio positivo afinal se traduz, *ratio* e a *auctoritas*, convertendo assim o *ethos* (a validade) em *ius* (direito positivo). E se a *ratio* compete especificamente ao *momento de validade*, o *momento constituinte* põe-nos também especificamente perante a questão da *auctoritas constituinte*, a questão tanto da legitimação como dos modos legítimos da constituinte positivação jurídica. Questão cuja perspectiva de solução só pode ser esta: há que convocar a comunidade (a comunidade para a qual se constitui o direito) e a sua experiência jurídica (a experiência que nela se possa reconhecer como normativo-juridicamente constituinte), pois é a comunidade o titular originário e o destinatário último da juridicidade – bem poderíamos falar aqui de um radical «princípio democrático». Além de que, se é através da comunidade ou por referência a ela que, como vimos, se revelam as prossupostas intenções axiológicas e normativas que se impõem como o fundamento de validade do jurídico, é igualmente nela e por ela (pela adesão prática manifestada na intencionalidade do seu comportamento) que o direito vê lograda ou frustrada a sua vigência – é pela sua assimilação intencional no comportamento comunitário que o direito chega a ser um «dever-se que é», um vínculo normativo vigente".

dos dados tem o direito de obter do responsável pelo tratamento a limitação do tratamento, entre outras, nas seguintes situações: *a) contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão* ["o titular dos dados pode, concomitantemente com a apresentação de um pedido de rectificação, exigir a limitação do tratamento dos dados cuja exatidão conteste, durante a pendência de um processo de verificação dessa mesma observância"[164].]; *b) o tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização* ["a expressão ilicitude é também aqui empregue numa acepção estrita e não numa acepção ampla, pelo que o apagamento apenas poderá ser exigido quando o tratamento não surja sustentado em qualquer um dos fundamentos previstos no artigo 6º. A simples violação de um preceito do RGPD (…) ou de legislação extravagante aplicável não basta"[165].]; *c) o responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial* ["de acordo com o princípio geral da limitação da conservação (…), os dados apenas podem ser conservados, de forma a que possibilitem a identificação dos responsáveis titulares, porquanto isso for necessário à prossecução de finalidades determinadas. O responsável está, consequentemente, obrigado a apagar os dados logo que estas finalidades se encontrem esgotadas"[166].]; *d) se tiver oposto ao tratamento*

---

[164] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 286.

[165] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 286.

[166] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 287.

nos termos do artigo 21º, nº 1, até se verificar que os motivos legítimos do responsável prevalecem sobre os do titular dos dados[167][o titular dos dados pode, conjuntamente com a apresentação de um pedido de oposição, exigir a limitação do tratamento dos dados durante a pendência de um processo de oposição. (…) a obtenção da limitação do tratamento apenas pode ser requerida quando o fundamento do tratamento seja necessário para a prossecução de interesses legítimos (…) ou necessários para o exercício de funções de interesse público ou ao exercício de autoridade pública (…), desde que não existam interesses legítimos prevalecentes"[168].].

Exercido o direito à limitação, os dados pessoais objecto desse exercício, só podem ser tratados nas seguintes situações: 1) mediante consentimento do seu titular; 2) para efeitos de declaração, exercício ou defesa de um direito num processo judicial, 3) para defesa de direitos de outra pessoa singular ou colectiva, ou 4) por motivos ponderosos de interesse público (da União Europeia ou de um Estado-Membro). A única excepção que escapa a este elenco é o tratamento para conservação dos dados.

6.7 Direito de portabilidade de dados

Este direito não vem descrito na LPDP. Ao nível europeu não foi fácil a sua colocação no RGPD: apesar de ter sido reconhecido por alguma legislação sectorial, ainda assim não deixou de levantar dúvi-

---

[167] Os comentários a este preceito vêm expendidos por Carlos Jorge GONÇALVES, na obra *Comentários ao Regulamento Geral de Proteção de Dados*, 372.

[168] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 287.

das e críticas[169]. Possivelmente, encontra-se aqui algum paralelismo quanto às razões do direito e quanto à sua concretização na LPDP.

Corresponde ao direito receber uma cópia dos dados pessoais que forneceu ao médico/responsável que o atende, à farmácia que frequenta, a qualquer entidade do sistema de saúde ou ao serviço de seguro de saúde, se estiver nele inscrito. Assim, o titular poderá requerer que os seus dados sejam transmitidos tanto para si como para outra pessoa por si designada, desde que tecnicamente possível, ou seja, pode solicitar a transferência das suas informações pessoais para terceiros (como o seu médico pessoal). Com a evolução da informática e a elevada utilização de sistemas de IA, a portabilidade passou a variar, sendo possível identificar portabilidades a partir de sistemas ou de plataformas. Como bem assinala GRAÇA CANTO MONIZ[170], "neste contexto, na ausência de uma definição legal e simplificando a explicação, na portabilidade cabem os mecanismos de transmissão da informação entre diferentes sistemas de informação e de plataformas digitais".

Cumpre precisar o modo como deve a portabilidade operar. Atente-se ao seguinte exemplo: O paciente A tem os seus registos no processo clínico depositado no hospital X e pretende solicitar a portabilidade dos seus dados para o hospital Y onde pretende passar a ser assistido. Este paciente pode solicitar que os dados lhe sejam entregues no formato que lhe aprouver? A resposta apresenta-se problemática. Primeiro, não temos no nosso ordenamento jurídico indicação deste direito, mas socorrendo-nos mais uma vez da experiência europeia, o GT 29 oferece o caminho: o formato pode

---

[169] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 290. Também, Graça Canto MONIZ, *Manual de Introdução à Protecção de Dados Pessoais*, Coimbra, Almedina, 2023, 187.

[170] *Manual de Introdução à Protecção de Dados Pessoais*, 188.

"variar e será normal que assim seja, dependendo do sector de actividade em questão, e que o ideal seria existir uma colaboração entre as partes interessadas do sector e as associações [no ramo da saúde] por forma a que estes formatos sejam interoperáveis (…)"[171]. Pela natureza sensível atribuída aos dados de saúde, há razões para optarmos por propor que o formato seja uniforme quando estivermos a tratar de dados da saúde; isto minimizaria os riscos próprios do armazenamento (portabilidade), utilização e transferência dos dados. Se os estabelecimentos hospitalares forem do sector público, haverá razões bastantes para a uniformização, pois não fará sentido que dentro da administração pública haja formatos diferentes. Se a transferência ocorrer entre um estabelecimento hospitalar público e um privado, prevalecerá a importância dos dados a proteger e, sendo da saúde, será utilizado o formato mais seguro. Se for entre instituições do sector privado da saúde, o que as partes considerarem o mais seguro na interoperatividade, ocorrendo o mesmo quando a transferência for entre um hospital e uma empresa de seguros que tenha interesse nos dados dos seus clientes cuja apólice de seguro seja da área de saúde ou com ela relacionada.

É um direito associado ao direito de acesso, permitindo que os participantes tenham acesso às informações sobre eles e que um responsável pelo tratamento detém, para poderem corrigir, alterar ou excluir essas informações, quando incorretas, salvo se os encargos ou despesas de fornecimento de acesso forem desproporcionais em relação aos riscos para a privacidade do indivíduo, ou se os direitos de outras pessoas para além do titular dos dados forem violados.

---

[171] Eduardo Castro MARQUES, "Análise de direito de portabilidade e a sua (não) compatibilização com o normativo administrativo", in Isabel Celeste M. FONSECA, coord., *Estudos de E-Governação, Transparência e Proteção de Dados*, Coimbra: Almedina, 2021, 63.

Do que foi referido supra, este direito está repartido em outros três direitos, designadamente, o direito de receber os dados pessoais que tenha fornecido a um responsável pelo tratamento, o direito de transmitir esses dados a outro responsável pelo tratamento, e o direito a que os dados pessoais sejam transmitidos directamente entre responsáveis pelo tratamento. No essencial, a portabilidade dos dados tem por conteúdo a promoção do controlo dos titulares sobre os seus dados pessoais e assegura que realizam a finalidade para a qual foram recolhidos e tratados[172]. Neste sentido, assiste-lhe um *direito de interrogar* ou *direito à curiosidade*, que segundo, ANA DIAS[173], "confere ao titular dos direitos de dados o direito de interrogar o responsável pelo tratamento sobre se os dados pessoais que lhe dizem respeito são ou não objecto de tratamento". O que fundamenta este direito à curiosidade e o direito à autodeterminação informativa, que confere a qualquer titular de dados o poder de interrogar qualquer responsável pelo tratamento no sentido de saber se este tem arquivados dados relativas à sua pessoa para tratamento, ou se o tratamento está a respeitar os termos do seu consentimento[174].

6.8 Direito à oposição

É o direito de se opor ao tratamento dos dados pessoais a qualquer momento. A partir do momento da referida objecção, o responsável pelo tratamento cessa o tratamento dos seus dados pessoais. O art.

---

[172] Alexandre Sousa PINHEIRO, coord., *et al.*,, *Comentários ao Regulamento Geral de Proteção de Dados*, 376.

[173] "A Dimensão Processual da Proteção de Dados: Uma breve referência à luz do regulamento geral de proteção de dados", 10.

174 Catarina Sarmento e CASTRO, *Direito da Informática, Privacidade e Dados Pessoais*, Coimbra: Almedina, 2005, 242.

27º da LPDP determina que o titular dos dados tem direito de: *a)* se opor em qualquer altura a que os dados que lhe digam respeito sejam objecto de tratamento quando existam razões ponderadas e legítimas relacionadas com a sua situação particular, devendo neste caso o responsável excluir do tratamento tais dados; *b)* se opor ao tratamento dos seus dados em outras circunstâncias previstas na LPDP e em outra legislação específica.

De acordo com o Considerando 69 do RGPD, o legislador europeu expendeu a seguinte ideia: "No caso de um tratamento de dados pessoais lícito realizado por ser necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento ou ainda por motivos de interesses legítimos do responsável pelo tratamento ou de terceiros, o titular não deverá deixar de ter o direito de se opor ao tratamento dos dados pessoais que digam respeito à sua situação específica. Deverá caber ao responsável pelo tratamento provar que os seus interesses legítimos imperiosos prevalecem sobre os interesses ou direitos e liberdades fundamentais do titular dos dados". Este Considerando está alinhado com o disposto no art. 12º, nº 2, al. *d)* e *e)*, *ex vi* art. 27º, al. *a)* da LPDP, que impõe como requisitos gerais para o tratamento de dados pessoais e dispensa o consentimento para o efeito, bastando que ocorra: "(…) *d)* execução de uma missão de interesse público ou no exercício de autoridade pública em que esteja investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados; *e)* prossecução de interesses legítimos do responsável pelo tratamento ou de terceiro a quem os dados sejam comunicados, desde que não devam prevalecer os interesses ou os direitos, liberdades e garantias do titular dos dados". Só nestes casos é que o direito de oposição não é funcional.

Podem ser apontados dois caminhos para quem consultar um qualquer ramo da saúde, e puder concretizar este direito: *a)* um direito geral de oposição, em que se podem elencar os referentes à saúde, vida sexual, incluindo os dados genéticos; e *b)* direito de oposição relativo a tratamento para fins de investigação científica em saúde.

A investigação em saúde implica sempre a disponibilização dos dados pessoais conforme o art. 14º, nº 1, carecendo sempre do consentimento do seu titular e/ou da autorização da APD. O facto de a lei dispensar o consentimento prévio ao tratamento de dados, correspondentes ao constante no nº 2, não significa que o titular dos dados não se possa opor ao tratamento dos mesmos, bastando que a(s) finalidade(s) tenha(m) sido desvirtuada(s). Por isso, se a investigação científica tiver por meio o tratamento de dados para fins de medicina preventiva, de diagnóstico médico, de assistência médica consentida, de gestão e estatística de serviços de saúde ou quando se trate de uma emergência médica ou justificada pelo interesse público, mas a finalidade prática for outra, o titular pode também exercer o seu direito de oposição.

É igualmente atendível que o titular se oponha ao tratamento dos seus dados pessoais, quando ficar a saber que os mesmos podem vir a ser reutilizados para outros fins e ele não tenha dado o seu consentimento ou o consentimento seja dispensável, como ocorre naqueles casos em que o tratamento é realizado para os fins que não sejam aqueles para os quais os dados pessoas foram recolhidos. Nos casos de reutilização, mesmo que na primeira vez o tratamento tenha sido para a execução de uma missão de interesse público, para exercício de autoridade pública ou na prossecução de interesse legítimo do responsável pelo tratamento, o titular dos dados fica investido dos poderes ou faculdade de se opor ao tratamento.

Uma vez que haja riscos iminentes pela utilização de meios informáticos ou da IA, o tratamento automatizado de dados será sempre objecto de oposição do seu titular, desde que demonstre, tendo em atenção as particularidades ponderosas e legítimas da sua situação, que o início, execução ou conclusão do tratamento pode resultar num prejuízo.

Como o tratamento de dados da saúde, da vida sexual ou genéticos deve ser realizado apenas por profissional de saúde com registo na ordem profissional correspondente, o titular dos dados poderá

opor-se sempre que verificar que o responsável pelo tratamento não tem as qualificações legalmente exigidas, até porque, quando o responsável é a entidade legalmente legitimada, estará coberto pela obrigação legal do dever de sigilo (art. 14º, nº 3).

No tocante ao direito à oposição, ainda que não tenha consagração constitucional expressa, o seu reconhecimento na lei está valorado como manifestação da natureza pessoal do direito à autodeterminação informacional[175].

6.9 Outros direitos

No âmbito do tratamento dos dados pessoais e do nosso sistema nacional de saúde, não temos registos de conflitos dignos de serem aqui discutidos. No entanto, não há dúvidas de que há falhas graves no cumprimento de deveres legais e éticos que resultam em comportamentos ilícitos danosos. Não há, neste âmbito, lei que regula determinados deveres que se reputam importantes, pelo que vão aqui enumerar alguns, até porque há uma gritante falta de literacia nesta área. Em primeiro lugar, o direito a conhecer os direitos próprios (*right to know your rights*). O titular dos dados deve saber, preferencialmente através de suporte físico, os seus direitos. Como sabemos, além da falta de literacia, nos países como o nosso, onde há diversos problemas básicos, a questão dos direitos é muitas vezes colocada em ponto subalterno. Ainda que a CRA, a LPDP e a lei de bases do sistema nacional de saúde (lei nº 21-B/92, de 28 de Agosto) detalhem direitos dos titulares de dados pessoais e dos pacientes, a verdade é que na prática há um distanciamento alarmante.

---

[175] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 299.

O direito de comunicação (e explicação) dos direitos dos titulares de dados e dos pacientes implica que o responsável pelo tratamento tenha o dever de explicar os seus direitos e responsabilidades. Ligado a este está o direito de fazer perguntas (*right to ask questions*[176]). Relacionado com questões éticas, implica um relacionamento entre o responsável pelo tratamento e o titular dos dados que possa facilitar que este entenda bem o que vai prestar, constituindo um direito não apenas à informação, mas a questionar.

[176] Entende George D. POZGAR, que "patients should not hesitate to ask for the following: clarification of a caregiver's instructions; interpretation of a caregiver's handwriting; instructions for medical usage (e.g., frequency, dosing, drug-drug or drug-food interactions, contraindications, side effects); clarifications of a phisician's hand-washing policy; a description of the hospita's procedures to prevent wrong-site surgery; consultations and secand opinions. *Legal and Ethical Essential of Health Care Administrations*, 255.

7. RESPONSÁVEL PELO TRATAMENTO

7.1 Questões introdutórias

A LPDP oferece, no art. 5º, al. *i)*, a definição de responsável pelo tratamento: "A pessoa singular ou colectiva, a autoridade pública ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais. Sempre que as finalidades e os meios de tratamento sejam determinados por disposições legislativas, regulamentares ou outras, o responsável pelo tratamento deve ser indicado no respectivo diploma". A primeira parte do conceito deixado expresso corresponde ao constante no art. 4º, nº 7 do RGPD, que no original é tratado como *data controller*. A segunda parte transfere para lei específica a identificação do responsável, como ocorre, por exemplo, numa lei sobre tratamento de dados pessoais para efeitos de prevenção, detenção, investigação ou repressão de infracções penais; lei de protecção de dados pessoais e privacidade nas telecomunicações; lei sobre informação genética pessoal e informação de saúde, ou até mesmo uma lei sobre informação administrativa e ambiental e reutilização dos documentos administrativos, legislação que Angola não tem, mas que muita falta faz. No entanto, o que presenciamos no nosso país é a existência de determinada legislação específica, como a lei de videovigilância ou lei da procriação humana medicamente assistida, que fazem remissão para a lei geral de protecção de dados pessoais, não identificando ela mesma o responsável pelo tratamento.

O responsável pelo tratamento de dados, ou *data controller*, tem o dever de determinar os propósitos (finalidades) e os meios de pro-

cessamento de dados. Determina o porquê e o como da realização de uma operação de tratamento dos dados. Por isso, o responsável pelo tratamento de dados orienta-se pelo princípio da *accountability*, cujo conteúdo indica que ao responsável não é exigível a garantia de que a publicidade ou tratamento indevido de dados nunca ocorrerá, mas deve garantir uma prova de que cumpre com a legislação relativa à protecção de dados.

A CUACPDP define responsável pelo tratamento de dados como "qualquer pessoa singular ou colectiva, pública ou privada, qualquer outra organização ou associação que sozinha ou em conjunto com outras pessoas decida recolher e processar dados pessoais e determinar a sua finalidade".

Outra importante nota a referir sobre o conceito de responsável pelo tratamento é o facto de ser "alheio às categorias nacionais de pessoas: não releva a natureza jurídica ou a forma que em concreto assuma"[177]. A lei prefere a pessoa colectiva, e não o funcionário ou o seu representante que, nos casos concretos, é quem determina as finalidades e os meios de tratamento lícitos utilizados, o que não o desresponsabiliza dos efeitos civis, criminais ou administrativos aplicáveis em caso de violação da lei[178].

Acrescendo à importância de identificar o sujeito sobre quem recaem os deveres e a possibilidade de imputação de responsabili-

---

[177] Cfr. A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 307.

[178] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 308. Refere o autor que há uma excepção a regras anunciada: "se um trabalhador utilizar os dados para a prossecução de fins próprios ou fora do âmbito das actividades da entidade empregadora, essa pessoa singular será considerada, para todos os efeitos legais, como responsável de facto pelo tratamento. A identificação do responsável é central no processo de imputação de deveres e de responsabilidades".

dades, é fundamental ter em atenção cada caso específico. Assim, para o tratamento de dados sensíveis, o art. 13º estabelece os requisitos gerais, e o art. 14º requisitos específicos, designadamente (nº 1) consentimento inequívoco, expresso e escrito do seu titular ou do representante legal; e/ou autorização da APD. O consentimento é afastado quando (nº 2) o tratamento de dados for necessário para efeitos de medicina preventiva, de diagnóstico médico, de assistência médica consentida, de gestão e estatística de serviços de saúde, ou quando se trate de uma emergência médica ou justificada pelo interesse público[179]. O nº 3 acrescenta outra exigência: o responsável pelo tratamento de dados da saúde deve ser efectuado por um profissional de saúde com registo na ordem profissional correspondente, obrigado a cumprir o dever de sigilo profissional.

Em resumo, os deveres do responsável pelo tratamento de dados pessoais estão estruturados em duas perspectivas: uma formal, que corresponde ao dever de realizar o tratamento de dados pessoais no estrito cumprimento da legislação aplicável e, noutra perspectiva, a material, correspondendo ao dever de realizar o tratamento de da-

---

[179] O nosso país pode ser considerado como um país com um perfil epidemiológico complexo. Há muitas doenças que surgem, tendem a desaparecer e a voltar a surgir. São as chamadas doenças infecciosas emergentes e reemergentes, aquelas cuja incidência em humanos vem aumentando nas últimas décadas. O estudo sobre os problemas das doenças e o comportamento epidemiológico que vem alterar a forma de lidar com elas, mostra que podem ser previsíveis utilizando todos os dados de saúde e sociológicos que as envolvem. São os dados estatísticos dessas doenças, do surgimento de novos problemas relacionados com novos agentes infeciosos; a introdução de agentes já conhecidos em novas populações de hospedeiros susceptíveis de criar alterações importantes no padrão de manifestação de doenças só é detectável com registos de doenças anteriores e de comportamentos, tanto dos agentes infeciosos, como dos humanos receptores (hospedeiros). Daí a importância dos dados em saúde e do facto de poder ser dispensável a manifestação do consentimento para o registo e tratamento de dados desta natureza.

dos pessoais no estrito respeito pelos direitos dos titulares dos dados eventualmente afectados[180]. Sem qualquer pretensão de hierarquização, o nosso tema versa sobre dados sensíveis, aqueles ligados à saúde. Por isso, a obrigação de realização de tratamento em conformidade com as estipulações legais (formal) e, no rigoroso respeito pelos direitos à autodeterminação informacional dos titulares dos dados (material), concretiza-se da seguinte forma – art. 30ª da LPDP:

1. dever de aplicar as medidas técnicas e organizatórias adequadas, estabelecer níveis de segurança adequados, para proteger os dados pessoais contra a destruição total ou parcial, acidental ou ilícita, a perda acidental, a alteração total ou parcial, a difusão ou o acesso não autorizados (nº 1);
2. dever de aplicar as medidas de segurança que devem assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação (nº 2);
3. dever de assegurar detalhes dos níveis de segurança, os recursos a proteger e as funções e obrigações das pessoas com acesso aos dados, de acordo com as regras de segurança (nº 3).
4. o especial dever dos sistemas de garantirem a separação lógica entre os dados referentes à saúde e à vida sexual, incluindo os genéticos, dos restantes dados pessoais (art. 31, nº 2).

Cabe à APD determinar em que casos a circulação em rede de dados pessoais sensíveis – de saúde, da vida sexual, incluindo os dados genéticos, constantes do art. 14º, que possam pôr em risco direitos, liberdades e garantias dos respectivos titulares – deve a transmissão ser cifrada.

A abordagem do tratamento de dados pessoais (*risk based approach*) sobre a saúde dos seus titulares, convoca à tomada de especiais

---

[180] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 316.

diligências do responsável pelo tratamento para atender "a todo tempo e em relação a todas as decisões que tome e aos actos que pratique, aos riscos que daí possam decorrer para os titulares dos dados. Na prática, espera-se que o responsável pelo tratamento adeque a sua actuação às especificidades concretas de cada caso"[181], se dizem respeito à saúde do titular, se para efeitos gerais de saúde pública. Possivelmente, uma das medidas que o Governo deveria tomar seria a da implementação de uma Rede Nacional de Dados Pessoais de Saúde, conectada com todas as unidades pertencentes ao Sistema Nacional de Saúde. Esta proposta tem em vista a promoção da melhoria da gestão no uso da informação, das soluções da tecnologia de informação e da saúde digital, com vista a um melhor controlo dos dados dos utentes do SNS e mitigação do risco de mau uso desta informação ou publicação/transferência sem autorização devida. Seria um passo para a credibilização dos responsáveis, da protecção dos direitos dos titulares e do asseguramento de uma livre circulação do fluxo de dados. Aliás, a qualificação dos dados pessoais de saúde como "sensíveis" impõe aos responsáveis a sujeição a condições de tratamento específicas para se evitar que estes dados possam gerar processos discriminatórios.

Como não há um instrumento normativo positivado com vista a dotar os estabelecimentos hospitalares de padrões de segurança, obrigam-nos a criarem normas próprias para que as condições de atendimento e recolha de dados dos utentes estejam em conformidade com a LPDP.

A CUACPD na Secção V do Capítulo II, sob a epígrafe "Obrigações do Responsável dos Dados Pessoais", determina o cumprimento de obrigações de confidencialidade (art. 20º), devendo o proces-

---

[181] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 317.

samento de dados pessoais ser feito "exclusivamente por indivíduos que agem sob a autoridade do responsável dos dados e somente sob suas instruções"; obrigações de segurança (art. 21º), no sentido de "tomar todas as precauções apropriadas, de acordo com a natureza dos dados e, em particular, evitar que esses dados sejam alterados ou destruídos, utilizados por pessoas não autorizadas"; obrigações de conservação (art. 22º), já que "os dados pessoais não devem ser conservados para além do período necessário para o fim pelo qual se fez a sua recolha e o seu processamento", e; obrigações de manutenção (art. 23º), disposição que obriga o responsável pelos dados a "tomar as medidas necessárias com a vista a assegurar que os dados pessoais processados possam se explorados independentemente do dispositivo técnico utilizado no processo" *a)* e, o funcionário ao serviço do responsável "deve, em particular, assegurar que as mudanças tecnológicas não constituem um obstáculo para a utilização dos dados", *b)*. Em resumo, no contrato com a pessoa singular ou colectiva que a lei considera como responsável pelo tratamento deve constar *(i)* o objecto, a duração, a natureza e a finalidade do tratamento de dados, *(ii)* o tipo de dados objecto de tratamento, *(iii)* a categoria de titulares de dados em processo de tratamento e, *(iv)* obrigações e direitos do responsável (*data controllers*).

A Convenção da União Africana elenca um princípio muito importante atinente à actuação do responsável pelo tratamento: o princípio da responsabilidade, obrigando-o ao dever de demonstrar que a sua actuação está em conformidade com a lei, com os demais princípios gerais sobre o tratamento de dados, atendendo a que os dados pessoais foram obtidos e tratados de forma lícita, justa e, na medida do possível, transparente, sem deixar de fora a salvaguarda de segurança.

7.2. O subcontratado

É também tratado como *data processor* pelo RGPD. Regulado na LPDP, está expresso no art. 23º, sob a epígrafe "comunicação

de dados a subcontratado". Mas no art. 21º, está determinado que, caso ocorra a comunicação de dados pessoais pelo responsável a um destinatário, este fica adstrito às seguintes regras:

a) se os dados pessoais forem comunicados ao destinatário para efeitos de prossecução de finalidades próprias deste, o destinatário será considerado também responsável pelo tratamento dos mesmos, devendo cumprir as disposições legais que lhe são aplicáveis; Nesta alínea não se regista a separação funcional e de assunção de responsabilidades entre responsável e subcontratado. Se considerarmos como critério de distinção as finalidades que cada uma das figuras segue no âmbito do tratamento de dados, então, se os dados comunicados ao subcontratado forem para fins distintos do responsável, aquele será considerado igualmente responsável.

b) se os dados pessoais forem comunicados ao destinatário para efeitos de prossecução das finalidades do responsável que comunica os dados, tratando o destinatário os dados em nome e em representação do responsável, o destinatário é considerado um subcontratado, devendo cumprir as disposições legais que lhe são aplicáveis; O subcontratante é uma figura distinta do responsável, pois é diferente materialmente e do ponto de vista formal. Como o preceito indica, o subcontratante (destinatário) realiza o tratamento dos dados em nome e no interesse do responsável, assumindo a titularidade de uma posição fiduciária[182]. Desta forma, terá de existir um acordo que estabeleça um vínculo entre ambos, em que o subcontratado fica obrigado a cumprir o disposto na LPDP

[182] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 309. Veja-se também o nosso *Negócio Fiduciário, Caracterização, Constituição e Efeitos*, Coimbra, Angolanae Dissertationes, 2019,418 e 469 seg.

e a actuar de acordo com as instruções do responsável pelo tratamento e notificar a APD (art. 23º, nº 1); se assim não for, fica o subcontratado obrigado a não comunicar os dados pessoais a outros destinatários, a cumprir as medidas e níveis de segurança estabelecidas na lei e a destruir os dados pessoais ou devolvê-los ao responsável pelo tratamento finda a relação convencional (nº 2). Com estas obrigações, ao subcontratado fica vedada a possibilidade de realizar o tratamento de dados pessoais para finalidades próprias; tãopouco pode comunicar a outros destinatários, sob pena, caso o faça, de ser considerado responsável pelo tratamento dos mesmos (nº 3).

c) *se os dados pessoais forem comunicados ao destinatário, não se verificando nenhuma das condições constantes dos pontos anteriores nem estando este sob autoridade directa do responsável pelo tratamento ou de subcontratado, o destinatário será considerado terceiro.* Já quando os dados são comunicados para um destinatário que não seja subcontratante, manda a lei qualificá-lo como terceiro, exigindo que haja consentimento do titular dos dados e notificada a APD (nº 1, art. 23º). Este artigo impõe as circunstâncias em que a comunicação de dados é feita a um subcontratado: *a)* conclusão de contrato ou outro documento com valor jurídico, reduzido a escrito, cujo conteúdo estabelece a obrigação de o subcontratado cumprir o disposto na presente lei e actuar de acordo com as instruções do responsável pelo tratamento; *b)* notificação à Agência de Protecção de Dados. O nº 2 impõe obrigações ao subcontratado, salvo se o responsável pelo tratamento o instruir de forma contrária: *a)* obrigação de não comunicar os dados pessoais a outros destinatários; *b)* obrigação de cumprir as medidas e níveis de segurança estabelecidas na presente lei; *c)* obrigação de destruir os dados pessoais ou de devolvê-los ao responsável pelo tratamento finda a relação contratual.

Está vedado ao subcontratado o tratamento dos dados pessoais para finalidades próprias, nem os pode comunicar a outros destinatários em desrespeito às suas obrigações legais, sob pena de, caso o faça, ser considerado responsável pelo tratamento dos mesmos (nº 3). Significa que o subcontratado actua em nome e sob comando ou instruções do responsável pelo tratamento dos dados.

Não será assim, dispensado o consentimento, quando a comunicação de dados de saúde decorra da lei ou de decisão judicial, ou verificadas as condições que legitimam o tratamento de dados pessoais sem consentimento do seu titular, nos termos do art. 13º, nº 1, al. *b), iii)* e nº 2, bem como do art. 14º, nº 2.

Pode haver responsáveis conjuntos pelo tratamento. Quando o tratamento de dados pessoais em saúde é realizado com a intervenção de mais do que um sujeito, ela é considerada conjunta; aliás, da definição legal de responsável pelo tratamento, extrai-se que "a pessoa singular ou colectiva, autoridade pública ou qualquer outro organismo que, individualmente ou *em conjunto* (…), se vai apresentando como um facto comum e com tendência para aumentar. É o que se regista com grupos de sociedades, organizações matriciais, *outsourcing* ou colaborações mais ou menos formais"[183].

A LPDP trata da disciplina do tratamento conjunto no art. 24º, cuja epígrafe é "Interconexão de dados pessoais". O primeiro requisito para a sua concretização é a autorização da APD (nº 1). Em segundo lugar, a autorização referida só pode ser dada se a interconexão *a)* for adequada à prossecução das finalidades legais ou estatutárias e dos interesses legítimos dos responsáveis pelo tratamento; *b)* não implicar discriminação, lesão ou diminuição dos

---

[183] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 311. O autor fortalece o seu posicionamento com indicação de bibliografia alemã. Itálico nosso.

direitos liberdades e garantias fundamentais dos titulares e; *c)* estiver rodeada de adequadas medidas e níveis de segurança (nº 2). É ainda exigível que todos os responsáveis contribuam com o mesmo empenho, podendo-se ainda algumas vezes registar que cada um dos responsáveis pode estar envolvido em etapas diferentes do tratamento, com excepção do momento da determinação das finalidades e dos meios, que deve ser feita por todos.

A determinação do tratamento conjunto deve ser firmada por acordo ou outro documento com valor jurídico, reduzido a escrito, cujo conteúdo estabeleça a obrigação de o outro responsável cumprir o disposto na LPDP. É um corolário do princípio da transparência e o conteúdo do acordo deve ser levado ao conhecimento dos titulares de dados objecto de tratamento.

8. TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS

A transferência internacional de dados é enquadrável no âmbito da aplicação territorial da LPDL, conforme o art. 3º, nº 2. A regra é a de considerar que o tratamento é, em princípio, realizado no território angolano (l. *a)*) nos seus navios ou aeronaves militares, conforme dispõe o art. 24º, nº 2 do CC. No entanto, pode ocorrer quando o responsável realiza o tratamento dentro do território angolano, mas tenha a sua sede no estrangeiro, fora de Angola, em local onde a legislação pátria seja aplicável por força do direito internacional público ou privado, ou o responsável pelo tratamento é uma entidade sem estabelecimento fixado em Angola, faça recurso aos meios situados em território angolano para realizar o tratamento.

A transferência internacional de dados para países que asseguram um nível de protecção adequado está sujeita a notificação à APD (art. 33, nº 1). O entendimento que deve haver é o de que um país (de destino ou da fonte da transferência dos dados) assegura um nível de protecção adequado quando o mesmo garanta, no mínimo, um nível de *protecção igual* ao estabelecido em Angola (nº 2). Ser igual é um critério difícil de estabelecer, mas parametrizar segundo os requisitos estabelecidos para o tratamento de dados no nosso país é um critério mais razoável e equilibrado. As realidades legislativas, organizatórias, políticas, culturais e sociais dos países são diferentes, o que impossibilita a exigência de igualdade para a transferência de dados.

Parece que o nosso legislador foi longe de mais. E este critério embate com o que a própria norma do nº 2 reforçada com a do

nº 3 do artigo em referência estabelece: "cabe à Agência de Protecção de Dados decidir se um Estado assegura um nível de protecção adequado, mediante a emissão de parecer a este respeito". Como se constata, "igual" é diferente de "adequado". Naquele significa o que tem a mesma natureza, dimensão, quantidade, qualidade e duração de protecção. Já "adequado" significa que corresponde exactamente a um objectivo ou situação, que se ajusta ou se adequa com a protecção requerida. Assim, a bitola de comparação a ser utilizada pela APD, na materialização da protecção da transferência internacional de dados e da aplicação do decisor judicativo na resolução de conflitos, é a adequação das medidas de segurança cujo nível detenha correspondência com o nível adequado às medidas de segurança em Angola. O nosso posicionamento é reforçado pelo conteúdo do nº 4 do mesmo artigo: "a adequação do nível de protecção de dados num Estado é apreciada pela APD em função" (i) "de todas as circunstâncias que rodeiam a transferência ou o conjunto de transferências de dados", (ii) "atendendo em especial à natureza dos dados, à finalidade do tratamento ou tratamentos projectados", (iii) "aos países de destino final", (iv) "às regras de direito, gerais ou sectoriais, em vigor no Estado em causa", (v) "incluindo as regras profissionais" e (vi) "as medidas de segurança que são respeitadas nesse Estado". Fica a discussão esclarecida.

Nos casos em que os países de destino dos dados a serem transferidos não assegurarem um nível de protecção adequado, deve haver autorização da APD, mas só quando verificadas, especialmente quanto a dados referentes à saúde, as seguintes circunstâncias (art. 34º, nº 1): o consentimento inequívoco, expresso e escrito do titular dos dados; se a transferência for realizada ao abrigo de acordos internacionais em que Angola é parte; a transferência de dados terá de ter por finalidade exclusiva a resposta ou pedido de ajuda humanitária; se a transferência for necessária para proteger interesses vitais do titular dos dados, ou para prevenção, diagnóstico ou tratamento médico e o titular estiver física ou legalmente incapaz de declarar o

seu consentimento; se a transferência de dados for realizada a partir de uma fonte acessível publicamente e; se o destinatário dos dados assegurar contratualmente, perante o responsável pelo tratamento, um nível de protecção adequado aos dados transferidos.

Devido aos cuidados que merece o tratamento de dados pessoais, a sua transferência merece cuidados redobrados. Por isso, a lei estabelece formalidades para notificação e obtenção de autorização junto da Agência de Protecção de Dados. Desde logo, a regra geral é a de que o tratamento de dados pessoais está sujeito a notificação prévia à APD. Existe a *mera notificação* (nº 2, art. 35º) segundo a qual a Agência de Protecção de Dados deve pronunciar-se sobre o pedido do responsável pelo tratamento no prazo de trinta dias após a sua recepção, findo o qual se entende que o tratamento foi devidamente notificado. Também se fala da *notificação simplificada ou isenção da notificação* – nº 3 – utilizada para determinadas categorias de tratamento que, atendendo às especificidades dos dados, não sejam susceptíveis de pôr em causa os direitos, garantias e liberdades fundamentais dos seus titulares, atendendo aos critérios de celeridade, economia e eficiência. A autorização de isenção deve, entre outras questões, especificar as finalidades do tratamento, os dados ou categorias de dados a tratar, a categoria ou categorias de titulares dos dados, os destinatários ou categorias de destinatários a quem podem ser comunicados os dados e o período de conservação dos dados (preservando sempre a igualdade e a não discriminação).

Se a finalidade do tratamento de dados for unicamente a manutenção de registos que se destinem a informação do público e possam ser consultados pelo público em geral ou por qualquer pessoa que provar um interesse legítimo, não se colocam as condicionantes referidas *supra*. É o caso, por exemplo, dos dados anonimizados cujo tratamento tem por finalidade estabelecer elementos estatísticos sobre endemias, epidemias ou pandemia, ou estudos sobre mortalidade e morbilidade por doenças infeciosas (veja-se, em continuidade do exemplo, a relação existente entre epidemiologia e saúde públi-

ca). Esta recebe daquela explicações para problemas de saúde das populações, permitindo-lhe definir quando e como agir, quais os hipotéticos cenários de evolução dos problemas, facilitando os decisores a optarem por um posicionamento assente em diferentes pressupostos, pois, normalmente, nestas circunstâncias já se encontram municiados com mais informação/dados das pessoas e das populações, "capacitando-os a formular juízos decisórios com um maior nível de consciência, de compreensão e de intervenção quanto ao que se está a passar, tanto pelos profissionais, como pela população"[184], ou os chamados "dados abertos", aqueles em que qualquer pessoa pode ter acesso, usar, modificar ou partilhar livremente, para qualquer finalidade, preservando-se a sua origem e abertura. Acaba por ser um dos corolários do princípio da transparência da governação digital, pois constitui uma metodologia de publicação de dados do governo em formatos reutilizáveis. A política de dados abertos conta com regulamentação jurídica na EU – Directiva 2019/1024, que estabelece o quadro geral das condições de reutilização de dados e documentos do sector público, cujas vantagem têm sido apontadas como a transparência e responsabilização, escrutínio democrático; instituições mais eficientes e eficazes, procuram o acesso a dados mais facilitados, interoperatividade de sistemas; maior credibilidade das decisões, políticas públicas mais informadas, esclarecidas e sustentadas; respostas mais rápidas e adequadas em contextos de crise e; desenvolvimento económico.

O conteúdo das notificações e dos pedidos (art. 36º) deve conter as seguintes informações: nome e endereço do responsável pelo tratamento ou do seu representante; a finalidade a que se propõe para o tratamento dos dados, determinando-a, que seja explícita e

---

[184] Teodoro BRIZ, "Epidemiologia e Saúde Pública", *Revista Portuguesa de Saúde Pública*, Número Especial 25 Anos (2009) 31-50.

legítima; descrição da ou das categorias de titulares dos dados e dos dados ou categorias de dados ou categorias de dados pessoais que lhe respeitem – para o nosso estudo valerá a categoria de dados relacionada com a saúde, vida sexual e genéticos, garantindo-se assim a reserva da vida privada, bem como os direitos, liberdades e garantias públicas fundamentais; destinatários ou categorias de destinatários a quem os dados podem ser comunicados e em que condições, valendo aqui as entidades cujo tratamento de dados de saúde interessa e a garantia do princípio da veracidade; caso não seja o responsável a realizar o tratamento dos dados, deverá ser informada a identidade da entidade encarregada pelo processamento; eventuais interconexões de tratamento de dados pessoais; tempo de conservação dos dados pessoais, como manifestação do princípio da duração do período de conservação, pois os mesmos devem ser conservados de forma a permitir a identificação dos seus titulares apenas durante o período necessário à prossecução das finalidades que originaram a sua recolha ou tratamento; forma e condição como os titulares dos dados podem exercer os seus direitos, para que não sejam prejudicados, valendo aqui como princípio fundamental a dignidade da pessoa humana; transferências de dados previstas para países terceiros; descrição geral que permita avaliar de forma preliminar a adequação das medidas tomadas para se garantir a segurança do tratamento.

A já referida Directrizes da OCDE para a Protecção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais estabelece um conjunto de princípios, também já referidos, que devem ser aplicados a nível nacional, mesmo em contexto de movimento de dados pessoais além das fronteiras nacionais. Na Parte V, relativa à cooperação internacional, determina que "os países Membros devem, quando exigido, levar a conhecimento dos outros países Membros detalhes sobre a observância dos princípios definidos nestas Directrizes. Os países Membros também devem assegurar-se de que os procedimentos relativos aos fluxos transfronteiriços de dados pessoais e à protecção da privacidade e da liberdade individual sejam

simples e compatíveis com os dos outros países Membros que respeitam estas Directrizes. Os países Membros devem estabelecer procedimentos para facilitar: *(i)* a troca de informações relacionadas com estas Directrizes, e *(ii)* o auxílio mútuo nos assuntos processuais e de investigação envolvidos".

9. PARTILHA DE DADOS ENTRE RESPONSÁVEIS DE DADOS PESSOAIS

A questão mais problemática, e já deixada referida quando tratámos do consentimento, designadamente do interesse público, é a partilha de dados entre responsável do sector público e responsável do sector privado. Os requisitos convocados para uma melhor abordagem sobre a questão são o da transparência, da necessidade e da finalidade. Não voltaremos a explicá-los, pois já discorremos bastante sobre os mesmos ao longo do trabalho. Na verdade, o compartilhamento de dados pessoais entre entidades públicas e privadas pode decorrer da necessidade de regular o exercício de diversas actividades e políticas públicas na área de saúde. É o caso, por exemplo, da necessidade de criação de um banco de dados de doadores de órgãos, tecidos e células, bem como para doadores de sémen para a procriação humana medicamente assistida.

A exigência aqui válida será a existência de uma previsão legal, o respaldo num contrato, convénio ou instrumento equiparável, onde constem a finalidade e sua necessidade de partilha.

10. DISPOSIÇÕES ESPECÍFICAS APLICÁVEIS AO TRATAMENTO DE DADOS PESSOAIS NO SECTOR PÚBLICO

A Secção VIII do Capítulo II, sobre o tratamento de dados, estabelece normas específicas em matéria de tratamento de dados pessoais sobre saúde no sector público. Nos termos do art. 39º, neste sector e no cooperativo, o tratamento de dados está sujeito *a)* às disposições constantes na LPDP e *b)* ao disposto nas regras especiais constantes desta secção e de legislação especial.

O tratamento de dados no sector público não deve estar dissociado da reforma geral da Administração Pública, a que têm sido atribuídas muitas denominações, designadamente *eGovernment*, *E-Digital Public Services*. A implementação da digitalização da Administração Público é o ponto central da reforma, e a protecção de dados pessoais um pilar importante. O Código do Procedimento Administrativo prevê, no art. 19º, o princípio da administração digital. Este artigo descreve a possibilidade da prática de actos administrativos por meios digitais para tornar a gestão mais simples e rápida, com acesso dos interessados à informação e ao procedimento de forma ágil (nº 2). Determina também que os meios digitais devem garantir a integridade, conservação, confidencialidade e segurança da informação (nº 4). Por fim, a utilização de maios digitais por parte da administração pública não pode ser feita de modo a lesar direitos e garantias dos particulares (nº 6).

A recolha e prestação de informação da administração pública constitui uma missão fundamental para a proximidade às populações. Já referimos a questão dos dados abertos e a sua vantagem. Remetemos para lá todo o que aqui poderia ser dito.

A informação é um activo que oferece à Administração os *inputs* necessários para a criação e implementação de políticas públicas, dado que a centralidade da informação, apresentada como dados pessoais, tem implicações no processo de Governação Pública Digital e da Protecção de dados Pessoais. A sua harmonização é um imperativo teleológico. Aliás, o acesso das entidades públicas aos dados pessoais em grandes bases de dados (*Big Data*) é inquestionável, assim como o tratamento computarizado em larga escala para a obtenção de padrões e ligações (*profiling*). Também podemos mencionar a utilização de algoritmos preditivos para notação das pessoas utentes dos serviços públicos, e a internet das coisas, geram dados cuja capacidade de mensuração não será em *gigabytes*, mas em *zettabytes* ou *yobibytes*, o que por si só manifesta os riscos associados, reclamando da parte da administração pública uma autorresponsabilidade baseada no referido risco[185].

Com os níveis de digitalização (muito residual, neste momento) que a administração pública angolana tem, as dificuldades sentidas durante a pandemia da Covid-19 por parte de funcionários e agentes administrativos despertou a necessidade de se enveredar pelo caminho da digitalização, tendo sido aprovados vários instrumentos jurídicos sobre a matéria, destacando-se o teletrabalho. A digitalização do funcionamento da administração pública implica um alto grau de responsabilização e segurança, como já referimos, pois implica, neste ambiente, a conservação e confidencialidade da informação que transita nestes meios de trabalho. Assim, a criação, modificação e eliminação de ficheiros da Administração Pública, dos Tribunais ou de outros órgãos com competência, apenas podem ser efectuadas

---

[185] Vasco CAVALEIRO, "A proteção de dados no contexto do vínculo do emprego público", in Isabel Celeste M. FONSECA, coord., *Estudos de E-Governação, Transparência e Proteção de Dados*, Coimbra: Almedina, 2021, 73.

ao abrigo das disposições gerais da LPDP, ou de legislação com elas conexa, a qual deve conter expressamente ou por remissão para diploma autónomo, a seguinte informação (art. 40º, nº 1 – LPDP): *a)* o responsável pelo tratamento; *b)* as finalidades do tratamento; *c)* os processos de recolha e tratamento dos dados pessoais; *d)* a estrutura básica do ficheiro; *e)* os tipos de dados incluídos no ficheiro; *f)* as comunicações de dados a destinatários, caso aplicável; *g)* a transferência de dados para países terceiros, se aplicável; *h)* os serviços ou unidades perante os quais os titulares dos dados podem exercer os seus direitos; *i)* as medidas de segurança aplicáveis, incluindo mediante a indicação de critérios de acesso discriminados, se aplicável. Caso a Administração Pública decida pela eliminação de ficheiros, deve indicar o destino dos mesmos ou dos seus dados e as medidas a adoptar para a sua destruição (nº 2). É uma exigência compreensível e aceitável, tendo em consideração a necessidade de garantia ético-axiológica da nossa pessoalidade vista na nossa comunitária intersubjectividade, justamente numa sociedade mais falível do que parecia, na qual não está tudo dado por garantido, e onde o que ontem foi certo pode hoje ser errado ou incerto e amanhã poderá ser normal ou socialmente certo.

A comunicação de dados pessoais por órgãos da Administração Pública (art. 41º), não pode ser feita para outras entidades, organismos, serviços ou outros que tenham competências materiais distintas, salvo nas seguintes circunstâncias: *a)* tal comunicação é permitida por disposição legal ou autorização pela APD e, *b)* a comunicação tenha por objecto o tratamento posterior dos dados para fins históricos ou estatísticos.

Foi aprovada a Agenda de Transição Digital da Administração Pública, pelo Decreto Presidencial nº 178/24, de 31 de Julho. Como a APD é superintendida pelo Titular do Poder Executivo que pode delegar ao Departamento Ministerial responsável pelo Sector das Telecomunicações e Tecnologias de Informação, vamos consultar o que esta Agenda prevê para este Departamento Ministerial. Con-

tém três grandes projectos, e cada um deles tem vários objectivos. No projecto com a identificação 457TDAP.IMA.27, importa referir um objectivo: "Melhorar a segurança das comunicações, garantindo a privacidade e a confidencialidade das informações transmitidas". No Projecto 456ATDA.IMA.27, os objectivos são: "Implementar dois centros de dados para suportar a Infraestrutura, Cloud do Governo de Angola, construir uma infra-estrutura de TIC confiável e uma nuvem de Governo unida como pilares e motores para capacitar a nova era do governo digital. (…)". Por último, o Projecto 455ATDAP.IMA.27 prevê como objectivos "Construir e apetrechar um Centro de Resposta e Segurança Cibernética. (…)". Estando em causa o estudo de protecção de dados pessoais na saúde, vamos verificar de que é que o Ministério da Saúde foi beneficiado. Foram três projectos. O primeiro, com a identificação 409ATDAP.IMA.27, tem por objectivos "Implementar um cadastro único do utente, permitindo uma identificação precisa e unificada dos pacientes em todo o sistema de saúde; facilitar a comunicação entre as diferentes plataformas de gestão hospitalar, garantindo uma troca de informações eficiente e segura; promover uma maior partilha de informação entre os profissionais de saúde, melhorando a coordenação e a qualidade dos cuidados prestados aos pacientes". O Projecto 405ATDAP.IMA.27 tem por objectivos: "garantir o *backup* de todas as informações geradas pelas diversas unidades sanitárias; servir como local de *disaster recovery* em casos de interrupção de serviços em qualquer unidade; actuar como *failover* de qualquer unidade sanitária em caso de indisponibilidade de serviços; ser um ponto de sincronização de informação para as diferentes unidades". Estes desafios são importantíssimos para uma gestão eficiente, mas a implementação de medidas de segurança e dos princípios de protecção de dados pessoais é um imperativo, pois o Governo passará a ter sob sua posse uma quantidade considerável de dados dos utentes das diversas unidades hospitalares, podendo disponibilizá-los sob o formato de anonimato ou de dados abertos.

Já reflectimos sobre os princípios fundamentais do tratamento de dados pessoais no geral. Para o sector público, os princípios que importa elencar são quatro: o da legalidade, da transparência, da necessidade e da finalidade, que podem ser encontrados na LPDP e também no Código de Procedimento Administrativo. Neste instrumento legislativo, o fim precípuo desta questão é o mesmo da LPDP, pois constituirá um forte mecanismo de defesa dos titulares dos dados, mas também uma obrigação da administração pública de proceder sem violação dos direitos das pessoas. Vamos atender aos princípios constantes neste último diploma[186].

O *princípio da legalidade* (art. 14º): impõe que os órgãos da administração pública devem agir em obediência à lei, dentro dos limites dos poderes que lhes forem conferidos e em conformidade com os respectivos fins. É um princípio com uma função eminentemente garantística, assente na ideia do Estado de Direito. Legalidade corresponde a uma exigência de exercício do processamento de dados pessoais, tendo como *standard* a racionalidade jurídico-dogmática do dever de tutela por parte do responsável pelo tratamento[187], o que significa que o princípio da legalidade imputa à legislação uma

---

[186] Veja-se as explicitações doutrinárias que Luís Manuel PICA nos oferece em As Garantias dos Contribuintes no Tratamento dos Dados Pessoais pela Administração Tributária, Coimbra, Almedina, 2025, 24-34. Os valores da aplicação dos princípios jurídicos relativos à protecção de dados pessoais na esfera pública, designadamente na Administração Fiscal, valem para o nosso tema.

[187] A. Castanheira NEVES, "O princípio da legalidade criminal", in *Digesta*, vol. 1, Coimbra: Coimbra Editora, 349-473. O autor desenvolve o seu pensamento sobre o princípio da legalidade no âmbito do direito criminal. Diz o professor de Coimbra que "(…) com os valores jurídicos formais da legalidade concorrem as intenções jurídicas materiais dos fundamentos axiológicos, com a justiça generalizante da juridicidade abstracta oferecida pela lei a justiça individualizante só susceptível de conseguir-se na judicativa decisão concreta", cfr. nota 57,366.

"prerrogativa juridicamente constitutiva e mesmo uma «reserva de lei»" em matéria de protecção de dados pessoais, sem desmerecer a função judicial, "a qual só se cumpre na problematicamente concreta e normativo-materialmente adequada realização do direito"[188].

O *princípio da transparência* (art. 30º): determina que os órgãos da administração pública devem prosseguir a realização do interesse público com visibilidade, lisura, respeito do acesso à informação e sua divulgação[189].

O *princípio da necessidade* apresenta dois planos: um primeiro, resultante do facto de a administração pública ser o guardião da prossecução do interesse público (art. 16º). Este desiderato implica, num segundo plano, imposição à administração pública da obrigação de continuamente adoptar regras e procedimentos de segurança e privacidade dos titulares dos dados.

---

[188] A. Castanheira NEVES, "O princípio da legalidade criminal", 367.

[189] Este princípio tem concretizações que importa indicar, conforme apontou Ana Flávia MESSA, "Transparência na Gestão Pública", in Isabel Celeste M. FONSECA, coord., *Estudos de E-Governação, Transparência e Proteção de Dados*, Coimbra: Almedina, 2021, 175-204. Para a autora, a primeira concretização está na "expansão electrónica", que é "a ampliação do governo electrónico, permitindo a acessibilidade dos cidadãos ao governo não como um fim em si mesmo, mas para garantir o uso inclusivo e pedagógico para os cidadãos; depois, a "expansão da responsabilidade" entendida como a "expansão do conceito de responsabilização de um processo de prestação de contas que permite o acompanhamento público da atuação administrativa, visando reduzir a assimetria informacional entre o gestor público e os cidadãos, e aumentar o controle social sobre a eficácia, eficiência e efetividade das estruturas administrativas"; em terceiro lugar, "expansão participativa", que significa "dar vozes aos cidadãos e às suas comunidades, transformando-os em agentes ativos na produção de bens públicos"; por fim, a "expansão da anticorrupção" cujo entendimento requer a combinação entre "elementos preventivos e repressivos no combate da corrupção, com a cooperação sistemática da sociedade civil (…) e o emprenho de instituições oficiais (…) no aumento da eficácia de suas ações", 201.

Por fim, o *princípio da finalidade* (art. 16º), segundo o qual os órgãos da administração pública devem prosseguir o interesse público em todos os seus domínios de actuação, no respeito pelos direitos e interesses legalmente protegidos dos particulares.

Do que resulta da Agenda de Transição Digital da Administração Pública e dos princípios acabados de referir, a grande importância ao nível do fim e do conteúdo assenta a sua *ratio*, na necessidade de protecção dos dados pessoais, sustentada pela tutela da dignidade da pessoa humana, particularmente do direito à privacidade.

11. TUTELA ADMINISTRATIVA E JURISDICIONAL

11.1 Aspectos gerais

O acesso ao direito e a tutela jurisdicional efectiva vêm consagrados no art. 28º da nossa Constituição, dispondo o nº 1 que "a todos é assegurado o acesso ao direito e aos tribunais para defesa dos seus direitos e interesses legalmente protegidos, não podendo a justiça ser denegada por insuficiência dos meios económicos". Este preceito não é um motor que por si só faz movimentar toda a engrenagem. Necessita de *inputs*. O primeiro deles é o acesso à informação por parte dos cidadãos (nº 2), e o segundo um sistema de procedimentos judiciais céleres, prioritários e executados em tempo útil (nº 4 e 5). Na verdade, se consultarmos o comum dos cidadãos sobre o estado do acesso à justiça (quer graciosa, quer jurisdicional), a resposta não poderá distanciar-se da ideia de que ela é lenta, cara, incompreensível e imprevisível. Por isso, quando falamos do acesso ao direito e aos tribunais não podemos apenas invocar os dispositivos legais de garantia. Devemos avaliar o estado de disponibilidade de informação e patrocínio judiciário para aqueles que pretendem defender seus direitos e interesses com tutela legal, avaliar se estão garantidas as condições para que as decisões judiciais sejam tomadas em prazo razoável e mediante processo equitativo. Enquanto direito fundamental, deve assegurar-se a sua vinculação axiológica à *Res Publi-*

ca[190], afastando-se da concepção formal dos direitos fundamentais, que vê as pessoas como sujeitos abstratos, quando nelas devemos reconhecer a existência de um "substracto axiológico e uma densidade normativa de valor"[191].

A LPDP veio reforçar a tutela dos direitos de personalidade, pois definiu com alcance muito relevante aspectos substantivos, designadamente os que definem os direitos dos titulares de dados, as obrigações dos responsáveis pelo tratamento (incluindo os subcontratantes), assim como as condições de responsabilização civil, contraordenacional e, muito especificamente, criminal. Também há que assinalar o elemento orgânico-institucional, que ditou as questões que estabelecem o perfil, as atribuições e os poderes das autoridades nacionais de controlo, nomeadamente a APD e os tribunais, os mecanismos de cooperação e controlo entre as autoridades congéneres (para uma melhor, segura e confiável transferência de dados)[192].

Quanto à matéria da tutela dos direitos do titular do direito dos dados, em síntese, podemos agrupá-los em:

a) direito de apresentar reclamação (ou outras garantias graciosas admissíveis) à autoridade de controlo (APD);

b) direito à acção judicial contra a autoridade de controlo;

c) direito à acção judicial contra um responsável pelo tratamento ou um subcontratante.

---

[190] Ana Raquel Gonçalves MONIZ, *Os Direitos Fundamentais e a Sua Circunstância,* 51.

[191] Ana Raquel Gonçalves MONIZ, *Os Direitos Fundamentais e a Sua Circunstância,* 51.

[192] Cfr. José Duarte COIMBRA, "Contencioso da Proteção de Dados", in Tiago SERRÃO / José Duarte COIMBRA, coord., *Contencioso Administrativo Especial*, Lisboa: AAFDL Editora, 2021, 389 seg.

O sistema de protecção de dados pessoais encabeçado pela LPDP, para além de relevantes normas de âmbito substantivo (como as que tutelam os direitos dos titulares de dados pessoais, as obrigações dos responsáveis pelo tratamento/subcontratantes e, também, as condições de responsabilidade civil, contravencional ou até criminal) e orgânico-institucional (principalmente as que estabelecem o perfil, as atribuições e os poderes da ANP), assim como os mecanismos de cooperação e de controlo de transferência de dados, não colocou de fora a previsão de importantes mecanismos de tutela administrativa e jurisdicional, para garantir a efectividade da operacionalização do seu regime substantivo. Por isso, a tutela dos direitos constantes da LPDP e de outra legislação com ela conexa, concentra os "mecanismos de *enforcement* do Direito da Protecção de Dados"[193], novo marco de referência da construção dogmática dos direitos de personalidade ou dos direitos fundamentais. Uma nova zona de tutela dos direitos das pessoas relacionadas com os fenómenos ligados ao impacto das tecnologias de comunicação e informação no tratamento dos dados e na capacidade de se transformar num activo económico da maior importância. Utilizando as palavras de Filipa Urbano Calvão, afirmamos que "em especial, a perceção de que a utilização de tecnologia para recolher, conservar e analisar informação relativa às pessoas, por facilitar o relacionamento da informação e permitir conservar e relacionar mais informação, importava domínio sobre a informação relativa a outrem, máxime pelo poder público, com riscos acrescidos de afetação da privacidade e de gerar discriminação, o que, no conjunto, se revela suscetível de condicionar o livre-arbítrio e as liberdades individuais"[194].

---

[193] José Duarte COIMBRA, "Contencioso da Proteção de Dados", 391.

[194] Filipa Urbano CALVÃO, "O regime de proteção de dados pessoais e os desafios na sua aplicação", "O regime de proteção de dados pessoais e os desafios

11.2 Tutela Administrativa

A tutela administrativa corresponde à possibilidade de qualquer pessoa apresentar queixa à Agência de Protecção de Dados, de acordo com os meios administrativos, para garantir o cumprimento das disposições em matéria de protecção de dados pessoais, conforme dispõe o nº 1 do art. 47º.

O CPA, aprovado pela lei nº 31/22, de 30 de Agosto, estabelece a reclamação e o recurso administrativo. O art. 235º estabelece o princípio geral de que "os interessados têm o direito de solicitar a revogação, suspensão ou modificação de actos administrativos que os afectem, bem como reagir contra omissão ilegal, em violação do dever de decidir solicitando a prática do acto pretendido (…)". Daqui decorrem importantes constatações normativas: desde logo, aquela que em está em causa a sindicância de acções e omissões imputáveis as entidades "materialmente públicas", ou seja, que desempenham funções administrativas, ficando por isso de fora do âmbito da reclamação ou do recurso hierárquico a actuação ou omissão imputáveis a entidades privadas. Depois, o objecto de recurso aos instrumentos de reclamação ou recurso incide sobre as actuações ou omissões em questão, e devem traduzir a emissão ou não de actos administrativos ou normas regulamentares (como por exemplo a adopção, pelo responsável do tratamento de dados, de "(…) pôr em prática as medidas técnicas e organizativas e estabelecer níveis de segurança adequados (…)" (art. 30º, nº 1 da LPDP). Por fim, a legitimidade para apresentar reclamações ou interpor recursos administrativos

---

na sua aplicação", *Privacidade e Dados Pessoais: Revista do Centro de Estudos Judiciários* 2 (2023) 5.

não se limita aos titulares de dados pessoais, mas assiste a "qualquer pessoa", conforme dispõe o art. 47º, nº 1, da LPDP.

Perante a estrutura garantística dos direitos dos particulares, as duas formas de processos são a reclamação e o recurso: no primeiro, o titular dos dados pode pedir ao autor do acto lesivo que reaprecie, solicitando a sua revogação, anulação, modificação ou substituição. Trata-se, no fundo, de um apelo a quem proferiu a decisão; no segundo, o titular dos dados de saúde pede a outro órgão, situado hierarquicamente acima do órgão que praticou o acto, para que o aprecie.

Na norma do CPA a que acabamos de aludir, na sua última parte existe o direito do titular dos dados de reagir perante os casos de omissão ilegal de actos administrativos, quer reclamando quer apresentando recurso hierárquico. Este direito é consequência da existência, por parte da Administração Pública, do dever de decidir, consagrado na CPA, no art. 24º, "princípio da decisão", segundo o qual, nº 1, "os órgãos administrativos têm, (…) o dever de se pronunciar sobre todos os assuntos da sua competência que lhes sejam apresentados pelos particulares e, nomeadamente: *a)* sobre os assuntos que disserem directamente respeito aos requerentes; *b)* sobre quaisquer petições, reclamações ou queixas formuladas em defesa da Constituição, das leis ou do interesse público". O nº 6 dispõe claramente que "a omissão do dever de decidir é judicialmente impugnável".

Com a descrição feita supra, podemos concluir que a LPDP não é autossuficiente, necessitando de uma remissão inter-sistemática para se apoiar no CPA com a intenção de realizar a justiça. Nestes termos, na convocação dos mecanismos constantes no CPA: *a)* devem estar em causa acções e omissões imputáveis a entidades *materialmente* públicas verificáveis no desempenho da função pública, em consequência, ficam de fora a reclamação e o recurso previsto na CPA de acções e omissões imputáveis a entidades privadas; *b)* essas acções e omissões devem corresponder à emissão ou não de actos administrativos ou normas regulamentares, já que, nos termos do CPD, esse é o âmbito estrutural da reclamação e dos recursos admi-

nistrativos; *c)* diferentemente do que ocorre com a apresentação de queixa à APD, a legitimidade para apresentar reclamações e recursos não se delimita aos titulares de dados pessoais, estendendo-se a qualquer pessoa singular ou colectiva, privada ou pública, detentora de legitimidade, conforme dispõe o art. 237º do CPA: "têm legitimidade para reclamar ou para interpor recurso administrativo os titulares de direitos subjectivos ou interessados legalmente protegidos que se considerem directamente lesados pelo acto administrativo ou pela omissão". Este artigo deve ser conjugado com os arts. 89º e 90º do mesmo diploma legal.

Das decisões da Agência de Protecção de Dados cabe recurso contencioso administrativo (nº 2, art. 47º da LPDP) que será visto de seguida.

Sendo a ANP uma entidade sujeita à superintendência (art. 4º do Estatuto Orgânico da Agência de Protecção de Dados), é possível reclamar ou recorrer administrativamente dos actos e regulamentos aprovados ao Departamento Ministerial responsável pelo Sector das Telecomunicações e das Tecnologias de Informações. Funcionam aqui as regras constantes do CPA sobre a matérias.

11.3 Tutela jurisdicional

O recurso contencioso da decisão tomada pela APD segue na sala do cível e administrativo do tribunal de comarca e o seu procedimento é o constante no CPC.

A protecção eficaz da privacidade deve incluir mecanismos que garantem a conformidade com os princípios da protecção de dados pessoais, o recurso para as entidades a quem se referem os dados afectados por não-conformidade com os princípios e as consequências para o responsável quando os princípios não são seguidos. No mínimo, tais mecanismos devem incluir *a)* estarem prontamente disponíveis e acessíveis mecanismos de recurso independentes pelos quais as queixas de cada indivíduo e as disputas são investigadas e

resolvidas com referência aos princípios e indemnizações, caso a lei aplicável ou as iniciativas privadas o prevejam; *b)* procedimentos de acompanhamento para verificar se as afirmações que as empresas fazem sobre suas práticas de privacidade são verdadeiras e foram implementadas, tal como apresentado; *c)* a obrigação de resolver os problemas decorrentes de não cumprimento dos princípios por responsável anunciando a sua adesão às obrigações do responsável e as consequências para este.

Retomando o nosso posicionamento inicial que considera a protecção dos dados pessoais como direito com dignidade constitucional, então devemos concordar com GOMES CANOTILHO[195] em que o princípio do acesso ao direito e aos tribunais constitui um dos pilares guardiães do regime geral dos direitos fundamentais. Este princípio merece ser olhado com uma ampla visão pois, visa não apenas garantir que as pessoas tenham acesso aos tribunais, mas abrir aos cidadãos a possibilidade continuada de uma defesa dos seus direitos e interesses legítimos protegidos por lei por meio de um acto jurisdicional.

A garantia mais forte de defesa dos dados pessoais é o "direito à protecção jurídica através dos tribunais"[196]. O tribunal competente para a realizar a protecção requerida bem como a forma de processo está já legalmente definido. O princípio em alusão oferece subprincípios, ou corolários, nomeadamente o direito a um processo justo, direito a uma protecção jurisdicional adequada, direito a uma decisão fundada no direito e direito à execução das decisões dos tribunais.

De resto, o art. 47º, que estatui o direito à tutela jurisdicional, determina que "qualquer pessoa, nos termos da lei, [pode] recorrer a

---

[195] *Direito Constitucional e Teoria da Constituição*,433.

[196] J. J. Gomes Canotilho, *Direito Constitucional e Teoria da Constituição*, 492.

meios (…) jurisdicionais para garantir o cumprimento das disposições legais em matéria de protecção de dados pessoais". Este direito tem assento na CRA, nomeadamente no art. 29º.

11.4 Pressupostos

11.4.1 Exclusão da culpa

Durante muito tempo os modelos de responsabilidade civil tiveram na culpa a sua "coroa". Com o desenvolvimento das várias áreas da vida e da sociedade, surgiu uma discussão sobre se a configuração do instituto é suficiente para responder às novas realidades.

De outro lado, no plano probatório, as dificuldades de o titular dos dados pessoais carregar o ónus e assim conseguir demonstrar os elementos de imputabilidade pela complexidade dos meios tecnológicos empregues nos processos de recolha, tratamento e armazenamento de dados, e pela complexidade de interpretar a aplicabilidade das regras e princípios que a ordem jurídica oferece, podem enfraquecer a posição do lesado e, em consequência, enfraquecer também a culpa como pressuposto da responsabilidade civil. Por outro lado, a necessidade ética axiológica de ressarcir um determinado tipo de danos, independentemente de culpa, tem constituído factor de disrupção da dogmática da responsabilidade civil no geral.

11.4.2 Ilicitude

Como já anunciámos, o art. 47º da LPDP determina um âmbito de aplicação não fechado: admite a propositura de acções de responsabilidade civil por qualquer violação "para garantir o cumprimento das disposições legais em matéria de dados pessoais".

A ideia central é a de que, no difícil processo do cumprimento da LPDP, o responsável pelo tratamento dos dados pessoais deve orientar-se pelo princípio da *accountability*, de acordo com o qual

não é exigida ao responsável a garantia de que não existirá uma fuga ou tratamento indevido de dados. O que se exige é a garantia de que o responsável conseguirá provar que cumpre com as leis, ou seja, que o tratamento dos dados está coberto pela garantia protectiva em conformidade com a LPDP, designadamente, que os dados pessoais foram recolhidos de forma legítima e estão limitados às finalidade pré-definidas; que os dados pessoais estão actualizados, seguros e confidenciais; que tem e aplica políticas, procedimentos, códigos de conduta e instruções internas formalizados e capazes de serem disponibilizados às entidades de supervisão (Agência de Protecção de Dados); que possui sistemas para monitorar a aplicação das políticas e medidas de segurança e procedimentos[197].

Há aqui duas situações que reclamam mais desenvolvimento: a primeira é que a ilicitude nos casos sobre tratamento de dados pessoais é constituída pela exigência do cumprimento de um dever legal, devendo assim ser assinalada a existência de um comportamento contrário à ordem de conduta, independentemente de ter cometido com dolo, enquanto representação e vontade de realizar o referido resultado proibido ou praticado o acto com negligência, enquanto violação do cuidado objectivamente imposto. Na segunda, deve atender-se ao resultado, pois a lei (art. 48º) exige que deve haver "prejuízo moral ou patrimonial" pelo uso indevido de dados pessoais. A locução utilizada pela lei, "uso", deve ser interpretada de forma ampla, ou seja, como o processo de tratamento de dados, desde a recolha, processamento e o seu armazenamento.

A ilicitude pressupõe a lesão da protecção de dados pessoais, o que significa a violação de direitos de personalidade. Mas apresenta

---

[197] Filipa Matias MAGALHÃES / Maria Leitão PEREIRA, *Regulamento Geral da Proteção de Dados. Manual Prático.* 3.ª ed., revista e atualizada, Porto: Vida Económica, 2020, 37.

uma questão que foge ao princípio geral em matéria de ilicitude, tornando-se problemática no debate doutrinário, pois "é contrário ao plano do *dever-ser* que a personalidade de alguém seja ofendida"[198]. Não havendo consentimento para o tratamento dos dados, o problema da ilicitude não se colocará, pois haverá ainda assim tratamento dos dados pessoais quando a conduta do lesante corresponder ao exercício de um direito (o tratamento de dados ser necessário à declaração, exercício ou defesa de um direito em processo judicial e ser efectuado exclusivamente com essa finalidade (art. 13º, nº1, al. *b)*, *(v)*) ou ao cumprimento de um dever (quando o tratamento for necessário para efeitos de medicina preventiva, de diagnóstico médico, de assistência médica consentida, de gestão e estatística de serviços de saúde, ou quando se trate de uma emergência médica ou justificada pelo interesse público – art. 14º, nº 2). Estaremos perante uma "defesa por excepção de direito material, a excepção do exercício de um direito ou do cumprimento de um dever, que exige uma ponderação de interesses que têm de ser pesados uns em face dos outros"[199].

Afinal a ilicitude exprime uma decisão sobre o comportamento, pelo que é exigível a um dever de conduta, cuja violação vai determinar o desvalor da conduta ao espoletar a produção do resultado proibido: o "prejuízo moral ou patrimonial". A contrariedade do comportamento à ordem de conduta imposta ao responsável estabelece uma diferença entre ofensas dolosas e ofensas negligentes. Nas violações dolosas, o responsável prevê a realização do *iter* causal necessário ao nascimento do resultado ilícito que visa alcançar, e então o "desvalor ético inerente ao dolo de resultado implica a consumpção axiológica do desvalor associado à contrariedade do com-

---

[198] Pedro Pais de VASCONCELOS*, Direito de Personalidade*, Coimbra: Almedina, 2006, 136.

[199] Pedro Pais de VASCONCELOS*, Direito de Personalidade*, 136.

portamento à norma [a legislação sobre protecção de dados], sendo, portanto, falho de sentido jurídico fazer sobressair a oposição a um comportamento que foi imposto para prevenir um dado resultado quando, afinal, se queria realizar esse preciso resultado"[200]. Age com culpa, violando por exemplo o dever objectivo de informar ou o dever de segurança, o responsável pelo tratamento cujo procedimento fica aquém do *standard* técnico de actuação exigível ao profissional médio, nas circunstâncias do caso concreto.

Nas violações negligentes, o responsável pelo tratamento não age como querendo a produção do resultado ilícito. Apenas pode ser-lhe imputado quando se registar discrepância entre a conduta devida e a conduta efectivamente desenvolvida. Assim, enquanto o juízo de ilicitude dolosa está visível pela discrepância entre a vontade e o resultado, para cuja realização o comportamento foi mero instrumento de acção, ou seja, o responsável adoptou voluntariamente o comportamento ilícito como meio para alcançar o resultado querido, o juízo de ilicitude negligente exige sempre uma comparação entre conduta devida e conduta adoptada, já que não é possível fundamentar a imputação do resultado ao responsável com base na intenção de o produzir. Nestes termos, apenas pode o decisor, na sua actividade judicativa, afirmar o ilícito negligente se estabelecer a contrariedade entre a conduta imposta pela lei (LPDP) e a conduta efectivada pelo responsável, pois ocorreu uma violação de um dever objectivo de cuidado (correspondente à violação de várias medidas de segurança estabelecidas na lei).

---

[200] Rui Paulo Coutinho de Mascarenhas ATAÍDE, *Direito da Responsabilidade Civil*, Coimbra: GestLegal, 2023, 157.

11.4.3 Dano

A LPDP (art. 48º) prevê a ocorrência de danos morais e patrimoniais. Há danos que não entram na equação do ressarcimento em matéria de violação do tratamento de dados, designadamente os danos contra as pessoas, ou seja, os danos de relação, aqueles que atingem o relacionamento social, afectando de forma indirecta a capacidade da vítima em obter rendimentos de caracter laboral. O dano biológico, como a lesão à integridade físico-psíquica, medicamente comprovável, com repercussões prejudiciais de carácter extrapatrimonial. O dano existencial, que não tendo nada a ver com a integridade físico-psíquica. O dano como perda de chance, como o prejuízo reparável segundo os processos gerais de imputação, não implicando entorse às regras da responsabilidade civil. Não se trata de ressarcir o prejuízo sofrido em consequência do resultado negativo final, mas o dano provocado pela perda da possibilidade de obter essa vantagem.

Quanto à diversidade de relações entre as pessoas susceptíveis de causar danos, há uma heterogeneidade material dos mesmos, o que leva a responsabilidade civil a trabalhar com um conceito amplo de dano[201]. Daí a necessidade de delimitar a sua abordagem no presente estudo, pois trata-se só de questões sobre tratamento de dados pessoais. Nestes termos, a responsabilidade civil deve ser um instrumento protector dos dados pessoais[202] pois o direito à protecção de da-

---

[201] Rui Paulo Coutinho de Mascarenhas ATAÍDE, *Direito das Obrigações*, vol. I, Coimbra: GestLegal, 2023,401.

[202] Rafael de Freitas Valle DRESCH / Lílian Brandt STEIN, "A Responsabilidade Civil como Mecanismo de Incentivo à Observância do Direito Fundamental à Proteção de Dados: Uma Análise da Interpretação do art. 42º e Seguintes da LGPG", *Revista de Direito da Responsabilidade*, Coimbra, 5 (2023) 978.

dos funciona, em relação a outros direitos, como um guarda-chuva, nomeadamente o direito à identidade, direito à igualdade, direito à honra, direito à privacidade, o que nos conduz a considerar a possibilidade de surgirem danos patrimoniais ou danos não patrimoniais[203].

Poderá interrogar-se sobre a natureza patrimonial dos dados pessoais; o seu valor económico justifica essa reflexão. O armazenamento e processamento de enorme quantidade de dados – *Big Data* – têm permitido que grandes empresas os explorem para os mais diversos fins (económicos), apoiados por meios tecnológicos com elevado desenvolvimento, ao ponto de ter-se dito que "o recurso mais valioso do mundo [já] não é o petróleo, mas os dados"[204].

Como já referido, o art. 48º da LPDP prevê o "prejuízo moral ou patrimonial". Atenta a intenção normativa espelhada no RGPD, particularmente no considerando 85 e no art. 82º, que dispõem haver "(…) danos materiais ou imateriais às pessoas singulares (…)" e "qualquer pessoa que tenha sofrido danos materiais e imateriais (…)", respectivamente, parece podermos fixar dogmaticamente que, em consequência da violação de dados pessoais, verificados os devidos pressupostos da responsabilidade civil e atendendo às especificidades da teleologia da protecção de dados, os danos podem ser patrimoniais ou não patrimoniais, cujo ressarcimento desenvolveremos mais adiante. Os danos ocupam um ponto fulcral no âmbito da estrutura e operacionalização da responsabilidade civil, pois, atendendo às suas finalidades, a reparadora está alicerçada nos danos e serve de fundamento à função preventiva, no sentido de prevenir futuros danos.

---

[203] Mafalda Miranda BARBOSA, "O problema do ressarcimento dos danos não patrimoniais", *Revista de Direito da Responsabilidade*, Coimbra, 5 (2023) 183.

[204] Leonardo Valverde Susart dos SANTOS, "Compensação de danos não patrimoniais causados pela violação de normas de protecção de dados pessoais", *Revista de Direito da Responsabilidade*, Coimbra, 4 (2022) 955 seg.

Na verdade, quando falamos de danos, estamos a referir a repercussão negativa de uma lesão de um direito ou interesse na esfera jurídica de um sujeito concreto. No entanto, não há uma absoluta relação paralela entre natureza do bem jurídico atingido e a natureza do prejuízo sofrido, ou seja, os danos não patrimoniais podem resultar da violação de direitos de natureza patrimonial ou da violação de direitos de natureza pessoal; assim, os danos patrimoniais podem ser o resultado da violação de direitos de natureza pessoal ou de lesão de direitos de natureza patrimonial. É certo que a lesão de determinados direitos pessoais produz necessariamente danos não patrimoniais, já a violação de direitos patrimoniais pode ou não dar causa a um dano não avaliável monetariamente[205]. Como explicita Mafalda Miranda Barbosa[206], "a emergência de danos não patrimoniais explica-se como resultado da dimensão axiológica do direito subjectivo que, para lá do seu conteúdo concreto, apresenta uma ligação estreita à pessoa, à qual vai buscar o seu sentido e fundamentos últimos. Mas pode explicar-se, igualmente, noutras situações, pela preterição de uma ou mais faculdades inerentes ao conteúdo do direito subjectivo violado. Se no primeiro caso somos confrontados com os danos morais (propriamente ditos), a traduzir-se em dores, angústias, ansiedade, sofrimento; no segundo, lidamos com danos extrapatrimoniais (de que aqueles são apenas uma categoria)".

Como referido anteriormente, a LPDP admite a existência de duas modalidades de danos: a patrimonial e a não patrimonial. Como podem elas ser operacionalizadas no contexto de protecção de dados de saúde, vida sexual e dados genéticos?

---

[205] Mafalda Miranda BARBOSA, "O problema do ressarcimento dos danos não patrimoniais", 183.

[206] "O problema do ressarcimento dos danos não patrimoniais", 183.

Comecemos pelos danos não patrimoniais. Nos termos do art. 496º, nº 1 do CC, os danos não patrimoniais são reparáveis desde que, pela sua gravidade, mereçam a tutela do Direito. O decisor deve fixar a indemnização em termos equitativos (art. 496, nº 4) tomando em atenção não só a extensão dos danos causados, mas também o grau de culpa do agente, a situação económica deste e do lesado e as circunstâncias do caso.

Tendo em atenção a intencionalidade normativa que nos oferece a LPDP, a determinação do dano relevante para a tutela reparatória indica o sentido personalista do Direito que defendemos. Logo, a função reparatória da responsabilidade civil abrange a protecção das pessoas singulares como parte frágil (atente-se na relação íntima com outros direitos, como o direito à identidade, à igualdade, à honra e ao bom-nome, à privacidade e à intimidade), não só quando são objecto de recolha e tratamento por parte de instituições com um poder organizatório e tecnológico que nos tempos presentes vai aumentando o seu potencial de intrusão na esfera de intimidade e privacidade das pessoas, mas fundamentalmente porque a pessoa é centro do Direito, a sua estrutura ético-axiológica constitui o princípio e o fim da nossa ordem jurídica. Nada espanta que os danos que possam surgir da violação da esfera física, material e espiritual da pessoa mereçam tutela jurídica. E mais, a utilização económica e a circulação internacional dos mesmos exigem o asseguramento de regras de defesa dos titulares dos dados pessoais e de reparação dos danos. Neste quadro, impõe-se a atenção sobre os danos não patrimoniais, uma vez que os danos causados aos titulares de dados de saúde, vida sexual e genéticos são em quantidade superior aos danos patrimoniais[207]. A LPDP nada indica para as situações em estudo,

[207] O que não significa que, do ponto de vista do valor monetário, os danos não patrimoniais possam valer mais do que os danos patrimoniais. Aliás, no nosso

como deve o decisor proceder em casos de danos não patrimoniais, devendo, pensamos, fazer-se recurso às coordenadas metodológicas do art. 496º CC, em homenagem ao princípio da harmonia e segurança do sistema.

Não há grandes dificuldades sobre a reparação dos danos patrimoniais, mas relativamente aos danos não patrimoniais grandes são as divergências doutrinárias a apontar. Porque os primeiros são considerados economicamente avaliáveis em dinheiro. O art. 564º CC é elucidativo. O nº 1 designa os danos emergentes e os lucros cessantes. "Os primeiros correspondem aos prejuízos sofridos, ou seja, à diminuição do património (já existente) do lesado; os segundos, aos ganhos que se frustram, aos prejuízos que lhe adviriam por não ter aumentado, em consequência da lesão, o seu património"[208]. Mas há que ter em atenção que as questões de avaliação pecuniária podem resultar de danos subsequentes de um dano primário. Veja-se o que o acórdão do Supremo Tribunal de Justiça de Portugal[209] expende: "(…) lesão corporal sofrida em consequência de um acidente de viação constitui um dano real ou dano-evento, designado por dano biológico, na medida em que afecta a integridade físico-psíquica do lesado, traduzindo-se em ofensa do seu bem 'saúde'. Trata-se de um 'dano primário', do qual podem derivar, além das incidências negativas não susceptíveis de avaliação pecuniária, a perda ou di-

sistema jurídico, ao contrário dos sistemas do *common law*, os danos não patrimoniais nunca são determinados por valores altos.

[208] Pires de LIMA / Antunes VARELA, *Código Civil Anotado*, vol. I, 4.ª ed., revista e actualizada, colab. M. Henrique Mesquita, Coimbra: Coimbra Editora, 1987, anotação ao art. 564º, 579.

[209] Acórdão de 06 de Dezembro de 2017, *apud,* Henrique Sousa ANTUNES, Anotação ao artigo 564º, in José Brandão PROENÇA, coord., *Comentário ao Código Civil, Direito das Obrigações em Geral*, Lisboa: Universidade Católica Editora, 2018, 563.

minuição da capacidade do lesado para o exercício de actividades económica, como tais susceptíveis de avaliação pecuniária".

Depois de um longo caminho para ultrapassar a questão da admissibilidade dos danos não patrimoniais e definir quais os critérios, a fundamentação dogmática da sua afirmação foi a consideração axiológica dos danos, ou seja, e tomando de empréstimo as palavras de SINDE MONTEIRO[210], "a consciência jurídica actual exige para as pessoas um tratamento diferente do reservado para as coisas", pois estão em causa valores morais ou espirituais relativos à pessoa e sua família, à sua dignidade, sua saúde, honra e bom nome, liberdade e bem estar.

Ultrapassada a primeira barreira, seguiu-se a discussão – e não tem sido pacífica – sobre quais os danos não patrimoniais que deveriam ser ressarcidos[211]. Tais danos, porque com dignidade axiológica, são a perda de prestígio, os vexames, as dores físicas, os desgostos e outros de ordem espiritual[212].

A Convenção Africana de Protecção de Dados Pessoais define danos como sendo "qualquer prejuízo à integridade ou à disponibilidade de dados, de um programa, sistema ou uma informação" (art. 1º). Os conceitos de dano devem integrar no seu conteúdo uma de duas soluções: *a)* caracterização do dano como uma consequência, pois coloca acento tónico nas vantagens ou utilidades juridicamente protegidas que deixaram de poder ser desfrutadas, ou *b)* como a

---

[210] "Reparação dos danos pessoais em Portugal", *CJ* 4 (1986) 11.

[211] Mafalda Miranda BARBOSA, "Danos não patrimoniais: apontamentos", in *Revista de Direito da Responsabilidade*, Ano 5, 2023,27-87. A autora explicita as controvérsias em torno do ressarcimento dos danos não patrimoniais e elabora uma lista de autores explicitando as diferenças de opiniões sobre o tema.

[212] Antunes VARELA, *Das Obrigações em Geral*, vol. I, 10.ª ed., Coimbra: Almedina, 2000, 601.

deterioração de certos bens ou interesses juridicamente protegidos, ou seja, como um evento[213]. O conceito que a Convenção oferece pode ser dogmaticamente criticável, pois é importante que uma determinada perda ou prejuízo seja tratada como um dano para o Direito, devendo a ordem jurídica atribuir uma protecção ao bem ou interesse do titular de dados que concretamente foi prejudicado.

O CC consagra uma solução (art. 496º), aquela que estabelece as directrizes para a compensação de danos não patrimoniais, ou seja, é uma cláusula geral que consagra a ressarcibilidade dos danos não patrimoniais. A sua operacionalização está sob condição. A primeira condição (geral) corresponde às exigências de requisitos gerais da responsabilidade civil, ou seja, que haja ilicitude, culpa do agente causador do dano. A segunda condição refere o facto de que o dano deve ser grave e que mereça a tutela do direito[214], sendo um mecanismo de exclusão de vontades indemnizatórias que correspondam a pretensões pessoais voluntariosas[215]. Na verdade, a gravidade do dano e o merecimento da tutela do direito como critério delimi-

---

[213] Guilherme CASCAREJO, *Danos Não Patrimoniais dos Familiares da Vítima de Lesão Corporal Grave*, Coimbra: Almedina, 2016, 25.

[214] Maria Manuel VELOSO, "Danos não patrimoniais", in *Comemorações dos 35 Anos do Código Civil e dos 25 Anos da Reforma de 1977*, Vol. III, Coimbra, Coimbra Editora, 2007,501, entende que o "art. 496º, nº 1, erigiu a gravidade do dano como (única) condição de ressarcibilidade".

[215] Tomás PRIETO ÁLVAREZ, "El Derecho Constitucional al Desarrollo de la Personalidad. ¿Procede Identificarlo con la Libertad General de Acción?", *Boletim da Faculdade de Direito,* Coimbra, 94/2 (2018) 1213 seg. O autor, citando a Professora Le Pourhier, entende que "(…) las sociedades post-modernas favorecen la pretensión de «transformar a *priori* en 'derecho' cualquiera reivindicación, aspiración, deseo o pulsión» de las personas. De modo que se habla – también en Francia – del fenómeno de la multiplicación de los derechos de las personas y de la familia". Neste mesmo sentido, BARBOSA, Mafalda Miranda, "Danos não patrimoniais: apontamentos",35, entende que "afastam-se, por esta

tador de indemnizar danos não patrimoniais constitui, primeiro, uma absoluta barreira a desejos ou interesses *hipersubjectivos* (que apontam para uma auto-institucionalização do estatuto jurídico de cada sujeito, um perigoso *hiperindividualismo*[216]), como o chamado *right to be wrong*[217], em que se pretende instituir um direito de "comportar-se irracionalmente", e depois abre a porta a ponderações alicerçadas na ineliminável dignidade dos bens ou interesses jurídicos ligados à pessoa humana. Não pode ser um qualquer dano não patrimonial que deve merecer reparação compensatória através da indemnização pecuniária, que dependerá sempre do arbítrio do juiz, em virtude do facto de haver uma impossibilidade em determinar o montante exacto do dano[218].

A gravidade da lesão convoca um debate adicional. O critério para aferir da gravidade que estamos a referir é o critério tendencialmente objectivo para que seja considerado não apenas o valor do bem jurídico afectado, mas também o choque ou impacto que o dano produziu na esfera de protecção do lesado, devendo o aplicador ter ainda em atenção o factor temporal quando medir o grau de censura da conduta do lesante e as dignas particularidades da situação do lesado, atinentes, *v.g.*, a vulnerabilidades de vária ordem, mas que não constitua um dano no *limiar do bagatelar*, conforme desig-

via, os danos bagatelares e aqueles que correspondam a uma suscetibilidade exacerbada do lesado".

[216] Tomás PRIETO ÁLVAREZ, "El Derecho Constitucional al Desarrollo de la Personalidad. ¿Procede Identificarlo com la Libertad General de Acción?", 1214. Adverte o autor que não devemos confundir "libertad de autodeterminarse" com "derecho general de autodeterminación".

[217] Francisco Javier Laporta SAN MIGUEL *apud* Tomás PRIETO ÁLVAREZ, "El Derecho Constitucional al Desarrollo de la Personalidad. ¿Procede Identificarlo com la Libertad General de Acción?", 1223.

[218] Adriano Vaz SERRA, "Reparação do dano não patrimonial", *BMJ* (1959) 69-111.

nação alemã *Bagatellschwelle*[219]. É a natureza do dano como grave que determina que os mesmos sejam objecto de compensação[220]. Nesta esteira, o Tribunal da Relação do Porto decidiu nos seguintes termos: "Os meros incómodos, desgostos e transtornos não merecem a tutela do direito, como danos patrimoniais"[221].

11.4.4 Nexo de imputação

A lei determina que "a obrigação de indemnizar só existe em relação aos danos que o lesado provavelmente não teria sofrido se não fosse a lesão" (art. 563º CC). Tradicionalmente tem-se imputado a esta norma a consagração legal da teoria da causalidade adequada. Não iremos seguir este caminho nem ofereceremos as justificações por considerarmos que não é aqui a sede para tal debate[222]. Preferimos seguir outro caminho, a saber, o entendimento de que a causalidade já não se baseia numa visão unitária e naturalística do nexo de causalidade, mas numa visão binária: a causalidade fundamentadora da responsabilidade e a causalidade preenchedora ou delimitadora da responsabilidade. A primeira versa sobre a relação que liga a conduta e o resultado ilícito (seja ela uma lesão ou perigo de lesão do bem ou direito tutelado), analisando-se interrogativamente se esse

---

[219] Mafalda Miranda BARBOSA, "O problema do ressarcimento dos danos não patrimoniais", 193.

[220] Capelo de SOUSA, *O Direito Geral de Personalidade*, 555. O autor defende que os danos insignificantes e cuja compensação pecuniária não se justifica, devem ser suportados por todos, pelo imperativo da adequação social.

[221] Acórdão de 23-09-2024, processo RP202409238384/20,8T8PRT.P1, encontrado em www.dgs.pt a 20 de Novembro de 2024.

[222] Entre todos, Mafalda Miranda BARBOSA, "Haftungsbegründende Kausalität e Haftungsaustüllende Kausalität: Algumas Especificações", *Revista de Direito da Responsabilidade* 4 (2002) 192-213.

resultado pode ser objectivamente imputável à conduta do lesante. A segunda, sendo consequência da primeira, estabelece o nexo entre o evento que determina a responsabilidade (facto ilícito e culposo) com o dano sofrido pelo lesado. Delimita, então, os danos que devem ser ressarcidos, determinando aqueles que foram produzidos como consequência do facto ilícito do agente (censurado objectiva e subjectivamente) e os que, não sendo resultado directo de tais factos, devam também ser reparados[223]. Exemplificando com a matéria em estudo, diríamos que, se o responsável pelo tratamento de dados de uma clínica especializada em doenças sexualmente transmissíveis não cuidar dos aspectos de segurança inerentes, e os dados se tornarem públicos, afectando a privacidade e possivelmente a honra do titular dos dados, cancelarem a realização de um negócio de venda de roupas que estava prestes a ser assinado, perguntar-se-á se ao responsável deve ser imputada responsabilidade indemnizatória pela fuga dos dados que deveriam ser confidenciais e, sendo a indagação respondida afirmativamente, saber se os rendimentos que o lesado deixou de ter pelo cancelamento do negócio também devam ser reparados ou se a namorada que o deixou por ter tomado conhecimento da sua situação de saúde causando-lhe danos psíquicos fortes deverá também se indemnizada pelo responsável.

---

[223] Veja-se, Jorge Sinde MONTEIRO, *Responsabilidade por Conselhos, Recomendações ou Informações*, Coimbra: Almedina, 1989, 240 e 270, Manuel A. Carneiro da FRADA, *Teoria da Confiança e Responsabilidade Civil*, Coimbra: Almedina, 2007, nota 291,311. Paulo da Mota PINTO, *Interesse Contratual Negativo e Interesse Contratual Positivo*, Coimbra: Coimbra Editora, 2008, 640, 924 (nota 1834), 928 (nota 2605). Mafalda Miranda BARBOSA, *Responsabilidade Civil Extracontratual: Novas Perspectivas em Matéria de Nexo de Causalidade*, Cascais, Principia, 2014,9 seg. Rui Paulo C. de Mascarenhas ATAÍDE, *Direito da Responsabilidade Civil*, pág278 seg.

As duas ligações causais encontram fundamento legal no art. 483º, nº 1, que centraliza a imputação. Transplantando para o coração deste preceito, a compreensão da estruturação binária do nexo causal torna-se clara. A norma dispõe nos seguintes termos sistemático-explicitantes: primeiro, "Aquele que (…) viola ilicitamente o direito de outrem ou qualquer disposição legal destinada a proteger interesses alheios (…)", para depois, numa segunda ligação, ordenar a indemnização dos "danos resultantes da violação". Como justificar a opção pela teoria binária da causalidade. Em primeiro lugar, a responsabilização dispensa saber se o agente deve prever os danos subsequentes, assentando na violação do direito subjectivo ou da norma de protecção de interesses alheios. O nexo de causalidade é visto como "bivalência funcional"[224], e assim não serão apenas os danos que estão directamente ligados ao facto ilícito e culposo objecto de procedimento indemnizatório, mas também os danos subsequentes, que não estão dependentes da regra do "risco geral da vida, mas sim um risco específico criado pela ofensa sofrida"[225].

11.4.5 Responsabilização

O princípio geral do direito ressarcitório é o de que "quem estiver obrigado a reparar um dano deve reconstituir a situação que existiria, se não se tivesse verificado o evento que o obriga à reparação" (art. 562º CC), sendo operacionalizado por meio da reintegração natural ou através da indemnização em dinheiro (art. 566º, nº1). Este preceito demonstra a finalidade reparadora ou indemnizatória

---

[224] António Barroso RODRIGUES, *O Concurso de Responsabilidade Civil: Ensaio sobre o concurso das modalidades delitual e obrigacional de responsabilidade civil*, 2.ª ed., Coimbra: Almedina, 2024, 201.

[225] Rui Paulo C. de Mascarenhas ATAÍDE, *Direito da Responsabilidade Civil*,280.

do instituto da responsabilidade civil. A finalidade é a de tornar indemne o sujeito que, por meio de uma acção ilícita e culposa, sofreu um prejuízo. Por meio deste mecanismo, obriga-se o lesante a colocar o lesado na situação em que estaria se não tivesse ocorrido a lesão. Deve ser visto não como um mero formalismo, que visa ser útil e eficiente numa lógica de equilíbrio custo-benefício, mas antes, numa visão axiológica da responsabilidade civil, onde impera o entendimento segundo o qual as categorias da acção e do comportamento humano são avaliáveis na base do justo (no sentido de limitar a própria responsabilidade, sendo convocável apenas quando há danos e no sentido de limitar a liberdade, que terá "de assumir um quadro de deveres de responsabilidade pelo outro, sob pena de ser responsabilizado perante o outro"[226]) e da validade axiologicamente material[227]. Neste sentido, o nexo de imputação do facto ao lesante não se baseia exclusivamente na culpa (factor subjectivo[228]), mas reconhece-se (amplamente aceite) um nexo de imputação objectiva, no sentido de resguardar as situações em que a actividade em causa potencia o risco de invasão da esfera jurídica de outrem. A abordagem do risco para atender à necessidade de responsabilização pode ser entendida pré-compreendendo o que é o risco: é referido como um eventual acontecimento perigoso que apenas pode ser previsto até determinado ponto, pelo que o risco é utilizado para que, quem tiver responsabilidades de agir num sentido, possa tomar decisões

---

[226] Angelino Gomes COELHO, "Sentido ético-axiológico da responsabilidade civil", *Revista de Direito da Responsabilidade*, Coimbra, 3 (2021) 726.

[227] Angelino Gomes COELHO, "Sentido ético-axiológico da responsabilidade civil", 727.

[228] Ensina Mafalda Miranda BARBOSA, a propósito da responsabilidade pelo risco, que "a especial perigosidade da actividade, que alicerça a responsabilidade assim pensada, é então definida com base em elementos subjectivos e objectivos". *Estudos a Propósito da Responsabilidade Objectiva*, Cascais: Principia, 2014, 126.

na base da avaliação de futuros eventos. Depois da avaliação dos eventos perigosos olhados para o futuro, os elementos constitutivos das decisões são estruturados por duas operações que, distintas, são unidas e interdependentes, designadamente, *(i)* capacidade de previsão dos eventos futuros, quer sejam negativos quer sejam positivos, e *(ii)* tomar decisões com base nos eventos pré-avaliados,[229]. A necessidade da pré-avaliação do evento futuro é que define o risco como a combinação da probabilidade de um evento e das suas consequências negativas ou positivas. Ora, o tratamento de dados pessoais, quer manual (muito pouco utilizado) quer automatizado ou com utilização da IA, oferece riscos[230].

Para que o risco em causa seja base da responsabilidade objectiva, não bastará um risco normal da vida em intercomunicação comunitária ou risco geral da vida; terá de ser um risco com uma intensidade quantitativa e qualitativa que torna determinada actividade perigosa e geradora frequente de danos, em que apenas um especialista naquela área tem as competências para poder evitar a materialização do perigo[231]. Na protecção de dados terá de ser o responsável pelo tratamento de dados, respeitando a responsabilidade pelo *especial* encargo de tomar as medidas adequadas de protecção, especialidade que deve ser compatível com uma *forte possibilidade* de ocorrer o evento perigoso e não uma *simples* probabilidade.

---

[229] Cinthia Obladen de Almendra FREITAS, "Riscos e Proteção de Dados Pessoais", *RRDIS*, Curitiba, 2/4 (2022) 225-247.

[230] Veja-se, Lilian MITROU, "Data Protection, Artificial Intelligence and Cognitive Service: is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?", *Societal Science Research Network*, Nova Yorque, 2019, 1-90. Também, Claudio NOVELLI *et al., Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity*. ArXiv Working Paper n. 2401.07348, Nova Iorque, 2024.

[231] Mafalda Miranda BARBOSA, *Estudos a Propósito da Responsabilidade Objectiva*, 126-127.

O art. 493º, nº 2 dispõe o seguinte: "Quem causar danos a outrem no exercício de uma actividade, perigosa por sua própria natureza ou pela natureza dos meios utilizados, é obrigado a repará-los, excepto se mostrar que empregou todas as providências exigidas pelas circunstâncias com o fim de os prevenir". Apesar das observações que se fazem sobre a formulação desta norma[232], e sobre a qual não

---

[232] Mafalda Miranda BARBOSA, *Estudos a Propósito da Responsabilidade Objectiva*. A autora entende que "o artigo em apreço não pode deixar de suscitar dúvidas". Justifica dizendo que "em primeiro lugar, somos conduzidos a uma ideia de perigosidade que permite esboçar – com contornos esfumados – uma esfera de risco/responsabilidade antes de haver qualquer ação por parte do putativo lesante. Isso justifica, aliás, a presunção de culpa a que somos conduzidos pela intencionalidade problemática da norma. Contudo, tal não nos condena à confusão conceptual com a responsabilidade objectiva. É que ali, contrariamente ao que sucede nesta, o sujeito tem a possibilidade de provar que empregou todas as providências exigidas pelas circunstâncias com o fim de prevenir o dano.

Em segundo lugar, se alguém viola as providências exigidas pelas circunstâncias com o fim de prevenir o dano, isto significa que esse alguém não adequou o seu comportamento ao que era expectável em face do perigo concreto. Ora, isto quer dizer que a pessoa atuou em contravenção com os deveres de cuidado que lhe eram impostos. Só que a partir do momento em que se presume que, verificado o dano, esta culpa, assim discernida, existe, isso significa que se presume, também, o desvio comportamental, ou seja, contravenção dos princípios e regras que, densificando um princípio de prevenção, recaíam sobre o sujeito.

Como condição de exclusão da responsabilidade oferece-se a prova da *exculpação* do agente. A perigosidade da atividade, a recortar um âmbito específico de relevância da hipótese normativa, justifica, em termos materiais, a solução plasmada.

Mas, ao fazê-lo, implica, *mutatis mutandis*, a compreensão da existência de um dever de prevenção do perigo que aquela atividade concreta comporta. Com a consequência de resvalarmos para a *faute*. Na verdade, como presumir a culpa daquele que sobre ele recai a obrigação de não os causar? E como desconsiderar que a preterição – ainda que não intencional – desse dever atenta contra o ordenamento jurídico, devendo, por tal, ser considerada ilícita? E, *in fine*, chegados aí, como dualizar a ilicitude e a culpa?

ofereceremos discussão, podemos dela extrair duas perspectivas de risco: uma que vê o perigo na actividade, ou seja, na prática de actividades perigosas, e outra que o vê sob o ângulo de perigosidade da coisa utilizada, quer dizer, no controlo que deve ser utilizado sobre as coisas perigosas.

Voltemos ao debate sobre questões ressarcitórias. A regra do cumprimento do comando constante do art. 562º CC é a reintegração natural, que tem primazia sobre a indemnização em dinheiro, e que só é admitida quando a reconstituição natural não for possível, não repare integralmente ou seja excessivamente onerosa para o lesante, conforme dispõe o nº 1 do art. 566º CC. Na confrontação destes comandos normativos do CC com o art. 48º da LPDP, podemos considerar que na protecção de dados o preceito cobre a intenção teleológica que as várias normas do CC prevêem. O art. 48º determina que "qualquer pessoa que tiver sofrido um prejuízo moral ou patrimonial por uso indevido de dados pessoais, tem o direito de exigir a reparação por danos sofridos por via judicial, cabendo ao juiz graduar a lesão objectivamente". Estão aqui identificados os pressupostos da responsabilidade civil: a ilicitude (… o uso indevido dos dados pessoais …) a culpa (… dolo ou negligência no uso indevido dos dados …) os danos (qualquer pessoa que tiver sofrido um prejuízo moral ou material …) e o nexo de imputação (a ligação normativa entre o uso indevido dos dados pessoais e o surgimento de danos patrimoniais e não patrimoniais).

O responsável pelo tratamento de dados está vinculado a um conjunto de deveres que, nos termos da LPDP, são as medidas de segurança, medidas técnicas e organizativas (estabelecendo níveis

---

Há quem, entre nós, sustente que o artigo 493 CC consagra o modelo da *faute* napoleónica. Contra este entendimento, muitos autores conectam o preceito com a primeira modalidade de ilicitude".

de segurança adequados), medidas especiais de segurança (no âmbito dos impedimentos de acesso, utilização de suportes, introdução não autorizada e vigilância) no sentido de evitar o "uso indevido dos dados pessoais", fazendo a demonstração de conformidade, ou dito por outras palavras, o dever de prestar contas sobre a conformidade das medidas técnicas e organizacionais, assim como a demonstração do efectivo cumprimento dos princípios constantes da LPDP; por outro lado, o responsável deve demonstrar a sua vinculação ao dever de sigilo, conforme artigos 30º, 31º e 32º da LPDP. Assim, a responsabilidade de que se trata tem duas facetas: uma primeira que corresponde ao cumprimento de deveres ("assunção de um especial encargo[233]"), e a segunda a responsabilidade civil pelo incumprimento dos referidos deveres que consubstanciam o uso indevido dos dados pessoais.

O formato metodológico para definir a estrutura de pressupostos da responsabilidade civil, como instituto capaz de reparação dos danos causados ao titular de dados pessoais, deve atender a determinadas especificidades. É neste sentido que autores brasileiros trataram de abordar este fenómeno, titulando um estudo como "responsabilidade civil como mecanismo à observância do direito fundamental à protecção de dados (…)"[234]. A protecção de dados pessoais, ainda que não contemplada expressamente na CRA, vem implícita no instituto do *Habeas Data* e configura um direito fundamental autónomo, cujo conteúdo absorve não só a privacidade e a intimidade, mas

---

[233] Neste sentido, Mafalda Miranda BARBOSA, "Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil", *Revista de Direito Comercial* (Março, 2018) 477. A autora entende que "o encarregado da protecção de dados poderá ser responsabilizado em face dos titulares dados, por violação dos deveres que lhe são impostos no quadro regulamentar".

[234] Rafael de Freitas Valle DRESCH / Lílian Brandt STEIN, "A Responsabilidade Civil como Mecanismo de Incentivo à Observância do Direito Fundamental à Proteção de Dados", 978-995.

contempla questões relativas à autodeterminação informativa, à não discriminação, abrange fins económicos, com a tutela da livre iniciativa, livre concorrência, além da protecção do consumidor (considerando o utente dos serviços de saúde). Neste quadro normativo com intenção preventiva, há que equacionar como garantir que o responsável pelo tratamento seja efectivamente incentivado a adoptar práticas que assegurem a protecção de dados. Para este desiderato a responsabilidade civil é uma solução prática[235]. Na verdade, mesmo que consideremos a força obrigatória que é própria do direito como ordem normativa, implica algo mais do que uma simples protecção de existência. O responsável pelo tratamento deve tomar os seus actos com a intencional sabedoria de justiça e de cumprimento obrigatório das regras que lhe incumbem[236].

As questões especiais apontadas, levam a uma pré-conclusão: a de que a responsabilidade no âmbito da LPDP é objectiva e especial, ainda que em determinados casos a culpa seja convocada. Desde logo, não é fundamental que haja o registo efectivo de um dano, bastando que o responsável tenha violado o comando normativo da lei. De resto, o art. 47º, que estatui o direito à tutela jurisdicional, garante a "qualquer pessoa, [que] nos termos da lei, [possa] recorrer a meios (…) jurisdicionais para garantir o cumprimento das disposições legais em matéria de protecção de dados pessoais".

A responsabilidade, vista como *accountability*, um polo da responsabilidade que tem por arena o direito público, no âmbito da

---

[235] Rafael de Freitas Valle DRESCH/ Lílian Brandt STEIN, "A Responsabilidade Civil como Mecanismo de Incentivo à Observância do Direito Fundamental à Proteção de Dados", 979.

[236] Cfr. A. Castanheira NEVES, *Lições de Introdução ao Estado do Direito*, proferidas ao curso do 1º ano jurídico de 1969-69, Coimbra, 1969, 262, na parte em que o Professor explicava a relação entre "o direito, a liberdade e a coação".

recolha, utilização e tratamento de dados pessoais, é um princípio que fundamenta a protecção de dados pessoais na ordem jurídica angolana e que obriga as autoridades públicas a cumprirem as normas e regulamentos relativos ao cargo de responsável pelo tratamento, bem como a prestar contas dos seus actos, o que constitui o contraponto do direito do titular à informação, ao acesso, à oposição e à rectificação. Este princípio estrutura a ideia de que o responsável pelo tratamento é responsável também pelo cumprimento dos demais princípios normativos sobre a protecção de dados (que nos termos gerais seria tratado como deveres especiais de cuidado), estando obrigado a provar o cumprimento (e não a garantir o seu cumprimento e a demonstrar perante o titular, a autoridade de controlo ou outra entidade, o cumprimento dos referidos princípios.

Alinha a favor deste posicionamento o facto de a lei estabelecer como um dos deveres principais do responsável o "dever de segurança", sem a qual os dados pessoais não são protegidos, conforme os artigos 30º e 31º; ou seja, a LPDP estabelece a responsabilidade objectiva especial que se registará quando se comete o ilícito por parte do responsável pelo tratamento: o incumprimento de deveres impostos pela lei (ou legislação especial sobre protecção de dados pessoais), em especial os deveres de segurança, quais sejam dever de "pôr em prática as medidas técnicas e organizatórias, e estabelecer níveis de segurança adequados", o dever de "elaborar um documento com as medidas, normas e procedimentos de segurança aplicáveis ao tratamento de dados pessoais, detalhando os níveis de segurança", entre outros que os artigos suprarreferidos estatuem[237]. Uma se-

[237] No comentário ao regulamento geral de protecção de dados da UE, mais especificamente no artigo 24º (responsabilidade do responsável pelo tratamento),Carlos Jorge Gonçalves afirma que "a primeira obrigação de aplicação das medidas técnicas e organizativas adequadas para assegurar e poder comprovar que o

gunda pré-conclusão é a de que ao responsável (e ao subcontratado) incumbe não só a responsabilidade pelos dados (ou pelo não cumprimento de um dever), também chamada *liability*, mas também a responsabilidade que deve ser assumida pela protecção dos dados de outrem, ou *role responsibility*[238].

O que se deixou dito indica que o legislador optou pelo estabelecimento da responsabilidade objectiva dos responsáveis pela colecta, tratamento e armazenamento de dados pessoais. A ocorrência eventual do incumprimento do dever geral e especial de segurança (artigos 30º e 31º), e dos princípios gerais constantes na LPDP, constitui uma forma de ilicitude, por violação de deveres *standardizados* de conduta, quer dizer, pelo incumprimento do dever de protecção dos dados pessoais. Quando esses deveres não forem respeitados, a própria lei faz espoletar a situação de incumprimento, cuja consequência é a responsabilização civil[239].

Na sequência do que acabamos de dizer, devemos compreender o sentido e conteúdo do art. 48º (responsabilidade civil no tratamento de dados pessoais) da LPDP, que dispõe nos seguintes termos: "qualquer pessoa que tiver sofrido um prejuízo moral ou patrimonial por uso indevido de dados pessoais, tem o direito de exigir a reparação por danos sofridos por via judicial, cabendo ao juiz graduar a lesão objectivamente". Ora, o responsável pelo tratamento (bem como o

tratamento é realizado em conformidade com o RGPD, tendo em conta a natureza, o âmbito, o contexto, as finalidades do tratamento dos dados, os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, e a eficácia das medidas (cfr. Considerando (74))". Alexandre Sousa PINHEIRO, coord., *et al.*, *Comentário ao Regulamento Geral de Proteção de Dados*, 396.

[238] Mafalda Miranda BARBOSA, "Data controllers e data processors", 425.

[239] Rafael de Freitas Valle DRESCH / Lílian Brandt STEIN, "A Responsabilidade Civil como Mecanismo de Incentivo à Observância do Direito Fundamental à Proteção de Dados", 982.

subcontratado) está adstrito à responsabilidade pelo tratamento de dados alheios, estruturada num espaço de controlo, normativamente ligado a especiais deveres de cuidado que quando violados fazem nascer a responsabilidade civil pela violação de dados pessoais. É aqui que o citado art. 48º entra em acção. Nele cabe a responsabilização do responsável e do subcontratante. Nos termos deste preceito, quem define os meios e a finalidade (e também estabelece as medidas de segurança) do tratamento dos dados é o responsável pelo tratamento dos dados, mas quem assumir a decisão de determinar nova finalidade, passa a estar investido na qualidade de responsável (art. 21º, nº 1). Cabe agora revisitar a responsabilidade por facto de outrem, uma vez que, além do responsável, podem também fazer tratamento de dados pessoais os subcontratados.

Como o subcontrato actua de acordo com as instruções do responsável pelo tratamento, fica também com a responsabilidade pela reparação de eventuais danos que causar, vinculada às regras da responsabilidade contratual objectiva, nos termos do art. 800º CC (actos dos representantes legais ou auxiliares). A regulamentação constante neste preceito constitui uma excepção ao regime geral da responsabilidade obrigacional, pois dispensa a culpa para responsabilizar o responsável. A justificação desta excepção funda-se no facto de que, servindo-se do subcontratado (auxiliar) para o cumprimento da obrigação do responsável (do tratamento dos dados), este amplia a sua esfera de prestação até à actividade do subcontratado (auxiliar), e assim como adquire benefícios da sua decisão, deve suportar os prejuízos inerentes à utilização do subcontratante (auxiliar). Voltemos ao art. 23º, nº 1, al. *a)* para fazermos uma conexão com a intenção teleológica e normativa do art. 800º CC. Assim dispõe: "a comunicação de dados a subcontratado só pode ser efectuada verificadas as seguintes circunstâncias: conclusão de um contrato ou outro documento com valor jurídico, reduzido a escrito, cujo conteúdo estabeleça a obrigação de o subcontratado cumprir o disposto na presente lei e actuar de acordo com as instruções do responsável pelo

tratamento". Só não será assim se o subcontratado violar o acordo, pois "não pode tratar dados pessoais para finalidades próprias, nem os pode comunicar a outros destinatários em desrespeito do número anterior, sob pena de, caso o faça, ser considerado responsável pelo tratamento dos mesmos" (nº 3) e assim ganhar estatuto autónomo de devedor obrigado a reparar os danos causados aos titulares de dados pessoais.

A convocação do art. 800º CC para a problemática responsabilizatória do responsável pela actuação do subcontratado no tratamento dos dados pessoais exige a existência de quatro pressupostos[240], designadamente: a existência de uma obrigação (do responsável para o cumprimento das regras e princípios sobre o tratamento de dados); a relação entre o responsável e o subcontratado utilizado no cumprimento (a existência de um contrato entre o responsável e o subcontrato); a actuação do subcontratado no cumprimento (as obrigações constantes no nº 2 do art. 23º) e a actuação de facto do subcontratado.

Haverá situações em que o subcontratado age como comissário do responsável. Aqui será o art. 500º CC que oferecerá o regime jurídico da relação. A relação entre responsável e subcontratado deverá respeitar aos requisitos que são apontados à relação entre os sujeitos constantes no art. 500º CC. Em primeiro lugar, é exigível que no âmbito da relação de comissão o acto praticado pelo subcontratado tenha sido praticado no exercício das suas funções, ou seja, o subcontratado tenha praticado o acto no âmbito geral das suas competências, que foram atribuídas pelo comitente/responsável. Pois bem, sempre que o subcontratado actuar fora dos poderes que lhe foram conferidos, os danos que surgirem estarão fora do quadro de previsibilidade; logo, fora do âmbito da sua responsabilidade, pois

---

240 Mafalda Miranda BARBOSA, "Data controllers e data processors", 470.

a intenção axiológica e normativa do legislador com este tipo de responsabilidade é a de "delimitar o âmbito de risco que vai repercutir no comitente"[241]. É por isso importante saber e levar em consideração se as funções atribuídas ao subcontratado potenciaram o risco de surgimento de danos, ou se os danos poderiam igualmente ter surgido, mesmo que a comissão não existisse, tendo o seu surgimento uma mera ocasião[242]. Só se fala da responsabilidade do comitente/responsável quando o acto praticado pelo comissário/subcontratado tenha sido intencional ou contra as instruções do comitente/responsável. Daí a LPDP colocar expressamente que o subcontrata-

---

[241] António Menezes CORDEIRO, *Tratado de Direito Civil Português*, II, Direito das Obrigações, Tomo III, Coimbra: Almedina, 2010, 614.

Mafalda Miranda BARBOSA entende "ser preferível sustentar, na esteira do entendimento mais restritivo, que a lesão deve ser vista como concretização do risco funcional, exigindo-se, por isso, a atuação no quadro geral de competências ou dos poderes conferidos ao comissário, com o que ficam excluídos os atos que não se inscrevem no esquema do exercício da função (que foi para o surgimento deles mera ocasião), embora se incluam os que se ligam àquela por um nexo meramente instrumental (designadamente nas hipóteses de abuso de funções). Simplesmente, para tanto, não aderimos a qualquer critério causal, assente quer na condicionalidade, que alargaria desmedidamente a responsabilidade do comitente, para além de todos os outros problemas dogmáticos que arrastaria, quer na causalidade adequada, por ser a probabilidade a que ali se alude uma verdadeira fórmula vazia para lidar com o problema". "Data controllers e data processors", 459-460.

[242] Na explicitação de Jorge Ribeiro de FARIA, *Direito das Obrigações*, actualizada e ampliada por Miguel Pestana de Vasconcelos e Rute Teixeira Pedro, vol. II, 2023, 24, "o nexo do facto ilícito com as funções de comissário deve ser interno, directo, causal. Não basta uma simples relação indirecta, externa, puramente ocasional". Veja-se também Nunes de CARVALHO, "A responsabilidade do comitente", *Revista da Ordem dos Advogados* 48 (1988) 85, que entende que "o comitente só será chamado à responsabilidade nos casos em que o ato praticado pelo comissário tenha determinado nexo causal com a comissão", não bastando "que haja uma mera conexão temporal ou local com a função".

do não pode tratar dados pessoais para finalidades próprias, nem os pode comunicar a outros destinatários em desrespeito do estabelecido convencionalmente num contrato ou num documento com valor jurídico, sob pena de, caso o faça, ser considerado responsável pelo tratamento dos mesmos. Depois, como outro requisito, a prática dos actos do comissário/subcontratado resultem em danos materiais ou morais, contanto que os mesmos ocorram no âmbito da comissão em causa. Em terceiro lugar, para que a responsabilidade objectiva do responsável exista é necessário que sobre o subcontratando recaia também a obrigação de indemnizar; quer dizer, no âmbito da comissão, o comissário/subcontratado deverá incorrer em responsabilidade, quer seja da forma delitual, quer pelo risco. Só assim o nº 3 do art. 500º é funcional: o direito de regresso do comitente/responsável, sendo que o responsável estaria, nas palavras de MENEZES CORDEIRO[243], "a exercer um direito próprio contra o comissário", pois, "na lógica do artigo 500º, a responsabilidade do comitente é uma obrigação principal. Ela funciona de modo autónomo, com regras de configuração que não equivalem, necessariamente, à imputação feita ao comissário. Basta ver que, a este, podem ser imputados danos diversos e, designadamente, danos que não se inscrevam no âmbito da comissão".

---

[243] *Tratado de Direito Civil,* vol. VIII, Direito das Obrigações, Reimpressão da 1ª edição do tomo III da parte II de 2010, Coimbra, Almedina, 2014,607- 616. Explica também este mestre de Lisboa que "a expressão 'também culpa' deve ser interpretada em sentido amplo: 'culpa' implica, aqui, 'imputação', seja qual for o título. A lei prevê a hipótese de o dano, imputável ao comitente a título de comissão, poder ser-lhe também imputado, directamente, a qualquer outro título. Surgem várias hipóteses: (i) que o dano seja imputável a ambos, comitente e comissário, a título de ilicitude e culpa; (ii) que seja imputável ao comitente, a título de culpa e ao comissário, a título de risco; (iii) que seja imputável ao comitente a título de risco, por um instituto diverso do do artigo 500º e ao comissário, a título de ilicitude e culpa ou, até, a título de risco",616.

11.5 Acção penal

Pensamos que a existência de crimes na LPDP tem como razão de ser acautelar os riscos decorrentes da utilização das novas tecnologias de informação e comunicação e da IA, aumentando a tutela dos direitos fundamentais em causa quando a abordagem é o tratamento de dados pessoais. Como temos vindo a referir, os elementos essenciais de um conteúdo informativo com referência a uma determinada pessoa singular que a possa identificar, goza de determinados requisitos protectores, designadamente serem de caracter sigiloso e carecerem de consentimento ou autorização para a sua recolha, tratamento, armazenamento, transferência e destruição. Assim, tais informações podem estar em suportes que denominamos de documento, cujas características seriam a sua inteligibilidade, possibilidade de reconhecimento do seu emitente (ou produtor) e idoneidade do próprio documento para provar um facto ou situação juridicamente relevante. O documento pode estar expresso em papel ou de forma digital, o que torna a sua utilização mais complexa, podendo ser objecto de vários crimes de falsificação e de devassa. Daí a importância da tipificação de determinados crimes. Sendo o Direito Penal um direito de *ultima ratio*, os crimes em referência só serão convocados como critérios funcionais para dirimir crimes, quando estiver em causa a indispensável protecção de bens jurídicos essenciais, protegendo de modo legítimo e punindo com autoridade estadual as ofensas aos bens jurídicos fundamentais do indivíduo e da sociedade. Como também já anotado, os dados de saúde das pessoas singulares são considerados dados sensíveis, logo, elementos informativos essenciais das pessoas singulares de natureza de bens jurídicos fundamentais.

A LPDP prevê na Secção III do Capítulo IV os "Crimes", supondo a entrada do Ministério Público enquanto titular da acção penal. De resto, está constitucionalmente consagrado no art. 186º CRA. O art. 49º da LPDP determina que o "regime sancionatório

estabelecido na presente lei não prejudica a aplicação dos regimes sancionatórios vigentes em legislação especial". Outra norma que convoca o Ministério Público a agir é a constante do art. 62º, que no nº 1 dispõe que "se o mesmo facto constituir, simultaneamente, crime e contravenção, o agente é punido sempre a título de crime". Ora, havendo crime, o Ministério Público é o titular da acção penal.

A lei prevê cinco crimes, pune a tentativa e admite a aplicação de penas acessórias. Os crimes são o *incumprimento das obrigações reguladas na lei* (omissão de um pedido de autorização à APD, fornecimento de falsas informações na notificação ou nos pedidos de autorização para o tratamento de dados pessoais, ou neste proceder a modificação não consentida; promoção ou efectivação de uma interconexão ilegal de dados pessoais) – art. 55º – cuja pena de prisão varia entre 3 a 18 meses ou multa correspondente; *acesso indevido* (quem aceder, sem autorização, a dados pessoais cujo acesso lhe está vedado, quando for conseguido através de violação de regras técnicas de segurança; tiver possibilitado ao agente ou a terceiro o conhecimento de dados pessoais e tiver proporcionado ao agente ou a terceiros, benefício ou vantagem patrimonial) – art. 56º – cuja pena vai de 6 meses a 2 anos ou multa correspondente; *viciação ou distribuição de dados pessoais* (quem, sem a devida autorização, apagar, destruir, danificar, suprimir ou modificar dados pessoais tornando-os inutilizáveis ou afectando a sua capacidade de uso) – art. 57º – cuja pena vai de 18 meses a 3 anos ou multa correspondente; *desobediência qualificada* (quem, depois de notificado para o efeito, não interromper, cessar ou bloquear o tratamento de dados pessoais, ou recusar, sem justa causa, a colaboração que concretamente lhe for exigida pela APD; não proceder ao apagamento, destruição total ou parcial de dados pessoais, ou não proceder à destruição de dados pessoais, findo o prazo de conservação estabelecido) – art. 58º – cuja pena vai até 3 anos ou multa correspondente; e o crime de *violação de dever de sigilo* (quem, estando obrigado a sigilo profissional, nos termos da lei, sem justa causa e sem o devido consentimento, revelar

ou divulgar no todo ou em parte dados pessoais, agravando a pena quando o crime é praticado por funcionário público ou equiparado, quando a informação é revelada com a intenção de obter qualquer vantagem patrimonial ou outro benefício ilegítimo, ou quando a informação revelada coloque em perigo a reputação, a honra e consideração ou a intimidade da vida privada do titular dos dados) – art. 59º – cuja pena de prisão vai até 18 meses ou multa correspondente, podendo ser agravada até 2 anos ou multa correspondente aos casos que o mesmo artigo, nº 2, estabelece.

Muitos destes ilícitos penais têm os seus conteúdos muito semelhantes aos previstos no Código Penal. No art. 438º "acesso ilegítimo a sistemas de informação e devassa através de sistema de informação"; no art. 440º "danos em dados informáticos"; e no art. 444º "reprodução ilegítima de programa de computador, bases de dados e tipografia de produtos semicondutores". Muitas vezes esta aproximação normativa entre tipos de ilícitos provoca confusão. Entendemos que por exemplo o art. 438º do Código Penal seria suficiente, pois pune todo aquele que, "sem autorização, aceder à totalidade ou à parte de um sistema de informação de que não for titular". O ilícito penal previsto na LPDP – art 56º – determina que "quem, sem autorização, aceder a dados pessoais cujo acesso lhe está vedado, incorre em crime punível (…)". Veja-se, pois, que o plano da intenção teleológica e a defesa de valores radicados na dignidade da pessoa humana, são os mesmos[244].

---

[244] Consulte-se o Acórdão do Tribunal da Relação de Évora, processo nº 679/05.7TAEVR.E2, de 05 de 11 de 2013, que no seu sumário determinou "(…) IV. O Código Penal pune no art. 193º (devassa por meio de informática) quem 'criar, mantiver ou utilizar ficheiro automatizado de dados individualmente identificáveis e referentes a convicções políticas, (…) à filiação partidária (…) à vida privada", sendo irrelevante o número de pessoas que constam no ficheiro para determinação do número de crimes cometidos, pois o tipo protege um bem jurídico

No âmbito internacional podemos apontar, ao nível de África, a CUACPDP. que oferece directrizes ou um "Quadro Jurídico" sobre a Cibersegurança que os Estados Parte devem adoptar na sua ordem interna, como normas de cumprimento obrigatório. No preâmbulo desta Convenção é dito que "Conscientes de que se destina a uma particularidade que envolve uma área tecnológica e com vista a responder às grandes expectativas de vários actores com diferentes interesses, a presente Convenção fixa as normas de segurança essenciais para criação de um espaço digital credível para as transacções essenciais, protecção de dados pessoais e luta contra o cibercrime". No Capítulo III da Convenção estabelece-se a promoção da cibersegurança e a luta contra o cibercrime, estabelecendo para o nível nacional as medidas a serem tomadas (nomeadamente, no quadro da cibersegurança nacional abrange a política nacional, a estratégia nacional; depois as medidas legais, que abrangem legislação sobre combate à cibersegurança, sobre as autoridades reguladoras nacionais, sobre os direitos dos cidadãos e sobre a protecção de infraestruturas críticas; quanto ao sistema nacional de cibersegurança, aponta-se a cultura de cibersegurança, o papel dos governos, as parcerias público-privadas, a educação e formação; no que se refere às estruturas nacionais de acompanhamento da cibersegurança, atende à gestão de cibersegurança, o quadro institucional) e quanto à cooperação internacional (que visa harmonizar as medidas legislativas, a cooperação judiciária, a troca de informações e os meios de cooperação).

---

supra-individual – a interdição absoluta do tratamento informático de determinados conteúdos. V. Entre o crime de não cumprimento de obrigações relativas a protecção de dados (do art. 43º da Lei de Protecção de Dados Pessoais), e o crime de violação do dever de sigilo (do art. 47º) verifica-se uma situação de *concurso efectivo*, pois uma coisa é *obter os dados* fora das condições legais e *incorporá-los e tratá-los* em ficheiro, outra, *publicar o conteúdo* desse ficheiro, assim violando efectivamente a privacidade de pessoas concretas". In <www.dgsi.pt> visto a 14 de Agosto de 2024.

A Convenção contém uma Secção sobre disposições penais e, no art. 29º, cuja epígrafe é "Ofensas específicas contra as tecnologias de informação e comunicação", prevê como delitos criminais "ataques contra sistemas informáticas", "violação de dados informatizados", "infracções relativas ao conteúdo" e "infracções relativas às medidas de segurança das trocas comerciais electrónicas". Uma grande novidade da Convenção é a previsão da responsabilidade penal das pessoas colectivas – art. 30º, nº 2.

A Europa tem a Convenção sobre o Cibercrime, também chamada Convenção de Budapeste, de 23 de Novembro de 2001. Este instrumento traz tipificadas condutas criminosas. Quanto ao direito penal material, refere as infracções contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos (nomeadamente, acesso ilegítimo, interceptação ilegítima, interferência em dados, interferência em sistemas, uso abusivo de dispositivos); infracções relacionadas com computadores (falsidade informática e burla informática); infracções relacionadas com o conteúdo (infracções relacionadas com pornografia infantil); infracções relacionadas com a violação do direito de autor e direitos conexos (infracções relacionadas com a violação do direito de autor e dos direitos conexos); outras formas de responsabilização e sanções (tentativa e cumplicidade, responsabilidade de pessoas colectivas)[245].

[245] Para mais desenvolvimentos da Convenção de Budapeste, veja-se Manuel David MASSENO, "Dos ataques ransamware na Convenção de Budapeste sobre o crime cibernético. Um ensaio de qualificação alternativa", "Dos ataques ransomware na Convenção de Budapeste sobre o crime cibernético. Um ensaio de qualificação alternativa", in *Privacy and Data Protection Magazine*, Lisboa, 7 (2024) 63-82. O autor mostra como é o funcionamento desta Convenção, indicando outros estudos sobre a matéria.

12. CONTRAVENÇÕES E MULTAS

No âmbito das competências do Presidente do Conselho de Administração da APD, nos termos do art. 17º, nº 2, al. *j)*, deve "aplicar medidas sancionatórias decorrentes da violação da legislação sobre protecção de dados pessoais". Na LPDP, no art. 44º, nº 1, al. *f)*, determina que compete à APD "exercer a sua função sancionatória em matéria de protecção de dados pessoais, nos termos da presente lei". É competência da APD a aplicação das multas (art. 53º, nº 1) e a deliberação da APD que determina a multa constitui título executivo (nº 2) para, em caso de incumprimento e não ser impugnada dentro do prazo legal, se socorrer dos tribunais para o cumprimento coercivo (art. 45º, 46º, al. *d)* LPDP *ex vi* art. 45º e seguintes do CPC).

Significa que à Agência de Protecção de Dados está legalmente confiada a função sancionatória, limitada à ocorrência de contravenções e multas. Assim, segundo o art. 51º, nº 1 da LPDP, constitui contravenção punida com multa em montante equivalente a moeda nacional a seguir indicadas a prática dos seguintes actos:

a) USD 75 000, 00 a USD 150 000, 00, no caso de: *(i)* incumprimento das obrigações estabelecidas nos artigos 14º (sobre os requisitos específicos para o tratamento de dados sensíveis, de saúde e da vida sexual), 15º, 16º, 17º, 20º, 30º (sobre segurança no tratamento dos dados), 31º (sobre medidas especiais de segurança) e 32º, sobre o sigilo profissional); *(ii)* incumprimento com negligência da obrigação de notificação à Agência de Protecção de Dados, ou o seu

cumprimento com prestação de falsas informações ou com inobservância do disposto na lei; *(iii)* incumprimento de ordem da Agência de Protecção de Dados para cessar o acesso às redes abertas de transmissão de dados a responsáveis que não cumpram o disposto na lei.

b) USD 65 000,00 a USD 130 000, 00, no caso de não cumprimento dos princípios gerais do sistema de protecção de dados constantes nos artigos 6º a 11º, de não obtenção do consentimento do titular dos dados para o tratamento, salvo se se verificarem as circunstâncias que o dispensem, bem como do incumprimento do disposto nos artigos 18º, 19º e 21º a 24º (sobre a comunicação e interconexão de dados pessoais).

O nº 2 do art. 51º determina que, "tratando-se de pessoas colectivas, sociedades e meras associações de facto, as contravenções previstas" e acima referidas "são agravadas no triplo dos respectivos limites". Pensamos que a teleologia deste preceito assenta no facto de que as organizações têm o dever de melhor estarem preparadas em termos de recursos humanos, técnicos e tecnológicos para o cumprimento das obrigações legais. É mais fácil uma pessoa colectiva montar uma estrutura com juristas, informáticos e engenheiros para responder aos deveres que a lei impõe. O nº 3 determina que a tentativa nas contravenções é punível.

O quadro legal sancionatório em matéria de protecção de dados pessoais pode ser distinguido da seguinte forma: em primeiro lugar, a LPDP, na parte em que são previstos delitos civis, a obrigação reparatória sustenta-se com a existência de violação de direitos absolutos ou do normativo contratual, por acções e omissões; em segundo lugar, verificamos a existência de contravenções e multas, onde a tentativa e a negligência são puníveis e, em terceiro lugar, prevê os ilícitos criminais, onde, perante o concurso de infracções, o mesmo facto pode constituir, simultaneamente, crime e contravenção.

13. SUPERVISÃO · REGULAÇÃO

13.1 Enquadramento geral

A protecção dos dados pessoais supõe a atribuição de obrigações ao responsável pelo tratamento de dados, e estes devem estar sob supervisão de uma entidade com poderes públicos, no sentido de exercer poderes de controlo. Em Angola é a Agência de Protecção de Dados, pessoa colectiva de direito público, dotada de personalidade jurídica, com autonomia administrativa, financeira e patrimonial (art. 1º do seu estatuto orgânico). Deveria ser considerada uma entidade administrativa independente; no entanto, tem uma relação de superintendência com o Titular do Poder Executivo, que pode delegar os poderes desta relação no Departamento Ministerial responsável pelo sector das telecomunicações e das tecnologias de informação (art. 4º do estatuto orgânico). Faltam-lhe determinados pressupostos para ser entidade administrativa independente, designadamente *a)* autonomia orgânica, funcional e sem direcção, superintendência e tutela administrativa do Poder Executivo; *b)* órgãos, serviços, pessoal e património próprios; *c)* autonomia de gestão pessoal; *d)* poderes de regulação, de regulamentação, de supervisão, de fiscalização e de aplicação de sanções; *e)* possibilidade de resolução de processos com base na conciliação, mediação, arbitragem e negociação, sem prejuízo de recurso aos serviços públicos ou privados especializados, nos termos da legislação em vigor (art. 6º da lei nº 27/21, de 25 de Outubro). Parece que a APD apenas exerce, no actual figurino, os poderes constantes na al. *d)*.

Falta à APD a independência, no seu sentido mais rigoroso. A sua efectivação será possível quando a superintendência não for capaz de influenciar as decisões que tomar no âmbito das suas atribuições. Para concretizar a independência desta instituição é exigível que os membros dos seus órgãos sejam também independentes e imparciais, criando assim uma zona tampão que os protege de qualquer influência directa ou indirecta do exercício das respectivas funções[246]. No entanto, o formato constitutivo da APD, que lhe concede autonomia administrativa, financeira e patrimonial, garante a sua isenção e independência exigidas pela sua função de supervisão e regulação. A existência de um regime patrimonial e financeiro equiparado aos dos entes públicos empresariais garante a autonomia da APD, que assim se vê munida de certo grau de liberdade. Além do que foi dito, não existe tutela de mérito sobre os actos praticados pelos titulares dos órgãos da APD pelo Departamento Ministerial responsável pelo Sector das Telecomunicações e das Tecnologias de Informação, que nos termos da lei exerce a superintendência.

A Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais estabelece no art. 11º o estatuto, composi-

---

[246] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 402.

O modelo europeu de protecção de dados pessoais iniciou com as *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, de 1980, que veio a culminar na *Convenção de Estrasburgo sobre a Protecção de Dados Pessoais*, também chamada *Convenção nº 108*, de 28 de Janeiro de 1981; tratou da introdução de uma autoridade independente para protecção dos dados pessoais, que veio a efectivar-se em 2001, pois, segundo o entendimento do legislador europeu, a lei por si só não era eficaz, estabeleceu através do art. 8º no nº 3 que "*Compliance with these rules shall be subject to control by an independent authority*". Cfr. Matteo COLOMBO, *Regolemento EU sulla Privacy: principli generali e roulo del data protection Officer*, Milão: ASSO/DPO, 2015, 7.

ção e organização das Autoridades Nacionais de Protecção de Dados Pessoais, determinando o nº 1, al. *a)* que "cada Estado Parte deve criar uma autoridade responsável pela protecção de dados pessoais". Na al. *b)* vem disposto que "a autoridade nacional de protecção é um órgão administrativo independente e autónomo, com a tarefa de garantir que o processamento de dados pessoais seja feito em conformidade com as disposições da presente Convenção". Significativo para a efectivação da independência deste órgão é o que consta deste mesmo artigo no nº 7º, al. *a)*, ao determinar que, "sem prejuízo das legislações nacionais, os membros das autoridades nacionais de protecção gozam de imunidade total em relação às opiniões expressas durante o exercício ou em conexão com o exercício das suas funções". A al. *b)* impõe que, "no exercício das suas atribuições, eles não recebem instruções de nenhuma autoridade".

13.2 Agência Nacional de Protecção de Dados

A Agência de Protecção de Dados (APD) é a autoridade nacional de controlo, cuja função é executar e fiscalizar o cumprimento da LPDP. A importância da APD manifesta-se no facto de ser considerada "a guardiã dos direitos dos titulares dos dados pessoais"[247].

O Conselho de Administração é constituído por sete membros e é nomeado por Decreto Presidencial do Titular do Poder Executivo (art. 11º do estatuto orgânico), cuja composição é a seguinte: três membros designados pelo Titular do Poder Executivo, dos quais nomeia o Presidente, três membros eleitos pela Assembleia Nacional e um que deve ser magistrado judicial eleito pelo Conselho Superior de Magistratura Judicial. Dos membros do Conselho Administrativo,

---

[247] A. Barreto Menezes CORDEIRO, *Direito da Protecção de Dados à Luz do RGPD,* 398.

três devem ser membros executivos, um dos quais deve ser o Presidente e quatro não executivos. Os requisitos para ser membro deste órgão são: ser uma pessoa com reconhecida idoneidade e com competência nas matérias que constituem a sua finalidade e atribuições da APD.

O estatuto da APD não contém normas que dizem respeito ao estatuto de independência requerida para um órgão desta dimensão. Apesar de o art. 13º (Duração e cessação de mandato) prever no nº 1 que o mandato do Conselho de Administração tem a duração de cinco anos renováveis por um ou dois anos, o nº 2 atribui ao Titular do Poder Executivo a competência para interromper o mandato, bastando decretar a sua exoneração a todo o tempo. Falta a garantia da inamovibilidade e da perda de mandato, que deveria estar sujeita a requisitos objectivos, como por exemplo a verificação de incapacidade ou incompatibilidade ou violação do dever de sigilo (conforme consta do art. 46º do estatuto, que determina no nº 1 que "os titulares dos órgãos da APD, respectivos trabalhadores bem como os mandatários, pessoas ou entidades qualificadas devidamente credenciadas, estão especialmente obrigados ao dever de sigilo profissional sobre os factos cujo conhecimento lhes advenha do exercício das suas funções na APD").

13.3 Competência

São atribuições da APD, nos termos do nº 1 do art. 5º do seu estatuto orgânico, *a)* "assessorar o governo na regulação, supervisão e fiscalização da aplicação das disposições legais em matéria de protecção de dados pessoais, assim como no âmbito das suas atribuições sancionar o seu incumprimento". As outras atribuições que importa referir são: *b)* "velar pelo cumprimento da legislação sobre a matéria de protecção de dados pessoais", *e)* "promover a implantação dos códigos de conduta no âmbito da protecção de dados pessoais", *g)* "apreciar e pronunciar-se sobre a transferência internacional de dados pessoais, nos termos da legislação em vigor". Além do estatuto orgânico, a LPDP também dispõe sobre competências da APD. No art. 44º, nº 1, atribui o poder de fiscalizar a aplicação da lei de pro-

tecção de dados pessoais e a emissão de recomendações, orientações e instruções sobre as melhores práticas no tratamento de dados pessoais, emissão de parecer sobre o acesso aos documentos nominativos, parecer sobre o sistema de classificação de documentos, apreciar e decidir sobre as reclamações que lhe sejam dirigidas e garantir o exercício do direito de acesso, de rectificação, actualização e cancelamento de dados, registar e publicar o registo de ficheiros de dados pessoais; garantir aos titulares dos dados pessoais a obtenção de informação precisa sobre os seus direitos no âmbito do tratamento dos seus dados; orientar a aplicação das medidas técnicas e de segurança necessárias e adequadas, e cooperar com as autoridades internacionais em matéria de protecção de dados pessoais, e fiscalizar os movimentos internacionais de dados pessoais.

13.4 Função

A função fundamental da APD é o exercício de acções no âmbito da regulação, supervisão e fiscalização da aplicação das disposições legais em matéria de protecção de dados pessoais, assim como, no âmbito das suas atribuições, sancionar o seu incumprimento.

As funções da APD devem ser exercidas de forma independente, transparente e sancionatória (art. 5º, nº 2 do estatuto orgânico).

O art. 7º tem por epígrafe "Fiscalização". O nº 1 determina que "A APD deve fiscalizar e supervisionar o cumprimento da lei e dos regulamentos relativos às matérias de protecção de dados, bem como o cumprimento, por parte das entidades responsáveis pelo tratamento de ficheiros de dados pessoais". O nº 2 dispõe que "estão sujeitas a supervisão e fiscalização da APD, todas as entidades responsáveis pelo tratamento de ficheiros de dados pessoais". "No exercício das suas funções de fiscalização, a APD deve instaurar e instruir processos sancionatórios e punir as infracções administrativas às leis e regulamentos cuja implementação ou supervisão lhe compete, bem como as resultantes do incumprimento das suas próprias decisões" (nº 3).

Compete ao Presidente do Conselho de Administração (art. 17º, nº 2 - *h)*) "ordenar actividades inspectivas e apreciar os relatórios de inspecções", *j)* "aplicar medidas sancionatórias decorrentes da violação da legislação sobre a protecção de dados pessoais". A APD tem na sua orgânica um Conselho Técnico a quem compete, entre outras, a função de (art. 25º, nº 1 - *b)*) "assegurar os instrumentos de coordenação na conexão e transferência internacional de dados"; *c)* "garantir a adopção das medidas técnicas, económicas, financeiras, jurídicas e de segurança das matérias de protecção de dados pessoais".

Continuando no âmbito da fiscalização, o art. 45º atribui poderes à APD para aceder às instalações, equipamentos e serviços das entidades sujeitas à supervisão e fiscalização. Averiguar os ficheiros ou suportes informáticos, bem como os elementos não automatizados que contenham dados pessoais. Analisar os sistemas de transmissão, comunicação e acesso aos dados pessoais. Solicitar os processos de transferência internacional de dados pessoais. Identificar, para posterior autuação, todas as empresas ou indivíduos que infrinjam a legislação ou as decisões da APD cuja observância devem respeitar. Realizar auditorias aos sistemas de tecnologias de informação e comunicação. Solicitar o envio da documentação necessária para o exercício da actividade inspectiva e de fiscalização.

Em suma, atendendo às competências e funções que a APD desempenha, podemos extrair três tipos de poderes que têm, nomeadamente: *poder normativo* (assessorar o Governo na regulação e supervisão, apoiar o governo na elaboração de políticas, estudos, programas e projectos sobre a aplicação e controlo legislativo em matéria de protecção de dados pessoais, emitir recomendações, orientações e instruções sobre as melhores práticas no tratamento de dados pessoais); *poder fiscalizador* (fiscalização e supervisão da aplicação das disposições legais em matéria de protecção de dados); e *poder sancionatório* (exercer a função sancionatória em matéria de protecção de dados pessoais.

BIBLIOGRAFIA

ALVES, Joel A., "A regulação europeia de proteção de dados e a sua aplicação à administração pública", in Isabel Celeste M. FONSECA, coord., *Estudos de E-Governação, Transparência e Proteção de Dados*, Coimbra: Almedina, 2021.

ANDRADE, José Carlos Vieira de, *Os Direitos Fundamentais na Constituição Portuguesa de 1976*, 5.ª ed., Coimbra: Almedina, 2012.

ANTUNES, Henrique Sousa, Anotação ao artigo 564º, in José Brandão Proença, coord., *Comentário ao Código Civil, Direito das Obrigações em Geral*, Lisboa: Universidade Católica Editora, 2018.

ÀVILA NEGRI, Sérgio Marcos Carvalho de / KORKMAZ, Maria Regina Detoni Calvacanti Rigolon, "A normatividade dos dados sensíveis na lei geral de proteção de dados: ampliação conceitual e proteção da pessoa humana", *Revista de Direito, Governança e Novas Tecnologias*, Goiânia, 5/1 (2019).

ARAÚJO, Raúl Carlos Vasquez / NUNES, Elisa Rangel, *Constituição da República de Angola Anotada*, Tomo I, Luanda, 2014.

ATAÍDE, Rui Paulo Coutinho de Mascarenhas, "Direito ao Esquecimento", *RDC* 2/2 (2018).

— *Direito da Responsabilidade Civil*, Coimbra: GestLegal, 2023.

— *Direito das Obrigações*, vol. I, Coimbra: GestLegal, 2023.

BARBOSA, Mafalda Miranda, "Haftungsbegründende Kausalität e Haftungsaustüllende Kausalität: Algumas Especificações", *Revista de Direito da Responsabilidade* 4 (2002).

— *Estudos a Propósito da Responsabilidade Objectiva*, Cascais: Principia, 2014.

— "Data Controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil", *Revista de Direito Comercial* (Março, 2018).

— *Lições de Teoria Geral de Direito Civil*, 2.ª ed., Coimbra: GestLegal, 2022.

— "O problema do ressarcimento dos danos não patrimoniais", *Revista de Direito da Responsabilidade*, Coimbra, 5 (2023).

— "Conceitos indeterminados e flexibilização do sistema: considerações a propósito da negligência", *Revista de Direito da Responsabilidade* 5 (2023).

BERIAN, I., "Legal issues regarding gene editing at the beginning of live: an EU perspective", *Regenerative Medicine* 12/2 (2017).

BRANDÃO, Diogo / MONIZ, Graça Conto, "O papel do médico do trabalho à luz do RGPD", *Privacidade e Dados Pessoais: Revista do Centro de Estudos Judiciários* 2 /2º Semestre (2023).

BRIZ, Teodoro, "Epidemiologia e Saúde Pública", *Revista Portuguesa de Saúde Pública*, Número Especial 25 Anos (2009).

BRONZE, Fernando Pinto, *Introdução ao Estudo do Direito*, 2.ª ed., Coimbra: Coimbra Editora, 2006.

CALVÃO, Filipa Urbano, "O regime de proteção de dados pessoais e os desafios na sua aplicação", *Privacidade e Dados Pessoais: Revista do Centro de Estudos Judiciários* 2 (2023).

CAMPOS, Luís, "A tecnologia no contexto do relacionamento médico-doente", in *A Relação Médico-Doente: Um contributo da Ordem dos Médicos,* Lisboa: By the Book, 2019.

CANOTILHO, J.J. Gomes, *Direito Constitucional e Teoria da Constituição*, 7.ª ed., Coimbra: Almedina , 2003.

CAPEÇA, Norberto Moisés Moma, "Privacidade e a Protecção de Dados Pessoais", in *Estudos de Direito Privado*, II, Luanda: Editora Caneta de Estilo, 2022.

— "Protecção de dados Pessoais e Responsabilidade Civil. Realidade Angolana", in *Estudos de Direito Privado*, II, Luanda: Editora Caneta de Estilo, 2022.

— *A Privacidade do Trabalhador como Garantia Constitucional*, Coimbra: Almedina, 2021.

CARVALHO, Nunes de, "A responsabilidade do comitente", *Revista da Ordem dos Advogados* 48 (1988).

CARVALHO, Sílvia Menezes de, *Manual de Direito das Comunicações Electrónicas. Mercado e Regulação*, Luanda: Literaria-Editora, 2021.

CASCÃO, Rui Miguel Prista Patrício, "O dever de documentação do prestador de cuidados de saúde e responsabilidade civil", *Lex Medicinae: Revista Portuguesa de Direito da Saúde* 4/4 (2007).

CASCAREJO, Guilherme*, Danos Não Patrimoniais dos Familiares da Vítima de Lesão Corporal Grave*, Coimbra: Almedina, 2016.

CASTRO, Catarina Sarmento e, *Direito de Informática, Privacidade e Dados Pessoais*, Coimbra: Almedina, 2005.

CAVALEIRO, Vasco, "A proteção de dados no contexto do vínculo do emprego público", in Isabel Celeste M. FONSECA, coord., *Estudos de E-Governação, Transparência e Proteção de Dados*, Coimbra: Almedina, 2021.

COELHO, Angelino Gomes, "Sentido ético-axiológico da responsabilidade civil", *Revista de Direito da Responsabilidade*, Coimbra, 3 (2021).

COIMBRA, José Duarte, "Contencioso da proteção de dados", in Tiago SERRÃO / José Duarte COIMBRA, coord., *Contencioso Administrativo Especial*, Lisboa: AAFDL Editora, 2021.

COLOMBO, Matteo, *Regolamento EU sulla Privacy: principi generali e ruolo del data protection officer*, Milão: ASSO/DPO, 2015.

CORDEIRO, A. Barreto Menezes, *Direito da Proteção de Dados à Luz do RGPD e da Lei nº 58/2019*, reimpressão, Coimbra: Almedina, 2022.

— *Comentários ao Regulamento Geral de Proteção de dados e à Lei nº 58/2019*, CIDP, Faculdade de Direito da Universidade de Lisboa, Coimbra: Almedina, 2021.

CORDEIRO, António Menezes, *Tratado de Direito Civil Português*, I, *Parte Geral,* Tomo III, Coimbra: Almedina, 2004; II, *Direito das Obrigações,* Tomo III, Coimbra: Almedina, 2010,

— "Vulnerabilidades e Direito Civil", *Revista da Faculdade de Direito da Universidade de Lisboa*, Número Temático: Vulnerabilidade(s) e Direito, 62/ 1, Tomo I, (2021).

COSTELA, Elisabete / COSTA, Tiago Branco da, "A investigação clínica na era do altruísmo dos dados: algumas considerações em torno da proteção de dados pessoais", in *Anuário da Proteção de dados*. Centro de I&D sobre Direito e Sociedade, Faculdade de Direito da Universidade Nova de Lisboa, 2023.

CUSTERS, Bart, "Profiling as Inferred Data. Amplifier Effects and Positive Feedback Loops", in Emre BAYAMILIOĞLU, *et al.,* org., *Being profiled: cogitas ergo sum 10 Years of "Profiling the European citizen"*, Amsterdam: Amsterdam University Press, 2019.

DANTAS, Eduardo, "Dilemas Bioéticos na Literacia em Saúde: Consentimento Informado, o Exercício da Autonomia e o Analfabetismo Funcional", *Lex Medicinae: Revista Portuguesa de Direito da Saúde* 21/4 (2024).

DEODATO, Sérgio, *Proteção de Dados Pessoais de Saúde*, Universidade Católica Editora, 2017.

DIAS, Ana Francisco Pinto, "A Dimensão Processual da Proteção de Dados: Uma breve referência à luz do regulamento geral de proteção de dados", *Revista de Direito da Responsabilidade*, Coimbra, 4 (2022).

DOTTI, René Ariel, "É possível defender um direito ao esquecimento?", *Gazeta do Povo,* disponível em <https://gazetadopovo.com.br/colunista/rene-ariel-dotti/e-possivel-defender-direito-ao-esquecimento-i-238ck-dlqguwr2djwoy59ggbm>, acedido a 01 de Março de 2024.

DRESCH, Raquel de Freitas Vale / STEIN, Lilian Brandt, "A Responsabilidade Civil como Mecanismo de Incentivo à Observância do Direito Fundamental à Proteção de dados: uma análise da interpretação do art. 42º e seguintes da LGPD", *Revista de Direito da Responsabilidade*, Coimbra, 5 (2023).

FARIA, Jorge Ribeiro de, *Direito das Obrigações*, actualizada e ampliada por Miguel Pestana de Vasconcelos e Rute Teixeira Pedro, vol. II, 2023.

FERNÁNDEZ-COSTAS MUÑIZ, Javier, "El tratamiento y protección de los datos de salud de los trabajadores en el ordenamiento español", in Francisco Pereira COUTINHO / Graça Conto MONIZ, *Anuário da Proteção de dados*, Centro de I&D sobre Direito e Sociedade, Faculdade de Direito da Universidade Nova de Lisboa, 2023.

FERNANDES, Gabriel Páris, *Comentário ao Código Civil. Parte Geral*, Coord. Luís Carvalho FERNANDES / José Brandão PROENÇA, Faculdade de Direito: Universidade Católico Editora, 2014.

FERNANDES, Luís A. Carvalho, *Teoria Geral do Direito Civil*, I, 5.ª ed., revista e actualizada, Lisboa: Universidade Católica Editora, 2009.

FERRIN, Stephanie *et al., The Personal Information and Electronic Documents Act*, Toronto: Irwin Law Inc, 2001.

FREITAS, Cinthia Obladen de Almendra, "Riscos e Proteção de Dados Pessoais", *RRDIS*, Curitiba, 2/4 (2022).

FRADA, Manuel A. Carneiro da, *Teoria da Confiança e Responsabilidade Civil*, Coimbra: Almedina, 2007.

FRANCISCO, João A., *Manual de Direito da Informática*, Luanda: Editora das Letras, 2019.

GODINHO, Adriano Martelo, *Transhumanismo e Pós Humanismo em seu Limiar*, nº 2, Instituto Jurídico / Faculdade de Direito da Universidade de Coimbra, 2024.

GONÇALVES, Diogo Costa, *Lições de Direitos de Personalidade. Dogmática Geral e Tutela Nuclear*, Cascais: Principia, 2022.

GUIMARÃES, Maria Raquel, "O *phishing* de dados bancários e o pharming de contas. Análise jurisprudencial", in Luís Miguel Pestana VASCONCELOS, coord., *III Congresso de Direito Bancário*, Coimbra: Almedina, 2018.

HÖRSTER, Heinrich Ewald, *A Parte Geral do Código Civil Português*, *Teoria Geral do Direito Civil,* 4.ª reimpressão da edição de 1992, Coimbra: Almedina, 2007.

JOHNSON, Deborah B., *Computer Ethics,* 4.ª ed., New Jersey: Pearson, 2008.

KANT, Immanuel, *Fundamentação da metafísica dos costumes*, Lisboa, Edições 70, 2008.

KAUFMANN, Arthur, *Filosofia do Direito*, trad. António Ulisses Cortês, 2.ª ed., Lisboa: Fundação Calouste Gulbenkian, 2007.

LAGOUTE, Miguel, "O processo clínico enquanto documento administrativo: da transparência à intrusão",*@publica*, CJP-CIDP / Faculdade de Direito da Universidade de Lisboa, 6/1 (2019).

LIMA, Pires de / VARELA, Antunes, *Código Civil Anotado*, vol. I, 4.ª ed., revista e actualizada, colab. M. Henrique Mesquita, Coimbra: Coimbra Editora, 1987.

LIZARDO, João Palla, "Exames médicos e direito de personalidade – acórdão do Tribunal da Relação de Lisboa de 25 de Outubro de 2000", *Questões Laborais* 11/25 (2004).

LOPES, Inês Camarinha, *Os Dados Sensíveis dos Menores à Luz do RGPD*, Coimbra: GestLegal, 2021.

LOUREIRO, João Carlos, *Constituição e Biomedicina: Contributo para uma teoria dos deveres bioconstitucionais na esfera da genética humana*, Faculdade de Direito da Universidade de Coimbra, 2003, Tese de doutoramento.

LUJÁN ALCARAZ, J., *Uso y controle en la empresa de los médios informáticos de comunicación*, Aranzi Social, Tomo III, 2005.

MACHADO, Diego, *Algoritmos e Proteção de Dados Pessoas. Tutela de Direitos na Era dos Perfis*, São Paulo: Almedina, 2023.

MAGALHÃES, Filipa Matias / PEREIRA, Maria Leitão, *Regulamento Geral da Proteção de Dados. Manual Prático.* 3.ª ed., revista e atualizada, Porto: Vida Económica, 2020.

MANOELA, Bogdan, "E-Commerce and profiling in Romania: what is going on and who cares about privacy?", in Niklas CREEMERS *et al*. *Profiling Technologies in Practice: Applications and impact on Fundamental Rights and Values*, Oiterwijk: Wolf Legal Publishers, 2017.

MARQUES, Eduardo Castro, "Análise de direito de portabilidade e a sua (não) compatibilização com o normativo administrativo", in Isabel Celeste M. FONSECA, coord., *Estudos de E-Governação, Transparência e Proteção de Dados*, Coimbra: Almedina, 2021.

MENKE, Fabiano, "A proteção de dados e o direito fundamental à garantia da confidencialidade e da Integridade dos Sistemas Técnico-Informacionais do Direito Alemão", *RJLB* 5/1 (2019).

MESSA, Ana Flávia, "Transparência na Gestão Pública", in Isabel Celeste M. FONSECA, coord., *Estudos de E-Governação, Transparência e Proteção de Dados*, Coimbra: Almedina, 2021.

MASSENO, Manuel David, "Dos ataques ransomware na Convenção de Budapeste sobre o crime cibernético. Um ensaio de qualificação alternativa", in *Privacy and Data Protection Magazine*, Lisboa, 7 (2024).

MITROU, Lilian, "Data Protection, Artificial Intelligence and Cognitive Service: is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?", Societal Science Research Network, Nova Iorque, 2019.

MOREIRA, Sónia, "O RGPD e a sua aplicação transfronteiriça: até aonde estão protegidos os nossos dados pessoais", *Revista do Centro de Estudos Judiciais* 2 (2023).

MONIZ, Ana Raquel Gonçalves, *Os Direitos Fundamentais e a sua Circunstância. Crise e Vinculação Axiológica entre o Estado, a Sociedade e a Comunidade Global*, Coimbra: Imprensa da Universidade de Coimbra, 2017.

MONIZ, Graça Canto, *Manual de Introdução à Proteção de Dados Pessoais*, Coimbra: Almedina, 2023.

MONTEIRO, Jorge Sinde, "Reparação dos danos pessoais em Portugal", *CJ* 4 (1986).

— *Responsabilidade por Conselhos, Recomendações ou Informações*, Coimbra: Almedina, 1989.

MULHOLLAND, Caitlin Sampaio, "Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (lei 13.709/18)", *Revista de Direito e Garantias Fundamentais*, Vitória, 19/3 (2018).

NEVES, A. Castanheira, "Fontes de Direito: Contributo para a Revisão do seu Problema", in *Digesta*, vol. 2, Coimbra: Coimbra Editora, 1995.

— "O princípio da legalidade criminal", in *Digesta*, vol. 1, Coimbra: Coimbra Editora, 349-473.

— *Lições de Introdução ao Estado do Direito*, proferidas ao curso do 1º ano jurídico de 1969-69, Coimbra, 1969.

NOVAIS, Jorge Reis, *Os Princípios Constitucionais Estruturantes da República Portuguesa*, Coimbra: Coimbra Editora, 2004.

NOVELLI, Claudio *et al., Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity*. ArXiv Working Paper n. 2401.07348, Nova Iorque, 2024.

OLIVEIRA, Silva, "Pensamento africano em perspectiva comparada", in *História Unisinos*, Universidade do Vale do Rio dos Sinos, 23/3 (2019).

OSSWALD, Walter, "Limites do consentimento informado", in *Estudos de Direito de Bioética*, Coimbra: Almedina, 2009.

PEREIRA, Alexandre Libório Dias, "Big data, e-health e «autodeterminação informativa»: a lei nº 67/98, a jurisprudência e o regulamento 2016/679", *Lex Medicinae: Revista Portuguesa de Direito da Saúde* 29 (2018).

PEREIRA, André Gonçalo Dias, "Dever de documentação, Acesso ao Processo Clínico e sua Propriedade. Uma Perspectiva Europeia", *Revista Portuguesa de Danos Corporal* 15/16 (2006).

— *Direitos dos Pacientes e Responsabilidade Médica*, Coimbra: Coimbra Editora, 2015.

PICA, Luís Manuel, As Garantias dos Contribuintes no Tratamento dos Dados Pessoais pela Administração Tributária, Coimbra: Almedina, 2025.

PINHEIRO, Alexandre Sousa, *Privacy e Protecção de Dados Pessoais: a Construção Dogmática do Direito à Identidade Informacional*, Lisboa: AAFDL, 2015.

PINHEIRO, Alexandre Sousa / GONÇALVES, Catarina Pina, *Comentários ao Regulamento Geral de Proteção de Dados,* Alexandre Sousa PINHEIRO *et al.,* coord., Coimbra: Almedina, 2018.

PINHEIRO, Joaquim, "A autonomia na pessoa com doença crónica", *Revista Portuguesa de Bioética* 9 (2009).

PINHEIRO, Guilherme Pereira / PINHEIRO, Alexandre Pereira, "Covid-19 e geolocalização: entre a saúde e a proteção de dados pessoais", *Revista Jurídica da Presidência*, Brasília, 24/132 (2020) 245-268.

PINTO, Carlos Alberto da Mota, *Teoria Geral do Direito Civil*, 4.ª ed., por António Pinto Monteiro e Paulo Mota Pinto, Coimbra: Coimbra Editora, 2005.

PINTO, Paulo Mota, *Interesse Contratual Negativo e Interesse Contratual Positivo*, Coimbra: Coimbra Editora, 2008.

POZGAR, George D., *Legal and Ethical Essential of Health Care Administration*, 3.ª ed., Burlington: Jones Bartlett Learning, 2021.

PRIETO ÁLVAREZ, Tomás, "El Derecho Constitucional al Desarrollo de la Personalidad. ¿Procede Identificarlo con la Libertad General de Acción?", *Boletim da Faculdade de Direito,* Coimbra, 94/2 (2018).

QUEIROZ, Cristina, "A proteção constitucional de recolha e tratamento de dados pessoais autonomizada", in *Homenagem da Faculdade de Direito de Lisboa ao Professor Doutor Inocêncio Galvão Telles – 90 Anos*, Coimbra: Almedina, 2007.

QUINTA, Paula, *Manual de Direito da Segurança e Saúde no Trabalho*, 5.ª ed., Coimbra: Almedina, 2023.

REGO, Carlos, "Exames Médicos e Direitos de Personalidade – o Acórdão do Tribunal da Relação de Lisboa de 25 de Outubro de 2000", *Questões Laborais* 11/24 (2004) 215-224.

REIS, Rafael Vale e, *Procriação Medicamente Assistida: Gestação de substituição, anonimato do doador e outros problemas*, Coimbra: GestLegal, 2022.

RIBEIRO, Vera Masagão, "Alfabetismo funcional: Referências conceituais e metodologia para a pesquisa", *Revista de Educação & Sociedade*, Pontifica Universidade Católica de São Paulo, 18/60 (1997).

RODRIGUES, Álvaro da Cunha Gomes, "Consentimento Informado – Pedra Angular da Responsabilidade Criminal Médico", in *Direito da Medicina*, I, Centro de Direito Biomédico / UC, 2002.

RODRIGUES, António Barroso, *O Concurso de Responsabilidade Civil: Ensaio sobre o concurso das modalidades delitual e obrigacional de responsabilidade civil*, 2.ª ed., Coimbra: Almedina, 2024.

RODRIGUES, Jorge Maciel Silva, "Sistema de Vídeo Vigilância Digital e Gestão Remota. Análise da sua aplicação à Telemedicina", dissertação de mestrado em instrumentação e microelectrónica – especialidade em instrumentalização e controlo industrial, da Faculdade de Ciências e de Tecnologia (Departamento de Física) da Universidade de Coimbra, 2006.

SÁNCHEZ-CARO, J. / ABELLÁN, F., *Telemedicina y Protección de Datos Sanitários, Aspectos Legales y Éticos*, Granada: Comores, 2002.

SANTOS, Leonardo Valverde Susart dos, "Compensação de danos não patrimoniais causados pela violação de normas de proteção de dados pessoais", *Revista de Direito da Responsabilidade*, Coimbra, 4 (2022).

SARMENTO, António, "Quando o doente está privado de liberdade", in *A Relação Médico-Doente, Um contributo da Ordem dos Médicos*, Lisboa: By the Book, 2019.

SCHWARTZ, Paul M., "The EU-U.S. Privacy Collision: a turn to institution and procedures", *Harvard Law Review* 126 (2013).

SILVA, Artur Flamínio da, "Ética e Inteligência Artificial no Direito Administrativo", in Isabel Celeste M. FONSECA, coord., *Estudos de E-Governação, Transparência e Proteção de Dados*, Coimbra: Almedina, 2021.

SILVA, Carlos Burity, *As Pessoas e o Direito. Reflexões sobre o Direito das Pessoas*, Colecção da Faculdade de Direito da Universidade Agostinho Neto, 2002.

SILVA, Rafael Meira / OLIVEIRA, Cristina Godoy Bernardo de, "Inteligência Artificial e Proteção de Dados: Definição de Perfil e Desafios", in <https://www.migalhas.com.br/coluna/migalhas-de-proteçao-de-dados-/339300/ia-e-proteçao-de-dados--definiçao-de-perfil-e-desafios>.

SOUSA, Rabindranath V. A. Capelo de, *O Direito Geral de Personalidade*, Coimbra: Coimbra Editora, 1995.

TINCQ, Henri *et al., As Grandes Religiões do Mundo. Judaísmo, Cristianismo, Islão*. Vol. I, coord. Henri Tincq, Lisboa: Edições Texto&Grafia, 2016.

WELLS, Barbara G. *et al., Manual de Farmacoterapia*, 9.ª ed., McGraw Hill Education, 2016.

WESTIN, Alan F., *Privacy and Freedom*, New York: Atheneum, 1967.

VARELA, Antunes, *Das Obrigações em Geral*, vol. I, 10.ª ed., Coimbra: Almedina, 2000.

VASCONCELOS, Pedro Pais de, *Direito de Personalidade*, Coimbra: Almedina, 2006.

SERRA, Adriano Vaz, "Reparação do dano não patrimonial", *BMJ* (1959).

VENTURA, Miriam / COELI, Cláudia Medina, "Para além da privacidade: direito à informação na saúde, proteção de dados pessoais e governação", *CSP Cadernos de Saúde Pública* 34/7 (2018).

VITOR, Paula Távora, "Os dados de saúde de crianças e jovens – capacidade e competência decisória", *Revista de Centro de Estudos Judiciários* 2 (2023).

ISBN 978-989363201-7