ALBA
ISFIC RESEARCH AND SCIENCE JOURNAL
31 - 03 | 2024

ALBA - ISFIC RESEARCH AND SCIENCE JOURNAL
ISSN: Em trâmite
1ª Ed, Vol. 1, No. 3, Março, 2024
https://alba.ac.mz/index.php/alba/issue/view/3
albaisfic@gmail.com; alba@isfic.ac.mz

DADOS SENSÍVEIS E A SEGURANÇA DE INFORMAÇÃO

Sensitive data and information security

Seguridad de la información y los datos confidenciales

Katy Fernandes[1], Nsitukemba Vieira Viegas[2]

[1]Universidade Portucalense do Porto, Portugal, fernandeskaty8@gmail.com.
[2]Instituto Politécnico de Gestão e Tecnologia, Portugal, https://orcid.org/0000-0003-1891-9093, fernandeskaty8@gmail.com
Autor para correspondência: fernandeskaty8@gmail.com

***Data de recepção:** 16-11-2023*
***Data de aceitação:** 16-02-2024*

***Como citar este* artigo:** Fernandes, K., & Viegas, N. (2024). Dados Sensíveis e a Segurança de Informação. *ALBA - ISFIC Research and Science Journal, 2*(3), pp. 127-136.

RESUMO

Com o aumento de ataques no Ciberespaço, os dados pessoais passaram a ser o alvo principal e hoje, mais do que nunca, a Cibersegurança e a manutenção de um espaço digital resiliente são objectivos de qualquer estado que pretende ver o seu cidadão protegido (cidadania digital), imbuído dos seus direitos e sujeitos de proteção de direitos. O espaço de liberdade permitida e possibilitado no mundo digital tem impactos na realidade das pessoas, pelo que, a protecção dos indivíduos verdadeiramente integral e efectivam deve abarcar a esfera digital. Dai que, a segurança de informação tornou-se um desígnio e um desiderato a ser perseguida pelos estados e isso implica além da criação, alteração e adaptação de medidas legislativas, mas sobretudo da melhoria das medidas de segurança que sejam implementadas e da forma como são executadas, a fim de preservar os direitos humanos e fundamentais das Cite zens (Cidadãos digitais).

Palavras-chave: Cibersegurança, Comportamento humano, Privacidade dos dados.

ABSTRACT

With the increase in attacks in Cyberspace, personal data has become the main target and today, more than ever, Cybersecurity and the maintenance of a resilient digital space are objectives of any state that wants to see its citizen protected (digital citizenship), imbued with their rights and subject to rights protection. The space of freedom allowed and made possible in the digital world has impacts on people's reality, therefore, the truly comprehensive and effective protection of individuals must encompass the digital sphere. Hence, information security has become a goal and a desideratum to be pursued by states and this implies, in addition to the creation, alteration and adaptation of legislative measures, but above all the improvement of the security measures that are implemented and the way in which they are carried out in order to preserve the human and fundamental rights of Citizens (Digital Citizens).

Keywords: Cybersecurity, Human behavior, Data privacy.

RESUMEN

Con el aumento de los ataques en el Ciberespacio, los datos personales se han convertido en el principal objetivo y hoy, más que nunca, la Ciberseguridad y el mantenimiento de un espacio digital resiliente son objetivos de cualquier Estado que quiera ver a sus ciudadanos protegidos (ciudadanía digital), imbuidos de sus derechos y sujetos a

protección de derechos. El espacio de libertad permitido y posibilitado en el mundo digital tiene impactos en la realidad de las personas, por lo que la protección verdaderamente integral y efectiva de las personas debe abarcar el ámbito digital. De ahí que la seguridad de la información se haya convertido en una meta y un desiderátum a perseguir por parte de los estados y esto implica, además de la creación, alteración y adaptación de medidas legislativas, pero sobre todo el mejoramiento de las medidas de seguridad que se implementan y la forma en que se implementan. se llevan a cabo con el fin de preservar los derechos humanos y fundamentales de los Ciudadanos (Ciudadanos Digitales)..

Palabras llave: Ciberseguridad, Comportamiento humano, Privacidad de datos.

INTRODUÇÃO

A Preocupação com a privacidade e proteção de dados, não é um fenómeno exclusivo da atual sociedade de informação contemporânea, em 1980, nos finais do século XX, Samuel Warren publicou um artigo intitulado The right to privacy no qual defendia pela primeira vez o reconhecimento do direito à privacidade e à reserva da vida privada.

Preocupação que só obteve consideração ao nível da comunidade internacional em 1948, aquando da proclamação pela Assembleia Geral das Nações Unidas da Declaração Universal dos Direitos do Homem, onde se refere no artigo 12.º, que "ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques, foi reconhecido a toda a pessoa um direito à protecção da lei, ficando assim consagrado o princípio do respeito pela vida privada, como reconhecimento da dignidade humana.

Posteriormente, em 1950, a Convenção Europeia dos direitos do Homem veio a considerar que "toda a pessoa tem direito ao respeito à sua vida privada e familiar, do seu domicílio e da sua correspondência".

O Conselho da Europa (CE) em 1981, viria a adoptar a convenção 108 para a protecção das pessoas relativamente ao tratamento automatizado de dados pessoais, dando especial atenção aos dados sensíveis, como são os relativos à saúde, vida sexual ou condenações penais.

Em 1995, a União Europeia aprovou a directiva sobre a protecção de dados pessoais, que veio a ser substituído pela GRPD - Regulamento Geral sobre a Proteção de Dados - relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.

Em 2000, o conselho de Nice proclamou a carta dos direitos fundamentais da União Europeia que, nos seus artigos 7º e 8º, confirma o direito ao respeito pela vida privada e à proteção dos dados pessoais.

No mesmo ano, a União Africana adoptou a convenção da União Africana sobre a Cibersegurança e proteção de dados pessoais (2000), fixando as normas de segurança essenciais para a criação de um espaço digital credível para as transações eletrónicas, proteção de dados pessoais e luta contra o cibercrime.

O direito fundamental à privacidade comporta três facetas. A primeira diz respeito ao direito a desfrute de uma vida privada livre, sem intervenção ou intrusão de terceiros; a segunda, consagra o direito a comunicar com terceiros sem medo de ser-se vigiado, e a terceira, comporta o direito a controlo e o acesso a informações pessoais - base do direito à autodeterminação informativa. O valor superior da dignidade humana e da identidade individual de cada titular de dados pessoais legitimam a protecção da privacidade e intimidade das pessoas, a nível constitucional. Conforme podemos constatar infra,

"El tema de la protección de datos personales comporta y debe comportar el reconocimiento de los derechos fundamentales que tienen que ser tutelados por el estado. Estos derechos constituyen el núcleo de identidad de las personas, sus patrones, perfil personal e individual, sus modos de vida, sus propósitos o

proyectos, enfin, el memorial destacado de la personalidad, del individuo en cuyo seno está contenida toda clase infogenética de la caracterización social y individual" (La Protección de Datos Personales en Internet y Habeas data -, Revista Derecho y Tecnología n.º 13/2012 - ISSN: 1317-9306)

Num mundo mediado por tecnologias emergentes e de ponta - as TIC´s (Tecnologias de informação e de comunicação), considerado por muitos a Era dos dados ou Geitzest do século XXI, falar de dados pessoais é além de necessária, fundamental para que possamos, pelo seu caráter cross-sectorial (transversal a todas as áreas, rectius gestão administrativa, contabilística, financeira, na saúde, justiça, e outras) nos orientar e tomar as decisões precisas, de forma cuidada, com plena e real eficácia no mundo real.

Por isso, é preciso reconhecermos, como o fez Amadeu Guerra (A Lei de proteção de dados pessoais - in direito da sociedade da informação, volume II, coimbra editora 2001), que "a informática se apresenta como instrumento adequado à sistematização, produção e distribuição da informação, bem cedo se deparam ao direito novos problemas advenientes da concepção de programas, da recolha, tratamento automatizado e distribuição da informação".

Dados pessoais

Uma definição ilustrativa de dados pessoais nos é dada pela Convenção da União Africana sobre a Cibersegurança e proteção de dados pessoais, como sendo qualquer informação relativa a uma pessoa singular identificada ou identificável, através essa pessoa pode ser identificada, directa ou indirectamente, em particular através de inferência a um número de identificação ou a um ou vários factores específicos à sua identidade física, fisiológica, mental, económica, cultural ou social.

Já dados sensiveis refere-se a informações que tratam de características da personalidade do indivíduo, tais como origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caracter religioso, filosófico ou político, dado referente a saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Dentre a panóplia especial dos dados sensíveis ou especiais temos os dados de saúde ou do domínio da saúde, no termos da mesma convenção, como sendo qualquer informação sobre o estado físico e mental de uma pessoa (física ou natural) titular dos dados, incluíndo informações genéticas.

Na doutrina, numa colocação mais singela, José Van Djick define "dados" como sendo qualquer tipo de informação em um formato apto a ser utilizado por um computador (se entiende cualquier tipo de información en un formato apto para su utilización por parte de una computadora), ou dispositivo eletrónico, acrescentamos nós, como sejam um texto, uma imagem, um som e números, nome, o género, data de nascimento e o código postal (solicitados quando se inscreve numa plataforma digital).

Nessa particular, importante diferenciarmos dados públicos dos dados privados. Por um lado, como "aqueles que são do conhecimento geral, fazendo parte do conhecimento e acervo da sociedade, como os que constam de cadastro à disposição do público e os dodos registados em cartórios, repartições públicas, não cobertos pelo sigilo", nesse sentido, são públicos dados como o nome, endereço, número de telefone, sexo, dados de nascimento, profissão, identidade civil e/ou proficioal, estado civil, filiação partidiária.

Por seu turno, dados privados, "são os relativos à pessoa fisica ou pessoa jurídica que se mantêm na esfera da vida privada do cidadão ou da empresa, sem ser do conhecimento geral", estão aqui incluídas informações confidenciais, sigilosas, as estritamente pessoais e que não devam cair no conhecimento público.

Assim dados referentes à vida pessoal do cidadão, hábitos de consumo, preferências no lazer, a correspondência recebida e a expedida, as ligaçoes telefónicas, os conteúdos das mensagens eletrónicas recebidas e expedidas, as páginas de internet com restriçoes de acesso.

No meio, estão os dados privados autorizadados, ou seja, aqueles cujo titular

permite ou outoriza a sua inclusão em uma determinada base de dados.

Constituições de vários países, vide a Cabo Verdiana (artigo 45.º) e a Angolana (artigo 32.º) considerou um núcleo restrito de dados insuscetíveis de tratamento, como sejam, os de convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização legal, com garantias de nao discriminação e quando os mesmos destinem a processamento de dados estatisticos não individualmente indentificáveis. Significando que a limitação imposta ao tratamento daqueles rol de dados, em princípio são proibidos, havendo a possibilidade de tratamentos mediante condições específicas.

É preciso precisar no entanto, que a Constituição Cabo-Verdiana, coisa que o Constituinte Angolano não fez, autonomizou o direito à proteção de dados pessoais no artigo 45.º cuja a epigrafe é "Utilização de meios informáticos e proteção de dados pessoais", o que vai de encontro posicionamento relativamente à proteção de dados pessoais latu sensu, além da esfera da vida privada, como assertivamente expõe Ingo Wolfgang Scarlet, in verbis,

Nessa perspetiva, é crucial que se tenha presente que embora a protecção de dados tenha sido deduzida (associada), em diversos casos, do direito a privacidade (v.g., nos EUA, o conceito de informational privacy) ou, pelo menos, também do direito a privacidade, como no caso da Convenção Europeia de Direitos Humanos (nos termos da exegese do artigo 8.º levada a efeito pela CEDH), o fato e que o objecto (âmbito de protecção) do direito a protecção de dados pessoais e mais amplo, porquanto, com base num conceito ampliado de informação, abarca todos os dados que dizem respeito a uma determinada pessoa natural, sendo irrelevante a qual esfera da vida pessoal se referem (íntima, privada, familiar, social), descabida qualquer tentativa de delimitação temática. O que se pode afirmar, sem temor de incorrer em erro, e que seja na literatura jurídica, seja na legislação e jurisprudência, o direito a protecção de dados vai além da tutela da privacidade, cuidando-se, de tal sorte, de um direito fundamental autónomo, directamente vinculado a protecção da personalidade. Alias, não é a toa que Bruno Ricardo Bioni alertou para o facto de que o entendimento, hoje amplamente superado, de que o direito fundamental a protecção de dados consiste em mera evolução do direito a privacidade, e uma "construção dogmática falha".

Tratamento de dados sensíveis

Grosso modo, tratamento de dados é toda operação realizada com dados pessoais, tais como colecta, utilização, armazenamento, compartilhamento, eliminação, etc. havendo a faculdade de tais operações poderem ser materializadas de forma automática ou não.

Para aferirmos o verdadeiro sentido de tratamento dos dados, trazemos a definição disposta na Convenção da União Africana sobre a Cibersegurança e Protecção de dados pessoais, sendo o tratemento aí considerado como qualquer operação ou conjunto de operação efectuados sobre os dados pessoais, que através de meios automáticos ou não, tais como recolha, registo, organização, armazenamento, adaptação, alteração, recuperação, suporte, cópia, consulta, utilização, divulgação, ou qualquer outra forma de distribuição, ou de outro modo, fazendo disponibilização, alinhamento ou ou distribuição de dados pessoais.

O Regime Jurídico dos dados pessoais, na esteira do previsto na Constituição (CV), proíbe o tratamento de dados especiais no artigo 8.º (legislador infraconstitucional preferiu essa expressão, ao - dados sensíveis -), e é mais abrangente, além da proibição de tratamento de dados relativos a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, proíbe o tratamento de dados genéticos , dados biométricos, os relativos à saúde, à vida sexual, ou orientação sexual, salvo, o tratemento mediante consentimento do titular ou autorização legal, com garantias de não discriminação e com medidas de segurança adquadas;

Quando tenham por fim o tratamento ou processamento de dados estatísticos, não individualmente identificáveis, com adotação de medidas de segurança adequadas; ou ainda, mediante autorização da autoridade nacional de protecção de dados, justificada em interesse público ou para prossecução de interesse legítimo do responsável pelo tratamento, salvaguardas que sejam, o direito a não discriminação e aplicadas as medidas de seguranças adequadas.

O que vém a ser essas medidas de seguranças adequadas, atenta à sensibilidade dos dados em causa e que visam reforçar o controlo de entradas nas instalações, o acesso aos dados e suportes de dados, o controlo da utilização dos sistemas de tratamento automatizados por pessoas não autorizadas ou o controlo da transmissão dos dados?

No que aos dados sensíveis de saúde diz respeito, essas medidas se reportam às situações assegurem, "a implementação de medidas destinadas a impedir o acesso indevido de terceiros aos processos clínicos e aos sistemas informáticos que contenham informação de saúde, incluíndo as respectivas cópias de segurança, assim como a separação lógica entre dados de saúde e dados administrativos", e as que resultem, "necessária a identificação das potenciais vulnerabilidades do sistema, bem como uma previsão do impacto que essas falhas de segurança possam causar, de modo a proceder a uma análise e avaliação de riscos correcta e realista que conduzam a uma definição eficaz das medidas de segurança que melhor poderão dar resposta às necessidades da Instituição" . Nesse sentido vide o artigo 24.º do regime de protecção de dados pessoais de pessoas singulares de cabo verde, a relativa á segurança e confidencialidade no tratamento.

Tendo o legislador descriminado no artigo 25.º do mesmo diploma um rol de medidas consideradas especiais de tratamento, tendo previsto no seu número 1, "que os responsáveis pelo tratamento dos dados referidos nas alíneas do número 1, nos números 4 e 5 do artigo 8.º (dados especiais) e no número 1 do artigo 11.º devem tomar as medidas adequadas e acrescidas de segurança da informação, designadamente para:

a) Impedir o acesso de pessoa não autorizada às instalações utilizadas para o tratamento desses dados (controlo da entrada nas instalações); b) Impedir que suportes de dados possam ser lidos, copiados, alterados por pessoa não autorizada (controlo dos suportes de dados); c) Impedir a introdução não autorizada, bem como a tomada de conhecimento, a alteração ou a eliminação não autorizadas de dados pessoais inseridos (controlo da inserção); d) Impedir que sistemas de tratamento automatizados de dados possam ser utilizados por pessoas não autorizadas através de instalações de transmissão de dados (controlo da utilização); e) Garantir que as pessoas autorizadas só possam ter acesso aos dados abrangidos pela autorização (controlo de acesso); f) Garantir a verificação das entidades a quem possam ser transmitidos os dados pessoais através das instalações de transmissão de dados (controlo da transmissão); Garantir que possa verificar-se, a posteriori, em prazo adequado à natureza do tratamento, a fixar na regulamentação aplicável a cada sector, quais os dados pessoais introduzidos, quando e por quem (controlo da introdução); h) Impedir que, na transmissão de dados pessoais, bem como no transporte do seu suporte, os dados possam ser lidos, copiados, alterados ou eliminados de forma não autorizada (controlo do transporte).

Mais, segundo dispõe o número 2 da mesma norma, caso a comissão de protecção de dados entender, pode dispensar a existência de certas medidas de segurança, atendendo à natureza das entidades responsáveis pelo tratamento e o tipo de instalações em que é efectuado. Essa mesma entidade pode determinar que a transmissão seja cifrada, nos casos em que a circulação em rede de dados pessoais referidos nos artigos 8.º e 11.º possa pôr em risco direitos, liberdades e garantias dos respetivos titulares (4).

Além das questões ligadas à privacidade, intimidade e autoterminação informativa, Amadeu Guerra defende que outras "interrogações" poderão ser levantadas quanto à possibilidade de tratamento de dados de origem étnica, designadamente em matéria de

investigação policial e prevenção criminal - especialmente em sede de cooperação policial - e no domínio da medicina preventiva ou diagnóstico médico".

De entre a panóplia dos dados considerados especiais ou sensíveis, o legislador de vários países é rigoroso em reconhecer e classificar como sendo proibida o seu tratamento, salvo as enumeradas excepções acima indicadas, tomamos, nessa pequena dissertação, como exemplo intuitivamente os dados de saúde.

Os dados de saúde são o elixir da medicina do futuro, enfatiza Francisca R. Fernández, no sentido de que, nas palavras da autora, "una medicina que se caracterizara por la predicción ayudada por la inteligencia artificial. Si la medicina del siglo 20 fue preventiva, la del siglo 21 es predictiva, anticipandose a las enfermidades que podamos padecer, y precisamente para poder disponer de aplicaciones de diagnostico y tratamiento que se basan en los datos facilitados y que le permitira disenar tratamientos "diana" para combatirlas, precisamente basandose en la informacion de otras personas que la hayan padecido anteriormente, atraves de sus datos".

A mais remota possibilidade de se ter livre acesso aos dados pessoais de saúde das pessoas traz ao de cima a preocupação de se estar a desnudar a pessoa juntamente com o seu historial médico, genético muito além do seu titular. O tratamento desse tipo específico de dados exige além de acrescidos métodos de segurança, a máxima confidencialidade e sigilo quando permitida o seu tratamento, sob peno de estar a violar o valor - direito também de teor constitucional, que a reserva da intimidade e a protecção ao direito privacidade (artigo 42.º n.º 2 CRCV).

Hoje em dia, os ataques mais comuns se derigem a estabelecimentos de saúde, precisamente pelo carácter dos dados, os criminosos informáticos sabem que uma vez sequestrados esses dados a probabilidade de haver pagamento pelo respetivo resgate é maior do que nas outras categorias de dados, tornando-se assim uma indústria apelativa aos criminosos cibernéticos.

E a preocupação aumenta, quanto considerarmos que a tutela dos dados sensíveis de saúde ou genético vai muito além da preserva da intimidade e a privacidade do seu titular, exige igualmente que se assegure evitando a discriminação de acesso à saúde e ao tratamente devido, acesso ao seguro de saúde, acesso ao emprego, contratação, promoção, pode levar à desciminaçáo da pessoa nos locais de trabalho, pode levar a demissão de um funcionário, estigmatização social do indivíduo pelas circunstáncias da sua saúde ou da sua aparência fisicia associada a condições de saude.

A colecta descontextualizada e o tratamento indiscriminado desse tipo de dados põe em causa a dignidade do seu titular pelas consequências lesivas que poderá acarretar ao seu titular.

Daí que, além da exigência e imposição por força da CRCV e do próprio RJGPDP de adopção de acrescidas medidas de protecção, obedecendo a critérios "restritos, cautelosos e que demonstrem segurança quanto a devida e justa protecção" por parte dos responsáveis pelo tratamento.

Descrevendo a realidade de São Tomé e Príncipe, durante a pandemia do Covid-19 e num mundo pós-pandêmico, Baía realça que na gestão de dados pessoais de saúde é fundamental ter-se presente o fato de que [...] cada vez mais utilização dos meios informatizados para processar dados e informações que alimentam o funcionalismo que ajuda a manter activo as redes de sistemas de saúde, o problema da protecção de dados e, por inerência, o conjunto de informações do histórico clínico dos seus titulares, coloca-se perante às insuficiências e muito frágil sistemas e métodos de tratamento existentes em STP", cenário que descreve a situação dos demais Países Africanos de Língua Oficial Portuguesa, Cabo Verde concretamente.

Ainda, os dados vertidos nos relatórios produzidos em perícias médico-legais tanto de pessoas vivas como as que estão mortas são considerados dados sensíveis, conforme o sentido do Parecer da Procuradoria Geral da República Portugues em 2005,

"os elementos recolhidos nos exames médico-legais de pessoas vivas, e vertidos nos respectivos relatórios, constituem dados pessoais sensíveis, que beneficiam da protecção conferida à reserva da vida privada pelo artigo 26º, nº 1, da Constituição; Os elementos recolhidos nos exames médico-legais de cadáveres, e vertidos nos respectivos relatórios, merecem igualmente protecção, com fundamento no princípio da dignidade humana (artigo 1º da Constituição), precipitado num direito geral de personalidade, que é acolhido no artigo 26º, nº 1, da Constituição e que se projecta nos falecidos quanto ao segmento respeitante à reserva da vida privada."

"A recolha e interconexão de dados pessoais, particularmente de dados sensíveis, são outra das ameaças mais correntemente citadas: os serviços da administração do Estado, bem como grandes empresas e instituições financeiras, recolhem informações sobre as pessoas e com elas constituem grandes bases de dados pessoais, necessárias ao cumprimento das suas atribuições. Ao estabelecer uma interconexão entre essas bases é possível obter informações de carácter privado, como a religião ou a saúde, que se podem revelar discriminatórias em situação de candidatura a emprego ou outras similares.

Os danos derivados de um tratamento não adequado, sem aplicação de qualquer mecanismo segurança resulta em prejuízo à integridade ou à disponibilidade de dados, de um programa, sistema ou uma informação, tendo o potencial de causar danos e prejuízos a seu titular individualmente considerado, ou em termos gerais, acarretar dados falaciosos (falsos) ou enviesados num determinado resultado de pesquisa ou treinamento de um dados sistema de inteligência artificial (nesse sentido vide dados sintéticos).

A título de exemplo, aponta Franciano Beltramini, relativamente a informações referentes a saúde e a genética de uma determinada pessoa, que estão armazenadas nos bancos de dados de hospitais, dos planos de saúde e dos laboratórios, tem um potencial de impedir que uma seguradora ou empresa de plano de saúde aceite determinado cliente de maneira abusiva, gerando, assim, uma discriminação.

Nas palavras de Ana Vaz, a liberdade de circulação da informação, de forma segura, é um bem essencial à preservação dos direitos fundamentais e consequentemente ao funcionamento regular da sociedade, tanto que, para salvaguarda da privacidade e da protecção de dados pessoais, a segurança da informação é um valor indispensável.

Para protecção de dados pessoais de maior sensibilidade, o artigo 15.º (segurança de tratamento) do RJPDP exige medidas de segurança mais severas, bem como o controlo da inserção, utilização, acesso e transmissão desses dados. Determina ainda que os sistemas de tratamento da informação garantam a separação lógica entre os dados referentes à saúde e à vida sexual, incluindo os genéticos, dos restantes dados pessoais".

Princípios relativos à qualidade dos dados

O princípio fundamental sobre o tratamento de dados - transparência, licitude, com respeito pelas normas da boa fé, devendo os dados ser recolhidos para um fim determinado, explícitas e legítimas, e processadas de forma adequadas e pertinentes ao fim previsto que determinou a recolha, devendo aos titulares dos dados ser assegurados o direito de acesso, à informação, retificação, oposição e apagamento.

Consentimento

Dados sensíveis, para efeitos de tratamentos, estão sujeitos a limites e condições adicionais, além das exigidas num tratamento de dados pessoais que não tenham esse caráter especial.

O princípio do consentimento joga um papel fundamental em qualquer acto de tratamento de dados, mas com maior incidência no grupo dos dados especiais (sáude, biometria), devendo ser prestado forma explícito, informado, derivar da livre vontade do seu titular, e ser específica, atendo ao limite intrínseco imposto pelo princípio da finalidade.

O consentimento pode não ocorrer da mesma forma em todo tipo de tratamento de dados pessoais, haja vista, o seu peso é menor quando haja desequilíbrio no relacionamento, a título

de exemplo, o derivado da assimetria de poderes que deriva entre o empregador e o empregado. Nestes casos, o consentimento sozinho não é suficiente (por falta da declaração de vontade livre do empregado) para legitimar um tratamento, outros elementos devem ser considerados na avaliação, como seja o contrato ou acordo derivado do contrato de trabalho, sendo nestes casos, o tratamento de dados do empregado necessário para conformar a relação laboral.

Partilha da mesma opinião de Terresa Coelho Moreira ao considerar que o Regulamento Geral de proteção de dados (2018) atribui uma enorme importância à relação de trabalho e a definição de consentimento do titular de dados pessoais para tratamento de dados. Segundo a autora, "este Regulamento Geral retirou o acento tónico do consentimento como fundamento jurídico valido para o tratamento de dados pessoais quando, nos termos do considerando (34) 'exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento', como é o caso, claramente, da relação de trabalho. Este considerando e muito importante porque significa que, para que um tratamento de dados pessoais realizado pelo empregador seja valido, terá de assentar noutros princípios que não o mero consentimento do trabalhador".

Considera a mesma autora que "sem dúvida, que a noção de consentimento, entendido como uma manifestação de vontade livre, especifica e informada, e um conceito de difícil concretização e de difícil preenchimento no contexto de uma relação de trabalho" , o autor citado supra esclarece ainda que, considera-se que, no âmbito laboral, o requisito do consentimento fica relegado para um segundo plano, já que o trabalhador interessado se encontra numa posição de desigualdade em relação ao responsável pelo tratamento, isto e, o empregador, desigualdade na sua necessidade de obtenção de um posto de trabalho, no caso dos candidatos a emprego, ou de manutenção do mesmo, no caso de trabalhadores.

Não parece que neste tipo de relação se possa falar de um consentimento prestado livremente, principalmente quando o consentimento e requisito para a obtenção de um serviço essencial ou, no caso que aqui nos interessa, para a manutenção de um posto de trabalho, não podendo falar-se aqui de uma verdadeira liberdade de escolha146. Quando uma das partes esta submetida ao poder contratual de outrem, não usufruindo de suficiente margem de defesa dos seus próprios interesses e de autoafirmação, o seu consentimento em relação ao contrato e aos vários termos deste não confere qualquer garantia substancial de integrar uma manifestação verdadeira de autodeterminação".

Assim sendo, propõe Teresa Coelho Moreira que o acento tónico nesse tipo de relação não devia estar no consentimento à semelhança do que sucede no direito civil, mas que, na esfera do direito laboral (que deve proteger o trabalhador como parte mais fraca da relação) devendo-se priorizar o "princípio da finalidade e no prosseguimento de fins específicos e não de outros, colocando o acento tónico neste principio e na ideia do tratamento ser pertinente e necessário, respeitando sempre o principio da proporcionalidade" .

Assim sendo, conclui, o único pressuposto legitimador para tratamento de dados pessoas do trabalhador é aquele que derivar da prossecução de interesses legítimos da entidade empregadora aferíveis em função do caso concreto, e nos termos do art.º 6.º, n. 1, alínea b), do RGPD, quando o tratamento for necessário para a execução do contrato de trabalho.

Convenção da União Africana sobre a Cibersegurança e Proteção de Dados Pessoais considera consentimento [do sujeito do titular de dados] como sendo qualquer manifestação de vontade expressa, inequívoca, livre, específica e informada através da qual a pessoa interessada ou o seu representante legal, judicial ou convencional aceita que os dados sejam processados manual ou eletronicamente.

Embora tenhamos enfocado dados sensíveis na perspetiva da saúde, por ser aquela que intuitivamente poderia levar a uma maior discriminação das pessoas ou serem utilizadas com fins discriminatórias, na mesma convenção citada, é considerado dados

sensíveis outros tipos de dados além da de saúde,, verbi gratia, os relativos às opiniões ou actividades, religiosas, filosóficas, políticas, sindicais, bem como os relacionado à vida sexual ou raça, saúde, medidas sociais, processos judiciais, sanção penais ou administrativas.

Protecção

A questão da tutela dos dados pessoais vai além de uma questão puramente individual, no que tange aos direitos personalíssimos da pessoa, na actual sociedade de informação é condição necessária para uma democracia sã, onde a sociedade como colectividade, salvaguarda e tutela os direitos das pessoas.

"Sin una concreta protección del manejo de los datos personales muchos derechos individuales pueden quedar en la letra de la ley - cuanta maior la tutela de la persona frente al tratamiento de sus datos, maior vigencia del modelo de Estado democrático". (La Protección de Datos Personales en Internet y Habeas data -, Revista Derecho y Tecnología n.º 13/2012 - ISSN: 1317-9306)

Uma protecção efectiva dos dados pessoais sensíveis deve observar os princípios da responsabilidade, da limitação, da qualidade dos dados, confidencialidade, protecção da segurança, imparcialidade, autodeterminação informativa, consentimento do titular.

Excepção à proibição de tratamento de dados sensiveis.

O Regulamento Geral Europeu de proteção de dados, assim como as diversas leis que nele se inspirou reconhece como legitima algumas situações excepções à probiçao de tratamento de dados sensiveis, em especial, os dados genéticos e os dados de saúde, indica que situações de interesse público essencial, de medicina preventiva o laboral, e de saúde pública geral, protecção de ameaças transfronteiriças graves para a saúde, a salvaguarda de elevados níveis de qualidade e segurança sanitária e de produtos, incluindo medicamentos. Casos de investigação científica, histórica ou fins estatísticos, podem legitimar tratamentos de dados considerados sensíveis.

Com a crescente onda de digitalização da justiça, através de processamento eletrónico dos processos, torna-se imperioso, face aos desafios que o mundo digital comporta, em suas várias possibilidades de acções, id est, face a possibilidade de intrusões ilegítimas nas redes de dados judiciais, surge nítido "a necessidade de protecção dos dados pessoais constantes dos mesmos, que deve depois ser compatibilizada com o funcionamento do próprio sistema judicial", frisa Oliveira Fernandes.

Todavia, apesar da sua relevante e imperiosa importância, e porque, a finalidade e os pressupostos do sistema judicial compartilha com a tutela da vida privada, intimidade e dados pessoais igual valor constitucional, ainda que difícil, é essencial efetuar a concordância prática entre aqueles valores constitucionais, os direitos fundamentais garantidos aos sujeitos processuais (como, desde logo, o direito ao contraditório), e a tutela dos dados pessoais que estão recolhidos nos respetivos processos judiciais.

REFERÊNCIAS BIBLIOGRÁFICAS

La Cultura de la Conectividad, Una Historia Crítica de las Redes Sociales, Siglo Veintiuno Editores, 2016.

da Veiga, L. A., & Aires, j. R. (1994). Dados e Informações na Internet: é legitimo o uso de Robôs para formação de base de dados de clientes? (in Direito e Informática, editora Manole, 1ª edição.

Protecção de dados pessoais como direito fundamental autónomo na Constituição Brasileira de 1988, in Estudos sobre Lei Geral de Proteção de Dados, Doutrina e aplicação no âmbito Laboral, organizado por Luciane Cardoso Barzotto, Ricardo Hofmeister de Almeida Martins Costa - Porto Alegre: Escola Judicial do Tribunal Regional do Trabalho da 4a Região. Diadorim Editora, 202, página 144 e seguintes. (acesso 27.07.2023)

Tratamento de dados pessoais sensíveis ligados a saúde do trabalhador à luz da Lei Geral de Proteção de Dados

(LGPD), Marina Richard de Toledo, Ricardo Goldschmidt - in Estudos sobre Lei Geral de Proteção de Dados, Doutrina e aplicação no âmbito Laboral.

organizado por Luciane Cardoso Barzotto, Ricardo Hofmeister de Almeida Martins Costa - Porto Alegre: Escola Judicial do Tribunal Regional do Trabalho da 4a Região. Diadorim Editora, 202, página 144 e seguintes. (acesso 27.07.2023)

A Declaração Internacional sobre Dados Genéticos Humanos, de 16 de outubro de 2003, da UNESCO, define Dados biomédicos como sendo aquelas "información sobre las características hereditarias de las personas, obtenida por análisis de ácidos nucleicos outros análisis científicos" (https://es.unesco.org/about-us/legal-affairs/declaracion-internacional-datos-geneticos-humanos). Acesso 25.07.2023).

A Lei de Proteção de Dados Pessoais - in Direito da Sociedade da Informação, volume II, coimbra editora 2001, p. 156.

Privacidade da Informação no setor da Saúde – Serviços Partilhados do Ministério da Saúde, Portugal - https://spms.min-saude.pt/wp-content/uploads/2017/03/Guia-Privacidade-SMPS_RGPD_digital_20.03.172-v.2.pdf. acesso 28.07.2023

Protécción de Ddos de Salud en el Âmbito Laboral: Una Perspetiva Española, Francisca R. Fernández - O consentimento do Trabalhador e o Regulamento Geral de Proteção de Dados, in Estudos sobre Lei Geral de Proteção de Dados, Doutrina e aplicação no âmbito Laboral, organizado por Luciane Cardoso Barzotto, Ricardo Hofmeister de Almeida Martins Costa - Porto Alegre: Escola Judicial do Tribunal Regional do Trabalho da 4a Região. Diadorim Editora, 202, página 109 e seguintes. (acesso em 25.07.2023)

Baía, G. (2021). Breves Comentários à LPDP - da República Democrática de São Tomé e Príncipe, AAFDL, p. 77.

Segurança da Informação. Proteção da Privacidade e dos Dados Pessoais, Revista Nação e Defesa, n.º 117, 3ª série /2017.

Protécción de Ddos de Salud en el Âmbito Laboral: Una Perspetiva Española, Francisca R. Fernández - O consentimento do Trabalhador e o Regulamento Geral de Proteção de Dados, in Estudos sobre Lei Geral de Proteção de Dados, Doutrina e aplicação no âmbito Laboral, organizado por Luciane Cardoso Barzotto, Ricardo Hofmeister de Almeida Martins Costa - Porto Alegre: Escola Judicial do Tribunal Regional do Trabalho da 4a Região. Diadorim Editora, 202, p. 104 e seguintes. (acesso em 25.07.2023)

Porteção de Dados e o Sistema Judicial Português – Uma Síntese: José Joaquim Fernandes Oliveira Martins - in Estudos sobre Lei Geral de Proteção de Dados, Doutrina e aplicação no âmbito Laboral, organizado por Luciane Cardoso Barzotto, Ricardo Hofmeister de Almeida Martins Costa - Porto Alegre: Escola Judicial do Tribunal Regional do Trabalho da 4a Região. Diadorim Editora, 202, p. 112 e seguintes. (acesso 26.07.2023)

Porteção de Dados e o Sistema Judicial Português – Uma Síntese: José Joaquim Fernandes Oliveira Martins - in Estudos sobre Lei Geral de Proteção de Dados, Doutrina e aplicação no âmbito Laboral, organizado por Luciane Cardoso Barzotto, Ricardo Hofmeister de Almeida Martins Costa - Porto Alegre: Escola Judicial do Tribunal Regional do Trabalho da 4a Região. Diadorim Editora, 202, p. 112 e seguintes. (acesso 26.07.2023)