Parecer n.º 42

Tratamento de dados biométricos para efeitos de registo de tempos de trabalho e de assiduidade e pontualidade

I – Factos

1. O Regulamento Geral de Proteção de Dados (RGPD)[1] veio alterar substancialmente a responsabilidade de quem procede ao tratamento de dados pessoais, nomeadamente no que toca ao aumento da segurança e da proteção da privacidade dos titulares dos dados, cabendo ao responsável pelo tratamento garantir a conformidade com o Regulamento, designadamente a legitimidade para o tratamento dos dados.

2. O RGPD prevê que os Estados-Membros, em determinadas circunstâncias, legislem no sentido de legitimarem determinados tratamentos de dados.

3. A Lei n.º 58/2019, de 8 de agosto[2] ('nova LPDP'), que assegura a execução do RGPD na ordem jurídica nacional, veio permitir o tratamento de dados biométricos dos trabalhadores para controlo de assiduidade e de acesso às instalações da entidade patronal.

4. Com este enquadramento e demais legislação aplicável; com o intuito de verificar a adequação da instalação de equipamento de tratamento de dados biométricos dos trabalhadores da Universidade de Coimbra (UC); e, com o propósito de indicar medidas técnicas e organizativas destinadas a atenuar os riscos que possam evitar consequências negativas para a privacidade dos trabalhadores da UC e o seu direito fundamental à proteção de dados, emite-se o presente parecer.

II – Fundamentos

A. Conceitos e princípios essenciais

1. O RGPD é aplicável quando esteja em causa o tratamento de dados pessoais[3].

2. Não existe uma lista taxativa de tudo o que se considera como dados pessoais, porém, o Regulamento refere-os como os dados que permitem identificar ou tornar identificável uma pessoa.

3. Acrescenta-se ainda que, para efeitos de aplicação do RGPD, há dados pessoais que são considerados especiais (sensíveis), abrangidos pelo art.º 9.º, onde se inserem, entre outros, os dados biométricos, cujo tratamento, em regra, é proibido, exceto nas condições previstas no referido artigo[4] .

4. A distinção entre "dados sensíveis" e não sensíveis é complexa, não havendo, porém, dúvidas que os dados biométricos se revestem de grande sensibilidade, tanto mais que há autores que consideram existir tecnologia recente que permite identificar, por exemplo, a orientação sexual, a partir de fotos faciais[5] ou identificar a religião através da presença de determinadas peças de vestuário.

5. Dentro das Categorias Especiais de Dados Pessoais, incluem-se os identificadores que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, a saúde e a genética, a **biometria** que identifique uma pessoa de forma inequívoca, a vida sexual ou orientação sexual,

[1] RGPD - Regulamento (UE) 2016/679, de 27 de abril.
[2] Por questões de segurança, todas as hiperligações deste Parecer remetem para subdomínios de: www.uc.pt/protecao-de-dados
[3] Art.º 4.º/1 do RGPD, disponível aqui.
[4] Art.º 9.º do RGPD, disponível aqui.
[5] Algoritmo criado pela Universidade de Stanford – "Deep neural networks are more accurate than humans at detecting sexual orientation from facial images".

as condenações penais e infrações, as aptidões intelectuais e profissionais, os traços de personalidade ou desempenho profissional, entre outros aspetos sensíveis da vida de uma pessoa.

6. O RGPD define «Dados biométricos» como "dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos"[6].

7. O Grupo de Trabalho do artigo 29 (GT29[7]), através da WP136, define dados biométricos os que possuem caraterísticas físicas ou comportamentais mensuráveis, que podem ser utilizados para a verificação de uma identidade. Doutro modo, são "propriedades biológicas, características fisiológicas, traços físicos ou ações reproduzíveis, na medida em que essas características e/ou ações sejam simultaneamente únicas a essa pessoa e mensuráveis, mesmo que os padrões utilizados na prática para medi-las tecnicamente envolvam um certo grau de probabilidade".

8. Como exemplos mais comuns deste tipo de dados biométricos, temos as impressões digitais, os padrões da retina, a estrutura facial, a voz, mas também a geometria das mãos, os padrões das veias ou mesmo uma habilidade profundamente enraizada ou outra característica comportamental (tal como a assinatura manual, caligrafia, forma particular de andar ou falar, etc...)[8].

9. Ainda que o considerando (51) do RGPD refira expressamente que "O tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular", facilmente se conclui, pelas razões expostas no ponto anterior, que as imagens que identifiquem inequivocamente pessoas, podem vir a ser inseridas na categoria especial de dados pessoais.

10. À luz do Regulamento, o "tratamento de dados pessoais"[9] engloba todas as atividades que reflitam o ciclo de vida da informação, desde a sua recolha até à sua destruição.

11. As regras fundamentais que qualquer tratamento de dados pessoais deve observar, decorrem dos princípios consagrados no art.º 5.º do RGPD[10], competindo ao "responsável pelo tratamento"[11] de dados pessoais garantir o cumprimento daqueles princípios e ser capaz de comprovar que as operações de tratamento de dados decorrem em conformidade com os seguintes princípios:
    - Os dados são processados de forma legal, justa e transparente ("licitude, lealdade e transparência");
    - Os dados são recolhidos para finalidades determinadas, explícitas e legítimas e não serão tratados posteriormente de forma incontável com essas finalidades, sem prejuízo de tratamento adicional para fins de arquivo de interesse público, pesquisa científica ou histórica ou para fins estatísticos ("limitação das finalidades");
    - Os dados são adequados, pertinentes e limitados ao necessário em relação à finalidade para a qual são tratados ("minimização de dados");
    - Os dados são exatos e, sempre que necessário, atualizados ("exatidão");
    - Os dados não serão conservados mais tempo do que o necessário ("limitação da conservação");
    - Os dados são tratados de uma maneira que garanta a segurança apropriada, incluindo proteção contra processamento não autorizado ou ilegal e contra perda, destruição ou dano acidental, usando medidas técnicas ou organizacionais apropriadas ("integridade e confidencialidade").

---

[6] Art.º 4.º/14 do RGPD, disponível aqui.

[7] O GT29 foi um grupo de trabalho europeu independente, instituído pela Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995 (tendo em conta os artigos 29.º e 30.º da referida diretiva) que lidou com as questões relacionadas com a proteção de dados pessoais e da privacidade até 25 de maio de 2018 (data de aplicação do RGPD).

[8] As amostras de tecidos humanos, ou de sangue, são fontes de que se podem extrair dados biométricos, mas não são em si dados biométricos (tal como, por exemplo, um padrão de impressões é um dado biométrico mas o próprio dedo não o é). In WP136

[9] Art.º 4.º/2 do RGPD, disponível aqui.

[10] Artigo 5.º do RGPD - Princípios relativos ao tratamento de dados pessoais.

[11] Art.º 4.º/7 do RGPD, disponível aqui.

12. Por analogia, deve ainda ser considerado o disposto no art.º 25.º da 'nova LPDP', designadamente:
    - Obedecer aos princípios da finalidade e da minimização previstos no art.º 5.º do RGPD.

13. Por outro lado, qualquer tratamento de dados pessoais deve ser lícito e, portanto, deve assentar numa base legal válida que fundamente o tratamento dos dados (art.º 6 e 9.º do RGPD).

14. Mesmo que a condição para a licitude do tratamento não seja obtida através do consentimento, para garantia dos direitos dos titulares dos dados, o responsável pelo tratamento está sempre obrigado a facultar ao titular um conjunto de informações transparentes sobre as atividades de tratamento, bem como sobre os seus direitos e a forma do seu exercício[12].

15. Outros conceitos inscritos no RGPD, e relevantes no presente contexto, podem ser consultados aqui.

B. Dados biométricos e relação laboral

16. O art.º 202.º/1 do Código do Trabalho determina que "O empregador deve manter o registo dos tempos de trabalho, incluindo dos trabalhadores que estão isentos de horário de trabalho, em local acessível e por forma que permita a sua consulta imediata" e que deve manter este registo durante cinco anos, contendo a indicação das horas de início e termo do tempo de trabalho, bem como das interrupções ou intervalos que nele não se compreendam, por forma a permitir apurar o número de horas de trabalho prestadas por trabalhador, por dia e por semana.

17. Uma das possibilidades de manter o controlo de assiduidade e acesso em ambientes laborais é o recurso aos dados biométricos, atendendo ao facto de o êxito destes sistemas contribuírem para aumentar o nível de segurança na identificação, através de uma autenticação fácil, rápida e prática, garantindo simultaneamente a fiabilidade no cálculo dos tempos de trabalho.

18. No entanto, o desenvolvimento tecnológico que permite a citada fiabilidade, também se traduz no risco de uma possível discriminação genética ou em novas ameaças aos direitos fundamentais, como a perda do anonimato ou o rastreamento da circulação de pessoas (por exemplo, através de *smartphones*).

19. Apesar do exposto, o tratamento de dados biométricos é permitido em contexto laboral, desde que seja respeitado o art.º 18.º do Código do Trabalho[13], com exceção do disposto no n.º1).

20. Por outro lado, de acordo com o art.º 9.º/2/b, do RGPD, podem ser tratados dados sensíveis, designadamente dados biométricos, se "o tratamento for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social, na medida em que esse tratamento seja permitido pelo direito da União ou dos Estados-Membros ou ainda por uma convenção coletiva nos termos do direito dos Estados-Membros que preveja garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados".

21. No mesmo enquadramento legal, os dados biométricos só podem ser utilizados se esta utilização for adequada, pertinente e não excessiva, ficando o tratamento igualmente obrigado ao respeito pelo princípio da limitação da finalidade, juntamente com os outros princípios de proteção de dados; em especial, os princípios da proporcionalidade, da necessidade e da minimização dos dados.

---

[12] RGPD, Art.º 13.º - Informações a facultar quando os dados pessoais são recolhidos junto do titular e art.º 14.º - Informações a facultar quando os dados pessoais não são recolhidos junto do titular.

[13] "Dados biométricos
[...] 2 - O tratamento de dados biométricos só é permitido se os dados a utilizar forem necessários, adequados e proporcionais aos objectivos a atingir.
3 - Os dados biométricos são conservados durante o período necessário para a prossecução das finalidades do tratamento a que se destinam, devendo ser destruídos no momento da transferência do trabalhador para outro local de trabalho ou da cessação do contrato de trabalho. [...]
5 - Constitui contra-ordenação grave a violação do disposto no n.º 3."

22. Assim, ao analisar a proporcionalidade de um sistema biométrico, deve ponderar-se previamente:
- Se o sistema é necessário para suprir a necessidade identificada, isto é, se é essencial para suprir essa necessidade e não se é o mais prático ou o que tem melhor relação custo-eficácia;
- A probabilidade de o sistema ser eficaz para suprir essa necessidade pelo facto de recorrer às características especificas da tecnologia biométrica que tenciona utilizar;
- Se a perda de privacidade que daí decorre é proporcional aos benefícios previstos (se o benefício for relativamente pouco significativo, nomeadamente uma maior conveniência ou uma ligeira redução de custos, então a perda de privacidade não é adequada);
- Avaliar se a finalidade pode ser atingida com recurso a meios menos invasivos.

23. Com vista à dissipação de questões relacionadas com a licitude deste tipo de tratamento, o legislador nacional, através da 'nova LPDP', preocupou-se em autonomizar e em sistematizar num único artigo, o que se relaciona com as relações laborais:
- Quanto à legitimidade para o tratamento dos dados pessoais dos trabalhadores, por parte do empregador, o legislador demonstrou preocupação em esclarecer o que já vinha preconizado no RGPD, ou seja, que os dados pessoais podem ser tratados dentro das finalidades e dos limites definidos no Código do Trabalho, em legislação complementar ou em regimes setoriais;
- Quanto à utilização da biometria para o controlo de pontualidade e assiduidade do trabalhador, o legislador trouxe resposta a um vazio legal, uma vez que o RGPD proibia este tipo de tratamento de dados especiais, condicionando-o ao consentimento do titular dos dados pessoais ou a legislação própria de cada Estado-Membro. Ora, considerando que o consentimento nas relações laborais, em regra, não é válido[14], foi através 'nova LPDP' que se veio legitimar as práticas vigentes.

24. Assim, de acordo com o art.º 28.º/6 da 'nova LPDP': **"**O tratamento de dados biométricos dos trabalhadores só é considerado legítimo para controlo de assiduidade e para controlo de acessos às instalações do empregador, devendo assegurar-se que apenas se utilizem representações dos dados biométricos e que o respetivo processo de recolha não permita a reversibilidade dos referidos dados".

25. Ficou, no entanto, por esclarecer se a utilização deste sistema é apenas para controlo de assiduidade e de acesso às instalações físicas[15] da entidade patronal, ou se existe a possibilidade de se enquadrar aqui situações de acessos informáticos e/ou acessos a outras tecnologias.

26. Mais, esta disposição legal não dispensa o cumprimento das demais obrigações do RGPD, nomeadamente, dependendo do caso concreto, a necessidade de uma Avaliação de Impacto sobre a Proteção de Dados (AIPD), antes de se iniciar o tratamento dos dados biométricos.

C. Mecanismos de recolha de dados biométricos

27. Segundo o GT80, os sistemas biométricos são: «Aplicações de tecnologias biométricas, que permitem a identificação automática e/ou a autenticação/verificação de uma pessoa. As aplicações para fins de autenticação/verificação são frequentemente utilizadas para diversas tarefas em setores completamente diferentes e sob a responsabilidade de uma vasta gama de entidades.»[16].

28. "Os dados obtidos durante a inscrição podem ser armazenados localmente no centro de operações em que a inscrição decorrer (por exemplo, num leitor), para utilização posterior, ou num dispositivo que a pessoa traz consigo (por exemplo, num cartão inteligente), ou poderão ser enviados e armazenados numa base de dados centralizada à qual um ou mais sistemas biométricos têm acesso."[17]

---

[14] "A subordinação jurídica típica de uma relação de trabalho subordinado implica uma posição de supremacia do credor da prestação de trabalho e a correlativa posição de sujeição do trabalhador, cuja conduta pessoal, na execução do contrato, está necessariamente dependente das ordens, regras ou orientações ditadas pelo empregador, dentro dos limites do contrato e das normas que o regem. (In acórdão n.º 5/13.1T4AGD.C1, do TRC, de 2014.04.03). Ora, o consentimento conforme preconizado no RGPD tem de ser livremente obtido, o que não pode ser garantido numa relação se subordinação.

[15] Ver nota 22

[16] In Parecer 3/2012 (WP132) sobre a evolução das tecnologias biométricas do GT29.

[17] *Idem*.

29. Após a inscrição biométrica e o armazenamento biométrico há lugar às correspondências biométricas que configuram o "processo de comparação dos dados biométricos/modelo (obtidos durante a inscrição) com dados/modelos biométricos recolhidos a partir de uma nova amostra para efeitos de identificação, verificação/autenticação ou categorização".[18]

30. Aquando da inscrição biométrica podem ser recolhidos diversos dados pessoais, entre os quais a impressão digital, a retina, a voz, reconhecimento vascular da palma da mão, reconhecimento vascular do dedo ou reconhecimento facial.

C. AIPD

31. Uma AIPD é um processo contínuo que visa estabelecer e demonstrar a conformidade do tratamento de dados com o RGPD e deve ser encarada como um instrumento de apoio à tomada de decisão em relação ao tratamento de dados pessoais.

32. Neste processo são descritas as características dos dados pessoais e o tratamento a que vão ser sujeitos, é avaliada a sua necessidade e proporcionalidade, bem como as medidas necessárias para gerir os riscos para os direitos e liberdades das pessoas, assim como os efeitos do tratamento a privacidade dos titulares dos dados[19].

33. De acordo com o art.º 35.º/1 do RGPD, "Quando um certo tipo de tratamento for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento" a uma AIPD.

34. De acordo com o art.º 35.º/3/b do RGPD, a realização de uma AIPD é obrigatória, nomeadamente, no tratamento em grande escala de categorias especiais de dados a que se refere o art.º 9.º/1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o art.º 10.º.

35. Decorre do art.º 35.º/4, que a Comissão Nacional de Proteção de Dados (CNPD) elabora e torna pública uma lista dos tipos de operações de tratamento sujeitos ao requisito de AIPD[20].

36. Através do Regulamento n.º 798/2018, publicado a 30 de novembro, a CNPD aprovou a lista de tratamentos de dados pessoais sujeitos a AIPD, que acrescem à prevista no artigo 35.º/3 do RGPD, entre os quais, no n.º 7, o "Tratamento de dados biométricos para identificação inequívoca dos seus titulares, quando estes sejam pessoas vulneráveis[21], com exceção de tratamentos previstos e regulados por lei que tenha sido precedida de uma avaliação de impacto sobre a proteção de dados".

37. Assim, pretende-se de uma AIPD as recomendações de melhoria e a adotação de medidas adequadas e necessárias para assegurar e poder comprovar que os tratamentos de dados estão em conformidade com o RGPD, tendo em conta a natureza, âmbito, contexto e finalidades dos tratamentos de dados, bem como os riscos que deles podem decorrer para os direitos e liberdades dos cidadãos.

38. Pretende-se ainda, determinar as medidas necessárias para confirmar um nível de segurança do tratamento e que garantam a confidencialidade e a integridade dos dados e que previnam a destruição, perda e alterações acidentais ou ilícitas ou, ainda, a divulgação ou acesso não autorizados de dados.

39. Em resumo e de acordo com o art.º 35.º/7 do RGPD, a AIPD deve incluir, pelo menos:
• Uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento;

---

[18] Ibi*dem*.

[19] In "Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679" do GT29 (WP 248 rev.01).

[20] Do mesmo modo, o art.º 57.º/1/k refere que é atribuição da autoridade de controlo elaborar e conservar uma lista associada à exigência de realizar uma AIPD, nos termos do art.º 35.º/4.

[21] Cf. Critério 7 das Orientações citadas WP248 rev.01.

- A avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos;
- A avaliação dos riscos para os direitos e liberdades dos titulares dos direitos; e
- As medidas previstas para fazer face aos riscos previstos.

III – Considerações finais

1. Face ao enquadramento legal acima exposto e aos requisitos anunciados para um adequado tratamento de dados biométricos para controlo de assiduidade, ou para controlo de acesso às instalações da entidade patronal, entende-se que este tratamento é legitimo, salvo melhor opinião, apenas quando os métodos adotados sejam adequados, necessários e proporcionais face aos direitos dos trabalhadores e às garantias de equilíbrio entre os interesses e os direitos em presença.

2. Assim, sendo óbvio que este tratamento de dados biométricos é suscetível de contender com a privacidade dos trabalhadores, propõe-se[22] que o responsável pelo tratamento:
   - Procure sempre o meio menos invasivo, escolhendo, sempre que possível, um método não biométrico;
   - Questione as razões que o levaram a optar por um sistema de controlo biométrico, especifique o objetivo a atingir pelo sistema e avalie a proporcionalidade dos dados a incluir no sistema, utilizando para o efeito apenas os dados relevantes para que a finalidade seja atingida (dados estritamente necessários e indispensáveis);
   - Determine se as medidas de segurança adotadas são adequadas e eficazes, os direitos a atribuir aos trabalhadores e, se a aplicação dispõe de um mecanismo próprio para o exercício desses direitos;
   - Assegure que apenas são utilizadas representações dos dados biométricos e que não seja possível, através do processo de recolha, a reversibilidade dos referidos dados (por exemplo, não pode ser reconstituída a impressão digital através das representações dos dados biométricos);
   - Informe (transparência) o trabalhador sobre aspetos como as finalidades do tratamento, os sistemas e meios utilizados, o prazo e a informação guardada, quem pode aceder aos dados e em que circunstâncias, como é que os dados são protegidos e, também, os direitos dos trabalhadores, neste âmbito;
   - Utilize tecnologias que não envolvam qualquer violação dos direitos de personalidade dos trabalhadores;
   - Garanta que a recolha de dados biométricos não tem qualquer implicação com a integridade física do trabalhador, não afetando, igualmente, o seu direito à identidade pessoal e à intimidade da vida privada, ambos garantidos constitucionalmente no art.º 26.º da CRP;
   - Assegure que a localização dos equipamentos de leitura dos dados biométricos não permitem controlar a circulação dos trabalhadores no interior das instalações[23];
   - Conserve os dados pessoais pelo período necessário para a prossecução das finalidades do tratamento, destruindo-os no momento da transferência do trabalhador para outro local de trabalho ou da cessação do contrato de trabalho;
   - Obtenha parecer prévio da Comissão de Trabalhadores da UC, dando cumprimento ao disposto no artigo 24.º dos Estatutos daquela comissão.

3. Relativamente às medidas técnicas, sugere-se que o responsável pelo tratamento:
   - Mantenha registos de todas as atividades de tratamento[24], designadamente para controlo e garantia de que a finalidade original é respeitada;

---

[22] Atenta à deliberação de 26/02/2004, da CNPD, sobre os princípios aplicáveis ao tratamento destes dados para controlo de acessos e assiduidade dos trabalhadores, bem como sobre o enquadramento legal efetuado.

[23] Exemplifica o GT29: "Um empregador mantém uma sala com servidores onde os dados empresariais sensíveis, os dados pessoais relativos aos empregados e os dados pessoais relativos aos clientes são armazenados em formato digital. A fim de cumprir as obrigações jurídicas para proteger os dados contra o acesso não autorizado, o empregador tinha instalado um sistema de controlo de acesso que regista a entrada e a saída dos empregados que têm a devida autorização para entrar na sala. Caso qualquer peça de equipamento venha a desaparecer ou os dados sejam suscetíveis de acesso não autorizado, perda ou furto, os registos mantidos pelo empregador não lhe permitem determinar quem teve acesso à sala nessa altura. Dado que o tratamento é necessário e não prevalece o direito ao respeito da vida privada dos empregados, pode ser no interesse legítimo (...), se os empregados foram adequadamente informados sobre a operação do tratamento. No entanto, a monitorização contínua da frequência e da entrada e da saída exatas dos empregados não pode ser justificada, se esses dados forem também utilizados para outros fins, como, por exemplo, a avaliação do desempenho dos empregados." (in Parecer 2/2017 do GT29).

[24] Art.º 30.º RGPD - Registos das atividades de tratamento.

- Grave / armazene os dados em modelos biométricos próprios de modo a garantir que os trabalhadores só podem ser identificados num sistema;
- Utilize um sistema que permita a anulação da ligação de identidade, quer para a renovar, quer para a apagar definitivamente;
- Garanta a cifragem e decifragem biométricas na gravação / armazenamento;
- Utilize sistemas distintos para determinar se os dados biométricos são genuínos e se os mesmos se encontram associados a um trabalhador;
- Defina uma taxa de erro de aceitação e uma taxa de erro de rejeição próxima do zero (a utilização de sistemas com deficiente grau de desempenho[25] pode violar o princípio da exatidão[26] e o da qualidade dos dados[27] e podem comprometer a finalidade do tratamento e criar dificuldades acrescidas ao trabalhador, que se podem vir a refletir no exercício dos seus direitos);
- Exija garantia escrita do fabricante, de que as chaves dos algoritmos não são cedidas a terceiros, nem à própria UC, e de que os sistemas não permitem a reversão;
- Exija do seu fornecedor informação detalhada do software e das características dos equipamentos, bem como a apresentação de soluções mais seguras.

4. Do mesmo modo, propõe-se que o trabalhador deva conhecer:
   - A identificação e os contactos do responsável pelo tratamento dos dados ou de quem age por ele;
   - Os contactos do Encarregado de Proteção de Dados;
   - A finalidade e licitude do tratamento;
   - O prazo de conservação dos dados;
   - Os seus direitos e como os exercer;
   - Se existe interconexão deste sistema com o sistema de gestão de pessoal/remunerações;
   - As principais medidas técnicas e organizativas de segurança implementadas.

5. Por último, e para colmatar os possíveis riscos de ineficiência do sistema, propõe-se que o mesmo seja testado num período experimental, eventualmente com recurso a outras tecnologias complementares de dupla verificação/validação do registo, como a visualização do nome e/ou outros dados do trabalhador.

Coimbra, 31 de março de 2022

Maria João Carvalho (Correlatora)

Paulo Simões Lopes (EPD-Relator)

Ana Luísa Gonçalves (Correlatora)
Bolseira de Estágio Curricular

[25] Uma AIPD deve determinar, em especial, o risco de usurpação de identidade, o risco do desvio da finalidade e o risco de violação dos dados.

[26] Os dados são "Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («exatidão»);". in RGPD, art.º 5º/1/a - Princípios relativos ao tratamento de dados pessoais.

[27] "A aplicação dos princípios gerais de proteção de dados, nomeadamente a limitação das finalidades, a minimização dos dados, a limitação dos prazos de conservação, **a qualidade dos dados**, a proteção dos dados desde a conceção e por defeito, o fundamento jurídico para o tratamento, o tratamento de categorias especiais de dados pessoais, as medidas de garantia da segurança dos dados e os requisitos aplicáveis a transferências posteriores para organismos não abrangidos pelas regras vinculativas aplicáveis às empresas;". In RGPD, Art.º 47.º - Regras vinculativas aplicáveis às empresas.