

## PRINCÍPIOS SOBRE A UTILIZAÇÃO DE DADOS BIOMÉTRICOS NO ÂMBITO DO CONTROLO DE ACESSOS E DE ASSIDUIDADE

### *Considerando que*

1. O recurso a sistemas biométricos tem vindo, recentemente, a apresentar-se como um meio tecnológico que visa substituir ou reforçar a segurança dos meios tradicionais de controlo de entradas e saídas, sendo ainda de extrema utilidade quando se pretende – por razões de segurança ou de segredo – restringir, nomeadamente, o acesso a locais cuja entrada é privilégio de alguns.
2. Os sistemas biométricos têm outras vantagens em relação aos sistemas tradicionais, na medida em que a informação necessária para permitir o acesso não é «perdível» ou susceptível de apropriação ilícita. Por outro lado, a pessoa não necessita de recordar números, códigos ou qualquer outra chave de identificação.
3. Na introdução de novos sistemas não pode deixar de ser feita uma comparação, nas várias perspectivas relevantes (em particular em termos de protecção de dados) entre os sistemas que existem e aqueles que se pretendem instalar.
4. Para alguns autores a biometria assenta na mensuração e na enumeração, utilizando as estatísticas e o cálculo de probabilidades com o objectivo de dar aos fenómenos biológicos uma «expressão quantitativa plausível», o que permite afirmar que se a biometria traz um pouco de precisão, ela fá-lo em detrimento da certeza.
5. Os critérios a utilizar para a escolha de um sistema biométrico têm em conta, nomeadamente, o conforto na utilização, a precisão, a relação qualidade/preço e o grau de segurança.
6. As características biométricas não deixam de representar uma parte da individualidade das pessoas, estando ligadas intrinsecamente à própria pessoa.

7. A introdução do sistema no âmbito da relação de trabalho deverá procurar obter a adesão dos trabalhadores e não ser imposto, na medida em que a sua eficácia depende, também, em grande medida, de factores psicológicos que são determinantes para a aprendizagem na utilização do sistema e na cooperação dos utilizadores, quer no momento da captura quer na fase de comparação.
8. A vulgarização dos sistemas de videovigilância e o uso descontrolado desta nova forma de tratamento demonstra, em algumas situações, que é fundamental que se tomem medidas realistas para evitar que se instale no posto de trabalho, sem justificação visível, um «clima securitário» e de suspeição generalizado, quer em relação a clientes quer a trabalhadores.
9. Importa ter uma posição prudente e equilibrada que incentive os fabricantes de sistemas biométricos a adoptar soluções técnicas que, protegendo a privacidade, minimizem os riscos de utilizações indevidas.
10. Os equipamentos biométricos registam, normalmente, uma representação digital (*template*) e não uma amostra biométrica passível de ser reproduzida, ou seja, o *template* armazenado não tem utilidade nenhuma noutros sistemas e não pode ser usado para reproduzir os dados biométricos originais. Isto é, na generalidade dos casos, os sistemas biométricos não utilizam a tecnologia de digitalização da imagem obtida, mas fazem a «codificação» dos dados recolhidos.
11. O sistema biométrico que, através do processo de algoritmização, gerou o *template* que representa numericamente a característica biométrica captada, não permite fazer a reversão e, por conseguinte, descodificar e reproduzir, de forma digitalizada, a imagem da característica biométrica (v.g. representação digitalizada da impressão digital, da íris, da geometria da mão ou da geometria facial).
12. O responsável do tratamento não dispõe, por isso, de uma base de dados de características biométricas, mas de uma lista estruturada e numeralizada dessas características.
13. Será diferente para a invasão da privacidade o armazenamento através da digitalização e referência das características biométricas ou a constituição de uma base de dados dos *templates* dessas características.
14. A centralização das características biométricas em bases de dados apresenta perigos acrescidos para a privacidade, razão pela qual não é admissível, por princípio, o seu relacionamento com outro tipo de tecnologias (v.g. videovigilância).

15. Esse relacionamento não prejudica a possibilidade de utilização de «sistemas multimodais», caracterizados pelo recurso a mais de uma característica biométrica para conferir uma maior eficácia e rigor às operações de reconhecimento ou autenticação.
16. As empresas que comercializam sistemas biométricos garantem, muitas vezes, que está totalmente assegurada a privacidade uma vez que esses sistemas não permitem a «reversão» ou comparação dos *templates*, tanto mais que as chaves dos respectivos *templates* estão na posse do fabricante e são inacessíveis às entidades que fornecem ou adquiram os equipamentos.
17. O *template*, que representa a característica biométrica do indivíduo, pode ser gravado ou memorizado no sistema central, em terminais ou num suporte que o seu titular traz consigo (v.g. um cartão, um equipamento ou um código de barras).
18. Esta última tecnologia pode ser vantajosa, em termos de preservação da privacidade, para obviar à constituição de bases de dados centrais com armazenamento de características biométricas e permite uma maior rapidez na identificação do utilizador, em particular quando o sistema gere muitos utilizadores ou precisa de fazer a verificação remota. Porém, não será de esquecer que tem o inconveniente de exigir que o utilizador não se esqueça de transportar o cartão ou código de barras consigo, obrigando, ainda, à produção de novo cartão em caso de extravio ou má conservação.
19. A qualidade e aceitação de um sistema biométrico depende, fundamentalmente, da avaliação do seu grau de desempenho.
20. O grau de desempenho depende, em certa medida, da sua capacidade de resposta em termos de velocidade de identificação e, especialmente, da taxa de precisão ou de erro que apresenta.
21. Um sistema biométrico que não seja fiável cumpre de forma deficiente as finalidades que se propõe atingir, correndo o risco de tratar – especialmente em «sistemas de identificação» – informação desactualizada.
22. A existência de uma grande probabilidade de «falsos utilizadores» poderem ser aceites permite que – no contexto de uma empresa ou serviço público onde o sistema visa controlar o horário de trabalho – as apontadas deficiências no desempenho potenciem a troca de identificação de alguns trabalhadores (eventualmente com características semelhantes) e a consequente anotação de atrasos, faltas ou presenças de forma indevida.
23. A aquisição de sistemas biométricos passa pela adopção de soluções alternativas para suprir as suas insuficiências, especialmente as que resultam

- das taxas de falsas rejeições, aceitações ou impossibilidade temporária de o trabalhador apresentar o seu dado biométrico para autenticação ou reconhecimento.
24. Estes sistemas não são infalíveis e não vêm resolver todos os problemas de autenticação ou identificação, razão pela qual será de esperar que existam limitações e «imponderáveis» em matéria de qualidade de desempenho.
  25. Certos sistemas biométricos apresentam alguns riscos por não estarem convenientemente testados e por utilizarem técnicas recentes, cuja eficácia ainda não se mostra comprovada.
  26. O titular tem o direito de saber se a sua característica biométrica se encontra armazenada e obter a respectiva comprovação, nomeadamente através do desencadeamento da operação de reconhecimento ou de autenticação.
  27. A finalidade do tratamento assenta na necessidade de agilizar o cumprimento de um objectivo que a lei reconhece integrar-se no âmbito dos poderes de controlo da entidade responsável pelo tratamento: a fixação do horário de trabalho, o controlo da assiduidade e o registo do tempo de trabalho. Deste registo depende, ainda, a contabilização e o controlo do trabalho suplementar.
  28. A operação de recolha das características biométricas com a finalidade de controlo do horário de trabalho não envolve, em si mesmo, uma violação da integridade física do trabalhador, do seu direito à privacidade ou da sua intimidade.
  29. A peculiaridade deste novo método de controlo da assiduidade resulta da necessidade de o trabalhador ter de aceitar que elementos da sua identidade física, morfológica ou comportamental sejam captados e armazenados numa base de dados (ou noutra suporte) e apresentados perante um «sistema de reconhecimento» no início e termo do período de trabalho diário.
  30. Independentemente da autorização da CNPD, o titular dos dados pode, em abstracto, por força do artigo 12.º al. a) da Lei 67/98, opor-se ao tratamento sempre que haja «razões ponderosas e legítimas relacionadas com a sua situação particular» e que se apresentem com relevância para fazer prevalecer o seu direito sobre os interesses do responsável pelo tratamento.
  31. Quando a CNPD considerar que o dado biométrico se apresenta como o meio adequado para assegurar uma «finalidade legítima» – o controlo do horário de trabalho – e autorizar o tratamento com essa finalidade não cabe à CNPD pronunciar-se sobre os procedimentos e o dever de cooperação em tudo o que seja necessário à captação das características biométricas.

32. O dever de cooperação só se pode concretizar, no entanto, quando a entidade responsável pelo tratamento assegurar, junto do trabalhador, um efectivo dever de informação prévio em relação às finalidades determinantes da recolha, destinatários e condições de utilização daqueles dados, em cumprimento do disposto no artigo 10.º n.º 1 da Lei 67/98, bem como o esclarecimento de dúvidas e receios que esta nova tecnologia possa suscitar.
33. Os dados em si mesmos (impressão digital, geometria facial, íris ou retina) não se enquadram no conceito de «vida privada», nem as finalidades prosseguidas permitem um enquadramento dessas categorias de dados na previsão do artigo 7.º n.º 1 da Lei 67/98.
34. As «condições de legitimidade» do tratamento só poderão ser enquadradas numa das previsões do artigo 6.º da Lei 67/98.
35. Será de afastar o consentimento como «condição de legitimidade», em face da posição em que o trabalhador se encontra.
36. Será de afastar, igualmente, a aplicação da alínea b) do artigo 6.º na medida em que, perante a omissão do Código do Trabalho e da legislação aplicável à Função Pública em relação à possibilidade de controlo por meio de sistemas biométricos, não é possível concluir – perante disposições legais tão genéricas sobre “registo de horas de trabalho prestadas pelo trabalhador” – que se tenha pretendido fundamentar nessas disposições qualquer forma de controlo deste tipo.
37. Se não for estabelecido contratualmente o tratamento de dados biométricos por razões inerentes e determinadas pela especial natureza do contrato (v.g. entrada em locais de «alta segurança»), a mera celebração do contrato não determina, só por si, uma legitimação para o tratamento destes dados.
38. O simples facto de ter sido celebrado um contrato não implica, só por si, que o trabalhador esteja obrigado a fornecer «informações adicionais» relativas às suas características biométricas, tanto mais que esses elementos de identificação, contrariamente ao que acontece com o nome, não são imprescindíveis à perfeição da declaração negocial.
39. A legitimidade para o tratamento de dados com a finalidade de controlo do horário de trabalho (assiduidade) só poderá ter como fonte a previsão do artigo 6.º al. e) da Lei 67/98, uma vez que o tratamento é feito na «prossecação de interesses legítimos do responsável».
40. O artigo 6.º alínea e) da Lei 67/98 obriga a CNPD, em cada caso concreto, a apurar se «não prevalecem os interesses ou os direitos liberdades e garantias

- dos titulares dos dados» sobre o interesse legítimo invocado pelo responsável pelo tratamento.
41. Este procedimento é o que melhor se ajusta à aplicação do princípio da proporcionalidade e, por isso, o tratamento deve deixar de ser feito quando se revele injustificado, por ser desajustado e excessivo, ou quando – pela sua falta de fiabilidade – comprometa a finalidade determinante do tratamento.
  42. O princípio da proporcionalidade constitui, igualmente, o critério determinante das decisões relativas ao tratamento de dados biométricos tomadas pelas autoridades de protecção de dados.
  43. A eventual «invasão da privacidade» deve ser abordada nas duas fases do tratamento: (a) na fase do registo das características biométricas e do subsequente armazenamento no sistema e (b) na fase da identificação com o objectivo de assegurar o registo dos movimentos do trabalhador no local de trabalho.
  44. A operação de captação de dados biométricos – que implica a cooperação/anuência do trabalhador através da «exposição» da respectiva parte do seu corpo (dedos, mão, olho ou rosto) para tratamento das características físicas ou morfológicas da sua identidade pessoal que se pretendem coligir para fins de identificação ou autenticação – não pode ser realizada com violação da sua identidade pessoal (art.26.º da CRP), com lesão da sua integridade física (art. 25.º n.º 1 da CRP) ou com intromissão na intimidade da vida privada (artigo 26.º da CRP).
  45. Na apreciação do «grau de intromissão» importa considerar a forma como se obtêm os elementos de identificação e as finalidades que estão na base da colheita de características físicas dos trabalhadores (v.g. se representam finalidades discriminatórias).
  46. Na colheita de dados biométricos – normalmente a impressão digital, geometria da mão ou da face, padrão da íris ou reconhecimento da retina – a captação não tem qualquer implicação com a integridade física do trabalhador na medida em que a finalidade visada ou a forma como os elementos da identidade são captados não têm implicações no recato ou no pudor.
  47. A simples operação de recolha, em exclusivo, para fins de controlo da assiduidade do trabalhador não afecta o direito à identidade pessoal e da intimidade da vida privada, garantidas constitucionalmente no artigo 26.º da CRP.
  48. Em geral, a submissão à operação de recolha não se poderá traduzir numa discriminação ou violação do dever de respeito e dignidade do trabalhador,

nem afectar o recato ou pudor que a sua condição supõe, tanto mais que a finalidade que está subjacente à captação destes dados não envolve, por princípio, qualquer discriminação ou desconfiança em relação ao próprio trabalhador.

49. Não é o dado biométrico em si mesmo que pode afectar o direito à privacidade da pessoa, mas a finalidade com que é utilizado e os riscos que apresenta para a própria pessoa (risco de discriminação ou de cruzamento com outros sistemas, consequências produzidas em razão da sua falta de fiabilidade, efeitos na sua esfera pessoal no caso de falsificação ou usurpação da característica biométrica).
50. Se justifica alertar para a aplicação, com especial pertinência, do princípio contido no artigo 13.º da Lei 67/98, que proíbe a tomada de decisões com base, exclusivamente, em tratamento automatizado.
51. O princípio da proporcionalidade “impõe que qualquer tratamento de dados pessoais, atenta a sua finalidade concreta, deva ser avaliado em termos de idoneidade e de intervenção mínima”, o que envolve uma ponderação, casuística, entre a finalidade pretendida e o sacrifício ou limitação de direitos ou interesses dos trabalhadores que ela implica.
52. A utilização indevida pode ser melhor prevenida se as características biométricas não se encontrarem centralizadas numa base de dados, razão pela qual se defende, sempre que possível, o registo das características biométricas (em particular quando estiver em causa a impressão digital) em cartão que o trabalhador deve transportar.
53. A proliferação e massificação destas formas de tratamento e a possibilidade de relacionamento com outras tecnologias (v.g. videovigilância) são factores que, em termos de protecção da privacidade, não devem ser negligenciados.

**A CNPD alerta os responsáveis para a necessidade de cumprirem certos princípios de protecção de dados e informa que irá considerar os seguintes aspectos no momento da apreciação dos tratamentos de dados biométricos para controlo de acessos e de assiduidade:**

- I. O tratamento de dados biométricos, porque estamos perante dados pessoais, deve respeitar todas as condições estabelecidas na Lei 67/98, nomeadamente:
  - a) O tratamento deve ser feito com respeito pela reserva da vida privada (artigo 2.º) e para finalidades determinadas, explícitas e legítimas (art. 5.º n.º 1 al. b);
  - b) Os dados devem ser adequados, pertinentes e não excessivos em relação à finalidade e proporcionados aos objectivos que se pretendem atingir (art. 5.º n.º 1 al. c);
  - c) O responsável só pode proceder ao tratamento se, de acordo com a natureza dos dados (artigo 6.º e 7.º), estiverem preenchidas as «condições de legitimidade»;
  - d) O responsável deve fazer a notificação destes tratamentos à CNPD (art. 27.º n.º 1).
  - e) O responsável deve assegurar o direito de informação em relação à existência de tratamento, dados pessoais tratados, finalidades e entidades a quem os dados podem ser transmitidos (cf. artigo 10.º);
  - f) O responsável não pode utilizar os dados biométricos para finalidade diversa da determinante da recolha (artigo 5.º n.º 1 alínea b) da Lei 67/98);
  - g) Aos titulares dos dados deve ser assegurado o direito de acesso, rectificação ou oposição, nos termos dos artigos 11.º e 12.º alínea a).
- II. No requerimento de notificação devem ser indicadas, com detalhe, as características do sistema biométrico, as condições de tratamento e outras condições que permitam à CNPD apreciar o pedido em termos de necessidade e de proporcionalidade. Deverão ser indicados, nomeadamente:
  - a) A capacidade do sistema e o número de trabalhadores abrangidos;
  - b) Forma como é armazenada ou gravada a característica biométrica;
  - c) Taxas de falsas rejeições ou de falsas aceitações do sistema;
  - d) Formas como foi ou vai ser assegurado o direito de informação aos trabalhadores;
  - e) Especificação do tipo de relacionamento com outros tratamentos (v.g. gestão de pessoal ou de remunerações);

- f) Junção de declaração do fabricante comprovativa de que as chaves dos algoritmos não são cedidas e de que os sistemas não permitem a reversão.
- III. A preocupação primordial em relação à utilização de dados biométricos passa pela ponderação, no caso concreto, da idoneidade e da necessidade daquele meio e da conformidade dos motivos apresentados com o princípio da proporcionalidade.
- IV. A finalidade do tratamento insere-se no âmbito do exercício de poderes de controlo conferidos legalmente ao responsável do tratamento, correspondendo a uma «actividade legítima».
- V. O controlo de acessos e de assiduidade com recurso a dados biométricos apresenta-se como um meio adequado por corresponder a uma «finalidade legítima», razão pela qual esse controlo terá que ser enquadrado na previsão do artigo 6.º al. e) da Lei 67/98.
- VI. A CNPD deverá verificar, numa ponderação dos interesses em presença e em cada caso concreto, se «não prevalecem os interesses ou os direitos liberdades e garantias dos titulares dos dados» sobre o «interesse legítimo» invocado pelo responsável.
- VII. A recolha de dados biométricos – normalmente a impressão digital, geometria da mão ou da face, padrão da íris ou reconhecimento da retina – não tem qualquer implicação com a integridade física do trabalhador, não afectando, igualmente, o seu direito à identidade pessoal e à intimidade da vida privada, garantidos constitucionalmente no artigo 26.º da CRP.
- VIII. Em geral, a operação de recolha e comparação das características biométricas não constitui factor de discriminação ou violação do dever de respeito, nem afecta o recato ou pudor do trabalhador.
- IX. Se a inserção das características biométricas em cartão que o trabalhador traz consigo tem a vantagem de sossegar o trabalhador em relação ao não fornecimento da sua característica biométrica à entidade empregadora e de lhe permitir um controlo sobre a utilização dos seus dados biométricos, a verdade é que tem o inconveniente de exigir que o trabalhador tenha sempre o cartão consigo, obrigando o responsável a produzir novo cartão em caso de extravio ou mau estado de conservação.
- X. Não estando afastados riscos efectivos de falsificação ou «apropriação» das características biométricas, aspecto que tem consequências imprevisíveis para os titulares nomeadamente se caminhararmos para a utilização generalizada destes meios, a CNPD seguirá com atenção os novos desenvolvimentos tecnológicos.

- XI. A utilização de sistemas com deficiente grau de desempenho (v.g. uma elevada taxa de falsas aceitações ou de falsas rejeições) podem comprometer a finalidade do tratamento – o controlo de entradas e saídas – e criar dificuldades acrescidas ao trabalhador, que se reflectem no exercício dos seus direitos, tal como estão delineados na Lei 67/98.
- XII. Se houver este risco, deve entender-se que o sistema não reúne as condições legais para desempenhar as finalidades de controlo uma vez que, para além de a informação se encontrar desactualizada, é um factor de grande instabilidade e de falta de confiança no sistema, colocando aos trabalhadores grandes dificuldades de prova em relação à comprovação da «falsa entrada» que lhes foi atribuída pelo sistema.
- XIII. Se isso acontecer, o tratamento das características físicas intrínsecas do trabalhador contribui, nessas circunstâncias, para violar os princípios da qualidade dos dados e, em particular, o princípio da actualização, subjacentes à previsão do artigo 5.º da Lei 67/98.
- XIV. Este aspecto, que é uma «condição de licitude do tratamento», condicionará o sentido da decisão da CNPD.
- XV. Neste quadro, apresentam-se como bastante problemáticas as consequências jurídicas da utilização destas tecnologias uma vez que a «prova biométrica» tem vindo, cada vez mais, a ser questionada em face da reconhecida impossibilidade destes sistemas serem 100 por cento fiáveis.
- XVI. Por isso, impõe-se que o responsável do tratamento não encare, sem qualquer flexibilidade, a introdução destes novos sistemas como instrumentos «infalíveis» em termos de reconhecimento, devendo abordar com realismo as situações em que o trabalhador questiona a sua eficácia.
- XVII. Os fornecedores de equipamentos biométricos, que devem ser chamados pelos responsáveis dos tratamentos a detalhar as suas características, podem vir a ser envolvidos e ter um papel activo na apresentação de soluções mais seguras que impeçam a utilização de dados para outras finalidades ou que reforcem, de forma efectiva, a privacidade dos titulares dos dados.
- XVIII. Na linha do que já dispõe o artigo 17.º n.º 4 do Código do Trabalho, deve ser reconhecido ao trabalhador o «controlo sobre o tratamento dos seus dados pessoais» colocando ao seu alcance mecanismos para verificar – no momento da sua identificação/autenticação – se o sistema fez o seu reconhecimento (ou se fez um «falso reconhecimento»).
- XIX. Para obviar aos perigos decorrentes da falta de *performance* e eficácia no desempenho do sistema – que deve ser testado, na prática, durante um

período experimental adequado – será desejável que, no momento da validação/identificação do trabalhador pelo sistema, haja mecanismos de «validação» adicional que permitam um maior rigor no reconhecimento ou autenticação (por exemplo, um écran junto ao sensor que forneça o nome da pessoa ou n.º de funcionário que acabou de ser identificada, a digitação prévia do n.º de empregado a que se seguirá a apresentação da característica biométrica perante o sensor).

- XX. A utilização para finalidade não determinante da recolha carece, necessariamente, de autorização prévia da CNPD, nos termos dos artigos 23.º n.º 1 al. c) e 28.º n.º 1 al. d) da Lei 67/98.
- XXI. Os dados pessoais recolhidos não podem ser comunicados a terceiros.
- XXII. Os dados biométricos serão obrigatoriamente eliminados no momento da transferência do trabalhador para outro local de trabalho ou no caso da cessação do contrato de trabalho.
- XXIII. A CNPD considera que, pelo menos numa primeira fase, as autorizações podem vir a ser dadas por um período experimental.
- XXIV. Decorrido esse «período experimental» a CNPD fará uma avaliação destas tecnologias, podendo vir a fazer alterações, motivadas pela necessidade de observância de princípios de protecção de dados, em função das circunstâncias, condições de funcionamento e de desempenho dos sistemas biométricos.
- XXV. Os trabalhadores e os seus representantes são convidados a estar atentos ao funcionamento do sistema e a canalizar os elementos úteis para a avaliação da CNPD.

26 de Fevereiro de 2004