

## DELIBERAÇÃO N.º 984/2018

I - A Comissão Nacional de Protecção de Dados (CNPD) elaborou, em 17 de julho de 2018, projeto de deliberação, no qual foi imputada à arguida

a prática de duas violações previstas e puníveis nos termos das disposições conjugadas dos artigos 5.º, n.º 1 al. c) e artigo 5.º, n.º 1 al. f) com o artigo 83.º, n.º 5, al. a), do Regulamento Geral sobre a Protecção de Dados (Regulamento 679/2016, de 27 de abril, doravante RGPD), puníveis, cada uma delas, com coima de € 0,00 a € 20.000.000,00 ou até 4% do volume de negócios anual, consoante o montante que for mais elevado, bem como a prática de uma violação prevista e punível nos termos das disposições conjugadas do artigo 32.º, n.º 1, alíneas b) e d) e artigo 83.º, n.º 4, al. a), do RGPD, com coima de € 0,00 a € 10.000.000,00 ou até 2% do volume de negócios anual, consoante o montante que for mais elevado.

Notificada a arguida do teor do referido projeto e, nos termos do disposto no artigo 50º do Decreto-Lei nº 433/82, de 27 de outubro, para apresentar a sua defesa, veio alegar (cfr. fls. 38 a 82), em suma, que:

1. A CNPD não pode ser considerada como autoridade de controlo nacional, nos termos do artigo 51.º, n.º 1 do RGPD, porquanto não foi ainda indicada como tal formalmente. Admitir o contrário violaria o princípio da legalidade ínsito no artigo 266.º da Constituição da República Portuguesa (CRP);
2. As condutas previstas no RGPD como sancionáveis com as coimas do artigo 83.º não se encontram suficientemente densificadas, pelo que a intervenção do legislador nacional é indispensável para que as mesmas se apliquem, sob pena de violação do princípio da tipicidade formulado no artigo 29.º da CRP;
3. Reconhece a existência dos perfis de acesso nas condições relatadas no projeto de deliberação da CNPD;
4. Considera, todavia, que os profissionais com esses perfis de acesso (técnicos de ação/serviço social, nutricionistas, fisioterapeutas e psicólogos) estão sujeitos

- a obrigações de confidencialidade adequadas, nomeadamente as deontológicas;
5. Tais profissionais acedem a informação relevante e necessária para o desempenho das suas funções;
  6. Os sistemas utilizados não permitem tecnicamente a estratificação de acessos à informação com o detalhe ideal, algo que entende não lhe poder ser assacado uma vez que utiliza sistemas padronizados por terceiros, sem possibilidade de intervenção do e de uso obrigatório, dadas as determinações das entidades tutelares;
  7. Defende, ainda, que uma tal estratificação da informação será tendencialmente impossível, uma vez que, à partida, não se consegue determinar quais os dados em concreto que poderão ser relevantes para o desempenho das funções daqueles profissionais;
  8. Informa, todavia, que as últimas atualizações disponibilizadas pelos Serviços Partilhados do Ministério da Saúde resolveram algumas das questões levantadas pela CNPD, sobretudo quanto à gestão das credenciais de acessos;
  9. E declara igualmente ter já posto em prática várias das recomendações constantes da Deliberação n.º 674/2018, de 17 de julho, da CNPD;
  10. Quanto ao acesso à PDS (Plataforma de Dados da Saúde), declara que “tecnicamente um botão estar disponível para aceder à PDS não significaria que o utilizador conseguisse aceder, uma vez que o sistema informação da PDS é um sistema externo ao SClínico, pelo que deve validar por si só se o utilizador é médico ou enfermeiro”;
  11. Rebate os factos que no projeto de deliberação apontavam para a inexistência de logs de acesso ao sistema SClínico;
  12. Quanto às contas de utilizadores ativos associados ao grupo funcional de “MEDICO”, em número bastante superior aos quadros médicos declarados nos diversos relatórios e contas, admite a possibilidade de algumas dessas contas já não estarem ativas, embora advirta para a realidade da contratação de médicos em regime de prestação de serviços, o que explica alguma da disparidade entre o número de contas e o número de profissionais que efetivamente desempenham funções no

13. Assume, ainda relativamente a estas contas inativas, a correção dessas situações, com recurso a processos internos de verificação técnica;
14. Dada a impossibilidade de modelar, alterar ou corrigir os aspetos técnicos dos sistemas utilizados, entende ter agido sem culpa, logo não lhe sendo imputável qualquer conduta ilícita.

Juntou onze documentos e quatro testemunhas.

## II - Apreciação

- 1) Sobre a alegada existência de violação do princípio da legalidade em virtude de a CNPD se arrogar numa condição que, por via de lei, (ainda) não lhe pertencerá, sempre se dirá que tal argumento não procede. Desde logo, e como se explicitou no projeto de deliberação, a CNPD é, para todos os efeitos, e enquanto tal não for alterado, “a autoridade nacional que tem como atribuição controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de protecção de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei” (cfr. artigo 22.º, n.º 1 da Lei n.º 67/98, de 26 de outubro, alterada pela Lei n.º 103/2015, de 24 de agosto, doravante LPDP).
- 2) Uma tal disposição não encerra apenas uma vontade do legislador nacional em atribuir à CNPD qualquer matéria nacional ligada à proteção de dados pessoais, mas antes a distinta intenção de lhe confiar qualquer matéria desta natureza que não lhe seja especificamente vedada por lei. E não vemos como tal possa violar o princípio da legalidade.
- 3) Ademais, o RGPD encerra várias novidades tendentes a uniformizar os poderes das autoridades de controlo em toda a União Europeia (UE), justamente para permitir o efeito útil visado pela utilização deste instrumento jurídico. Tal respeita, por exemplo, à possibilidade de qualquer das autoridades de controlo na UE ser municiada com poderes de investigação e correção adequados, acabando-se, assim, com a disparidade que reinava até ao transato dia 25 de maio.

- 4) Sucede, todavia, que, em Portugal, há muito que a CNPD possui este tipo de poderes, não constituindo o RGPD relevante novidade, salvo no que toca às obrigações de cooperação com as demais autoridades de controlo da UE, sem que se olvide a transição paradigmática da heterorregulação (cuja face mais visível consistia na avaliação e autorização prévias dos tratamentos de dados pessoais) para a autoavaliação, cabendo agora aos responsáveis pelos tratamentos e subcontratantes prover pela legalidade dos tratamentos de dados pessoais que levem a cabo, sem que haja qualquer intermediação das autoridades de controlo.
- 5) A todos estes argumentos junta-se um outro, de ordem meramente formal, que é o da representação institucional de Portugal que a CNPD já assegura na UE. Com efeito, o novo Comité Europeu para a Proteção de Dados, previsto na secção 3 do Capítulo VII do RGPD, deve, nos termos do n.º 3 do artigo 68.º do regulamento, ser “composto pelo diretor de uma autoridade de controlo de cada Estado-Membro”. Este novo órgão da União Europeia pressupõe, então, que cada país seja representado pelo diretor (ou presidente) de cada autoridade de controlo dos vários Estados-membros, o que, no caso português, redundou na integração, como membro de pleno direito, da CNPD no CEPD, desde a primeira reunião datada de 25 de maio de 2018.
- 6) Quanto ao princípio da tipicidade invocado pela arguida, menos ainda nos parece ser atendível. Bastará, para o afastar, recordar, desde logo, o intuito uniformizador do regulamento, sobretudo em matéria de aplicação de coimas, expresso incontestavelmente no considerando 150 do RGPD “A fim de reforçar e harmonizar as sanções administrativas para violações do presente regulamento, as autoridades de controlo deverão ter competência para impor coimas. O presente regulamento deverá definir as violações e o montante máximo e o critério de fixação do valor das coimas daí decorrentes [sublinhado

nosso], que deverá ser determinado pela autoridade de controlo competente, em cada caso individual, tendo em conta todas as circunstâncias relevantes da situação específica, ponderando devidamente, em particular, a natureza, a gravidade e a duração da violação e das suas consequências e as medidas tomadas para garantir o cumprimento das obrigações constantes do presente regulamento e para prevenir ou atenuar as consequências da infração.”.

- 7) Para lá desta referência, o próprio Tribunal Constitucional já se referiu repetidamente ao grau de concretude exigível a normas tipificadoras de condutas contraordenacionais. Paulo Pinto de Albuquerque, no seu “Comentário do Regime Geral das Contra-Ordenações”, na anotação 16 ao artigo 2.º, ilustra-o exemplarmente quando refere que “a contra-ordenação baseada na violação de cláusulas gerais (deveres gerais de zelo e urbanidade) e outras obrigações específicas não viola o princípio da tipicidade (acórdão do TC n.º 338/2003, que incidiu sobre o artigo 82.º, al. b), do Decreto-lei n.º 422/89, de 2.12). O mesmo se pode concluir da violação do dever genérico respeitante à organização contabilística (acórdão do TC n.º 455/2006, relativo ao artigo 14.º da Lei n.º 56/98, e acórdão do TC n.º 198/2010, relativo ao artigo 29.º da Lei n.º 19/2003).”.
- 8) Relativamente à matéria de facto, é esclarecedor que a arguida confirme a existência dos perfis de acesso tal como vinham descritos no projeto de deliberação. Com efeito, a política de atribuição de credenciais de acesso permitiu que pelo menos 9 (nove) funcionários do grupo funcional “TÉCNICO/A” usufríssem do nível de acesso reservado ao grupo funcional “MÉDICO”, o que se traduz na possibilidade indiscriminada de consulta de processos clínicos de todos os utentes do hospital.
- 9) Independentemente de se reconhecer a padronização externa e disponibilização de um conjunto determinado de tipos de perfis, foi a arguida quem voluntaria e conscientemente determinou que aqueles profissionais pudessem, através de perfis não adequados às suas funções e categoria profissional, ter acesso indiscriminado aos processos clínicos de todo o hospital, ao invés de estabelecer



outros procedimentos, porventura mais morosos, mas seguramente menos intrusivos da proteção de dados pessoais que qualquer cidadão deve merecer.

- 10) Sem prescindir desse juízo crítico, compreendem-se os argumentos relativos à incapacidade de determinar, *a priori*, qual a informação relevante para cada um dos técnicos com os perfis de acesso supramencionados, dificuldade que é exponenciada pela arquitetura dos sistemas que não permitem a definição, a par e passo ou casuística do acesso a determinada informação clínica, facto que, novamente, não pode ser assacado a quem não dispõe dos instrumentos para remediar ou minorar os efeitos de tal construção.
- 11) Julgamos, até, que essa hipótese afasta o dolo direto da conduta da arguida, torna questionável o dolo necessário, mas não preclude, de forma alguma, a existência do dolo eventual. Tanto assim, que a arguida confessa ter sempre procedido com conhecimento da existência destas insuficiências do sistema, não se abstendo todavia de continuar a atribuir privilégios de acesso indevidos a um conjunto de profissionais que nunca deveriam poder aceder indiscriminadamente aos ficheiros clínicos dos clientes.
- 12) É insustentável defender que qualquer assistente social possa aceder à totalidade do ficheiro clínico do cliente para poder desempenhar a sua função, sendo ainda mais insustentável tal defesa se se possibilitar um acesso nesses moldes sem limite temporal.
- 13) Como igualmente indefensável é a existência de credenciais de acesso que permitam a qualquer médico, de qualquer especialidade, a qualquer altura aceder aos dados dos clientes de um determinado centro hospitalar. O princípio da minimização dos dados e o princípio da "necessidade de conhecer" (ou, no anglicismo "*need to know*"), vedam ou pretendem vedar a recolha, mas também o acesso e demais tratamentos a informação desnecessária para a finalidade visada.

- 14) Por tudo isto, a CNPD não pode admitir que a as limitações técnicas apontadas possam justificar a adoção irrestrita de procedimentos de validação de acessos que praticamente tornam irrelevante o núcleo essencial do direito fundamental à proteção de dados pessoais.
- 15) A alegação da arguida, que aponta uma muito maior restritividade dos perfis de acesso dos profissionais não médicos possuidores dos perfis do grupo funcional "TECNICO" e grupo de atividade "MEDICO" é manifestamente redutora já que, ainda que tais restrições existam, elas não foram suficientes para evitar sequer que os técnicos da CNPD vissem criado pelo SSI da arguida um utilizador de teste (justamente do grupo funcional "TECNICO" e grupo de atividade "MEDICO") que lhes permitiu "procurar por utentes registados naquela instituição hospitalar sem restrições e que tinha permissão de acesso a todos os elementos que compõem o processo clínico desses utentes", tal como constava do relatório anexo ao projeto de deliberação (cfr. fls. 6).
- 16) Ao consabidamente permitir a profissionais de várias categorias distintas o acesso a informação irrestrita sobre o processo clínico dos clientes do a arguida não cuidou minimamente de assegurar o cumprimento daquele princípio, tendo, ademais, contornado uma limitação dos sistemas que havia sido adotada por razões de segurança e privacidade.
- 17) A isto acresce que, de acordo com a defesa da própria, a arguida jamais terá cuidado de interceder junto da SPMS por forma a corrigir este aspeto do sistema que, como a atualização recente demonstra, devia e podia ser alterado previamente.
- 18) Diga-se, quanto à matéria da possibilidade de acesso a informação não necessária ou relevante permitida por estes perfis que, a equipa de fiscalização verificou e recolheu prova de acesso à PDS a partir da conta de utilizador de

✓

teste. Aliás, tanto quanto foi possível verificar em contexto de inspeção, a plataforma PDS não faz a validação da autenticação do utilizador, assim se explicando que tenha sido possível aceder à PDS com um “UTILIZADOR TESTE”, que não tinha associado qualquer número mecanográfico ou número de ordem (de médico ou enfermeiro).

- 19) Contrariamente à argumentação do                      cabe aos centros hospitalares e outras instituições de cuidados de saúde fazer a correta validação do utilizador e identificação do perfil correspondente, e não à PDS.
- 20) Já quanto à manutenção de perfis inúteis respeitantes a profissionais médicos que já não prestam serviços ao                      e que este não cuidou de eliminar, o juízo de censura mantém-se inalterado.
- 21) Relembre-se que, das 18 (dezoito) contas de utilizador que a CNPD verificou estarem efetivamente desativadas, apenas uma correspondia a um profissional médico
- 22) Admitindo-se que esta conduta não tenha causado danos concretos à proteção de dados pessoais dos clientes daquele centro hospitalar, não se pode, contudo, ignorar ou desconsiderar a violação de deveres objetivos dos responsáveis pelo tratamento, sobretudo quando em causa está o potencial acesso a categorias especiais de dados, conceito especificado no artigo 9.º, n.º 1 do RGPD, como são os dados de saúde.
- 23) Sublinhe-se que a arguida não negou a existência de tais perfis, limitando-se a arguir que alguns (poucos ou muitos) deles se devem à contratação, em regime de prestação de serviços, de médicos que apenas se encontram a desempenhar funções transitoriamente no                      . O desconhecimento concreto e rigoroso do universo de contas de acesso que deveriam ter sido eliminadas é bem demonstrativo da inexistência de um sistema de auditoria fiável.

- 24) Igualmente censurável mantém-se o procedimento de criação de contas que, ao contrário do que foi arguido, nem sequer é totalmente controlado pela administração do .
- 25) Com efeito, foram recolhidas provas em contexto de inspeção que demonstram que o processo de criação de contas nem sempre se rege pelo procedimento referido pela arguida. O Anexo I (de fls. 9) apresenta a transcrição de mensagens de correio eletrónico trocadas entre a Coordenadora do setor Fisioterapia do a Direção de patologia Clínica e o Serviço de Sistemas de Informação (SSI), que expressamente determinam o pedido de criação de contas de utilizadores, sem qualquer pronúncia por parte da administração do .
- 26) Ainda que se admita ter a arguida encetado um caminho de correção dessa situação, facto é que, à altura da inspeção, a criação de contas não respeitava minimamente os princípios do RGPD.
- 27) Relativamente à inexistência de LOGS de acesso, confirma-se que o técnico informático efetuou uma exportação da tabela «*sys\_log\_acessos*» com o nome «*log\_acessos\_assistente\_social.XLS*», que apresenta aquilo que parecem ser eventos de entrada e saída de um sistema. Presume-se que sejam associados a acessos ao SClinico, ainda que não se tenha conseguido confirmar esta informação.
- 28) Do ponto de vista de auditabilidade, o registo de entrada e saída numa aplicação fornece uma informação muito limitada sobre a sua utilização. A CNPD reconhece, no entanto, que a inclusão de maior nível de registo de atividade está dependente de alterações na lógica aplicacional e que essas alterações só estarão ao alcance da entidade que desenvolve o software – neste caso os SPMS.

r

29) Releva-se positivamente o cumprimento das recomendações da CNPD, inscritas na Deliberação n.º 674/2018, de 17 de julho, as quais se destinam justamente a corrigir elementos considerados críticos ou de substantiva relevância.

30) Reconhece-se a existência de atualizações dos sistemas proporcionados pelo SPMS que seguem o rumo correto, ainda que potencialmente não completo, de conformidade com as normas do RGPD.

Não foram ouvidas as testemunhas apresentadas dado que a matéria de facto foi genericamente confirmada e, quanto aos factos contestados não relevados, os mesmos não carecem de ulteriores esclarecimentos ou contraditório, donde resulta serem os eventuais depoimentos irrelevantes para a descoberta da verdade material.

Atenta a defesa apresentada pela arguida e o juízo crítico que sobre ela a CNPD efetuou, alteram-se alguns dos factos à luz das informações e esclarecimentos nela prestados.

III - Com os elementos constantes dos autos, com interesse para a decisão, consideramos provados os seguintes:

#### Factos

1. No dia 2 de julho de 2018 a Comissão Nacional de Protecção de Dados conduziu uma inspeção aos sistemas de gestão e acesso à informação nas instalações do
2. No contexto dessa inspeção verificou-se não existir qualquer documento onde esteja prevista a correspondência entre as competências funcionais dos utilizadores e os perfis de acesso à informação, designadamente informação clínica, ou onde estejam elencados os critérios que permitam fazer tal correspondência.
3. Resultou igualmente verificada a inexistência de qualquer documento onde estejam definidas as regras relativas ao procedimento de criação de conta de utilizadores do sistema de informação do ;

4. De resto, a determinação da criação de conta de utilizadores e dos perfis de acesso à informação é comunicada por e-mails dirigidos ao Serviço de Sistemas de Informação (SSI) tendo origem em dirigentes de serviços e outros profissionais;
5. Tal procedimento encontra-se em fase de revisão e correção.
6. O            utiliza o Sistema Integrado de Informação Hospitalar (SONHO) e o sistema de registo clínico hospitalar (SCLínico), aplicações disponibilizados pelos Serviços Partilhados do Ministério da Saúde, EPE (SPMS); o primeiro é usado para suporte administrativo do hospital e o segundo regista a informação clínica dos utentes, permitindo o acesso, a utilização e a partilha dessa informação entre profissionais de saúde;
7. O            tem autorizados os tratamentos de dados pessoais dos sistemas de informação SONHO e SAM (anterior designação da aplicação SCLínico)<sup>1</sup>.
8. Na aplicação SONHO, cada conta de utilizador possui dois atributos que permitem aos serviços hospitalares gerir os perfis de acesso ao sistema: o grupo funcional e o grupo de atividade, atribuindo-lhes códigos; o grupo funcional distingue as várias áreas funcionais que existem em ambiente hospitalar (v.g., "ADMINISTRATIVO/A", "TECNICO/A", "MEDICO", "INFORMATICO", "AUXILIAR"), enquanto o grupo de atividade permite distinguir diferentes áreas dentro de um grupo funcional (v.g., no grupo funcional de "MEDICO", há "CIRURGIAO", "ANESTESISTA" e "MEDICO");
9. Existe um grupo funcional denominado "TECNICO/A", no qual se incluem diferentes atividades - "NUTRICIONISTA", "FISIOTERAPEUTA", "PSICÓLOGO" e "SERVICO SOCIAL" (cf. anexo I);
10. O grupo funcional "MEDICO" corresponde ao código 5;
11. O grupo funcional "TECNICO/A" corresponde ao código 2;
12. Estão registados no sistema de informação SONHO do            10 profissionais da área de atividade "SERVIÇO SOCIAL" (cf. anexo II);
13. Estes 10 profissionais têm associado o código 2, que corresponde ao grupo funcional de "TECNICO/A";



14. Destes 10 profissionais, 9 têm também associado o código 5, que corresponde ao grupo funcional de “MEDICO” (cf. anexo III);
15. Os profissionais não médicos que têm associado o código 5 dispõem, por via desse código e perfil, de permissões de acesso a todo o processo clínico de todos os utentes do hospital, através do sistema SClínico;
16. Por iniciativa da CNPD, foi criada uma conta de utilizador de teste (com designação “UTILIZADOR TESTE”) com o perfil idêntico ao dos 9 técnicos do Serviço Social – com código 2 e 5 – tendo-se verificado que a mesma permitia o acesso, sem quaisquer restrições, ao processo clínico de utentes do \_\_\_\_\_, do qual consta o diagnóstico, os resultados dos meios auxiliares de diagnóstico e a demais informação registada na ficha clínica de cada utente (cf. Anexo IV);
17. Ainda dentro do SClínico, com a mesma conta de utilizador (com perfil de TECNICO/A – SERVICO SOCIAL), acedeu-se, via Plataforma de Dados de Saúde, uma vez que esta assim o permite, à informação residente noutro hospital do Serviço Nacional de Saúde \_\_\_\_\_ relativa a episódios clínicos associados a um utente do \_\_\_\_\_ (cf. Anexo V);
18. No ponto 4 das autorizações n.º 5795/2012 e 5796/2012, sob a epígrafe Medidas de Segurança, a CNPD expressamente determinou a necessidade do responsável adotar mecanismos de identificação e autenticação dos utilizadores, bem como de gestão dos perfis de acesso;
19. Os sistemas de informação disponibilizados pelos Serviços Partilhados do Ministério da Saúde, EPE (SPMS) não permitem aos utilizadores definirem parametrizações próprias, nomeadamente em matéria de perfis de acesso.
20. Existem 985 utilizadores ativos associados ao grupo funcional de “MEDICO”, no \_\_\_\_\_ ;
21. O ponto 5 (“Recursos Humanos”) do relatório e contas do \_\_\_\_\_ de 2017 (disponível em \_\_\_\_\_, indica, no mapa de pessoal aí inscrito, na página 33, a existência de 280 médicos;
22. O plano de recursos humanos, constante da página 14 do Plano de Atividades para 2018 desse mesmo centro hospitalar \_\_\_\_\_ aponta para a existência de 296 médicos ao serviço da dita EPE, no presente ano.

23. O                      reconheceu a existência de perfis inutilizados, ainda que salvaguardando a realidade dos contratos de prestação de serviços, que resultam na criação de perfis temporários de médicos contratados nesse regime, não logrando quantificar o fenómeno.
24. Existem apenas 18 contas de utilizadores inativas (15 técnicos, 1 farmacêutico e 1 médico), sendo que a inativação mais recente data de 11/11/2016 (cf. Anexo VI);
25. No ponto 4 das autorizações                      , sob a epígrafe Medidas de Segurança, a CNPD expressamente determinou, na alínea c), a necessidade de o  
*possuir um sistema de auditoria fiável.*
26. A arguida agiu deliberadamente, bem sabendo que estava obrigada a aplicar as medidas técnicas e organizativas indispensáveis à identificação e autenticação dos utilizadores, bem como à gestão e delimitação dos seus perfis de acesso à informação, estratificando-os de acordo com os diferentes privilégios de acesso correspondentes às categorias profissionais dos seus trabalhadores, e ainda à garantia da segurança da informação, para além de lhe competir dispor de um sistema de auditoria fiável de tais identificações, acessos e garantias de segurança.
27. A arguida atuou de forma livre, voluntária, conscientemente e sabendo que as suas condutas eram como são proibidas e punidas por lei

#### IV - Motivação da decisão de facto

Os factos dados como assentes resultaram:

- Do relatório de inspeção de fls. 4 a 10, onde se descrevem as circunstâncias em que os sistemas de acesso à informação operavam e as condições específicas dos acessos, permitindo a profissionais com perfis indevidamente atribuídos aceder a informação clínica de todos os clientes da arguida e não cuidando de garantir as condições mínimas de auditabilidade e segurança dos sistemas;
- Da defesa escrita da arguida, de fls. 38 a 82, onde se reconhecem as insuficiências detetadas quanto aos procedimentos de definição de contas e privilégios de acessos, quanto à incapacidade de determinar restrições no acesso à informação de acordo com a função específica dos trabalhadores do

e quanto à inobservância dos deveres de monitorização de contas inutilizadas e sua eliminação.

V - Verifica-se, em face da factualidade apurada, que se mostra suficientemente indiciada a prática pela arguida de duas contraordenações pela prática de duas infrações previstas e puníveis nos termos das disposições conjugadas do

- artigo 5.º, n.º 1 al. c) – violação do princípio da minimização dos dados, permitindo o acesso indiscriminado a um conjunto excessivo de dados por parte de profissionais que a eles só deveriam aceder em casos pontuais e previamente justificados; e artigo 83.º, n.º 5, al. a) – violação dos princípios básicos do tratamento, do Regulamento Geral sobre a Proteção de Dados (Regulamento 679/2016, de 27 de abril, doravante RGPD);

bem como do

- artigo 5.º, n.º 1 al. f) – violação do princípio da integridade e confidencialidade, em virtude da não aplicação de medidas técnicas e organizativas tendentes a impedir o acesso ilícito a dados pessoais; e artigo 83.º, n.º 5, al. a) – violação dos princípios básicos do tratamento, do Regulamento Geral sobre a Proteção de Dados (Regulamento 679/2016, de 27 de abril, doravante RGPD),

puníveis, cada uma delas, com coima de € 0,00 a € 20.000.000,00 ou até 4% do volume de negócios anual, consoante o montante que for mais elevado.

Mostra-se, de igual forma, suficientemente indiciada a prática, pela mesma arguida, de uma infração prevista e punível nos termos das disposições conjugadas do

- artigo 32.º, n.º 1, alíneas b) e d) – incapacidade do responsável pelo tratamento em assegurar a confidencialidade, integridade, disponibilidade e resiliência permanente dos sistemas e serviços de tratamento, bem como a não aplicação

das medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, nomeadamente de um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento; e artigo 83.º, n.º 4, al. a), do RGPD, com coima de € 0,00 a € 10.000.000,00 ou até 2% do volume de negócios anual, consoante o montante que for mais elevado.

\*

De acordo com o disposto no artigo 83.º, n.º 1, als. a) a k), a determinação da medida da coima é feita em função dos seguintes critérios:

- A natureza, a gravidade e a duração da infração tendo em conta a natureza, o âmbito ou o objetivo do tratamento de dados em causa, bem como o número de titulares de dados afetados e o nível de danos por eles sofridos – estamos perante duas infrações puníveis com a moldura mais grave prevista pelo RGPD e uma infração punível com o a moldura menos gravosa desse regulamento, sendo certo que, pelo menos, desde 25 de maio de 2018 vêm ambas as infrações a ser praticadas. O número de titulares afetado corresponde ao universo de clientes do , ou seja dos dois hospitais que o compõem, o

Sendo o

número preciso de clientes difícil de quantificar, o Relatório de Acesso relativo a 2017

possibilita extrapolar

em número situado nas várias dezenas de milhares. É, ainda, relevante, neste ponto, assinalar que estamos perante dados de saúde, enquadráveis nas categorias especiais de dados, o que aumenta consideravelmente o risco de danos para os titulares dos dados;

- O carácter intencional ou negligente da infração – considera-se ser dolosa a conduta relativa às infrações detetadas, ainda que a título de dolo eventual, uma vez que a arguida representou a prática da contraordenação como consequência possível da conduta e conformou-se com isso.

- A iniciativa tomada pelo responsável pelo tratamento ou pelo subcontratante para atenuar os danos sofridos pelos titulares – valoriza-se a conduta da arguida que adotou, desde o momento da inspeção, as medidas adequadas a retificar as insuficiências detetadas, as quais se encontram ou já implementadas ou em fase de implementação
- O grau de responsabilidade do responsável pelo tratamento ou do subcontratante tendo em conta as medidas técnicas ou organizativas por eles implementadas nos termos dos artigos 25.º e 32.º - considera-se ser elevada a responsabilidade da arguida quanto à violação das restrições dos níveis de acesso dos profissionais aos dados pessoais dos clientes, uma vez que conscientemente permitiu associar o grupo funcional de “MEDICO” a quem apenas deveria estar credenciado com perfil de “TECNICO”; Já quanto à inexistência de procedimentos de verificação da necessidade de manutenção dos perfis de acesso de médicos que já não estão ao serviço do não se pode deixar de considerar um grau de responsabilidade igualmente elevado por parte da arguida, uma vez que lhe competia exclusivamente garantir o controlo da necessidade e eliminação desses perfis, nomeadamente através de procedimentos de auditoria adequados.
- Quaisquer infrações pertinentes anteriormente cometidas pelo responsável pelo tratamento ou pelo subcontratante – que não se verificam.
- O grau de cooperação com a autoridade de controlo, a fim de sanar a infração e atenuar os seus eventuais efeitos negativos – que se reputa de adequado, face, não só, à correção das insuficiências detetadas, como ao cumprimento do conteúdo da Deliberação n.º 674/2018, de 17 de julho;
- As categorias específicas de dados pessoais afetadas pela infração – categorias especiais de dados pessoais, de acordo com o disposto no artigo 9.º, n.º 1 do RGPD, bem como outra informação de carácter não sensível, como a identificação dos clientes. Estes dados permitem a identificação dos seus titulares e o acesso indevido permitido com a conduta da arguida constitui uma grave ingerência na privacidade daqueles;
- A forma como a autoridade de controlo tomou conhecimento da infração, em especial se o responsável pelo tratamento ou o subcontratante a notificaram, e em caso afirmativo, em que medida o fizeram – tendo sido as infrações conhecidas

através de notícias da comunicação social e posteriormente confirmadas na ação inspetiva efetuada pela CNPD;

- O cumprimento das medidas a que se refere o artigo 58.º, n.º 2, caso as mesmas tenham sido previamente impostas ao responsável pelo tratamento ou ao subcontratante em causa relativamente à mesma matéria – não se aplicando este critério, já que inexistiam quaisquer medidas corretivas previamente determinadas;
- O cumprimento de códigos de conduta aprovados nos termos do artigo 40.º ou de procedimento de certificação aprovados nos termos do artigo 42.º - critério que também não se aplica, por inexistir qualquer código de conduta ou procedimento de certificação, nos termos apontados;

e

- Qualquer outro fator agravante ou atenuante aplicável às circunstâncias do caso, à luz da alínea k) do n.º 2 do artigo 83.º do RGPD, como os benefícios financeiros obtidos ou as perdas evitadas, direta ou indiretamente, por intermédio da infração - releva-se aqui, a título de fator
  - agravante, quanto à infração relativa à violação do artigo 32.º, n.º 1, alíneas b) e d) – a existência de autorizações prévias da CNPD onde, sob a epígrafe Medidas de Segurança, a CNPD expressamente determinou a necessidade de o *possuir um sistema de auditoria fiável*, não podendo a arguida desconhecer essa obrigação;
  - atenuante, a circunstância de os parâmetros de monitorização dos LOGS dos acessos à informação do SClínico não dependerem da arguida, mas antes da SPMS.
- Aplicação da coima

Atentos os critérios supramencionados, a CNPD entende como necessária a aplicação, no caso concreto, de uma coima à arguida, considerando ser esta a medida efetiva proporcionada e dissuasiva que se impõe dadas as concretas circunstâncias em que ocorreram as infrações.

Tal como se deixou exposto no projeto de deliberação, a moldura da coima abstratamente aplicável à arguida pelas infrações previstas e puníveis nos termos das

disposições conjugadas dos artigos 5.º, n.º 1 al. c) e artigo 5.º, n.º 1 al. f) com o artigo 83.º, n.º 5, al. a), do Regulamento Geral sobre a Proteção de Dados (Regulamento 679/2016, de 27 de abril, doravante RGPD), puníveis, cada uma delas, com coima de € 0,00 a € 20.000.000,00 ou até 4% do volume de negócios anual, consoante o montante que for mais elevado, bem como a prática de uma infração, em concurso, prevista e punível nos termos das disposições conjugadas do artigo 32.º, n.º 1, alíneas b) e d) e artigo 83.º, n.º 4, al. a), do RGPD, com coima de € 0,00 a € 10.000.000,00 ou até 2% do volume de negócios anual, consoante o montante que for mais elevado.

Sucedo, porém, que consultado o relatório e contas da arguida, relativo ao ano de 2017

se observa um resultado

líquido de

Tal significa que a moldura concreta das coimas a aplicar se fixam, no primeiro caso, entre € 0,00 a € 20.000.000,00 e, no segundo caso, entre € 0,00 a € 10.000.000,00.

Valorando a factualidade apurada à luz dos critérios acima enunciados, e ponderando a circunstância de a arguida ter diligenciado pela regularização da situação, a CNPD,

- nos termos do artigo 58.º, n.º 2, al. b) do RGPD, considera ajustada, a aplicação à arguida de duas coimas, cada uma delas, no valor de € 150.000,00 (cento e cinquenta mil e euros) pela prática de duas contraordenações previstas e puníveis nos termos das disposições conjugadas dos artigos 5.º, n.º 1 al. c) e 5.º, n.º 1, al. f), todos do citado regulamento;
- nos termos do artigo 58.º, n.º 2, al. i) do RGPD, a aplicação à arguida de uma coima no valor de € 100.000,00 (cem mil euros) pela prática da contraordenação prevista e punível nos termos das disposições conjugadas dos artigos 32.º, n.º 1, alíneas b) e d) e artigo 83.º, n.º 4, al. a), todos do citado regulamento.
- Em cúmulo, nos termos do artigo 83.º, n.º 3 do RGPD, a coima de € 400.000,00 (quatrocentos mil euros).



## VI - Conclusão

Face ao exposto, a CNPD delibera:

Aplicar à arguida observando o disposto no n.º 3 do artigo 83.º do RGPD, uma coima única, no valor de € 400.000,00 (quatrocentos mil euros) em razão da violação dos princípios da minimização dos dados e da integridade e confidencialidade, bem como da violação da obrigação de aplicação das medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, nomeadamente, um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

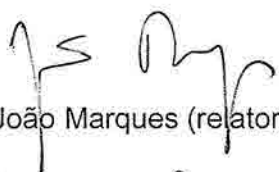
Nos termos preceituados nos artigos 58.º, n.ºs 2 e 3 do Decreto-Lei n.º 433/82, de 27 de outubro, atual redação, informar a arguida que:

- a) A condenação se torna definitiva e exequível se não for judicialmente impugnada, nos termos do artigo 59º do mesmo diploma;
- b) Em caso de impugnação judicial o Tribunal pode decidir mediante audiência ou, caso a arguida e o Ministério Público não se oponham, mediante simples despacho.

\*

Deverá a arguida proceder ao pagamento da coima no prazo máximo de 10 dias após o seu carácter definitivo, enviando à CNPD as respetivas guias de pagamento. No caso de impossibilidade do respetivo pagamento tempestivo, deve a arguida comunicar tal facto, por escrito, à CNPD.


Lisboa, 09 de outubro de 2018



João Marques (relator)



Luís Barroso



Maria Cândida Guedes de Oliveira



Pedro Mourão



José Grazina Machado



Filipa Calvão (Presidente)