COMISSÃO NACIONAL
DE PROTEÇÃO DE DADOS

Orientações para utilização de tecnologias de suporte ao ensino à distância

1. Introdução

O recurso a tecnologias de informação e comunicação para apoiar a atividade de ensino, nos seus diferentes níveis, tem vindo a ser intensificado na última década, enquanto instrumentos de agilização da comunicação e de divulgação mais eficiente de conteúdos. Recentemente, na sequência da pandemia provocada pelo novo coronavírus SARS-CoV-2 e pela doença Covid-19, adquiriu maior preponderância e visibilidade.

Na realidade, a imposição de confinamento e de isolamento social levou muitos estabelecimentos de ensino e profissionais deste setor a repensar as vias de comunicação e interação entre professores e alunos que se encontram em casa, estando a ser, nuns casos, ponderada a utilização de tecnologias de suporte ao ensino à distância e, noutros casos, a ser efetivada essa utilização.

Em causa está o recurso a plataformas eletrónicas de suporte ao ensino não presencial, que podem servir como meio de divulgação ou partilha de conteúdos pedagógicos, promover a interação entre os utilizadores ou adaptar conteúdos pedagógicos aos conhecimentos e capacidades de cada aluno.

A sua utilização implica a recolha e o subsequente tratamento de um conjunto alargado de informação relativa aos utilizadores e, nessa medida, porque estes correspondem a pessoas singulares que estão identificadas ou são identificáveis, implica um tratamento de dados pessoais[1], estando sujeito aos princípios e regras de proteção de dados pessoais[2].

Compreendendo-se o contexto especial que se vive, no quadro do qual se revela a necessidade ou conveniência de generalização do uso destas tecnologias, importa, paralelamente à perceção das vantagens daí decorrentes, alertar também para os riscos associados à sua utilização,

---

[11] Nos termos das alíneas 1) e 2) do artigo 4.º do Regulamento (UE) 2016/679, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados, doravante RGPD).

[2] A identificação ou identificabilidade da pessoa a quem diz respeito a informação pode decorrer do nome da pessoa, do endereço eletrónico, endereço IP, identificação das caraterísticas do sistema que efetua o acesso (e.g. *device fingerprinting*), etc.

COMISSÃO NACIONAL
DE PROTEÇÃO DE DADOS

recomendando-se uma cuidada ponderação antes da tomada de decisão de adotar, disponibilizar e promover e aquando da utilização destas tecnologias.

Na realidade, os principais riscos estão relacionados com o tratamento de informação que diz respeito à vida privada dos utilizadores, sejam eles os professores, sejam os alunos. Riscos que se acentuam quando os alunos são crianças e jovens, por força da sua maior vulnerabilidade, da sua menor consciência dos riscos e ainda do impacto decorrente da recolha, conservação e análise de dados pessoais ao longo de um extenso período de tempo com potenciais reflexos na sua vida adulta. Aliás, o regime de proteção de dados pessoais obriga os diferentes intervenientes nos tratamentos de dados a acautelar especialmente os direitos e interesses das crianças[3].

Com efeito, são geralmente recolhidos dados como as imagens dos utilizadores e do ambiente em que se encontram (*e.g.*, habitação), os relativos às declarações proferidas pelos participantes, seja por captação de som, seja por *messaging*. Mas também podem ser recolhidos dados de outros indivíduos presentes no ambiente em que os utilizadores se encontram, que podem ser também eles crianças (*e.g.,* filhos dos professores, irmãos dos alunos).
Além dos dados diretamente fornecidos pelos utilizadores e participantes, são ainda observados dados pessoais, tais como o número de acessos à plataforma, horas de acesso à plataforma, nível de participação nas atividades, dos quais é dedutível nova informação sensível dos utilizadores destas plataformas (*e.g.,* interesse nas atividades, capacidade de resolução de problemas) e que, no seu conjunto, permite a definição de perfis individualizados dos utilizadores.
Na verdade, estes contextos promovem a recolha automatizada de informação e a subsequente análise e previsão de aspetos relacionados, nomeadamente, com aptidões intelectuais, aptidões profissionais, traços de personalidade, desempenho profissional e mesmo com a saúde dos utilizadores. E tal é especialmente evidente nas plataformas que disponibilizam conteúdos pedagógicos especificamente adequados para cada utilizador, que se traduzem na tomada de decisões automatizadas assentes em sistemas de inteligência artificial que analisam o comportamento e desempenho dos alunos (*learning analytics*).
Por exemplo, certas plataformas são programadas para efetuar análise preditiva, baseada no desempenho dos alunos, também com o propósito de identificar situações de dislexia, distúrbios do espectro do autismo, deficiência intelectual, hiperatividade, distúrbios de atenção, de

[3] Cf. artigos 6.º, n.º 1, alínea *f),* 8.º, 12.º, n.º 1, e 57.º, n.º 1, alínea *b),* do RGPD e, no mesmo diploma, os considerandos 38 e 75, este último assinalando esta categoria de titulares de dados como um fator indiciador de elevado risco do tratamento de dados, para efeito da avaliação de impacto sobre a proteção de dados pessoais.

COMISSÃO NACIONAL
DE PROTEÇÃO DE DADOS

memória, de perceção, de linguagem ou de interação social ou outras perturbações dedutíveis em ambiente de aprendizagem.

Sendo certo que o tratamento destes dados pessoais pode estar legitimado em função das finalidades que expressamente justifiquem a utilização destas tecnologias, desde que assente em específicas condições de licitude[4], importa considerar os riscos que daquele decorrem para os direitos fundamentais dos utilizadores, em especial do direito ao respeito pela vida privada e familiar e do direito à igualdade, na vertente de não-discriminação.

Por um lado, existe o risco de discriminação e de estigmatização dos utilizadores decorrente destes tratamentos de dados, especialmente acentuada na reutilização dos dados pessoais para finalidades diferentes das que justificaram a recolha, aqui se incluindo a comunicação dos dados a terceiros.

A criação de perfis, relacionada com informação particularmente sensível (alguma da qual relativa a dados especialmente protegidos pela legislação de proteção de dados), como sucede com aptidões intelectuais e dados de saúde, utilizada em outros contextos pode estigmatizar as crianças e jovens, prejudicando a sua integração na sociedade e no mundo laboral. E o risco de utilização descontextualizada dessa informação não deve ser descurado.

Por outro lado, o ensino com recurso a plataformas de *e-learning,* que, de forma automatizada, analisam o comportamento e o desempenho dos alunos, importa o risco de erro de avaliação que, num contexto de recurso ao longo dos anos a este tipo de tecnologia, pode condicionar o acesso pelos mesmos alunos a certos conteúdos pedagógicos e, portanto, limitar a sua aprendizagem a níveis mais básicos ou menos aprofundados de conhecimento. O efeito estigmatizante é, aqui, evidente e não tem o mesmo impacto que a definição de perfil errada de *um* aluno por parte de um professor que está, pela natureza das coisas, temporalmente delimitada.

Mas também a vida privada e o desempenho dos professores podem ser analisados e originar perfis que os acompanhem ao longo da sua vida profissional e pessoal, o que coloca desde logo

---

[4] As quais ficam aqui limitadas aos termos definidos no n.º 2 do artigo 22.ºdo RGPD, mais especificamente às condições previstas nas alíneas *a)* e *g)* do artigo 9.º aí indicadas.

Nas demais situações de tratamento de dados pessoais por recurso a tecnologias de suporte ao ensino à distância, tem de estar verificada uma das condições do artigo 6.º do RGPD e eventualmente, caso abranjam dados especialmente protegidos, no n.º 2 do artigo 9.º do mesmo diploma. Alerta-se, todavia, para que o mero interesse legítimo do responsável pelo tratamento, previsto na alínea *f)* do n.º 1 do artigo 6.º, pode não ser admissível, se não estiverem suficientemente acautelados os direitos e interesses das crianças.

COMISSÃO NACIONAL
DE PROTEÇÃO DE DADOS

a dúvida quanto à legitimidade dessa análise no atual quadro legal português que proíbe o controlo remoto do desempenho dos trabalhadores[5].

Além disso, há ainda a destacar que a realidade de *bullying* não desapareceu, podendo até ser potenciada pelo confinamento e utilização massiva destas tecnologias, pelo que o risco de reutilização dos dados com partilha dos mesmos, sem legitimidade para o efeito, como poderá suceder com a publicação das imagens e som em redes sociais ou noutras plataformas, bem como o acesso indevido aos dados e sua utilização para finalidades não legítimas, deve merecer especial atenção.

Reconhecendo-se o quadro de evidentes vantagens no recurso a tecnologias de suporte ao ensino à distância, especialmente no estado atual provocado pela pandemia, compreende-se que se promova a utilização destes suportes, mas importa enquadrar essa utilização por um conjunto de obrigações legais e de boas práticas que mitiguem os riscos para a privacidade e que previnam a discriminação dos alunos e profissionais utilizadores destas tecnologias.

No exercício das suas atribuições e competências[6], a Comissão Nacional de Proteção de Dados define um conjunto de orientações para os diferentes intervenientes neste tratamento de dados pessoais de modo a garantir a conformidade dos tratamentos com o regime jurídico de proteção de dados e minimizar o impacto sobre a privacidade no contexto da utilização de tecnologias de suporte ao ensino à distância[7].

2. Objeto e destinatários

Objeto destas orientações são os tratamentos de dados pessoais realizados através de plataformas de ensino não presencial apoiadas em tecnologias de informação e comunicação

[5] Cf. n.º 1 do artigo 20.º do Código do Trabalho.

[6] Cf. alíneas *b)* e *d)* do n.º 1 do artigo 57.º e alínea *b)* do n.º 1 do artigo 58.º do RGPD e artigos 3.º e 6.º da Lei n.º 58/2019, de 8 de agosto.

[7] O presente texto segue de perto os seguintes documentos: *Working Paper on E-Learning Platforms*, International Working Group on Data Protection in Telecommunications, acessível em https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2017/2017-IWGDPT_Working_Paper_E-Learning_Platforms-en.pdf; *Resolution on e-Learning Plataforms*, 40th International Conference of Data Protection and Privacy Commissioners,23rd October 2018, Brussels, acessível em http://globalprivacyassembly.org/wp-content/uploads/2019/03/dewg-resolution-adopted-20180918.pdf.

COMISSÃO NACIONAL
DE PROTEÇÃO DE DADOS

(*e-Learning*) (*e.g., Moodle, Edmodo*), «cursos *online* abertos e massivos»[8] (*e.g., Coursera, Udemy*), áreas de trabalho contributivas para partilha de conteúdos (*e.g., Padlet*, *Google Drive*), sistemas de videoconferência e partilha de ficheiros (*e.g., Zoom*, *Microsoft Teams*), sistemas de *messaging* e partilha de ficheiros (*e.g., WhatsApp*).

As orientações aqui vertidas têm como destinatários todos os intervenientes nos tratamentos de dados realizados neste ambiente, sejam professores, alunos e pais ou encarregados de educação, mas, em especial, dirigem-se aos responsáveis pelos tratamentos e aos subcontratantes[9], assim como aos órgãos públicos que tomam as decisões que implicam a utilização destes tipos de tecnologias. A estes últimos cabe-lhes apoiar os estabelecimentos de ensino de modo a garantir a segurança na educação à distância[10].

3. Categorias de dados pessoais tratados

As categorias de dados objeto de tratamento variam em função do tipo de plataforma utilizada e das finalidades visadas com essa utilização, mas correspondem, grosso modo, para além de dados normalmente tratados no âmbito da atividade de ensino, relativos à vida privada dos utilizadores, podendo, em algumas plataformas, abranger dados relativos à saúde.
Aqui apenas se exemplificam algumas categorias de dados pessoais.
Dados pessoais suscetíveis de ser registados durante a utilização das plataformas e que revelam aspetos da vida privada dos mesmos: imagens dos participantes e do seu entorno (e.g., imagens da habitação); voz e declarações verbais dos participantes; declarações dos participantes em conversações em *messaging* e em fóruns; imagem, som e declarações de outras pessoas que se encontrem no mesmo espaço dos participantes; documentos partilhados pelos participantes através das plataformas (*e.g.* fotos, testes e respetiva avaliação).

Dados observáveis durante a utilização das plataformas e ainda os dados da vida privada deduzidos dos conjuntos de dados pessoais acima elencados: interesse nas atividades; capacidade de resolução de problemas; aptidões intelectuais; dificuldade de aprendizagem;

[8] Tradução da expressão inglesa *Massive Open Online Course* – MOOC.

[9] Para um esclarecimento dos conceitos aqui empregues, v. artigo 4.º, alíneas *7)* e *8),* do RGPD.

[10] Acrescente-se que, no caso dos organismos públicos, e ainda dos estabelecimentos de ensino privados que, nos termos do n.º 1 do artigo 37.º do RGPD e dos artigos 12.º e 13.º da Lei n.º 58/2019, de 8 de agosto, estão obrigados a ter um encarregado de proteção de dados, deve o mesmo ser consultado em primeira linha.

traços de personalidade; dados de saúde (*e.g.,* dislexia, distúrbios do espectro do autismo, deficiência intelectual, hiperatividade, distúrbios de atenção, de memória, de perceção, de linguagem, deficiência intelectual).

4. Principais riscos para a privacidade dos titulares

Na introdução deste documento foram já aflorados e contextualizados os principais riscos de utilização de tecnologias de suporte ao ensino à distância. Importa agora elencar, de forma sistematizada, os riscos para os direitos dos titulares dos dados.

- Risco de utilização indevida dos dados transferidos através das plataformas por parte dos responsáveis dos tratamentos, ou por subcontratantes que forneçam serviços dessas plataformas (por exemplo, em sistemas assentes em *cloud computing*);
- A falta de transparência relativamente à forma de armazenamento, tratamento e eventuais subcontratações realizadas por fornecedores de soluções de *e-learning* assentes em *cloud computing* pode resultar numa perda do controlo dos dados pelos respetivos titulares;
- Risco de definição de perfis ou avaliações, com base na informação observada da atividade dos utilizadores (professores ou alunos), que por sua vez pode gerar o tratamento discriminatório das pessoas a quem dizem respeito os perfis; em especial, o risco decorrente de decisões automatizadas assentes em sistemas de inteligência artificial que analisem o comportamento e desempenho dos alunos (*learning analytics*);
- A utilização de plataformas de comunicação que não garantam a segurança das comunicações ou cuja incorreta configuração resulte na divulgação ou acesso não autorizada pode colocar em risco a confidencialidade dos dados.
- Em especial, a partilha de computadores potencia riscos à confidencialidade;
- A ausência de uma atribuição clara das responsabilidades no contexto destas tecnologias promove situações em que, nem as instituições de ensino, nem os fornecedores das plataformas, adotam as medidas adequadas de segurança[11];
- Risco de vigilância à distância com a finalidade de controlar o desempenho profissional dos professores;

[11] Cf. a este propósito o disposto nos artigos 26.º e 28.º do RGPD.

COMISSÃO NACIONAL
DE PROTEÇÃO DE DADOS

- Ausência de um ponto de acesso para o exercício dos direitos pelos titulares dos dados junto das plataformas utilizadas e, com isso, risco de desproteção dos mesmos.

5. Recomendações

Formulam-se agora um conjunto de recomendações com o objetivo, já assinalado, de garantir que a utilização destas tecnologias de suporte ao ensino à distância não afete substancialmente os direitos fundamentais das pessoas que as utilizam, em particular os das crianças, através da adoção de soluções tecnológicas e medidas adequadas a proteger os dados pessoais e minimizar o impacto sobre os direitos dos titulares dos dados, em conformidade com o regime jurídico de proteção de dados. Vejamos.

- As plataformas escolhidas devem ter finalidades bem definidas e compatíveis com o ensino à distância;
- As plataformas a utilizar deverão recolher e tratar os dados estritamente necessários para as finalidades especificadas (princípio da minimização dos dados[12]);
- A adoção de cada plataforma de suporte ao ensino à distância deve ser precedida de uma avaliação de impacto na proteção de dados, de forma a identificar corretamente os riscos para a privacidade e permitir que sejam adotadas medidas mitigadoras desses riscos[13]. A avaliação pode ser feita pelas entidades que disponibilizam e gerem as plataformas, uma vez que, neste contexto do ensino à distância, a generalidade dos responsáveis pelos tratamentos (*e.g.,* estabelecimento de ensino) não dispõe de recursos técnicos para o efeito. Sublinha-se que as evoluções tecnológicas e sociais podem representar novos riscos e devem ser tidas em conta durante o tratamento de dados, podendo exigir avaliações de impacto subsequentes;
- As plataformas devem definir de forma clara os papéis e responsabilidades dos vários intervenientes no tratamento de dados pessoais, em especial a distribuição de funções e responsabilidades entre quem fornece e gere a plataforma e quem decide sobre a sua utilização;

[12] Cf. artigo 5.º, n.º 1, alínea *c),* do RGPD.

[13] Cf. artigo 35.º, n.º 1 e n.º 3, alíneas *a) e b),* do RGPD e Regulamento da CNPD n.º 798/2018, de 30 de novembro, em especial o n.º 9.

COMISSÃO NACIONAL
DE PROTEÇÃO DE DADOS

- As plataformas escolhidas devem estar desenvolvidas de forma que os princípios de privacidade desde a conceção sejam aplicados[14], pelo que as configurações de privacidade devem estar predefinidas e a sua desativação ser da iniciativa do utilizador;
- Os professores devem ser devidamente informados relativamente à utilização das plataformas. Em particular, devem conseguir identificar as corretas configurações para garantir que não decorrem riscos para a privacidade dos utilizadores, com especial enfoque nos alunos;
- Os estabelecimentos de ensino devem procurar sensibilizar a comunidade escolar (incluindo, pais dos alunos quando sejam crianças) para um conjunto de boas práticas e precauções a seguir na utilização destas tecnologias;
- Deve estar predefinida a informação que é conservada (que, em princípio, corresponderá à que é mantida no ensino presencial); do mesmo modo, devem ser prefixados os prazos da sua conservação[15];
- Os fornecedores das plataformas de suporte ao ensino à distância devem cumprir a obrigação de comunicação aos estabelecimentos de ensino das violações de dados pessoais que ocorram[16];
- Sempre que possível, deve optar-se por tecnologias que impliquem a menor exposição possível do titular e do seu ambiente familiar (*e.g.,* fóruns de discussão por oposição a videoconferência);
- Os estabelecimentos de ensino devem avaliar se dispõem de meios técnicos para implementar as plataformas de ensino à distância, para evitar optarem por tecnologias que sobrecarreguem os seus sistemas tecnológicos, tornando-os, por isso, inseguros;
- A utilização de quaisquer algoritmos de análise de desempenho (*learning analytics*) deve sempre ser criteriosa e feita de forma justa e transparente para com os titulares e apenas se estiver preenchida alguma das condições de licitude desse tratamento[17]. Importa aqui

[14] Cf. artigo 25.º, n.º 1, do RGPD.

[15] Cf. artigo 5.º, n.º 1, alínea *e),* do RGPD.

[16] Nos termos previstos nos artigos 33.º e 34.º do RGPD.

[17] Designadamente, se for necessário para a execução de um contrato de que o titular dos dados seja parte ou seja precedido do consentimento explícito, livre, informado e específico do titular dos dados (cf. n.º 1 e 2 do artigo 22.º do RGPD). Assinala-se que a solução será diferente, no caso de estarem em causa dados especialmente protegidos como sucede com os dados de saúde e sobretudo se disserem respeito a crianças (cf. n.º 4 do artigo 22.º do RGPD).

COMISSÃO NACIONAL
DE PROTEÇÃO DE DADOS

reforçar que nenhum estabelecimento de ensino pode impor a utilização desta específica tecnologia de inteligência artificial aos seus alunos, dependendo essa utilização de uma vontade informada, livre, específica e explícita do aluno ou, quando menor, de quem o representa. Deve ser dada clara informação aos titulares acerca do funcionamento dos algoritmos de análise, nomeadamente quando estiverem em causa decisões automatizadas. E deve ser sempre garantido o direito do titular dos dados de obter intervenção humana nesse processo[18].

Recomenda-se, assim, que o Ministério da Educação, os diretores dos agrupamentos escolares e os diretores dos demais estabelecimentos de ensino, nos seus diferentes níveis, recorram a plataformas adequadas para garantir que os sistemas usados no ensino à distância não apresentam riscos para a privacidade para os alunos e professores.

Recomenda-se, ainda, que toda a comunidade escolar siga as boas-práticas respeitantes à proteção de dados, designadamente abstendo-se de tratar dados pessoais que não sejam essenciais para a finalidade pedagógica e adotando comportamentos responsáveis quando disponham de acesso a dados pessoais de alunos, professores e outros titulares dos dados que possam incidentalmente ser visados por elas.

Lisboa, 8 de abril de 2020

[18] Cf. n.º 3 do artigo 22.º do RGPD.