A Utilização de Plataformas Eletrónicas de Suporte ao Ensino à Distância

Privacidade e Proteção de Dados

21.04.2020

Introdução

A pandemia da Covid-19 originou um incremento massivo da utilização das plataformas eletrónicas de suporte ao ensino não presencial apoiadas em tecnologia de informação e comunicação (*e-learning*), como o Moodle e o Edmodo; "cursos online abertos e massivos", como o Coursera e o Udemy; áreas de trabalho contributivas para partilha de conteúdos, como o Padlet e o Google Drive; sistemas de videoconferência e partilha de ficheiros, como o Zoom e o Microsoft Teams; e sistemas de *messaging* e partilha de ficheiros, como o WhatsApp (conjuntamente "plataformas").

No entanto, notícias recentes, como as associadas ao Zoom, que relatam a intrusão de terceiros na plataforma, a gravação e divulgação no Youtube das sessões decorridas, a utilização indevida de dados pessoais e, ainda, a sua venda na *dark web*, **têm suscitado a preocupação de várias entidades em relação à utilização de plataformas eletrónicas de suporte ao ensino à distância**.

A este propósito, assinale-se que o Ministério Público procedeu já à abertura de inquérito para averiguar queixas de entradas ilícitas nas plataformas e que a Federação Nacional dos Professores (FENPROF) manifestou publicamente a sua intenção de apresentar queixa na Procuradoria-Geral da República contra quem gravou e transmitiu no Youtube aulas lecionadas através da plataforma Zoom, que deveriam ter decorrido em circuito fechado.

A. As recomendações da Direção-Geral de Educação, em articulação com o Centro Nacional de Cibersegurança e a Comissão Nacional de Proteção de Dados

A Direção-Geral de Educação (DGE), em parceria com o Centro Nacional de Cibersegurança (CNCS) e a Comissão Nacional de Proteção de Dados (CNPD), divulgou as seguintes recomendações no uso de plataformas que permitem a comunicação vídeo e áudio (que podem ser consultadas em https://www.cncs.gov.pt/content/files/10_recomendaes_no_uso_de_plataformas_de_vdeo_e_udio.jpg):

SeguraNet

1. Pense antes de publicar informação sensível
2. Mantenha o *software* atualizado
3. Seja cuidadoso com a *webcam* e o microfone
4. Utilize formas seguras de convidar os participantes
5. Controle a partilha de ecrã
6. Crie uma sala de espera
7. "Tranque a porta"
8. Desligue a partilha nas mensagens
9. Escolha as opções de gravação mais adequadas
10. Não se esqueça de outros cuidados

Em acréscimo, foram ainda divulgadas medidas de segurança específicas para o uso de algumas plataformas, de modo a que a sua utilização, no âmbito do ensino à distância, se processe de forma segura:

- Microsoft Teams: https://www.cncs.gov.pt/content/files/microsoft-teams_2.pdf
- Moodle: https://www.cncs.gov.pt/content/files/moodle.pdf
- Zoom: https://www.cncs.gov.pt/content/files/zoom_2.pdf

B. As Orientações da Comissão Nacional de Proteção de Dados

De igual modo, a CNPD emitiu um conjunto de orientações para a utilização de plataformas eletrónicas de suporte ao ensino à distância, com o objetivo de garantir a conformidade dos tratamentos com o regime jurídico de proteção de dados e minimizar o impacto sobre a privacidade.

https://www.cnpd.pt/home/orientacoes/Orientacoes_tecnologias_de_suporte_ao_ensino_a_distancia.pdf

Quais os destinatários destas orientações?

As orientações aplicam-se a todos os intervenientes nos tratamentos de dados realizados neste ambiente, nomeadamente, aos professores, aos alunos, aos pais ou encarregados de educação e, em especial, aos Responsáveis pelos Tratamentos e aos Subcontratantes e, ainda, aos órgãos públicos que tomam as decisões que implicam a utilização deste tipo de tecnologias.

Que categorias de dados pessoais se encontram envolvidas?

De um modo geral, os dados que, em regra, são utilizados pelas plataformas correspondem, para além dos dados normalmente tratados no âmbito da atividade de ensino, a dados que estão intimamente ligados à esfera da vida privada dos utilizadores, podendo, em certos casos, abranger também dados relativos à saúde. Assim, a título exemplificativo, elencam-se as seguintes categorias:

- **Dados suscetíveis de ser registados durante a utilização das plataformas e que revelam aspetos da vida privada dos utilizadores**

  Por exemplo, imagens dos participantes e do espaço onde se encontram; voz e declarações verbais dos participantes; declarações dos participantes em conversações de *messaging* e em fóruns; imagem, som e declarações de outras pessoas que se encontram no mesmo espaço que os participantes; e documentos partilhados pelos participantes através das plataformas (como 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**

  Por exemplo, interesse nas atividades; capacidade de resolução de problemas; aptidões intelectuais; dificuldade de aprendizagem; traços de personalidade; e dados de saúde (como dislexia, distúrbios do espectro do autismo, deficiência intelectual, hiperatividade, distúrbios de atenção, de memória, de perceção, de linguagem e deficiência intelectual).

Quais os principais riscos associados à utilização destas plataformas?

A CNPD começa por destacar que os principais riscos relacionados com o tratamento de informação respeitam, naturalmente, à vida privada dos utilizadores, riscos esses que se acentuam nos casos em que os alunos são crianças e jovens, atenta a sua maior vulnerabilidade e a menor consciência dos riscos e do impacto decorrente da recolha, conservação e análise de dados pessoais ao longo de um período de tempo extenso, com potenciais reflexos na sua vida adulta.

Em concreto, a CNPD identifica os seguintes riscos:

1. Risco de utilização indevida dos dados transferidos através das plataformas por parte dos Responsáveis pelos Tratamentos ou por Subcontratantes que forneçam serviços dessas plataformas (por exemplo, em sistemas assentes em *cloud computing*);
2. Falta de transparência relativamente ao modo de armazenamento, tratamento e eventuais subcontratações realizadas por fornecedores de soluções de *e-learning* assentes em *cloud computing,* que pode resultar numa perda do controlo dos dados pelos respetivos titulares;
3. Risco de definição de perfis ou avaliações, com base na informação observada das atividades dos utilizadores (professores ou alunos), que, por sua vez, pode gerar o tratamento discriminatório das pessoas a quem respeitam 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*);
4. Utilização de plataformas de comunicação que não garantam a segurança das comunicações ou cuja incorreta configuração resulte na divulgação ou acesso não autorizado, o que pode colocar em risco a segurança dos dados;
5. Incremento dos riscos para a confidencialidade decorrente da partilha de computadores;
6. Ausência de uma atribuição clara das responsabilidades no contexto destas tecnologias, o que promove situações em que, nem as instituições de ensino, nem os fornecedores das plataformas, adotam as medidas de segurança adequadas;

7. Risco de vigilância à distância com a finalidade de controlar o desempenho profissional dos professores;

8. Ausência de um ponto de acesso para o exercício dos direitos pelos titulares dos dados junto das plataformas e, consequentemente, risco de desproteção desses direitos.

Quais as recomendações da CNPD para colmatar os riscos evidenciados?

1. As plataformas selecionadas devem ter finalidades bem definidas e compatíveis com o ensino à distância;

2. As plataformas devem recolher e tratar os dados pessoais estritamente necessários para as finalidades especificadas (princípio da minimização dos dados);

3. A adoção de cada plataforma deve ser precedida de uma avaliação de impacto sobre a proteção de dados (que pode ser realizada pelas entidades que disponibilizam e gerem as plataformas, considerando que a generalidades dos Responsáveis pelos Tratamentos não dispõem dos recursos técnicos necessários para o efeito), que identifique corretamente os riscos para a privacidade, permitindo que sejam adotadas medidas de mitigação desses riscos. Isto, sem prejuízo da eventual necessidade de serem realizadas avaliações de impacto subsequentes, em resultado dos novos riscos decorrentes das evoluções tecnológicas e sociais;

4. 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;

5. As plataformas devem estar desenvolvidas de modo a que o princípio da privacidade desde a conceção seja aplicado, pelo que as configurações de privacidade devem estar predefinidas e a sua desativação ser da iniciativa do utilizador;

6. Os professores devem ser devidamente informados relativamente à utilização das plataformas, devendo, em especial, conseguir identificar as corretas configurações para garantir que não decorrem riscos para a privacidade dos utilizadores (sobretudo dos alunos);

7. Os estabelecimentos de ensino devem procurar sensibilizar a comunidade escolar para um conjunto de boas práticas e precauções a seguir na utilização destas tecnologias;

8. Deve predefinir-se a informação que é conservada (em regra, corresponderá à que é mantida no ensino presencial) e os respetivos prazos de conservação;

9. Os fornecedores das plataformas devem cumprir a obrigação de comunicação aos estabelecimentos de ensino das violações de dados pessoais que ocorram;

10. Sempre que possível, deve optar-se por tecnologias que impliquem a menor exposição possível do titular e do seu ambiente familiar (por exemplo, fóruns de discussão em detrimento de videoconferência);

11. Os estabelecimentos de ensino devem avaliar se dispõem dos meios técnicos necessários para implementar as plataformas, evitando opções que sobrecarreguem os seus sistemas tecnológicos tornando-os, em consequência, mais inseguros;

12. A utilização de algoritmos de análise de desempenho (*learning analytics*) deve 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. Cumpre referir que os estabelecimentos de ensino não podem impor aos alunos a utilização desta específica tecnologia, dependendo essa utilização de uma vontade informada, livre, específica e explícita do aluno (ou, quando menor, de quem o representa). Importa ainda assinalar que deve ser dada informação clara aos titulares dos dados acerca do funcionamento dos algoritmos de análise quando estiverem em causa decisões automatizadas e que deve ser-lhes sempre garantido o direito de obter intervenção humana nesse processo.

C. Notas Finais

Assim, uma vez que são vários os riscos ao nível da cibersegurança e da proteção de dados pessoais associados à utilização de plataformas eletrónicas de suporte ao ensino à distância, **o cumprimento das recomendações divulgadas pela DGE, em parceria com o CNCS e a CNPD, bem como das orientações emanadas pela CNPD, é essencial para a sua mitigação**.

Deste modo, recomenda-se a todos os intervenientes que sigam as diretrizes apresentadas, adotando, em conformidade, comportamentos responsáveis e soluções adequadas à segurança na configuração e utilização das plataformas e à proteção dos dados pessoais dos alunos, professores e outros titulares que possam ser incidentalmente envolvidos.

Rita Gabriel Passos | ritapassos@pintoribeiro.pt
Margarida Amador | margaridaamador@pintoribeiro.pt
www.pintoribeiro.pt