

# VIGIAR E REPROVAR

**Carlos Germán Guerrero Argote**

- *Impacto dos softwares de e-proctoring •  
na privacidade de estudantes universitários*

## RESUMO

*O texto aborda a seguinte pergunta: Qual é o impacto do uso de programas de e-proctoring na privacidade de estudantes universitários? Partindo-se de um caso ocorrido em uma universidade do Peru, em 2020, são explorados os conceitos relacionados ao e-proctoring, à privacidade e à proteção de dados pessoais. Também é feito um relato sobre o grau de adoção dessas tecnologias, com especial foco na região da América Latina. Por fim, é apresentada uma análise sobre a interação entre o e-proctoring e as normas de proteção de dados pessoais que inclui a casuística mais recente sobre o tema.*

## PALAVRAS-CHAVE

*E-proctoring | Vigilância | Dados pessoais | Educação*

## 1 • Introdução

Embora existam há muitos anos, os *softwares* de *e-proctoring* ou *proctoring* remoto eram pouco conhecidos até antes da pandemia de Covid-19. Ao contrário de outras ferramentas educacionais, o *e-proctoring*, voltado à supervisão remota para avaliações *on-line*, tem uma capacidade disruptiva imensa que se deve principalmente ao uso intensivo de tecnologias de ponta, como biometria, reconhecimento facial e inteligência artificial.

A virtualização das aulas durante o ano de 2020 devido à pandemia marcou o início da adoção massiva desses programas em todo o mundo. Sua capacidade de permitir o controle de avaliações *on-line* e seu potencial para detectar condutas desonestas, como falsificação de identidade e plágio, também os tornaram uma solução muito atraente para as universidades.

No entanto, a implantação dessas tecnologias tem causado diferentes reações adversas nas comunidades estudantis. Talvez as mais específicas girem em torno da conveniência de adotar tecnologias consideradas muito invasivas à privacidade. Apesar desta e de outras objeções, em muitos casos as universidades forçaram seu uso com consequências nem sempre positivas.

Este artigo busca lançar mais luz sobre o impacto do uso dessas tecnologias na privacidade de estudantes universitários. Ainda que seu foco esteja na região da América Latina, especificamente no Peru, aborda-se um problema cujas características são semelhantes às de outros lugares onde esses programas foram implementados.

## 2 • O caso da Universidade San Marcos

Em agosto de 2020, a Universidade Nacional Maior de San Marcos (UNMSM), universidade pública mais importante do Peru, anunciou que seu Exame de Admissão Anual [equivalente a um exame de ingresso ou vestibular] seria realizado em formato virtual.<sup>1</sup> Essa notícia, divulgada após vários meses de incerteza devido às medidas implementadas para impedir a propagação da Covid-19, significou um alívio para muitos candidatos, ao mesmo tempo em que trouxe um novo conjunto de preocupações.

Em seu comunicado, a Universidade San Marcos também destacou que tinha estabelecido algumas medidas para evitar possíveis comportamentos desonestos que poderiam ocorrer em uma prova não presencial, mas não se aprofundou no assunto. Contudo, uma semana depois, em uma entrevista com o chefe do Escritório Central de Admissão da UNMSM, este apresentou mais detalhes:

*Agora que está decidido que o exame de admissão será virtual, surge uma série de questões, principalmente relativas à possibilidade de alguns estudantes trapacearem, de usarem o computador para*

*buscar as respostas em páginas da web, de alguém ajudar a responder às perguntas ou que haja falsa identidade do candidato. [...] Por meio de um aplicativo que utiliza a inteligência artificial, será verificado se o candidato em frente ao computador no dia do exame é o mesmo que se cadastrou biometricamente. [...] O aplicativo de segurança irá capturar as imagens a cada minuto e detectar se alguém abre uma página da web diferente da avaliação. Mas também detectará se o computador possui alguma conexão periférica, por exemplo, com uma tela, um cabo HDMI ou software remoto. O sistema também é capaz de registrar se alguém faz um copy-page [copiar página], uma captura de tela (screenshot) ou se mudanças são ativadas na janela do Windows.<sup>2</sup>*

Várias pessoas candidatas ao Exame de Admissão ficaram inicialmente céticas e depois expressaram sua reprovação a essa nova modalidade por diferentes motivos: alguns estavam relacionados ao contexto da pandemia, mas outros correspondiam a falhas estruturais, como exclusão ou desigualdade digital, e também ao medo que o uso de tecnologias – até então desconhecidas – despertava, e cuja importância era primordial para o normal desenvolvimento da prova. Nos meses seguintes, essas pessoas se organizaram e fizeram uma resistência coordenada para tentar impedir o Exame Virtual.

Entretanto, a UNMSM não recuou e, quando chegaram as datas estabelecidas em outubro, procedeu à realização do Exame Virtual, que teve uma participação reduzida: apenas 8 mil pessoas de um total inicial de mais de 15 mil.

Conforme previsto por muitos de seus detratores, vários incidentes foram relatados durante o Exame. Por exemplo, houve denúncia de que, embora fosse um requisito obrigatório, vários estudantes foram autorizados a fazer a prova sem a câmera ligada. As perguntas e as respostas do texto circularam em redes sociais. Incrivelmente, também houve denúncia de que o Exame foi transmitido ao vivo pela plataforma de *streaming* Twitch.<sup>3</sup>

Apesar das denúncias, que motivaram diferentes pronunciamentos de entidades como o Congresso da República,<sup>4</sup> a Superintendência Nacional de Ensino Superior Universitário (SUNEDU)<sup>5</sup> e inclusive a Autoridade de Proteção de Dados Pessoais (APDP),<sup>6</sup> a Universidade os ignorou e dias depois publicou os resultados do Exame de Admissão. Com o passar das semanas, o interesse sobre o caso foi diminuindo e, com exceção da APDP, que iniciou um processo de fiscalização administrativa, as demais entidades não deram continuidade a outros tipos de ação.

Durante os eventos já mencionados, a imprensa nunca abordou as “tecnologias que usavam inteligência artificial” para detectar o plágio e a falsificação de identidade que foram anunciadas pelas autoridades da UNMSM. Porém, em uma investigação posterior que realizamos no início de 2021, descobrimos que a tecnologia utilizada pela Universidade se

chamava SMOWL, um *software* criado e distribuído pela Smowltech, empresa espanhola especializada na prestação de serviços de *e-proctoring*.<sup>7</sup>

### 3 • *E-proctoring* na América Latina e a proteção de dados pessoais

Como foi dito, o caso da Universidade San Marcos nos levou a iniciar uma pesquisa sobre as implicações do uso dessas ferramentas tecnológicas. Assim, no final do primeiro trimestre de 2021, publicamos um relatório que incluía um mapeamento inicial da adoção do *e-proctoring* na região da América Latina, bem como uma coleta e análise da legislação aplicável sobre privacidade e proteção de dados pessoais.<sup>8</sup> A seguir, comentamos alguns de seus resultados.

#### 3.1 - Implantação de *e-proctoring* na América Latina

O estudo em questão escolheu três países para estudos de caso, Argentina, Chile e Peru, e realizou sobre estes uma pesquisa documental para identificar, por meio de consulta em fontes abertas, o grau de adoção de soluções de *e-proctoring* durante 2020, especificamente por universidades públicas e privadas.

Este levantamento inicial revelou o seguinte: na Argentina, foram detectados 10 casos de adoção de um ou mais *softwares* de *e-proctoring*, 2 deles em universidades públicas e 8 em privadas. No Chile, foram detectados 11 casos, 1 deles em universidades públicas e 10 em privadas. Por fim, no Peru foram detectados 25 casos, 12 em universidades públicas e 13 em privadas. Os três *softwares* de *e-proctoring* mais usuais foram, nesta ordem: SUMADI, SMOWL e METTL.<sup>9</sup>

Embora as evidências coletadas não tenham estabelecido padrões comuns entre as universidades, um fator recorrente foi que a maioria dos programas serviu quase exclusivamente para controlar avaliações realizadas *on-line* e, em geral, foram adotados como soluções de emergência. Talvez seja devido a este último motivo que a sua implantação tenha ocorrido quase sempre de forma inesperada e, em muitas ocasiões, sido realizada sem ao menos possibilitar processos adequados de familiarização de estudantes e docentes com o *software*.

Outro aspecto interessante a destacar é que a maioria dos programas de *e-proctoring* eram soluções que utilizavam tecnologias muito avançadas. Por exemplo, os três mais recorrentes funcionavam baseados em algoritmos de inteligência artificial, alimentados com dados obtidos em ferramentas como reconhecimento facial e biometria. Todos esses dados, além do mais, eram obtidos graças ao fato de que os programas assumiam o controle dos dispositivos onde o corpo de estudantes realizava suas provas, exigindo para isso que possuíssem elementos periféricos (câmeras, microfones) e um sistema operacional de acordo com suas necessidades.

### 3. 2 - Proteção de dados pessoais aplicáveis ao *e-proctoring*

O fato de que os *softwares* de *e-proctoring* exigiram o consumo de uma grande quantidade de dados produzidos pelo corpo discente durante o desenvolvimento das avaliações foi motivo de preocupação no caso da Universidade San Marcos, conforme mencionado na seção anterior. Quanto ao que pudemos identificar como preocupações diretamente relacionadas à privacidade, essas tecnologias foram percebidas como muito invasivas, pois gravavam constantemente estudantes e seu ambiente, registrando tudo o que era feito em seus dispositivos. Esse material era o insumo principal para desqualificá-los sob parâmetros nem sempre explicitados e geralmente confusos.

Nesse ponto, a pesquisa realizada mostrou que a maioria dos *softwares* de *e-proctoring* tratava dados pessoais como: endereço IP, histórico de navegação, imagem do rosto, nomes e sobrenomes, traços faciais e voz. Alguns destes dados, ademais, eram considerados dados sensíveis nos três países de estudo, o que implicava necessariamente a aplicação de diferentes normas que regulam seu tratamento, sobretudo aquelas relacionadas com a proteção de dados pessoais.<sup>10</sup>

Embora tenha sido identificado que os países tinham leis de proteção de dados pessoais de alcance nacional e disposições de cumprimento obrigatório nesse sentido, também foi descoberto que sua aplicação ao uso do *e-proctoring* não estava isenta de aspectos controversos. Por exemplo, havia o tema da jurisdição: nenhum dos três programas mais utilizados era fornecido às universidades por empresas domiciliadas no território, mas sim no exterior e pela internet. Uma possível anomia também foi identificada, resultante do fato de que o uso do *e-proctoring* não tinha sido previsto em nenhum regulamento anterior, de modo que não era claro o nível de exigência de obrigações como o cadastro de bancos de dados pessoais ou a solicitação de consentimento, principalmente em um contexto de crise como o que se vivia em 2020 por causa da Covid-19.

Não obstante o anterior, a pesquisa pôde verificar que pelo menos na Argentina e no Peru, uma vez superado o problema do alcance territorial das normas de proteção de dados pessoais, várias disposições gerais e específicas eram inteiramente aplicáveis, senão às empresas fornecedoras do *e-proctoring*, ao menos às universidades que contrataram seus serviços. No entanto, diante de uma avaliação de cumprimento, salvo exceções, na maioria dos casos parecia que as universidades haviam pensado que essas disposições não se aplicavam a elas ou simplesmente optaram por descumpri-las.

Um problema adicional para poder determinar com maior precisão em que medida as normas de proteção de dados pessoais desses três países foram descumpridas e que significava ter incorrido em infrações é que, exceto no Peru, não houve investigações ou processos de fiscalização pelas autoridades de proteção de dados. Portanto, a maioria das conclusões do estudo comentado tinha natureza especulativa e requeria pronunciamentos oficiais para que se tornasse mais sólida ou fosse descartada.

## 4 • Impacto na privacidade: o caso da Espanha e do Peru sobre o *e-proctoring*

Dissemos na introdução que, embora nosso foco de estudo seja a América Latina, as situações de conflito produzidas pela implantação do *e-proctoring* têm sido globais. Prova disso é que ao mesmo tempo em que a Universidade San Marcos, no Peru, anunciava o uso do SMOWL para controlar seu Exame Virtual, situações semelhantes ocorriam em outros países. Como na Espanha, país onde existe atualmente pelo menos um pronunciamento da Autoridade Espanhola de Proteção de Dados (AEPD) sobre um caso de uso de *e-proctoring* na Universidade de La Rioja (UNIR).

### 4.1 - O caso da UNIR na Espanha

Tal qual explicado nesta cronologia<sup>11</sup> do meio de comunicação Newtral, em março de 2021, a UNIR informou a seu corpo discente que, devido à pandemia de Covid-19, realizaria seus exames de julho em modalidade virtual. Após este anúncio, também foi indicado que um programa de “autenticação biométrica” seria implementado como medida de segurança. De modo muito similar ao ocorrido no caso da Universidade San Marcos, um expressivo grupo de estudantes espanhóis expressou suas críticas à mudança, mas não foi devidamente atendido. Inclusive, o *software* utilizado nesta ocasião era o mesmo que no Peru, o SMOWL.

O caso foi denunciado pelas pessoas afetadas aos tribunais e também à AEPD. Esta última emitiu um pronunciamento de advertência em julho deste ano.<sup>12</sup> Algumas das conclusões do documento incluíram:

- Que é conveniente realizar uma análise de impacto na privacidade, a fim de determinar se o uso de programas como os de *e-proctoring* é realmente a melhor opção para atingir os objetivos de avaliação educacional.
- Quanto ao tratamento de dados biométricos por meio de tecnologia de reconhecimento facial, embora possa ser conveniente para as universidades, isso não significa que seja necessário, condição indispensável no tratamento de dados sensíveis.

Além disso, os argumentos anteriores também são respaldados em informe divulgado pela AEPD, há um ano, sobre o uso de técnicas de reconhecimento facial na realização de provas de avaliação *on-line*,<sup>13</sup> no qual já havia sido indicado que:

- A situação de emergência sanitária não suspendeu o respeito aos direitos humanos, incluindo o direito à autodeterminação informativa na União Europeia.
- O consentimento não pode ser considerado livre nestes casos se quem o outorga não pode retirá-lo sem sofrer qualquer dano. Portanto, é necessário estabelecer alternativas que não envolvam o uso de tecnologias como o reconhecimento facial.

- Parece ser exigível uma norma, com força de lei, que possibilite e delimite o uso de tecnologias que coletam dados sensíveis (como o reconhecimento facial) no caso das avaliações *on-line*.

#### 4.2 - O caso da UNMSM no Peru

Não obstante o caso ocorrido no Peru ainda esteja pendente de resolução final pela Autoridade de Proteção de Dados, há vários elementos que fazem parte da denúncia apresentada naquela ocasião à autoridade e que se assemelham ao caso espanhol.<sup>14</sup>

Por exemplo, em relação ao princípio da legalidade no direito peruano, que pressupõe uma base legitimadora para o tratamento de dados pessoais, não existe, até o momento, nenhuma regulamentação específica no país sobre o uso de ferramentas como o *e-proctoring*. De acordo com a pesquisa mencionada na seção anterior, esta ausência parece ter sido entendida pela Universidade San Marcos como um fator que lhe permitia descumprir obrigações formais de nosso sistema, como o cadastro prévio de um banco de dados pessoais (requisito obrigatório).

Algo similar ocorre no caso do consentimento, que foi denunciado à Autoridade como ausente ou inválido, pois a Universidade não teria prestado informações suficientes, a quem se candidata, sobre a natureza do tratamento de seus dados pelo SMOWL. Outro argumento, no mesmo sentido, também indica que, ainda que fosse provada a solicitação de consentimento, este não poderia ser dado livremente, pois não outorgá-lo (e, portanto, não participar do Exame Virtual) causava sérios prejuízos às pessoas candidatas, que ficariam sem possibilidade de acesso à Universidade durante esse ano.

Há também a questão da proporcionalidade. Embora seja verdade que a norma peruana não é tão avançada como a norma espanhola, sendo a primeira inspirada em regulamentação anterior ao atual Regulamento Geral de Proteção de Dados da Espanha,<sup>15</sup> parece fazer sentido considerar a necessidade de avaliar se, efetivamente, uma ferramenta como o SMOWL, no contexto da pandemia de Covid-19, era um instrumento necessário e não apenas conveniente para cumprir o objetivo de realizar uma avaliação e evitar condutas desonestas.

Existem ainda outros aspectos que se afastam do ocorrido no caso da UNIR e não queremos deixar de mencionar, pois não é impossível que também se apresentem na Espanha e/ou em outros países onde são utilizadas tecnologias de *e-proctoring*, sobretudo em grande escala. Quanto a este ponto – que também aparece na denúncia – indica-se a aparente infração ao princípio de segurança que, na normativa peruana, é desenvolvido expressamente por uma Diretiva que estabelece obrigações específicas segundo o tipo de dados, a finalidade do tratamento e se o detentor do banco de dados é uma entidade pública ou privada. As violações a este princípio estariam refletidas nas diversas situações irregulares relatadas durante os dias do Exame Virtual, conforme mencionadas na segunda seção, como a ausência de cadastro prévio do banco de dados e a falta de divulgação das políticas de privacidade no portal da Universidade, entre outras.

## 5 • Conclusões

Algumas conclusões a partir de tudo o que foi dito neste artigo são:

- A adoção de programas de *e-proctoring* tem sido ampla no mundo em virtude da pandemia de Covid-19. Somente na América Latina, um total de 46 universidades os utilizaram durante 2020, principalmente para controlar suas avaliações *on-line*.
- Pelo menos no caso do uso do *software* SMOWL na Universidade San Marcos, durante 2020 ocorreram fatos que nos convidam a pensar criticamente sobre o impacto dessas tecnologias e a ameaça que representam para as/os estudantes, principalmente para sua privacidade.
- Um estudo anterior sobre *e-proctoring* identificou que pelo menos na Argentina, no Chile e no Peru havia regulamentação diretamente aplicável a estes programas, na medida em que envolvem dados pessoais diversos, alguns deles sensíveis. Contudo, não é claro até que ponto essa regulamentação é aplicável. Contribui para isso a falta de pronunciamentos sobre o assunto.
- Em 2021, a Autoridade Espanhola de Proteção de Dados emitiu uma resolução de advertência contra a Universidade de La Rioja pelo uso do *software* SMOWL após receber uma reclamação de estudantes dessa universidade. O principal argumento para recomendar que seu uso fosse evitado foi a ausência de necessidade e proporcionalidade.
- Em que medida esperar que a Autoridade peruana se pronuncie da mesma forma que a espanhola no caso da UNIR é uma pergunta de resposta incerta, mas sua decisão certamente poderia servir de modelo para resoluções em países da região onde a legislação é equivalente.

**Anexo 1:** Quadros de incidência do uso de *e-proctoring* nos países estudados<sup>17</sup>

### A - Argentina

Nome da Universidade	Tipo de instituição	Tecnologia de <i>e-proctoring</i>
Universidade Empresarial Siglo 21	Privada	KLARWAY
Universidade Argentina da Empresa	Privada	PROCTORIO
Universidade de Congreso	Privada	PROCTORIO
Instituto Tecnológico de Buenos Aires	Privada	RESPONDUS
Universidade de Morón	Privada	SUMADI
Universidade de Palermo	Privada	SUMADI



Universidade Católica de Salta	Privada	NÃO ESPECIFICADO
Universidade de San Andrés	Privada	RESPONDUS
Universidade Nacional de Córdoba	Pública	RESPONDUS
Universidade Nacional do Chaco Austral	Pública	SMOWL

## B - Chile

Nome da Universidade	Tipo de instituição	Tecnologia de <i>e-proctoring</i>
Universidade Diego Portales	Privada	RESPONDUS
Universidade de Las Américas	Privada	SMOWL, SUMADI
Universidade de Concepción	Privada	SUMADI
Universidade Católica de Temuco	Privada	SUMADI
Universidade Católica del Maule	Privada	SUMADI
Universidade Santo Tomás	Privada	SUMADI
Universidade San Sebastián	Privada	SUMADI
Universidade Mayor	Privada	SUMADI
Universidade Gabriela Mistral	Privada	SUMADI
Pontifícia Universidade Católica do Chile	Privada	NÃO ESPECIFICADO
Universidade do Chile	Pública	VÁRIOS

## C - Peru

Nome da Universidade	Tipo de instituição	Tecnologia de <i>e-proctoring</i>
Universidade San Ignacio de Loyola	Privada	EXAM
Universidade Nacional de San Agustín	Pública	METTL
Universidade Nacional de Juliaca	Pública	METTL
Universidade de Piura	Privada	METTL
Universidade Privada Antenor Orrego	Privada	METTL
Universidade Nacional Agrária La Molina	Pública	METTL
Universidade Nacional de Jaén	Pública	NÃO ESPECIFICADO

**VIGIAR E REPROVAR**

Universidade Nacional del Santa	Pública	NÃO ESPECIFICADO
Universidade Nacional de Piura	Pública	NÃO ESPECIFICADO
Universidade Nacional José María Arguedas	Pública	NÃO ESPECIFICADO
Universidade Nacional Autónoma Altoandina de Tarma	Pública	NÃO ESPECIFICADO
Universidade Católica San Pablo	Privada	NÃO ESPECIFICADO
Universidade de Lima	Privada	PROCTOR TRACK
Pontifícia Universidade Católica do Peru	Privada	PROCTOR TRACK
Universidade Nacional Autónoma do Alto Amazonas	Pública	SAFE EXAM BROWSER
Universidade Católica de Santa María	Privada	SAFE EXAM BROWSER
Universidade Nacional Mayor de San Marcos	Pública	SMOWL
Universidade Nacional de Engenharia	Pública	SMOWL
Universidade Nacional Jorge Basadre Grohmann	Pública	SMOWL
Universidade Peruana Cayetano Heredia	Privada	SMOWL
Universidade Privada San Juan Bautista	Privada	SMOWL
Universidade César Vallejo	Privada	SMOWL
Universidade do Pacífico	Privada	SUMADI
Universidade Privada do Norte	Privada	SUMADI
Universidade Peruana de Ciências Aplicadas	Privada	SUMADI

**Anexo 2:** Dados pessoais tratados por tipo de tecnologia<sup>18</sup>

<b>Ferramenta</b>	<b>Dados pessoais tratados</b>
Reconhecimento facial para validar identidade	Imagem, traços faciais, nome, documento de identidade
Monitoramento em tempo real por meio de câmera web	Imagem, voz, traços faciais, endereço IP

Gravação e/ou captura de imagem por meio de câmera <i>web</i>	Imagem
Monitoramento em tempo real por meio de câmera <i>web</i>	Imagem, voz, traços faciais, endereço IP
Gravação e/ou captura de áudio por meio de microfone	Voz
Qualificação, por meio de algoritmos, de condutas suspeitas	Imagem, voz, traços faciais, endereço IP, histórico de navegação
Bloqueio de ações (nos dispositivos)	Endereço IP, histórico de navegação

## NOTAS

1 • Karina Garay, “San Marcos anuncia examen virtual de admisión para el 2 y 3 de octubre”. Agencia Peruana de Noticias Andina, 28 de agosto de 2020, acceso em 9 de dezembro de 2021, <https://andina.pe/agencia/noticia-san-marcos-anuncia-examen-virtual-admision-para-2-y-3-octubre-811627.aspx>.

2 • “San Marcos: cómo evitarán plagios y suplantaciones en examen virtual de admisión”. Agencia Peruana de Noticias Andina, 1 de setembro de 2020, acceso em 9 de dezembro de 2021, <https://andina.pe/agencia/noticia-san-marcos-como-evitaran-plagios-y-suplantaciones-examen-virtual-admision-811770.aspx>.

3 • L. Ancajima, “Examen virtual de la UNMSM: Denuncian plagio, transmisiones en vivo y más durante su desarrollo”. RPP, 4 de outubro de 2020, acceso em 9 de dezembro de 2021, <https://rpp.pe/tecnologia/redes-sociales/examen-virtual-de-la-unmsm-denuncian-plagio-transmisiones-en-vivo-y-mas-durante-su-desarrollo-noticia-1296176>.

4 • “Congreso cita a rector de San Marcos por incidentes en el examen de admisión virtual”, Diario El Peruano, 3 de outubro de 2020, acceso em 9 de dezembro de 2021, [https://elperuano.pe/noticia/104779-congreso-cita-a-rector-de-](https://elperuano.pe/noticia/104779-congreso-cita-a-rector-de-san-marcos-por-incidentes-en-el-examen-de-admision-virtual)

[san-marcos-por-incidentes-en-el-examen-de-admision-virtual](https://elperuano.pe/noticia/104779-congreso-cita-a-rector-de-san-marcos-por-incidentes-en-el-examen-de-admision-virtual).

5 • “Sunedu sobre examen virtual de San Marcos: Existen suficientes indicios para iniciar una indagación”, Diario El Comercio, 3 de outubro de 2020, acceso em 9 de dezembro de 2021, <https://elcomercio.pe/lima/sucesos/sunedu-sobre-examen-virtual-de-san-marcos-existen-suficientes-indicios-para-iniciar-una-indagacion-unmsm-nndc-noticia/>.

6 • “La Autoridad Nacional de Protección de Datos Personales realiza acciones de fiscalización para verificar el adecuado tratamiento de los datos personales en el examen de admisión online realizado por la Universidad Nacional Mayor de San Marcos”, Comunicado de imprensa, 5 de outubro de 2020, acceso em 9 de dezembro de 2021, <https://www.redipd.org/es/noticias/la-autoridad-nacional-de-proteccion-de-datos-personales-realiza-acciones-de-fiscalizacion>.

7 • SMOWL, Homepage, 2021, acceso em 15 de outubro de 2021, <https://smowl.net/es>.

8 • Carlos Guerrero Argote, “¿Vigilados en la escuela?: Impacto en la privacidad a partir del uso de tecnologías de e-proctoring en la región de

Latinoamérica". Programa Líderes 2.0 de LACNIC, 2021, acesso em 9 de dezembro de 2021, <https://descargas.lacnic.net/lideres/carlos-guerrero/carlos-guerrero-informe.pdf>.

9 • Ver Anexo 1.

10 • Ver Anexo 2.

11 • M. Gonzalo, "Proctoring: cuando la evaluación de exámenes es vigilancia". Newtral, 12 de maio de 2021, acesso em 9 de dezembro de 2021, <https://www.newtral.es/proctoring-que-es-evaluacion-examenes-vigilancia-unir/20210512/>.

12 • "Resolución de Advertencia", Agencia Española de Protección de Datos, 2021, acesso em 15 de outubro de 2021, [https://www.newtral.es/wp-content/uploads/2021/08/documentoEnvio\\_624316-1.pdf?x60645](https://www.newtral.es/wp-content/uploads/2021/08/documentoEnvio_624316-1.pdf?x60645).

13 • Informe N/REF: 0036/2020 da Agencia Española de Protección de Datos.

14 • Carlos Guerrero Argote, "Denunciamos a la Universidad Nacional Mayor de San Marcos por el uso de software biométrico en su Examen Virtual". Hiperderecho, 22 de setembro de 2020, acesso em 9 de dezembro de 2021, <https://hiperderecho.org/2020/09/denunciamos-a-la-universidad-nacional-mayor-de-san-marcos-por-el-uso-de-software-biometrico-en-su-examen-virtual/>.

15 • Diríamos que seja mais próxima à Diretiva 95/46/CE e à Lei Orgânica de Proteção de Dados, de 1999, da Espanha.

16 • Diretiva de Segurança da Informação Administrada pelos Bancos de Dados Pessoais, de 2014, produzida pela Autoridade de Proteção de Dados do Ministério da Justiça.

17 • A base de dados original que contém o mapeamento consolidado dos três países pode ser consultada e baixada aqui: "Mapeando el uso de software de e-proctoring en universidades de Latinoamérica", [s.d.], acesso em 15 de outubro de 2021, <https://bit.ly/30qcud3>.

18 • A base de dados original que contém os dados pessoais tratados por tipo de ferramenta, bem como as ferramentas identificadas em cada tipo de software de e-proctoring podem ser consultadas e baixadas aqui: "Datos tratados por cada tecnología", [s.d.], acesso em 15 de outubro de 2021, <https://bit.ly/2YQgqml>.



**CARLOS GERMÁN GUERRERO ARGOTE** – Peru

Carlos Germán Guerrero Argote é diretor adjunto do Instituto para a Sociedade da Informação e Quarta Revolução Industrial, Centro de Pesquisa da Universidade La Salle de Arequipa (Peru).

Recebido em novembro de 2021.

Original em espanhol. Traduzido por Valéria Pandjiarjian.



"Este artigo é publicado sob a licença de Creative Commons Noncommercial Attribution-NoDerivatives 4.0 International License"