v. 18 n. 31 São Paulo Dic. 2021

sur

revista internacional
de derechos humanos

edición **31**

ARTÍCULO

VIGILAR Y REPROBAR

Carlos Germán Guerrero Argote

• *Impacto en la privacidad de estudiantes universitarios a partir del uso de software de eProctoring* •

RESUMEN

El texto aborda la siguiente pregunta: ¿Cuál es el impacto del uso de programas de eProctoring en la privacidad de estudiantes universitarios? Se parte de un caso de uso ocurrido en una universidad de Perú en 2020, a partir del cual se exploran los conceptos relacionados al eProctoring, la privacidad y la protección de datos personales. También se hace un recuento sobre el nivel de adopción de estas tecnologías, con especial foco en la región de Latinoamérica. Finalmente, se presenta un análisis sobre la interacción entre el eProctoring y las normas de protección de datos personales, que incluye la casuística más reciente sobre el tema.

PALABRAS CLAVE

eProctoring | Vigilancia | Datos personales | Educación

1 • Introducción

Si bien existen desde hace muchos años los softwares de eProctoring o proctoring remoto, eran poco conocidos hasta antes de la pandemia de COVID-19. A diferencia de otras herramientas educativas, el eProctoring posee una capacidad disruptiva abismal, que se debe principalmente al uso intensivo de tecnologías de punta como la biometría, el reconocimiento facial y la inteligencia artificial.

La virtualización de las clases durante el año 2020 con motivo de la pandemia marcó el inicio de la adopción masiva de estos programas en todo el mundo. Su capacidad para permitir el control de las evaluaciones en línea y su potencial de detectar conductas deshonestas como la suplantación y el plagio lo hicieron además una solución muy atractiva para las universidades.

Sin embargo, el despliegue de estas tecnologías ha provocado diferentes reacciones adversas en las comunidades estudiantiles. Tal vez las más puntuales giran en torno a si resulta conveniente la adopción de tecnologías percibidas como muy invasivas para la privacidad. A pesar de este y otros reparos, en muchos casos las universidades han forzado su uso con consecuencias no siempre positivas.

El presente artículo busca arrojar mayores luces sobre el impacto del uso de estas tecnologías en la privacidad de estudiantes universitarios. Si bien su foco está en la región de Latinoamérica y específicamente en el Perú, aborda un problema cuyas características son similares a otros lugares donde se han implementado estos programas.

2 • El caso de la Universidad San Marcos

En agosto del año 2020, la Universidad Nacional Mayor de San Marcos (UNMSM), la universidad pública más importante del Perú anunció que su Examen de Admisión Anual se realizaría en formato virtual.[1] Esta noticia, que se daba luego de varios meses de incertidumbre debido a las medidas desplegadas para detener la propagación del COVID-19, supuso un alivio para muchos postulantes, pero al mismo tiempo trajo consigo un nuevo conjunto de preocupaciones.

En su anuncio, la Universidad San Marcos señaló también que había establecido algunas medidas para evitar las posibles conductas deshonestas que podían ocurrir en una prueba no presencial, pero no ahondó más en el tema. Sin embargo, una semana después, en una entrevista al jefe de la Oficina Central de Admisión de la UNMSM, este dio más detalles:

> *Ahora que se decidió que el examen de admisión será virtual surgen una serie de interrogantes, principalmente referidas a la posibilidad de que algunos estudiantes hagan trampa, que use la computadora para buscar las respuestas en páginas webs, que alguien ayude a*

> *responder las preguntas o que haya suplantación del postulante. [...] Mediante un aplicativo que emplea la inteligencia artificial se verificará si el postulante que está frente a la computadora el día del examen es el mismo que se registró biométricamente. [...] El aplicativo de seguridad irá capturando las imágenes cada minuto y detectará si alguien abre una página web ajena a la evaluación. Pero además se detectará si la computadora tiene alguna conexión periférica, por ejemplo con una pantalla, un cable HDMI o un software remoto. El sistema, igualmente, es capaz de registrar si alguien hace un copy-page, una captura* (screenshot) *o si se activan cambios en la ventana del Windows.*[2]

Varias personas postulantes al Examen de Admisión se mostraron primero escépticas y luego manifestaron su rechazo a esta nueva modalidad por diferentes motivos: algunos estaban relacionados con el contexto de la pandemia, pero otros respondían a carencias estructurales como la brecha digital y también al temor que despertaba el uso de tecnologías previamente desconocidas cuya importancia era capital para el normal desarrollo de la prueba. A lo largo de los siguientes meses, estas personas se organizaron y ofrecieron una resistencia coordinada para intentar detener el Examen Virtual.

No obstante, la UNMSM no dio su brazo a torcer y al llegar las fechas establecidas en octubre, procedió a la realización del Examen Virtual, que contó con una participación reducida, solo 8 mil personas de un total inicial de más de 15 mil. Como era previsible para muchos de sus detractores, durante el Examen se reportaron múltiples incidentes. Por ejemplo, se denunció que, pese a que era un requisito obligatorio, se permitió a varios estudiantes rendir el mismo sin la cámara encendida. Se reportó que tanto las preguntas como respuestas de la prueba circulaban en redes sociales. Increíblemente, se denunció también que el Examen fue transmitido en vivo por la plataforma de streaming Twitch.[3]

Pese a las denuncias, que motivaron diferentes pronunciamientos de entidades como el Congreso de la República,[4] la Superintendencia Nacional de Educación Universitaria (SUNEDU)[5] e inclusive de la Autoridad de Protección de Datos Personales (APDP),[6] la Universidad hizo caso omiso y días después publicó los resultados del Examen de Admisión. Con el paso de las semanas el interés sobre el caso se diluyó y, salvo la APDP que inició un proceso administrativo fiscalizador, las demás entidades no prosiguieron con otro tipo de acciones.

Durante el transcurso de los eventos antes mencionados, nunca se abordó desde la prensa cuáles eran esas "tecnologías que usaban inteligencia artificial" para detectar el plagio y la suplantación que fueron anunciadas por las autoridades de la UNMSM. Sin embargo, en una investigación posterior desarrollada por nosotros a inicios del año 2021, descubrimos que la tecnología utilizada por la Universidad se llamaba SMOWL, un software creado y distribuido por Smowltech, una empresa española especializada en la provisión de servicios de supervisión remota para evaluaciones en línea, también conocidos como eProctoring.[7]

3 • eProctoring en latinoamérica y protección de datos personales

Como decíamos, el caso de la Universidad San Marcos nos llevó a emprender una investigación sobre las implicancias del uso de estas herramientas tecnológicas. Así pues, al final del primer trimestre de 2021 publicamos un reporte que incluía un mapeo inicial de la adopción del eProctoring en la región de Latinoamérica, así como un relevo de legislación sobre privacidad y protección de datos personales aplicable.[8] A continuación, comentaremos algunos de sus resultados.

3. 1 - Despliegue de eProctoring en Latinoamérica

El estudio en mención eligió tres países como casos de estudio; Argentina, Chile y Perú y realizó sobre ellos una investigación de escritorio para identificar, a través de la consulta de fuentes abiertas, el nivel de adopción de soluciones de eProctoring durante 2020, específicamente por parte de universidades públicas y privadas.

Este sondeo inicial arrojó lo siguiente: En Argentina, se detectaron 10 casos de adopción de uno o más softwares de eProctoring, 2 de ellos en universidades públicas y 8 en privadas. En Chile, se detectaron 11 casos, 1 de ellos en universidades públicas y 10 en privadas. Finalmente, en Perú se detectaron 25 casos, 12 en universidades públicas y 13 en privadas. Los tres softwares de eProctoring más recurrentes fueron, en este orden: SUMADI, SMOWL y METTL.[9]

Si bien la evidencia recolectada no alcanzó a establecer patrones comunes entre las universidades, un factor recurrente fue que la mayoría de los programas sirvieron casi exclusivamente para controlar evaluaciones realizadas en línea y, por lo general, fueron adoptados como soluciones de emergencia. Tal vez debido a esto último es que su despliegue además fue casi siempre inopinado y en muchas ocasiones se realizó sin siquiera habilitar procesos adecuados de familiarización de estudiantes y docentes con el software.

Otro aspecto interesante de resaltar fue que la mayoría de los programas de eProctoring eran soluciones que empleaban tecnologías muy avanzadas. Por ejemplo, los tres más recurrentes funcionaban a partir de algoritmos de inteligencia artificial, alimentados con datos obtenidos a partir de herramientas como el reconocimiento facial y la biometría. Todos estos datos además se obtenían gracias a que los programas tomaban control de los dispositivos donde los estudiantes rendían sus pruebas, exigiendo para ello que estos poseyeran periféricos (cámaras, micrófonos) y un sistema operativo acorde a sus requerimientos.

3. 2 - Protección de datos personales aplicables al eProctoring

El hecho de que para funcionar, los softwares de eProctoring requirieran consumir una gran cantidad de datos producidos por los/las estudiantes durante el desarrollo de las evaluaciones, fue motivo de preocupación en el caso de la Universidad San Marcos, tal como se ha mencionado en la sección anterior. En lo que podríamos identificar como preocupaciones directamente relacionadas con la privacidad estaba el hecho de que estas tecnologías se percibían como muy

invasivas pues grababan de forma constante a las/los estudiantes y su entorno, registrando todo lo que se hacía en sus dispositivos. Este material era el insumo principal para descalificar estudiantes bajo parámetros no siempre explicados y generalmente confusos.

En este apartado, la investigación realizada arrojó que la mayoría de los softwares de eProctoring trataban datos personales tales como: dirección IP, historial de navegación, imagen del rostro, nombres y apellidos, rasgos faciales y voz. Algunos de estos datos además eran considerados datos sensibles en los tres países de estudio, lo que implicaba necesariamente la aplicación de diferentes normas que regulan su tratamiento, pero especialmente aquellas relacionadas con la protección de datos personales.[10]

Pese a que se identificó que los países contaban con leyes de protección de datos personales de alcance nacional y disposiciones de obligatorio cumplimiento en ese sentido, se descubrió también que su aplicación al uso del eProctoring no estaba exenta de aspectos controversiales. Por ejemplo, estaba el hecho de la jurisdicción: ninguno de los tres programas más utilizados era provisto a las universidades por empresas domiciliadas en el territorio sino desde el extranjero y a través de Internet. También se identificó una aparente anomia producto del hecho que el uso del eProctoring no había sido previsto en ninguna regulación previa, por lo que no era claro el nivel de exigencia de obligaciones como la inscripción de bancos de datos personales o la solicitud del consentimiento, especialmente en un contexto de crisis como el que se vivía en 2020 por causa del COVID-19.

No obstante lo anterior, la investigación pudo comprobar que al menos en Argentina y Perú, superado el problema del alcance territorial de las normas de protección de datos personales, varias disposiciones generales y específicas resultaban enteramente aplicables sino a las empresas proveedoras del eProctoring, al menos a las universidades que contrataban sus servicios. Sin embargo, frente a una evaluación de cumplimiento, salvo excepciones, en la mayoría de los casos parecía que las universidades habían razonado que estas disposiciones no les eran aplicables o sencillamente habían optado por incumplirlas.

Un problema adicional para poder determinar con mayor exactitud hasta qué punto las normas de protección de datos personales en estos tres países se habían incumplido y eso significaba haber incurrido en infracciones era que, salvo en Perú, no existían investigaciones o procesos de fiscalización por parte de las autoridades de protección de datos. Así pues, la mayor parte de las conclusiones del estudio comentado tenían naturaleza especulativa y reclamaban pronunciamientos oficiales para volverse más sólidas o desecharse.

4 • Impacto en la privacidad: el caso de España y el de Perú sobre el eProctoring

Decíamos en la introducción que si bien nuestro foco de estudio estuvo en Latinoamérica, las situaciones de conflicto producidos por el despliegue del eProctoring han sido globales.

Prueba de ello es que al mismo tiempo en que en Perú la Universidad San Marcos anunciaba el uso de SMOWL para controlar su Examen Virtual, situaciones similares acontecían en otros países. Como en España, país en donde actualmente existe por lo menos un pronunciamiento de la Autoridad Española de Protección de Datos (AEPD) sobre un caso de uso de eProctoring en la Universidad de la Rioja (UNIR).

4.1. - El caso de UNIR en España

Tal como se explica en esta cronología del medio Newtral,[11] en marzo de 2021 la UNIR comunicó a sus estudiantes que debido a la pandemia de COVID-19 iba a realizar sus exámenes de julio en modalidad virtual. Posterior a este anuncio, se indicó también que se iba a implementar un programa de "autenticación biométrica" como medida de seguridad. De forma muy similar a lo acontecido en el caso de la Universidad San Marcos, un grupo importante de estudiantes españoles expresó sus críticas al cambio, pero no fueron atendidos apropiadamente. Inclusive el software empleado en esta ocasión era el mismo que en Perú: SMOWL.

El caso fue denunciado por las personas afectadas en tribunales y también ante la AEPD. Esta última, emitió un pronunciamiento de advertencia en julio de ese año.[12] Entre algunas de las conclusiones del documento estuvieron:

- Que es conveniente llevar a cabo un análisis de impacto en la privacidad, con el fin de determinar si el uso de programas como el eProctoring es realmente la mejor opción para lograr los objetivos de evaluación educativa.

- Que en lo que respecta al tratamiento de datos biométricos a través de tecnología de reconocimiento facial, si bien esto puede ser conveniente para las universidades, eso no significa que sea necesario, una condición indispensable cuando se tratan datos sensibles.

Además, los anteriores argumentos se sostienen también en un informe lanzado por la AEPD un año atrás acerca del uso de técnicas de reconocimiento facial en la realización de pruebas de evaluación en línea,[13] en donde ya había indicado:

- Que la situación de emergencia sanitaria no ha suspendido el respeto de los derechos humanos, entre ellos el derecho de autodeterminación informativa en la Unión Europea.

- Que el consentimiento no puede considerarse libre en estos casos si quien lo otorga no puede retirarlo sin sufrir perjuicio alguno. Por lo tanto, es preciso establecer alternativas que no impliquen el uso de tecnologías como el reconocimiento facial.

- Que parece exigible una norma con rango de ley que habilite y delimite el uso de tecnologías que recolectan datos sensibles (como el reconocimiento facial) en el caso de las evaluaciones en línea.

4. 2. - El caso de la UNMSM en Perú

Aunque el caso ocurrido en Perú todavía sigue pendiente de resolución final de la Autoridad de Protección de Datos, existen varios elementos que forman parte de la denuncia que se presentó en su momento ante la autoridad y que son similares al caso español.[14]

Por ejemplo, en torno al principio de legalidad en la norma peruana, que presupone una base legitimadora del tratamiento de datos personales, no existe a la fecha en el país ninguna regulación específica sobre el uso de herramientas como el eProctoring. Según la investigación mencionada en la sección anterior, esta ausencia parece haber sido leída por la Universidad San Marcos como un factor que le permitía incumplir con obligaciones formalistas de nuestro sistema como es la inscripción previa de un banco de datos personales (un requisito obligatorio).

Algo similar ocurre en el caso del consentimiento, que fue denunciado ante la Autoridad como ausente o viciado, pues la Universidad no habría ofrecido suficiente información a quien se postula, a acerca de la naturaleza del tratamiento de sus datos por parte de SMOWL. Existe además otro argumento en esa misma línea que indica que aún si se probara que se solicitó el consentimiento, este no podría ser prestado libremente, pues no otorgarlo (y por lo tanto no participar del Examen Virtual) generaba un grave perjuicio a los y las postulantes, que se quedaban sin la posibilidad de acceder durante ese año a la Universidad.

También está el asunto de la proporcionalidad. Si bien es cierto que la norma peruana no está tan avanzada como la norma española, siendo que la primera está inspirada en una regulación anterior al actual Reglamento General de Protección de Datos de España;[15] parece tener sentido considerar la necesidad de evaluar si efectivamente una herramienta como SMOWL, en el contexto de la pandemia de COVID-19 era un instrumento necesario y no solo conveniente para cumplir el objetivo de realizar una evaluación y evitar las conductas deshonestas.

Existen además otros aspectos que se apartan de lo acontecido en el caso de la UNIR, pero que no queremos dejar de mencionar pues no es imposible que pudieran presentarse también en España u o en otros países donde se utilicen tecnologías de eProctoring, sobre todo a gran escala. Este punto, que también figura en la denuncia, señala la aparente infracción del principio de seguridad que en la normativa peruana está desarrollado específicamente a través de una Directiva que posee obligaciones específicas dependiendo del tipo de datos, el propósito del tratamiento y si el titular de los bancos de datos es entidad pública o privada.[16] Las infracciones a este principio se verían reflejadas en las múltiples situaciones irregulares denunciadas durante los días del Examen Virtual que fueron mencionados en la segunda sección, la ausencia de inscripción previa de banco de datos, la falta de publicidad de las políticas de privacidad en el portal de la Universidad, entre otras.

5 • Conclusiones

Algunas conclusiones a las que podemos llegar a partir de todo lo dicho en este artículo son:

• La adopción de programas de eProctoring ha sido amplia en el mundo a propósito de la pandemia de COVID-19. Solo en Latinoamérica, un total de 46 universidades los utilizaron durante 2020, principalmente para controlar sus evaluaciones en línea.

• Al menos en el caso del uso del software SMOWL en la Universidad de San Marcos durante 2020 se produjeron hechos que invitan a pensar críticamente en el impacto de estas tecnologías y la amenaza que suponen para estudiantes, principalmente para su privacidad.

• Un estudio previo sobre el eProctoring identificó que por lo menos en Argentina, Chile y Perú existía regulación directamente aplicable a estos programas en la medida que estos tratan múltiples datos personales, algunos de ellos sensibles. Sin embargo, no es claro hasta qué punto dicha regulación es aplicable. A eso contribuye la falta de pronunciamientos sobre la materia.

• En 2021 la Autoridad Española de Protección de Datos emitió una resolución de advertencia contra UNIR por el uso del software SMOWL luego de recibir un reclamo por parte de estudiantes de dicha universidad. El argumento principal para recomendar que se evitara su uso fue la falta de necesidad y proporcionalidad.

• En qué medida es esperable que la Autoridad Peruana se pronuncie en forma similar a la autoridad española el caso de UNIR es una pregunta con respuesta incierta, pero su decisión ciertamente podría servir de modelo para resoluciones en países de la región en donde la legislación es equivalente.

Anexo 1: Cuadros de incidencia de uso de eProctoring en los países estudiados[17]

A - Argentina

Nombre de la Universidad	Tipo de institución	Tecnología de e-proctoring
Universidad Empresarial Siglo 21	Privada	KLARWAY
Universidad Argentina de la Empresa	Privada	PROCTORIO
Universidad de la Congreso	Privada	PROCTORIO
Instituto Tecnológico de Buenos Aires	Privada	RESPONDUS
Universidad de Morón	Privada	SUMADI
Universidad de Palermo	Privada	SUMADI

Universidad Católica de Salta	Privada	NO ESPECIFICADO
Universidad de San Andrés	Privada	RESPONDUS
Universidad Nacional de Córdoba	Pública	RESPONDUS
Universidad Nacional do Chaco Austral	Pública	SMOWL

B - Chile

Nome da Universidade	Tipo de institución	Tecnología de e-proctoring
Universidad Diego Portales	Privada	RESPONDUS
Universidad de Las Américas	Privada	SMOWL, SUMADI
Universidad de Concepción	Privada	SUMADI
Universidad Católica de Temuco	Privada	SUMADI
Universidad Católica del Maule	Privada	SUMADI
Universidad Santo Tomás	Privada	SUMADI
Universidad San Sebastián	Privada	SUMADI
Universidad Mayor	Privada	SUMADI
Universidad Gabriela Mistral	Privada	SUMADI
Pontifícia Universidade Católica do Chile	Privada	NO ESPECIFICADO
Universidad de Chile	Pública	VARIOS

C - Perú

Nome da Universidade	Tipo de instituição	Tecnologia de *e-proctoring*
Universidad San Ignacio de Loyola	Privada	EXAM
Universidad Nacional de San Agustín	Pública	METTL
Universidad Nacional de Juliaca	Pública	METTL
Universidad de Piura	Privada	METTL
Universidad Privada Antenor Orrego	Privada	METTL
Universidad Nacional Agrária La Molina	Pública	METTL
Universidad Nacional de Jaén	Pública	NO ESPECIFICADO

Universidad Nacional del Santa	Pública	NO ESPECIFICADO
Universidad Nacional de Piura	Pública	NO ESPECIFICADO
Universidad Nacional José María Arguedas	Pública	NO ESPECIFICADO
Universidad Nacional Autônoma Altoandina de Tarma	Pública	NO ESPECIFICADO
Universidad Católica San Pablo	Privada	NO ESPECIFICADO
Universidad de Lima	Privada	PROCTOR TRACK
Pontifícia Universidade Católica del Perú	Privada	PROCTOR TRACK
Universidad Nacional Autônoma do Alto Amazonas	Pública	SAFE EXAM BROWSER
Universidad Católica de Santa María	Privada	SAFE EXAM BROWSER
Universidad Nacional Maior de San Marcos	Pública	SMOWL
Universidade Nacional de Engenharia	Pública	SMOWL
Universidad Nacional Jorge Basadre Grohmann	Pública	SMOWL
Universidad Peruana Cayetano Heredia	Privada	SMOWL
Universidad Privada San Juan Bautista	Privada	SMOWL
Universidad César Vallejo	Privada	SMOWL
Universidad del Pacífico	Privada	SUMADI
Universidad Privada do Norte	Privada	SUMADI
Universidad Peruana de Ciências Aplicadas	Privada	SUMADI

Anexo 2: Datos personales tratados por tipo de tecnología[18]

Herramienta	Datos personales tratados
Reconocimiento facial para validar identidad	Imagen, rasgos faciales, nombre, documento de identidad
Monitoreo en tiempo real a través de cámara web	Imagen, voz, rasgos faciales, dirección IP

Grabación y/o captura de imagen a través de cámara web	Imagen
Grabación y/o captura de audio a través de micrófono	Voz
Calificación, mediante algoritmos, de conductas sospechosas	Imagen, voz, rasgos faciales, dirección IP, historial de navegación
Bloqueo de acciones (en los dispositivos)	Dirección IP, historial de navegación

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, visitado el 9 de diciembre 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 septiembre de 2020, visitado el 9 de diciembre 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 octubre de 2020, visitado el 9 de diciembre 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 octubre de 2020, visitado el 9 de diciembre de 2021, 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 octubre de 2020, visitado el 9 de diciembre 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", Nota de prensa, 5 de octubre de 2020, visitado el 9 de diciembre de 2021, https://www.redipd.org/es/noticias/la-autoridad-nacional-de-proteccion-de-datos-personales-realiza-acciones-de-fiscalizacion.

7 • SMOWL, Página principal, 2021, visitado el 15 de octubre 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, visitado el 9 de diciembre 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 mayo de 2021, visitado el 9 de diciembre 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, visitado el 15 de octubre de 2021, https://www.newtral.es/wp-content/uploads/2021/08/documentoEnvio_624316-1.pdf?x60645.

13 • Informe N/REF: 0036/2020 de la 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 septiembre de 2020, visitado el 9 de diciembre 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 más cercana a la Directiva 95/46/CE y la Ley Orgánica de Protección de Datos de 1999 de España.

16 • Directiva de Seguridad de la Información Administrada por los Bancos de Datos Personales de 2014, producida por la Autoridad de Protección de Datos del Ministerio de Justicia.

17 • La base de datos original que contiene el mapeo consolidado de los tres países puede ser consultada y descargada aquí: "Mapeando el uso de software de e-proctoring en universidades de Latinoamérica", [s.f.], visitado el 15 de octubre de 2021, https://bit.ly/30qcud3.

18 • La base de datos original que contiene los datos personales tratados por tipo de herramienta, así como las herramientas identificadas en cada tipo de software de eProctoring puede ser consultada y descargada aquí: "Datos tratados por cada tecnología", [s.f.], visitado el 15 de octubre de 2021, https://bit.ly/2YQgqml.

CARLOS GERMÁN GUERRERO ARGOTE – *Perú*
Carlos Germán Guerrero Argote es Director Adjunto del Instituto para la Sociedad de la Información y Cuarta Revolución Industrial, Centro de investigación de la Universidad La Salle de Arequipa (Perú).

Recibido en noviembre de 2021.
Original en español.