Impacto en la privacidad a partir del uso de tecnologías de e-proctoring en la región de Latinoamérica: Estudio del caso en universidades de Argentina, Chile y Perú

Revista Latinoamericana de Economía y Sociedad Digital

Issue 2, agosto 2021

Autores: Carlos Guerrero Argote

DOI: 10.53857/OBPB6056

Publicado: 25 agosto, 2021

Recibido: 8 marzo, 2021

Cita sugerida: Guerrero Argote, Carlos (2021) "Impacto en la privacidad a partir del uso de tecnologías de e-proctoring en la región de Latinoamérica: Estudio del caso en universidades de Argentina, Chile y Perú" en Revista Latinoamericana de Economía y Sociedad Digital, Issue 2

Tipo: Estudio de caso

Palabras clave: e-proctoring, educación en línea, inteligencia artificial, privacidad, proctoring

---

Resumen

Si bien existen desde hace años, los softwares de e-proctoring o proctoring remoto, no existía eran prácticamente desconocidos en la región de Latinoamérica hasta antes de la pandemia de COVID-19. A diferencia de otras soluciones tecnológicas aplicadas a la educación, el e-proctoring 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. El uso de estas tecnologías genera dudas acerca de los efectos que podrían tener en la privacidad de los estudiantes. Este estudio contribuye a despejar algunas de esas dudas al describir cuál es el nivel de adopción del e-proctoring en las universidades de tres países latinoamericanos: Argentina, Chile y Perú. Luego de este primer reconocimiento, se aborda qué regulaciones en materia de privacidad

existen en los países de estudio y cuáles resultan aplicables al uso de estas tecnologías. Finalmente, se analizan escenarios de posible vulneración a la privacidad de los estudiantes. En cuanto a las conclusiones, estas fueron que: la adopción de software de e-proctoring es amplia en los tres países, siendo mayor en las universidades privadas. También se corroboró que en todos los países existe regulación directamente aplicable al uso de estas tecnologías, específicamente las normativas de protección de datos personales. Se detectaron también posibles vulneraciones a la privacidad, como consecuencia del incumplimiento de las obligaciones de protección de datos previamente mapeadas.

Abstract

Even though the e-proctoring or remote proctoring software has existed for a long time, they were practically unknown in the Latin-American region before the pandemic COVID-19. Unlike the other technological solutions applied to education, e-proctoring has a vast disruptive capacity, due to mainly the intensive use of cutting-edge technology such as biometrics, facial recognition and artificial intelligence. The usage of these technologies raises doubts about the effects on the student's privacy. This paper contributes to dispel some doubts describing the level of adoption of e-proctoring in the universities of the three Latin-American countries: Argentina, Chile y Peru. After the first acknowledgement, we deal with the regulations related to privacy that are established in the countries that are studied and which ones are applicable to these technologies Finally, the scenarios of a possible invasion to the students' privacy are analyzed. The conclusions were: the three countries widely use the e-proctoring software, being wider at the private universities. It was also confirmed that, in all the countries, there is a regulation that is directly applicable to the use of these technologies, specifically the regulations related to personal data protection. Some possible invasions to privacy were identified as a consequence of the failure to comply with the obligation of the data protection of the previously mapped data.

Resumo

Embora existam há anos, os softwares de e-proctoring ou proctoring remoto eram praticamente desconhecidos na região da América Latina até antes da pandemia de COVID-19. Ao contrário de outras soluções tecnológicas aplicadas à educação, o e-proctoring tem uma capacidade disruptiva imensa, que se deve principalmente ao uso intensivo de tecnologias de ponta como biometria, reconhecimento facial e inteligência artificial. O uso dessas tecnologias levanta questões sobre os possíveis efeitos que poderiam ter em relação à privacidade dos estudantes. Este estudo contribui para esclarecer algumas dessas dúvidas ao descrever o grau de adoção do e-proctoring nas universidades de três países latino-americanos: Argentina, Chile e Peru. Após esse primeiro reconhecimento, dicute-se quais regulamentos em matéria de privacidade existem nos países de estudo e

quais são aplicáveis ao uso dessas tecnologias. Por fim, são analisados os cenários de possível vulneração da privacidade dos estudantes. Quanto às conclusões, temos: a adoção de software de e-proctoring é ampla nos três países, sendo maior nas universidades privadas. Também foi confirmado que em todos os países existe uma regulamentação diretamente aplicável ao uso dessas tecnologias, especificamente os regulamentos de proteção de dados pessoais. Também foram detectadas possíveis vulnerações de privacidade em decorrência do descumprimento das obrigações de proteção de dados previamente mapeadas.

Introducción

Es probable que antes de la pandemia de COVID-19, un profesor de una universidad latinoamericana no hubiera escuchado en su vida la palabra *proctoring*. Esto no resulta extraño por varios motivos, pero principalmente porque el significado del término y lo que implica, son nociones que hasta hace muy poco eran ajenas al ejercicio cotidiano de la educación en nuestra región. Sin embargo, como producto de los cambios que ha traído la pandemia, el *e-proctoring*[1] se está convirtiendo en una solución cada vez más atractiva para las instituciones educativas, especialmente las universidades.

Los diferentes *softwares* de *e-proctoring*, especialmente los más recientes, son criaturas fascinantes. La mayoría poseen un arsenal de tecnologías avanzadas como la biometría, el reconocimiento facial y la inteligencia artificial, las mismas que actualmente solo se encuentran en los sistemas más sofisticados de vigilancia. Debido al vertiginoso avance de la ciencia y la técnica detrás de estos desarrollos, actualmente estos programas no solo se comercializan en el mercado de las tecnologías educativas, sino que lo hacen a precios altamente competitivos.

Pero, ¿cuál es el objetivo de este despliegue inaudito de alta tecnología? Evitar que los estudiantes hagan trampa durante los exámenes. Por ejemplo, con el fin de evitar la suplantación, estos programas están diseñados para crear perfiles biométricos a partir de fotografías y con ellas corroborar, en tiempo real, si realmente el estudiante está detrás de la pantalla o ha sido reemplazado. Varios poseen algoritmos que les permiten detectar movimiento e incluso sonidos, algunos de los cuales etiquetarán como “sospechosos” y podrían servir de base para tomar decisiones automatizadas. También algunos son capaces de monitorear los dispositivos donde están instalados, restringiendo acciones y accesos.

Aunque el *e-proctoring* existe desde hace varios años y es ampliamente utilizado en todos los niveles de la educación en Estados Unidos y otros países del norte global, hasta hace muy poco había poca evidencia de que fuera masivamente adoptado en Latinoamérica. Sin embargo, con la virtualización forzada de casi todas las actividades durante el año 2020, las instituciones educativas de la región han comenzado a adoptar cada vez más estas soluciones para hacer viable la continuidad de sus actividades. No obstante, muchas de ellas

no parecen haber reparado en los posibles efectos negativos de su implementación, al menos respecto de los estudiantes, lo que sí ha ocurrido en regiones como Europa.[2]

Por ejemplo, en agosto de 2020, una universidad pública del Perú dispuso el uso de uno de estos *softwares* para la realización de su examen de admisión anual; un proceso que convoca a casi 20 mil postulantes de todo el país. Por un lado, esto supuso la exclusión de un grupo considerable de postulantes, debido a que el programa de *e-proctoring* solo podía ser instalado en una computadora (no en *tablets* o teléfonos móviles) y exigía ciertas características mínimas en cuanto a los periféricos y la conexión de Internet. Por el otro, sembró dudas acerca de la protección de la privacidad, debido a que la universidad jamás explicó el funcionamiento del *software* ni el destino de los datos recopilados (Garay, 2020). Algo similar, aunque en menor escala, ocurrió también en una universidad de Argentina, provocando el rechazo de parte de la comunidad estudiantil (Fernández, 2020).

Este estudio quiso explorar el impacto del uso de *software* de *e-proctoring* en un campo específico de nuestro interés: el de la privacidad. No obstante, al momento de iniciar esta tarea descubrimos que existía muy poca bibliografía académica específica sobre el tema, siendo que la mayoría además se enfocaba casi exclusivamente en el impacto del *proctoring* en los procesos educativos y el aprendizaje, especialmente en adolescentes. Más decepcionante aún fue hallar que de lo existente, nada correspondía a experiencias en países de Latinoamérica. Por estos motivos, decidimos que el estudio fuera exploratorio e identificara actores y estructuras, sobre los cuales se realizaría un análisis de impacto legal preliminar y no concluyente.

Debido a los recursos limitados, elegimos solo tres países como casos de estudio: Argentina, Chile y Perú. Estos fueron seleccionados en base a la disponibilidad de información sobre estos en relación al uso de *software* de *e-proctoring*, pero también debido a nuestros conocimientos previos acerca de su legislación en materia de privacidad, especialmente la relacionada a la protección de datos personales. Consideramos que, por sus características, constituían una muestra suficiente para un estudio exploratorio, pero del cual se podían extrapolar algunas de las conclusiones a otros países de la región.

El estudio está estructurado en tres partes. En la primera, abordamos el proceso de mapeo de universidades que utilizan o utilizaron programas de *e-proctoring* hasta febrero de 2021 de los tres países escogidos. En la segunda, presentamos el conjunto de legislación sobre privacidad aplicable al *e-proctoring* en estos tres países. En la tercera parte, se encuentra el análisis jurídico sobre posibles situaciones de vulneración de la privacidad, a partir del presunto incumplimiento de la legislación sobre privacidad aplicable. Finalmente, se presentan algunas conclusiones y recomendaciones.

Metodología

Al ser un estudio exploratorio, la recolección, análisis y presentación de información

extraída de fuentes primarias y secundarias fue la herramienta más empleada. Cabe señalar además que toda esta información fue extraída únicamente de fuentes disponibles a través de Internet, como portales de noticias, sitios web de las universidades, sitios web de las empresas de *e-proctoring*, entre otros afines. A continuación, se detalla mejor el proceso empleado en cada una de las tres partes que componen el estudio:

En la primera parte, se elaboró una lista con todas las universidades de los tres países de estudio, para lo cual se consultaron registros oficiales del sector educativo. Una vez hecho esto, se procedió a la búsqueda de fuentes de información en motores de búsqueda utilizando palabras clave como "*e-proctoring*", "*proctoring*", "*software* de monitoreo para exámenes", a las que se sumó el nombre de todas y cada una de las universidades. De esta manera, allí donde hubo coincidencias, se examinó la información para determinar si efectivamente daba a conocer más allá de toda duda que la institución había empleado alguna vez estos programas.

En la segunda parte, se consultó principalmente normas jurídicas de los tres países en materia de privacidad y artículos académicos que desarrollaban su contenido y alcances a nivel doctrinario. La mayor parte del material revisado está relacionado con los conceptos de derecho a la intimidad, derecho a la autodeterminación informativa y hábeas data, que son las denominaciones comunes más utilizadas en este campo. De este conjunto, se aisló aquellas obligaciones de privacidad aplicables al uso del *e-proctoring*.

También se procedió a clasificar los programas de *e-proctoring* identificados en la primera a través de un método de tres niveles, con el fin de conocer qué tipos de datos recopilaban y aislar aquellos que son datos personales y datos personales sensibles. Esto con el fin de proceder a una evaluación posterior en la tercera parte del estudio.

En la tercera parte, se hizo un ejercicio de contraste entre las obligaciones identificadas en la segunda parte y posibles escenarios de aplicación a partir del uso de *e-proctoring* por parte de las universidades. Se empleó la deducción e inferencia lógica, propia del análisis jurídico, tendiendo a favorecer el método de interpretación teleológica, es decir tratar las normas jurídicas a partir del fin que buscan lograr, sin restringirse al lenguaje formal que utilizan.

1. Universidades que utilizaron *software* de *e-proctoring*

La elaboración de la lista inicial, que se elaboró consultando bases de datos de entidades educativas, culminó con un recuento total de 267 universidades; 108 de Argentina, 55 de Chile y 104 de Perú. A partir de allí, consultamos fuentes de acceso abierto disponibles en Internet, con el fin de saber si en algún momento se había hecho pública la adquisición o uso de tecnologías de *e-proctoring*. En algunos casos fue sencillo, pues estos hechos habían trascendido a la prensa. En otros casos, solo fue posible deducir esta información a través

de documentos de gestión interna, manuales para estudiantes y comunicados de las universidades, todos accesibles desde Internet. Los resultados obtenidos fueron los siguientes[3]:

1.1 Argentina

Nombre de la universidad	***software* de *e-proctoring***
Universidad Empresarial Siglo 21	KLARWAY
Universidad Argentina de la Empresa	PROCTORIO
Universidad de Congreso	PROCTORIO
Instituto Tecnológico de Buenos Aires	RESPONDUS
Universidad de Morón	SUMADI
Universidad de Palermo	SUMADI
Universidad Católica de Salta	NO ESPECIFICADO
Universidad de San Andrés	RESPONDUS
Universidad Nacional de Córdoba	RESPONDUS
Universidad Nacional del Chaco Austral	SMOWL

Fuente: Elaboración propia

1.2 Chile

Nombre de la universidad	***software* de *e-proctoring***
Universidad Diego Portales	RESPONDUS
Universidad de Las Américas	SMOWL, SUMADI
Universidad de Concepción	SUMADI
Universidad Católica de Temuco	SUMADI
Universidad Católica del Maule	SUMADI
Universidad Santo Tomás	SUMADI
Universidad San Sebastián	SUMADI
Universidad Mayor	SUMADI
Universidad Gabriela Mistral	SUMADI
Pontificia Universidad Católica de Chile	NO ESPECIFICADO
Universidad de Chile	VARIOS

Fuente: Elaboración propia

1.3 Perú

Nombre de la universidad	***software* de *e-proctoring***
Universidad Nacional de Jaén	NO ESPECIFICADO
Universidad Nacional Autónoma de Alto Amazonas	SAFE EXAM BROWSER
Universidad Nacional Agraria La Molina	METTL
Universidad Nacional Mayor de San Marcos	SMOWL
Universidad Nacional de Ingeniería	SMOWL
Universidad Nacional Jorge Basadre Grohmann	SMOWL
Universidad Nacional de San Agustín	METTL
Universidad Nacional de Juliaca	METTL
Universidad Nacional del Santa	NO ESPECIFICADO
Universidad Nacional de Piura	NO ESPECIFICADO
Universidad Nacional José María Arguedas	NO ESPECIFICADO
Universidad Nacional Autónoma Altoandina de Tarma	NO ESPECIFICADO
Universidad Católica de Santa María	SAFE EXAM BROWSER
Universidad San Ignacio de Loyola	EXAM
Universidad Católica San Pablo	NO ESPECIFICADO
Universidad de Lima	PROCTOR TRACK
Universidad Peruana Cayetano Heredia	SMOWL
Universidad Privada San Juan Bautista	SMOWL
Universidad César Vallejo	SMOWL
Universidad de Piura	METTL
Universidad Privada Antenor Orrego	METTL
Pontificia Universidad Católica del Perú	PROCTOR TRACK
Universidad del Pacífico	SUMADI
Universidad Privada del Norte	SUMADI
Universidad Peruana de Ciencias Aplicadas	SUMADI

Fuente: Elaboración propia

1.4 Características de las universidades y del software de e-proctoring

Entre los tres países, de un total de 267 universidades, se identificaron 46 en donde se utilizó *software* de *e-proctoring*, siendo que en al menos en 38 de ellas se logró también individualizar el nombre de los programas utilizados. En cuanto a las características de las universidades podemos señalar lo siguiente:

– En Argentina, del total de 108 universidades mapeadas, se identificaron 10 usuarias de programas de *e-proctoring*; siendo 2 de ellas instituciones públicas y 8 privadas.

– En Chile, del total de 55 universidades mapeadas, se identificaron 11 usuarias de programas de *e-proctoring*, siendo 1 de ellas una institución pública y 10 privadas.

– En Perú, del total de 104 universidades mapeadas, se identificaron 25 usuarias de programas de *e-proctoring*; siendo 12 de ellas instituciones públicas y 13 privadas.

En la mayoría de los casos, no fue posible determinar el motivo por el cual estas instituciones decidieron adquirir estos programas, debido a que muy raramente hicieron pública esta información. Tampoco fue posible dilucidar si la adquisición se realizó antes o después del inicio de la pandemia de COVID-19. No obstante, nuestra apreciación general sobre estas dos interrogantes es que el principal motivo de adquisición fue el de apoyar la supervisión de exámenes y que la mayoría de las adquisiciones se realizaron a propósito de la pandemia.

En el caso de Argentina y Chile, las universidades privadas fueron las más recurrentes en el uso de *software* de *e-proctoring*, con relaciones de 1:4 y 1:11 respectivamente. Solo en el caso de Perú la cuenta es más o menos pareja entre ambos tipos de instituciones, con una relación de 12:13. No es materia de esta investigación explorar las causas de esta recurrencia, pero un factor importante, al menos en Argentina, parece ser que al momento de la llegada de la pandemia a la región, las universidades privadas se encontraban en mejor posición para desplegar este tipo de soluciones gracias a la experiencia de procesos previos de virtualización (Barbieri et al., 2020).

En lo que respecta al *software* de *e-proctoring*, se identificaron 9 tipos diferentes de programas, que en orden de recurrencia fueron:

– En primer lugar, SUMADI con 14 universidades usuarias.

– En segundo lugar, SMOWL con 9 universidades usuarias.

– En tercer lugar, RESPONDUS y METTL, cada uno con 5 universidades usuarias.

– En cuarto lugar, PROCTOR TRACK, PROCTORIO y SAFE EXAM BROWSER, cada uno con 2 universidades usuarias.

– En quinto lugar, EXAM y KLARWAY, cada uno con 1 universidad.

En términos de prestaciones, se corroboró mediante consulta en sus sitios web oficiales que todos los programas menos SAFE EXAM BROWSER poseían tecnología de reconocimiento facial. También que todos menos SAFE EXAM BROWSER Y EXAM realizaban monitoreo en tiempo real y captura de imagen y voz, además de calificación de comportamientos sospechosos mediante algoritmos. Finalmente, que todos menos EXAM permitían el bloqueo de accesos y acciones dentro de los dispositivos de los estudiantes.

En cuanto a la ubicación de las empresas fabricantes, PROCTOR TRACK, PROCTORIO, RESPONDUS y SUMADI son provistos por empresas con sede en Estados Unidos. EXAM es provisto por la misma universidad usuaria con sede en Perú. KLARWAY es provisto por una empresa con sede en Argentina. METTL es provisto por una empresa con sede en India. SAFE EXAM BROWSER fue desarrollado por la universidad de ETH Zurich con sede en Suiza, pero es de descarga y uso libre. Finalmente, SMOWL es provisto por una empresa con sede en España.

2. Legislación de privacidad aplicable al uso de *software* de *e-proctoring* en universidades

Dado que el objetivo del estudio era conocer el impacto en la privacidad del uso de los programas de *e-proctoring*, se hizo necesario hacer un relevo de la legislación que regula la privacidad en los tres países estudiados. Pero, ¿qué es la legislación sobre privacidad? Para este trabajo, decidimos conceptualizarla como el conjunto de normas jurídicas que definen el ámbito de protección de los derechos a la intimidad y la vida privada, así como el derecho a la autodeterminación informativa o protección de datos personales.

Históricamente, el primero se ha entendido como el derecho a mantener cierta parte de la vida lejos del escrutinio público, lo que en casi todos los países de la región se ha garantizado a nivel constitucional bajo el paraguas del secreto de las comunicaciones y la inviolabilidad del domicilio. El caso del segundo es más reciente y está intrínsecamente ligado a la aparición de la computación y la recolección masiva de datos que identifican o hacen identificable a las personas. El flujo cada vez mayor de estos datos, especialmente en Internet, hace necesario que se otorguen mayores herramientas de control sobre los mismos, con el fin de garantizar que su uso no se torna perjudicial para las personas.

Para encontrar este tipo de legislación consultamos principalmente normas jurídicas de diferente rango de los tres países, así como trabajos académicos en donde se desarrolla su contenido doctrinario. A partir de allí notamos que la regulación en todos ellos era similar en varios aspectos, pero con ciertas diferencias en términos de desarrollo e institucionalidad. Entre las características comunes encontramos que:

– Los tres países recogen en sus Constituciones tanto el derecho a la intimidad como la

autodeterminación informativa de forma específica.

– Los tres países contemplan la acción de hábeas data como mecanismo jurisdiccional para exigir la protección de los derechos relativos a la privacidad.

– Los tres países han desarrollado abundante legislación específica que incide directa o indirectamente en la privacidad (normas de telecomunicaciones, investigación criminal, etcétera).

– Los tres países poseen leyes específicas sobre protección de datos personales.

En cuanto a las diferencias, encontramos que:

– Argentina y Perú contemplan en sus leyes de protección de datos la existencia de una vía administrativa de reclamación de infracciones. Por el contrario, en Chile esta vía es solo jurisdiccional y el fuero judicial es el encargado de atender estas demandas.

– Argentina y Perú han establecido la existencia de una autoridad de protección de datos, encargada de velar por el cumplimiento de la ley de protección de datos personales y atender los casos de infracciones en vía administrativa. Chile no cuenta con una instancia de este tipo y los casos son conocidos por el Poder Judicial.

Ahora bien, con el fin de hallar qué parte de esta legislación resultaba aplicable al uso de *software e-proctoring*, concluimos que debíamos centrarnos en aquellas piezas de legislación que señalaran obligaciones concretas y exigibles a las universidades, de tal manera que pudiéramos emplear estas obligaciones como un tamiz para el análisis legal que queríamos realizar posteriormente. Así pues, decidimos descartar cualquier obligación genérica, cuyo contenido tuviera que ser dilucidado, caso por caso, en fuero administrativo o judicial.

A nivel constitucional, la legislación de privacidad en los tres países es principalmente declarativa y en ningún caso se desarrollan obligaciones específicas más allá del mandato de respetar el derecho descrito. En cuanto a las leyes de desarrollo del derecho a la intimidad, todos los países tienen contempladas leyes en varios ámbitos como el domicilio, las telecomunicaciones y la investigación penal. Sin embargo, sus obligaciones derivadas son múltiples y no todas aplican de igual forma a las universidades, al punto en que impiden una comparación efectiva entre los países.

Por el contrario, las leyes que desarrollan el derecho de la autodeterminación informativa o protección de datos personales son bastante homogéneas. Esto se debe en parte a que son desarrollos normativos inspirados en la regulación europea, que es pionera en este campo, y también al hecho de que son normas jurídicas que parten desde principios muy similares, a partir de los cuales desarrollan las obligaciones concretas (ADC, 2019). Esto hacía más sencillo y viable el ejercicio de comparación entre los tres países. Por estas razones, decidimos tomar las leyes de protección de datos personales como medida única para evaluar el impacto en la privacidad de los estudiantes que podría tener el uso de programas

de *e-proctoring*.

Con el fin de favorecer aún más la comparación, condensamos los diferentes principios contenidos en las leyes de cada país, de tal manera que pudieran utilizarse como categorías de evaluación. Estos principios podrían resumirse de la siguiente manera:

2.1 Argentina

En Argentina la norma de protección de datos vigente es la Ley N° 25326 de Protección de Datos Personales, que regula la forma del tratamiento de los datos personales desde el año 2000. El ente encargado de velar por su cumplimiento y sancionar las infracciones en sede administrativa es la Agencia de Acceso a la Información Pública (que reemplaza a la Dirección Nacional de Protección de Datos Personales). Los principios que rigen el tratamiento son:

– Principio de legalidad: El tratamiento de datos personales siempre está permitido, salvo en el caso de los datos sensibles, que solo pueden ser tratados por razones de interés general autorizadas por ley.

– Principio de consentimiento: En todos los casos, quien va a tratar datos personales debe requerir el consentimiento de forma previa, salvo excepciones previstas por ley. Además, dicho consentimiento debe cumplir con ser libre, expreso e informado y constar por escrito u otro medio análogo.

– Principio de calidad: En todos los casos, quien va a tratar los datos debe registrar previamente el archivo, fichero, registro o banco de datos ante la Agencia de Acceso a la Información Pública. Luego de obtener el consentimiento, el tratamiento debe ser proporcional a sus fines. La transferencia internacional de los datos está prohibida hacia países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados, salvo excepciones previstas por ley.

– Principio de seguridad: En todos los casos, quien va a tratar los datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos. Respecto de estas medidas, la Agencia de Acceso a la Información Pública emitió en 2018 diferentes recomendaciones sobre medidas de seguridad a ser aplicadas durante todo el ciclo de vida de los datos (recolección, control de acceso, control de cambios, respaldo, gestión de vulnerabilidades, entre otros).

2.2 Chile

En Chile la norma vigente es la Ley N° 19628 sobre Protección de la Vida Privada, que regula la forma del tratamiento de los datos personales desde el año 1999. El ente encargado de velar por su cumplimiento y sancionar las infracciones es el Poder Judicial, al cual se acude a través de la acción de hábeas data. Los principios que rigen el tratamiento son:

– Principio de legalidad: El tratamiento de datos personales siempre está permitido, salvo en el caso de los datos sensibles, que solo pueden ser tratados por ley que lo autorice, que exista consentimiento por parte del titular o que sea necesario para el otorgamiento de un beneficio de salud.

– Principio de consentimiento: En todos los casos, quien va a tratar datos personales debe requerir el consentimiento de forma previa, salvo excepciones previstas por ley. Además, dicho consentimiento debe cumplir con ser expreso e informado y constar por escrito, salvo excepciones previstas por ley.

– Principio de calidad: Solo en el caso de que quien va a tratar los datos sea una entidad pública, debe registrar previamente el archivo, fichero, registro o banco de datos ante el Servicio de Registro Civil e Identificación. Luego de obtener el consentimiento, el tratamiento debe ser proporcional a sus fines. La transferencia internacional de los datos no está regulada.

– Principio de seguridad: En todos los casos, quien va a tratar los datos debe cuidarlos con la debida diligencia, siendo responsable de los daños en caso contrario. Respecto de estas medidas, no existen directivas u otras normas de desarrollo por lo cual las medidas de seguridad adoptadas y la posible indemnización se evalúan caso por caso en sede judicial cuando existen demandas de los afectados.

2.3 Perú

En Perú la norma vigente es la Ley N° 29733 sobre Ley de Protección de Datos Personales, que regula la forma del tratamiento de los datos personales desde el año 2011. El ente encargado de velar por su cumplimiento y sancionar las infracciones en sede administrativa es la Autoridad Nacional de Protección de Datos Personales. Los principios que rigen el tratamiento son:

– Principio de legalidad: El tratamiento de datos personales siempre está permitido, salvo en el caso de los datos sensibles, en donde se requieren diferentes formalidades en el consentimiento.

– Principio de consentimiento: En todos los casos, quien va a tratar datos personales debe requerir el consentimiento de forma previa y este debe ser informado, expreso e inequívoco, salvo excepciones previstas por ley. En el caso de los datos sensibles, el consentimiento debe constar siempre por escrito, un requisito que puede ser cumplido además a través de medios electrónicos.

– Principio de calidad: En todos los casos, quien va a tratar los datos debe registrar previamente el archivo, fichero, registro o banco de datos ante la Autoridad Nacional de Protección de Datos Personales. Luego de obtener el consentimiento, el tratamiento debe ser proporcional a sus fines. La transferencia internacional de los datos está prohibida hacia países que no proporcionen niveles de protección adecuados, salvo excepciones

previstas por ley.

– Principio de seguridad: En todos los casos, quien va a tratar los datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad. Respecto de estas medidas, existe una Directiva de Seguridad que desarrolla qué medidas resultan exigibles dependiendo del tipo y volumen de datos tratados, así como de la naturaleza pública o privada de la entidad obligada.

2.4 Datos tratados por el *software* de *e-proctoring* y responsabilidad de las universidades

Para poder proceder con el análisis, fue preciso un paso previo más: Determinar la naturaleza de los datos personales tratados por los diferentes tipos de *software* de *e-proctoring*. Pero, ¿cómo saber qué datos trataba cada programa?

Ante la diversidad de fuentes de consulta, empleamos un método de verificación de tres niveles para producir una lista con datos mínimos para cada tipo de tecnología previamente identificada en la sección 1.4. El primer nivel consistió en la simple deducción lógica. Por ejemplo, en el caso de la tecnología de reconocimiento facial, resultaba lógico pensar que se iba a tratar el dato personal de imagen. También otros datos derivados de la misma como los rasgos faciales o documentos de comparación como el documento nacional de identidad.

El segundo nivel consistió en contrastar la información del primer nivel con la información disponible en los manuales de uso o los videos promocionales en Internet que abundan en detalles sobre cómo operan los diferentes *softwares*. Aquí nos dimos cuenta que había datos que no podían deducirse lógicamente. Por ejemplo, en el caso de la tecnología de monitoreo en tiempo real, parecía necesario que esta trate datos como dirección IP e historial de navegación, pues era requisito instalar el *software* en los dispositivos y otorgar permisos relacionados a estas acciones.

Finalmente, el tercer nivel consistió en revisar las políticas de privacidad de las empresas proveedoras con el fin de conocer qué otros datos podrían estar siendo tratados. Muchas de ellas operan en territorios con leyes muy estrictas de protección de datos como por ejemplo el Reglamento General de Protección de Datos (RGPD) que rige desde el año 2016 en toda la Unión Europea y por lo tanto están obligadas a transparentar esta información.

La siguiente tabla representa el resultado de este proceso, que contiene una enumeración referencial de los datos personales que podrían ser tratados por cada una de las tecnologías que han declarado poseer los diferentes *softwares* de *e-proctoring* detectados en las universidades[4]:

Tecnología	**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

Fuente: Elaboración propia

El segundo elemento estaba relacionado con un problema siempre presente a la hora de intentar aplicar normas jurídicas a tecnologías que funcionan empleando Internet: el problema de la jurisdicción. Aún cuando la jurisprudencia en los tres países parece seguir la "doctrina de los efectos", es decir; que la ley local es aplicable siempre que un hecho de relevancia jurídica o sus consecuencias se susciten dentro del territorio nacional, el peso de esta afirmación sigue siendo incierta (CEPAL, 2020). Lo es aún más cuando además se trataría de empresas tecnológicas que no se han establecido legalmente en el país donde operan, como es el caso de seis de los ocho programas de *e-proctoringe-proctoring* identificados, siendo EXAM y KLARWAY las únicas excepciones.

Pese a que en sede administrativa y judicial, las autoridades de Argentina y Perú parecen haber acogido también esta doctrina en el ámbito de la protección de datos personales (Del Campo, 2017), consideramos que podría ser problemático asumir que las empresas que proveen los programas de *e-proctoring* se someten de buen grado a la jurisdicción local, sobre todo si algunas de ellas ya cumplen leyes similares con estándares más estrictos, como es el caso de las que tienen sede en países pertenecientes a la Unión Europea.

No es objeto de este estudio dirimir si las leyes de protección de datos personales alcanzan

o no a las empresas proveedoras de estas tecnologías. Una discusión que por lo demás es innecesaria en el caso presente pues es preciso recordar que estas empresas son una suerte de intermediarios de otros sujetos que sí están obligados: las universidades. Por la forma en que están hechas las leyes de protección de datos personales en los tres países, en todos los casos de uso de estos programas, las universidades virtualmente son responsables y, llegado el caso, responden solidariamente por las infracciones que se cometan durante la ejecución de esta tarea, aún cuando haya sido encargada a un tercero.

3. Análisis legal de impacto en la privacidad

El análisis legal fue un ejercicio de contrastación entre las obligaciones contempladas por las leyes de protección de datos personales, que resumimos en la forma de principios, y posibles situaciones de incumplimiento. La mayoría de estas situaciones son puramente hipotéticas, por lo que salvo en un caso, las conclusiones no implican necesariamente que alguna de las universidades haya cometido infracciones. No obstante, el ejercicio permitió descubrir situaciones que, si bien no directamente relacionadas con el uso de *software* de *e-proctoring*, repercuten también en el cumplimiento que exigen las leyes[5].

3.1 Argentina

En las universidades argentinas, se detectaron los siguientes *softwares* de *e-proctoring*: KLARWAY, PROCTORIO, RESPONDUS, SUMADI Y SMOWL. Según la lista de datos personales tratados por cada uno de ellos y, asumiendo que estos programas desplegaron todas sus capacidades, se trataron por lo menos los siguientes datos: imagen, rasgos faciales, voz, nombre, documento de identidad, dirección IP e historial de navegación.

Así pues, en base a las categorías de principios establecidos en la sección anterior, podemos señalar que:

– Principio de legalidad: Los rasgos faciales y la imagen pueden considerarse como datos sensibles pues podrían revelar datos como la etnia de la persona. Por lo tanto, solo pueden ser tratados si una ley así lo autoriza. En la revisión normativa no se encontró ninguna ley que habilite de forma específica a las universidades o a las empresas proveedoras a tratar estos datos a partir del uso de *software* de *e-proctoring*. En todo caso, solo podrían invocarse normas genéricas relativas al acceso a la educación pública. *Este hecho podría implicar una infracción.*

– Principio de consentimiento: Si resulta legítimo que las universidades o empresas proveedoras traten datos sensibles invocando normas genéricas, aún así deberían solicitar el consentimiento de los estudiantes. Sin embargo, existen situaciones en las cuales el otorgamiento del consentimiento no cumpliría las formalidades requeridas para que sea válido. Por ejemplo, en el caso de que no se hayan dado alternativas a los estudiantes para elegir su forma de evaluación, pues el consentimiento no sería libre. *Este hecho podría*

implicar una infracción.

– Principio de calidad: Habiendo consultado el buscador del Registro Nacional de Bases de Datos Personales, corroboramos que solo 2 de las 10 universidades donde se identificó el uso de *software* de *e-proctoring* en este país contaban con un registro de propósito general ante la autoridad de protección de datos. Estas fueron: la Universidad Argentina de la Empresa y la Universidad de Palermo, ambas universidades privadas. En el caso de las empresas proveedoras, solo se encontró un registro a favor de KLARWAY. *Por lo menos, la no inscripción por parte de las universidades podría implicar una infracción.*

– Principio de seguridad: En todos los casos, resultó imposible corroborar qué tipo de medidas de seguridad implementaron las universidades o las empresas proveedoras. Tampoco se logró obtener información sobre brechas de seguridad o problemas de funcionamiento, al menos de fuentes de acceso público disponibles en Internet.

3.2 Chile

En las universidades chilenas, se detectaron los siguientes *softwares* de *e-proctoring*: RESPONDUS, SUMADI Y SMOWL. Según la lista de datos personales tratados por cada uno de ellos y, asumiendo que estos programas desplegaron todas sus capacidades, se trataron por lo menos los siguientes datos: imagen, rasgos faciales, voz, nombre, documento de identidad, dirección IP e historial de navegación.

Así pues, en base a las categorías de principios establecidos en la sección anterior, podemos señalar que:

– Principio de legalidad: Los rasgos faciales y la imagen pueden considerarse como datos sensibles pues se refieren a las características físicas o morales de las personas. Por lo tanto, solo pueden ser tratados si una ley así lo autoriza, si hay consentimiento o si sirven para la provisión de servicios de salud. En la revisión normativa no se encontró ninguna ley que habilite de forma específica a las universidades o a las empresas proveedoras de las mismas a tratar estos datos a partir del uso de *software* de *e-proctoring*. En todo caso, solo podrían invocarse normas genéricas relativas al acceso a la educación pública o exigirse el consentimiento. *Este hecho podría implicar una infracción.*

– Principio de consentimiento: Si resulta legítimo que las universidades o empresas proveedoras traten datos sensibles invocando normas genéricas, ya no requieren el consentimiento de los estudiantes. En todos los demás casos, el consentimiento previo bastará para permitir el tratamiento. *Si no se hubiera procedido de esta forma, este hecho podría implicar una infracción.*

– Principio de calidad: Habiendo consultado el Registro de Bancos de Datos Personales a cargo de organismos públicos corroboramos que la Universidad de Chile, única universidad obligada al registro por ser pública, no contaba con el mismo. Algo que llamó la atención mirando otros registros es que solo 2 de un total de 8 universidades públicas cuentan sus

bases de datos registradas. *Este hecho podría implicar una infracción.*

– Principio de seguridad: En todos los casos, resultó imposible corroborar qué tipo de medidas de seguridad implementaron las universidades o las empresas proveedoras. Tampoco se logró obtener información sobre brechas de seguridad o problemas de funcionamiento, al menos de fuentes de acceso público disponibles en Internet.

3.3 Perú

En las universidades peruanas, se detectaron los siguientes *softwares* de *e-proctoring*: EXAM, KLARWAY, PROCTORIO, PROCTOR TRACK, RESPONDUS, SAFE EXAM BROWSER, METTL SUMADI Y SMOWL. Según la lista de datos personales tratados por cada uno de ellos y, asumiendo que estos programas desplegaron todas sus capacidades, se trataron por lo menos los siguientes datos: imagen, rasgos faciales, voz, nombre, documento de identidad, dirección IP e historial de navegación[6].

Así pues, en base a las categorías de principios establecidos en la sección anterior, podemos señalar que:

– Principio de legalidad: Los rasgos faciales y la imagen pueden considerarse como datos sensibles pues se refieren a datos biométricos o pueden estar referidos al origen racial y étnico. Por lo tanto, solo pueden ser tratados si una ley así lo autoriza o si hay consentimiento. En la revisión normativa no se encontró ninguna ley que habilite de forma específica a las universidades o a las empresas proveedoras de las mismas a tratar estos datos a partir del uso de *software* de *e-proctoring*. En todo caso, solo podrían invocarse normas genéricas relativas al acceso a la educación pública o exigirse el consentimiento. *Este hecho podría implicar una infracción.*

– Principio de consentimiento: Si resulta legítimo que las universidades o empresas proveedoras traten datos sensibles invocando normas genéricas, ya no requieren el consentimiento de los estudiantes. En todos los demás casos, el consentimiento previo bastará para permitir el tratamiento y este además deberá ser escrito, no pudiendo ser tácito o verbal. *Si no se hubiera procedido de esta forma, este hecho podría implicar una infracción.*

– Principio de calidad: Habiendo consultado el Registro Nacional de Protección de Datos Personales, corroboramos que ninguna universidad pública contaba con registros ante la autoridad, mientras que todas las universidades privadas sí contaban con los mismos, con excepción de la Universidad César Vallejo. En el caso de las empresas proveedoras, no se encontró ningún registro. Por lo menos, *la no inscripción por parte de las universidades podría implicar una infracción.*

– Principio de seguridad: En todos los casos resultó imposible corroborar qué tipo de medidas de seguridad implementaron las universidades o las empresas proveedoras. Tampoco se logró, salvo en el caso de la Universidad Nacional Mayor de San Marcos

(Guerrero, 2020), obtener información sobre brechas de seguridad o problemas de funcionamiento, al menos de fuentes de acceso público. Por lo menos *el caso señalado de la Universidad San Marcos podría implicar una infracción.*

4. Conclusiones

Lo visto hasta este punto, nos permite señalar algunos hallazgos, no definitivos sobre los *softwares* de *e-proctoring*, su uso por parte de diferentes universidades en Latinoamérica, la legislación de privacidad que les es aplicable y el impacto que estos programas pueden tener en la privacidad de los estudiantes. A continuación, ofrecemos algunas conclusiones:

– El mapeo de universidades en los tres países de estudio arrojó una gran cantidad de instituciones que utilizan *software* de *e-proctoring*. No obstante, el porcentaje en relación al total de universidades en cada uno de los países es relativamente bajo, siendo de aproximadamente 10% en Argentina y 25% en Chile y Perú.

– No hay suficiente información que permita entender qué factores influyen en las universidades a la hora de decidirse por adquirir estos programas, más allá de las circunstancias provocadas por la pandemia de COVID-19 que parecen ser su único denominador común.

– Aunque por el tamaño de la muestra no puede decirse que es una tendencia regional, sí es un hecho que en Argentina y Chile, la mayoría de universidades que adquirieron *software* de *e-proctoring* son privadas, con relaciones de 1 a 4 y de 1 a 11 respecto de las universidades públicas. Solo en el caso de Perú existe un equilibrio entre universidades públicas y privadas, siendo la relación de 12 a 13.

– Ocho de los nueve programas de *e-proctoring* detectados utilizan por lo menos la tecnología de reconocimiento facial. Siete de ellos utilizan además la captura de imagen y voz en tiempo real, emplean algoritmos para detectar comportamientos sospechosos y permiten el bloqueo de los dispositivos de los estudiantes. Finalmente, cinco de ellos son provistos por empresas cuya sede principal está en Estados Unidos.

– En cuanto a la legislación sobre privacidad, los tres países tienen normas de protección de datos que contienen obligaciones similares, pero es de resaltar que los esquemas de protección parecen ser más robustos en Argentina y Perú y más laxos en Chile, especialmente en términos de ofrecer vías de acción administrativa y contar con autoridades de protección de datos personales.

– Todos los programas de *e-proctoring* salvo Safe Exam Browser tratan datos personales, incluyendo datos sensibles. Esto significa que, en principio, están obligados a cumplir con la legislación de protección de datos en cada uno de los tres países donde operan u operaron en algún momento de 2020. Esto es así independientemente de cualquier conflicto de jurisdicción. Si la empresa proveedora no es obligada directa, sí lo son las universidades que

contratan sus servicios.

– Respecto del impacto en la privacidad de los estudiantes, es de resaltar que en ninguno de los tres países parece estar claro si el tratamiento de datos sensibles por parte de las universidades requiere la existencia de leyes especiales o es posible apelar a las ya existentes cuando esto es un requisito para tratar los datos o prescindir del consentimiento del titular. No existen a la fecha pronunciamientos sobre este tema de parte de ninguna autoridad.

– En países como Argentina, en donde es un requisito inscribir de forma previa los ficheros, registros o bancos de datos personales ante la autoridad, existe poco o nulo cumplimiento de esta obligación tanto de las universidades públicas como de las privadas, con excepciones. En el caso de Perú, este incumplimiento se da casi exclusivamente por parte de las universidades públicas. En Chile, la única universidad obligada que es pública tampoco cumple estas disposiciones. No es posible determinar a qué se debe esta situación, pudiendo esto responder a una misma razón o a diferentes razones de índole legal, cultural, entre otras, en cada país.

– Salvo en Perú, en los otros dos países no fue posible verificar a través de información pública disponible en Internet que hayan existido fallos o brechas de seguridad a partir del uso de los *softwares* de *e-proctoring*. No obstante, aún en el caso de Perú, que incluye una denuncia ante la autoridad de protección de datos personales, no existe a la fecha un pronunciamiento sobre el estatus legal de estas tecnologías.

– Finalmente, es nuestra impresión general que este tema está sub registrado en los tres países estudiados, incluso cuando la existencia de estos programas ha llegado a ser noticia en los medios de comunicación, como es el caso de Argentina y Perú. Esto y la aparente novedad del uso de estas tecnologías podría estar limitando su estudio y las denuncias de los estudiantes por alguna de las posibles afectaciones a la privacidad expuestas en este trabajo.

5. Bibliografía

– Alessio, H. M., Malay, N., Maurer, K., Bailer, A. J., & Rubin, B. (2017). Examining the effect of proctoring on online test scores. *Online Learning*, *21*(1), 146-161.

– Área de Tecnología Educativa – Secretaría Académica (FFyH-UNC). (2020). *Informe acerca de la compra y de las implicancias de la implementación del software Respondus en la UNC.*
https://ffyh.unc.edu.ar/alfilo/wp-content/uploads/sites/11/2020/07/INFORME-ACERCA-DE-LA-COMPRA-Y-LAS-IMPLICANCIAS..pdf

– Asociación por los Derechos Civiles. (2017). *Desafíos de la biometría para la protección de los datos personales: Reflexiones sobre el caso SIBIOS.*

https://adc.org.ar/wp-content/uploads/2019/06/030-desafios-de-la-biometria-para-la-proteccion-de-datos-05-2017.pdf

– Asociación por los Derechos Civiles. (2019). *El sistema de protección de datos personales en América Latina: Oportunidades y desafíos para los derechos humanos.* https://adc.org.ar/wp-content/uploads/2019/06/023-A-El-sistema-de-protecci%C3%B3n-de-datos-personales-en-Am%C3%A9rica-Latina-Vol.-I-12-2016.pdf

– Atoum, Y., Chen, L., Liu, A. X., Hsu, S. D., & Liu, X. (2017). Automated online exam proctoring. *IEEE Transactions on Multimedia*, *19*(7), 1609-1624.

– Barbieri, A. (2020). *La universidad entre la crisis y la oportunidad : reflexiones y acciones del sistema universitario argentino ante la pandemia* https://www.unaj.edu.ar/wp-content/uploads/2020/12/La-universidad-entre-la-crisis-y-la-oportunidad.pdf

– Bernardo, M., & Bonta, E. Facing the COVID-19 Pandemic: Massive Distance Learning and On-Line Exams with Moodle, Collaborate, Smowl, Meet.

– Biblioteca del Congreso Nacional de Chile. (2014). *Régimen legal nacional de protección de datos personales.*

https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/20443/5/REG_NACIONAL_PROTECC_DATOS_PERSONALES%20(LV)_v5.pdf

– Buscador del Registro Nacional de Bases de Datos Personales. (s. f.). Gobierno de la República Argentina. https://www.argentina.gob.ar/aaip/datospersonales/reclama

– CEPAL, N. (2020). Elementos principales del informe sobre el estado de la jurisdicción de Internet en América Latina y el Caribe 2020.

– Del Campo, A.(2017). *Hacia una Internet libre de censura II : Perspectivas en América Latina* https://www.palermo.edu/cele/pdf/investigaciones/Hacia_una_internet_libre_de_censura_II.pdf

– Espinoza Vilchez, J. S. (2018). *El derecho a la intimidad y su protección en el sistema jurídico peruano.*

– Fernández, M. (30 de junio de 2020). *Polémica en la Universidad de Córdoba por un sistema de control facial que usarán para que los alumnos no se copien en los exámenes*. Infobae. https://www.infobae.com/educacion/2020/06/30/polemica-en-la-universidad-de-cordoba-por-un-sistema-de-control-facial-que-usaran-para-que-los-alumnos-no-se-copien-en-los-examenes/

– Garay, K. (28 de agosto de 2020). *San Marcos anuncia examen virtual de admisión para el 2 y 3 de octubre.* Agencia Peruana de Noticias Andina.

https://andina.pe/agencia/noticia-san-marcos-anuncia-examen-virtual-admision-para-2-y-3-octubre-811627.aspx

– Guerrero, C. (22 de Septiembre, 2020). *Denunciamos a La Universidad Nacional Mayor De San Marcos Por El Uso De Software Biométrico En Su Examen Virtual*. Hiperderecho. https://hiperderecho.org/2020/09/denunciamos-a-la-universidad-nacional-mayor-de-san-marcos-por-el-uso-de-software-biometrico-en-su-examen-virtual/

– Gobierno de la República Argentina. (2000). *Ley N° 25326 de Protección de Datos Personales*. https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/actualizacion

– Gobierno de la República de Chile. (1999). *Ley N° 19628 sobre Protección de la Vida Privada.* https://www.bcn.cl/leychile/navegar?idNorma=141599

– Gobierno de la República del Perú. (2011). *Ley N° 29733, Ley de Protección de Datos Personales.* https://diariooficial.elperuano.pe/pdf/0036/ley-proteccion-datos-personales.pdf

– González-González, C. S., Infante-Moro, A., & Infante-Moro, J. C. (2020). Implementation of e-proctoring in online teaching: A study about motivational factors. *Sustainability*, *12*(8), 3488.

– Grupo de Responsables de Docencia Online de las Universidades Públicas de Castilla y León (2020). *Guía de recomendaciones para la evaluación online en las Universidades Públicas de Castilla y León* [Archivo PDF]. https://www.usal.es/files/2020_04_03_Recomendaciones_evaluacion_online_para_las_Universidades_Publicas_de_Castilla_y_Leon_V0.7.pdf

– Hylton, K., Levy, Y., & Dringus, L. P. (2016). Utilizing webcam-based proctoring to deter misconduct in online exams. *Computers & Education*, *92*, 53-63.

– Kelley, J. (2020). Students Are Pushing Back Against Proctoring Surveillance Apps. *Electronic Frontier Foundation*.

– Masciotra, M., & LA ACCIÓN, I. P. A. A. (2004). La demanda de Hábeas Data. *Dossier: Habeas Data*, 384.

– Registro de Banco de Datos Personales. (s. f.). Ministerio de Justicia de Chile http://rbdp.srcei.cl/rbdp/html/Consultas/consultas.html

– Registro Nacional de Protección de Datos. (s. f.). Ministerio de Justicia del Perú. https://prodpe.minjus.gob.pe/prodpe_web/BancoDato_verResultado#

– Viollier, P. (2017). El estado de la protección de datos personales en Chile. *Santiago: Derechos Digitales. https://bit. ly/3c2UxCo*.

Acerca del Autor

Carlos Guerrero Argote: Argote es abogado por la Universidad Nacional Mayor de San Marcos (Perú). Actualmente cursa una maestría en Legaltech y Abogacía Digital en la Universidad de Salamanca (España). Ejerció como Director de Políticas Públicas de la ONG Hiperderecho entre 2015 y 2020. Actualmente es consultor para entidades públicas y privadas en materia de gobierno digital, políticas públicas sobre tecnología y derechos humanos.

Notas

↑1 Para este trabajo, y debido a la falta de una definición consensuada, hemos decidido definir al *e-proctoring* como: cualquier programa que permite controlar un proceso educativo que se realiza de forma remota (por ejemplo: un examen *online*) con el fin de mitigar la ocurrencia de conductas deshonestas por parte de los estudiantes como la suplantación o el plagio. El nivel de control varía dependiendo de las características de cada *software*, pudiendo recaer totalmente en herramientas automatizadas o incluir la intervención de humanos.

↑2 Para algunos ejemplos, ver el archivo PDF elaborado por el Grupo de Responsables de Docencia Online de las Universidades Públicas de Castilla y León(2020).

↑3 Se puede consultar la tabla completa, segmentada por país, en donde además se señala si la universidad es pública o privada, así como las fuentes de Internet desde donde se ha extraído la información que confirma el uso de *software* de *e-proctoring*; en este enlace.

↑4 Se puede consultar la tabla completa, segmentada por tecnología, en donde además se señala qué tecnologías poseen cada uno de los 9 programas de *e-proctoring* identificados en universidades de los tres países de estudio; en este enlace.

↑5 Se puede consultar la tabla completa, segmentada por países y por principios aplicables a cada tipo de tratamiento de datos, en este enlace.

↑6 Este análisis finalmente no contempla a SAFE EXAM BROWSER pues luego de haber hecho pruebas con este *software*, se corroboró que no trata datos personales en ningún caso, pues los datos que el programa procesa se almacenan única y exclusivamente en los dispositivos donde se instala y no se transfieren a terceros.