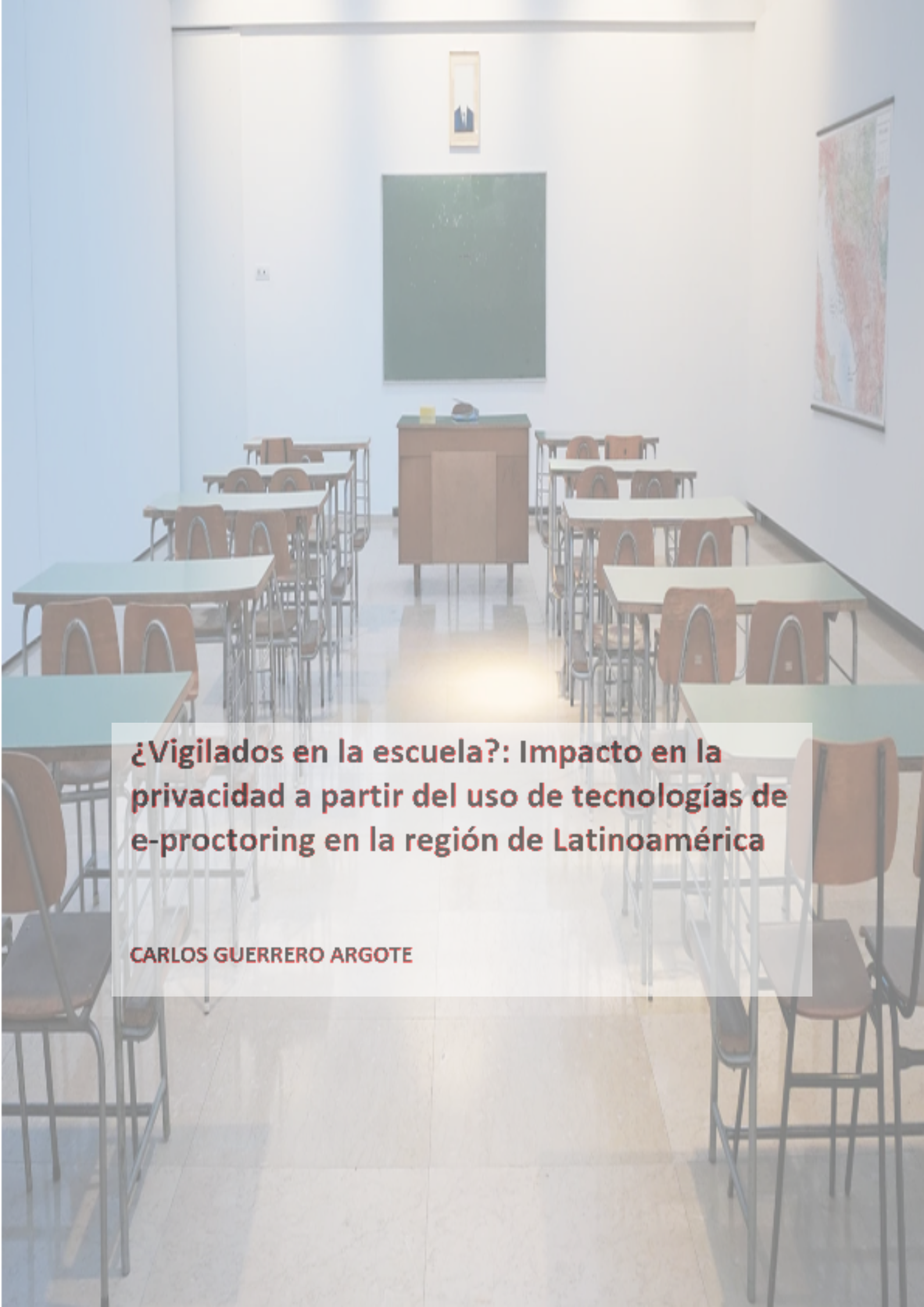

¿Vigilados en la escuela?: Impacto en la privacidad a partir del uso de tecnologías de e-proctoring en la región de Latinoamérica

CARLOS GUERRERO ARGOTE

Sobre el autor

Abogado por la Universidad Nacional Mayor de San Marcos. Actualmente cursa una maestría en Legaltech y Gestión Digital de la Abogacía en la Universidad de Salamanca. Entre 2016 y 2020 ha sido Director de Políticas Públicas de la ONG Hiperderecho. Actualmente es Director Adjunto del Instituto para la Sociedad de la Información y la Cuarta Revolución Industrial de la Universidad La Salle. En su tiempo libre, dirige un podcast sobre Derecho y Tecnología llamado Lima Legaltech.

Sobre esta investigación

Esta investigación ha sido posible gracias al auspicio económico del Registro de Direcciones de Internet de América Latina y Caribe (LACNIC), que en 2020 lanzó el programa Líderes 2.0, un llamado a proyectos de investigación sobre temas de Gobernanza de Internet en la región vinculados a Internet y la pandemia: el impacto en los derechos humanos; Inclusión digital; y Seguridad y confianza.
"¿Vigilados en la escuela?: Impacto en la privacidad a partir del uso de tecnologías de e-proctoring en la región de Latinoamérica" fue uno de los 16 proyectos seleccionados de la región y el único de Perú.

Foto de portada

Ivan Aleksic para Unsplash

Algunos derechos reservados

1. Introducción

Aunque las tecnologías de e-proctoring existen desde hace muchos años y son ampliamente utilizadas en Estados Unidos y Europa, hasta hace muy poco eran prácticamente desconocidas en Latinoamérica. Sin embargo, con la llegada de la pandemia de COVID-19 a la región, que obligó a la virtualización de casi todas las actividades incluyendo la educación, muchos de estos programas han ganado y siguen ganando una creciente popularidad en las instituciones educativas, especialmente en las universidades.

¿Pero qué son las tecnologías de e-proctoring? Podemos definir al e-proctoring como cualquier programa que permite controlar un proceso educativo que se realiza de forma remota (por ejemplo: un examen virtual) con el fin de mitigar la ocurrencia de conductas deshonestas como la suplantación o el plagio. El nivel de control varía dependiendo de las características de cada software, pudiendo ir desde el bloqueo de páginas web en el navegador del estudiante, hasta controlar sus movimientos a través de la cámara web empleando para ello algoritmos de reconocimiento facial.

Aunque el argumento central de quienes abogan por la implementación del e-proctoring es que permite la continuidad de los servicios educativos, en varios países se ha cuestionado su uso, argumentando principalmente que amplía la brecha digital y representa riesgos inaceptables para la privacidad. Esta discusión está a su vez atravesada por los problemas y limitaciones propias de la educación en Latinoamérica, situaciones que se han agudizado con la implementación (a veces forzada) de las TICs.

Este proyecto quiso explorar el impacto real o potencial del e-proctoring sobre la privacidad. Para ello, se hizo un levantamiento previo de información con el fin de calibrar el alcance del estudio y escoger la metodología más adecuada. Queríamos saber por ejemplo: ¿En qué países se estaban utilizando estas tecnologías? ¿Por parte de quiénes? ¿Con qué motivo? También si existían estudios previos en la región sobre estos temas que incluyeran la privacidad como línea de investigación.

En cuanto a los casos, había muchos, repartidos en casi todos los países de Latinoamérica. Estos casos además se presentaban tanto en instituciones educativas públicas como privadas, siendo su uso mayormente opcional, pero también obligatorio en ciertas circunstancias. Respecto de los estudios previos, no tuvimos tanta suerte. El impacto del e-proctoring en la privacidad no parece ser todavía un tópico interesante para investigadores o grupos de interés de la región, aún cuando involucran tecnologías controvertidas como la biometría y el reconocimiento facial.

En base a la información obtenida, tomamos las siguientes decisiones. Decidimos que el alcance del proyecto abarcaría solo tres países de estudio: Argentina, Chile y Perú. Además, restringimos el ámbito de investigación a las universidades, pues eran de lejos las instituciones educativas sobre las que existía mayor información disponible. Finalmente, debido a la ausencia de estudios previos sobre el tema, decidimos que este acercamiento sería exploratorio y se enfocaría principalmente en describir con el mayor detalle posible el

fenómeno del e-proctoring en Latinoamérica. A partir de allí, nuestro análisis sobre su potencial (¿y real?) impacto en la privacidad, no sería concluyente, pero sí buscaría alentar una discusión más informada sobre el uso de estas tecnologías.

Esperamos que los resultados de este proyecto animen a otros investigadores y organizaciones a generar sus propios estudios sobre el impacto del e-proctoring en la privacidad, no solo en virtud de su trascendencia actual, sino a propósito del futuro de estas tecnologías aplicadas a la educación.

2. Antecedentes

En agosto del año 2020, fuimos contactados por un grupo de postulantes a la Universidad Nacional Mayor de San Marcos -la más grande y antigua del Perú- porque esta había decidido realizar su Examen de Admisión en formato virtual.[1] Los postulantes no estaban de acuerdo con esta medida. Su argumento principal era que una prueba por Internet excluía a quienes no podían costear el equipo y la conectividad necesarias, lo que era equivalente a discriminarlos del acceso a la educación. Nos pedían ayuda, a ver si era posible convencer a las autoridades de detener el Examen o, en su defecto, cambiarlo a un formato presencial.

La educación es un derecho fundamental reconocido en la Constitución del Perú. Sin embargo, solo la educación básica es gratuita y está garantizada por el Estado Peruano. En el caso de la educación universitaria, el Estado provee este servicio gratuitamente, pero de forma limitada. Para acceder a la universidad pública es preciso pasar por diferentes pruebas, generalmente compitiendo con otros candidatos para alcanzar una plaza. Quienes no lo logran, tienen la opción de volver a presentarse nuevamente de forma indefinida u optar por acceder a una universidad privada, las cuales varían en costo y calidad.

Aunque inmediatamente entendimos el problema de los postulantes, nos sentimos frente a un predicamento: Si bien era cierto que un examen virtual marginaba a un grupo considerable, también lo era que permitía a otros rendir una prueba que, debido a la pandemia de COVID-19, ya se había retrasado mucho tiempo. Una situación similar había ocurrido con los estudiantes de esta y otras universidades, que meses atrás habían sido forzados a migrar a las clases virtuales para no perder el semestre, aún cuando eso significó la exclusión de aquellos que no tenían suficiente conectividad.

No obstante, pronto descubrimos que la brecha digital solo era una de las muchas aristas del problema. Días después de anunciar las fechas del Examen Virtual, autoridades de la Universidad San Marcos dijeron en una entrevista que, para evitar posibles conductas deshonestas durante la prueba virtual, se iba a hacer uso de “un aplicativo que emplea la inteligencia artificial”. Este aplicativo serviría para corroborar la identidad de los postulantes, así como para controlar que no sean reemplazados, reciban ayuda o utilicen dispositivos prohibidos.[2]

Aunque en la entrevista no se mencionaba nunca el nombre de la aplicación ni se incluía la palabra “e-proctoring”, una búsqueda rápida en Internet y el apoyo de los postulantes nos permitió entender mejor la situación. La aplicación en cuestión se llamaba Smowl, un programa de e-proctoring que efectivamente hacía todo lo que se decía. Debido a la falta de transparencia por parte de la Universidad, toda la información sobre este software fue

[1] Karina Garay, “San Marcos Anuncia Examen Virtual De Admisión Para El 2 y 3 De Octubre,” Noticias | Agencia Peruana de Noticias Andina, 28 de Agosto, 2020, 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,” Noticias | Agencia Peruana de Noticias Andina, 2020, https://andina.pe/agencia/noticia-san-marcos-como-evitaran-plagios-y-suplantaciones-examen-virtual-admision-811770.aspx

obtenida exclusivamente del sitio web de la empresa, así como de documentos que se enviaron a los postulantes con indicaciones para su participación en el Examen Virtual.

Encontramos problemático el uso de Smowl por varios motivos. El primero y más importante era el posible impacto negativo en el desarrollo de la prueba. Nunca antes en el país una universidad pública había hecho uso de software de e-proctoring para llevar a cabo un Examen de Admisión. Muchas cosas podían fallar, sobre todo teniendo en cuenta la complejidad de la tecnología de Smowl y el hecho de que al Examen de San Marcos concurrían aproximadamente 20 mil postulantes, conectados todos desde diferentes partes del país. Sin simulacros ni capacitaciones previas, forzar su uso era una receta para el desastre.

Otro motivo de preocupación era la protección de la privacidad de los postulantes. Como se verá a lo largo de esta investigación, Smowl forma parte de un conjunto de programas de e-proctoring que necesitan ser instalados en los dispositivos de quienes van a rendir una prueba y son particularmente invasivos: Tanto para la validación de identidad como para prevenir conductas sospechosas, Smowl accede y almacena múltiples datos como la imagen, los rasgos faciales, la voz, el historial de navegación, etc. Esto último lo convierte en responsable de tratamiento de datos personales, una actividad que está regulada en Perú de forma específica desde el año 2011.

La normativa peruana de protección de datos exige, entre otras cosas, que los titulares de los datos otorguen el consentimiento para su tratamiento; que se les explique qué datos van a ser recogidos, con qué fines y por cuánto tiempo; que no se compartan con terceros sin autorización previa; y que estos sean mantenidos de forma segura. ¿La Universidad San Marcos y Smowl cumplían con estas disposiciones? Luego de una exhaustiva investigación, detectamos cuatro posibles incumplimientos, principalmente de parte de la Universidad, todos ellos ligados a tratamiento de datos hecho por este software de e-proctoring.

Estos problemas y la convicción de que su origen estaba en el alto nivel de improvisación en torno a la realización del Examen Virtual, nos hizo tomar la decisión de emprender acciones contra la Universidad. A inicios de septiembre de 2020, presentamos una denuncia ante la Autoridad Nacional de Protección de Datos Personales notificando las irregularidades y exigiendo un pronunciamiento sobre el uso de Smowl. Resaltamos que, si bien no estábamos en contra de esta tecnología, considerábamos que en el caso puntual su uso representaba un peligro para la privacidad de los postulantes.[3] Si la Autoridad daba mérito a la denuncia, tenía incluso el poder de detener el Examen Virtual.

Pero no lo hizo. A pesar de la creciente oposición de la comunidad universitaria, la Universidad San Marcos no cambió de parecer y llevó a cabo la prueba en los días fijados. Como era previsible, se produjo el caos. Durante la realización del Examen, Internet se llenó de publicaciones denunciando todo tipo de fraudes, desde postulantes que daban la prueba

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

sin cámara web, hasta la transmisión de las preguntas y las respuestas a través de servicios de mensajería como Whatsapp y plataformas de streaming como Twitch.[4] Algunos días después del Examen Virtual, la Autoridad de Protección de Datos publicó un comunicado señalando que en los días previos había fiscalizado el software usado por la Universidad, pero que se tomaría los próximos 90 días (prorrogables por 45 más) para emitir una decisión sobre el caso.[5] Hasta la fecha, dicha decisión no se ha hecho pública.

Tras el final de esta amarga experiencia, nos quedaron muchas dudas acerca de la naturaleza de estas tecnologías que nunca antes habían jugado un rol tan importante en el panorama educativo. Por ejemplo: ¿Qué empresas las crean? ¿A quién se las ofrecen? ¿Existen conflictos en otros países además del Perú? ¿De verdad representan un peligro para la privacidad? ¿En qué casos? Con estas inquietudes encima decidimos elaborar esta investigación enfocada en la región de Latinoamérica. De esa manera quisimos generar información que permita a otros encontrarse en una mejor posición para defenderse de futuras situaciones de injusticia en donde se vean involucradas estas tecnologías.

[4] Leonardo Ancajima, “Examen Virtual De La UNMSM: Denuncian Plagio, Transmisiones En Vivo y Más Durante Su Desarrollo: Universidad San Marcos: Examen De Admisión,” RPP, 4 de Octubre, 2020, https://rpp.pe/tecnologia/redes-sociales/examen-virtual-de-la-unmsm-denuncian-plagio-transmisiones-en-vivo-y-mas-durante-su-desarrollo-noticia-1296176?ref=rpp

[5] “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.,” Gobierno del Perú, 5 de Octubre, 2020, https://www.gob.pe/institucion/minjus/noticias/305976-la-autoridad-nacional-de-proteccion-de-datos-personales-realiza-acciones-de-fiscalizacion-para-verificar-el-adecuado-tratamiento-de-los-datos-personales-en-el-examen-de-admision-online-realizado-por-la-universidad-nacional-mayor-de-san-marcos

3. Mapeando el uso de software de e-proctoring

Con el fin de conocer mejor en qué países de Latinoamérica se utilizaban más las tecnologías de e-proctoring, se hizo un levantamiento de información exclusivamente a través de Internet. Así pues, se consultaron fuentes primarias y secundarias a las que se llegó utilizando palabras claves en buscadores como “e-proctoring”, “e-proctoring en latinoamérica”, “proctoring”, “proctoring en universidades”, “software de monitoreo para exámenes”, entre otros.

Este relevo nos permitió ubicar más de una veintena de casos repartidos entre los siguientes países: Argentina, Brasil, Colombia, Ecuador, México, Perú, Puerto Rico y Uruguay. La mayoría de casos se presentaban en instituciones educativas universitarias. Por razones de afinidad y recursos disponibles, elegimos solamente tres países para realizar el estudio: Argentina, Chile y Perú. También optamos por centrarnos solamente en universidades, dado que estas concentraban casi la totalidad de los casos descubiertos.

Con el fin de conocer qué universidades en estos países habían hecho uso o planeaban usar software de e-proctoring, elaboramos tablas para cada país en donde creamos las siguientes categorías de información: “Nombre de la Universidad”; “País”; “Ciudad”; “Tipo de institución” (si privada o pública); “Tecnología de e-proctoring utilizada”; “Fuente de la información” y; “Principales Usos”. El motivo para proceder de esta forma fue favorecer la posibilidad de establecer comparaciones o hallar patrones interesantes en los datos recolectados.[6]

En total mapeamos un total de 267 universidades entre los tres países. A partir de allí, consultamos todo tipo de fuentes de acceso abierto, 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 muy sencillo, pues estos hechos habían trascendido a la prensa. En otros, solo fue posible deducir esta información a través de indicios o de documentos internos accesibles desde Internet.

Estos fueron los resultados obtenidos:

[6] Para mayor detalle, consultar la sección 9 de este Reporte, donde se han colocado enlaces hacia las bases de datos.

3.1 Argentina

En Argentina se mapearon 108 universidades, de las cuales 56 eran públicas y 52 privadas. Tras la búsqueda respectiva, se detectaron 10 casos de uso de software de e-proctoring, 2 de ellos en universidades públicas y 8 en privadas. Todos ellos se citan a continuación junto al nombre del software de e-proctoring:

Nombre de la Universidad	**Tecnología 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

Tal vez el caso que llamó más la atención en este país fue el de la Universidad Nacional de Córdoba: A finales de junio de 2020 apareció en la prensa argentina la noticia de que dicha universidad iba implementar un “sistema de control facial” para evitar que los estudiantes copien en los exámenes. Posteriormente, se supo que el software en cuestión era Respondus y que solamente sería aplicado en algunas facultades. Sin embargo, esto generó una gran polémica en la población.[7]

[7] Maximiliano Fernandez, “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 (Infobae, 30 de Junio 30 2020), 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/

3.2 Chile

En Chile se mapearon 55 universidades, de las cuales 16 eran públicas y 39 privadas. Tras la búsqueda respectiva, se detectaron 11 casos de uso de software de e-proctoring, 1 de ellos en universidades públicas y 10 en privadas. Todos ellos se citan a continuación junto al nombre del software de e-proctoring:

Nombre de la Universidad	**Tecnología 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

No encontramos casos que hubieran llamado la atención en este país. De hecho, aquellas universidad que dieron publicidad explícita al uso de estas herramientas, como es el caso de la Universidad Diego Portales[8] y Universidad de las Américas,[9] resaltaron más bien sus beneficios debido a las restricciones producto de la pandemia de COVID-19.

[8] "Facultad De Derecho Implementa Exámenes De Grado Virtuales Por Pandemia," Facultad de Derecho UDP - Universidad Diego Portales, 28 de septiembre, 2020, https://derecho.udp.cl/facultad-de-derecho-implementa-examenes-de-grado-virtuales-por-pandemia/
[9] Oscar Peñaherrera, "La UDLA Utiliza Sistema De Reconocimiento Facial Para Procesos Académicos y Administrativos," Universidad de Las Américas, 11 de Mayo, 2020, https://www.udla.edu.ec/2020/05/11/la-udla-utiliza-sistema-de-reconocimiento-facial-para-procesos-academicos-y-administrativos/

3.3 Perú

En Perú se mapearon 104 universidades, de las cuales 44 eran públicas y 60 privadas. Tras la búsqueda respectiva, se detectaron 25 casos de uso de software de e-proctoring, 12 en universidades públicas y 13 en privadas. Todos ellos se citan a continuación junto al nombre del software de e-proctoring:

Nombre de la Universidad	**Tecnología 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

Tal vez el caso que más llamó la atención en este país fue el uso de Smowl por parte de la Universidad Nacional Mayor de San Marcos,[10] pero también hay otros que, por haberse

[10] Para mayor detalle, ver la sección 2 de este Reporte, donde se narra esta historia.

producido fuera de la capital tuvieron una cobertura más limitada. Por ejemplo, está el caso de la Universidad del Santa, que tuvo que cancelar su prueba virtual porque se detectó un intento de fraude durante la misma.[11]

[11] "UNS Lanza Proceso De Admisión 2020-II En Modalidad Presencial," Radio RSD Chimbote (Radio RSD Chimbote, 15 de Julio, 2020), https://radiorsd.pe/noticias/uns-lanza-proceso-de-admision-2020-ii-en-modalidad-presencial

4. Tipos de software de e-proctoring

A pesar que la mayoría de las fuentes consultadas arrojaron que los principales usos de los programas de e-proctoring eran: reconocimiento facial para validar identidad; monitoreo en tiempo real; grabación en audio y video ; y bloqueo de acciones, no es posible ser concluyentes sobre esta afirmación pues no todos funcionan de la misma forma, y a veces las empresas proveedoras permiten a sus clientes (las universidades) escoger dentro de varias herramientas.

Por ello, lo siguiente fue definir qué tecnologías utilizan estos softwares, de tal manera que a partir de allí pudiéramos tener una real noción de todas sus capacidades, aunque en los casos concretos de uso, solo se hubieran utilizado algunas de ellas.

4.1 Exam[12]

Este programa fue desarrollado por la Universidad San Ignacio de Loyola (Perú) y solo se conoce que ofrece el servicio de reconocimiento facial, el cual está basado en el sistema Azure Cognitive de Microsoft, que provee servicios de Inteligencia Artificial desde la nube. No queda claro si requiere ser instalada en los dispositivos de los estudiantes.

4.2 Klarway[13]

Este programa fue desarrollado por Inteligencia Biométrica S.A (Argentina) y ofrece los servicios de validación de identidad mediante tecnología biométrica; administración del entorno a través de la grabación del estudiante desde su dispositivo; y detección de comportamientos sospechosos usando inteligencia artificial y computing vision. Requiere ser instalada en los dispositivos de los estudiantes.

4.3 Mettl[14]

Este programa fue desarrollado por una empresa india del mismo nombre y ofrece múltiples servicios de evaluación en línea. Su software de e-proctoring ofrece los servicios de validación de identidad mediante tres puntos (confirmación por e-mail, reconocimiento facial del documento de identidad y del rostro); detección de comportamientos sospechosos usando inteligencia artificial, a través de vigilancia humana o ambos; y bloqueo de acciones por medio de un navegador seguro. Requiere ser instalada en los dispositivos de los estudiantes.

[12] Fuente: https://gestion.pe/tecnologia/examenes-virtuales-usil-implementa-tecnologia-de-reconocimiento-facial-noticia/
[13] Fuente: https://klarway.com/
[14] Fuente: https://mettl.com/en/

4.4 Proctor Track[15]

Este programa fue desarrollado por Verificient Technologies (Estados Unidos) y ofrece múltiples servicios de evaluación en línea, lo que incluye productos específicos para escuelas de educación básica. Su software de e-proctoring ofrece los servicios de validación de identidad mediante autenticación biométrica; y detección de comportamientos sospechosos usando inteligencia artificial y machine learning. Además ofrece otras herramientas como revisión humana de resultados por un pago adicional. Requiere ser instalada en los dispositivos de los estudiantes.

4.5 Proctorio[16]

Este programa fue desarrollado por una empresa estadounidense del mismo nombre. Su software de e-proctoring ofrece los servicios de validación de identidad mediante reconocimiento facial; detección de comportamientos sospechosos usando inteligencia artificial, vigilancia humana o ambos; bloqueo de acciones en el dispositivo del estudiante; control anti-plagio; y verificación de que el contenido de los exámenes no se sube a Internet. Requiere ser instalada en los dispositivos de los estudiantes.

4.6 Respondus[17]

Este programa fue desarrollado por una empresa estadounidense del mismo nombre y ofrece múltiples servicios de evaluación en línea, lo que incluye productos específicos para escuelas de educación básica. Su software de e-proctoring ofrece los servicios de validación de identidad mediante reconocimiento facial; detección de comportamientos sospechosos usando inteligencia artificial; y bloqueo de acciones por medio de un navegador seguro. Requiere ser instalada en los dispositivos de los estudiantes, pero también ofrece una opción de servicios sin instalación.

4.7 Safe Exam Browser[18]

Este programa fue desarrollado por la universidad de ETH Zurich (Suiza) y ofrece el servicio de bloqueo de acciones por medio de un navegador seguro. El programa se ofrece de forma gratuita y es de código abierto. Requiere ser instalada en los dispositivos de los estudiantes.

4.8 Smowl[19]

Este programa fue desarrollado por Smowltech (España) y ofrece los servicios de validación de identidad mediante reconocimiento facial; detección de comportamientos sospechosos usando inteligencia artificial; monitorización del dispositivo del estudiante; y bloqueo de

[15] Fuente: https://www.proctortrack.com/
[16] Fuente: https://proctorio.com/
[17] Fuente: https://web.respondus.com/
[18] Fuente: https://safeexambrowser.org/news_en.html
[19] Fuente: https://smowl.net/es/

acciones en el dispositivos del estudiante. Requiere ser instalada en los dispositivos de los estudiantes, pero también ofrece una opción de servicios sin instalación.

4.9 Sumadi[20]

Este programa fue desarrollado por Laureate Ventures que pertenece a la corporación Laureate Education (Estados Unidos), que es propietaria de diferentes universidades en todo el mundo. Su software de e-proctoring ofrece los servicios de validación de identidad mediante reconocimiento facial biométrico y autenticación por medio de patrones de tecleo; detección de comportamientos sospechosos usando computer vision; y bloqueo de acciones en el dispositivo del estudiante. Requiere ser instalada en los dispositivos de los estudiantes.

[20] Fuente: https://sumadi.net/

5. Legislación de privacidad aplicable al uso de software de e-proctoring

Sabiendo qué universidades y qué tipo de programas de e-proctoring utilizaron, para evaluar su impacto en la privacidad fue preciso determinar qué legislación sobre privacidad existía en cada país estudiado. Pero, ¿qué es la legislación sobre privacidad? Podríamos definirla como el conjunto de normas que regulan la forma cómo se protege tanto el derecho a la intimidad y la vida privada, así como el derecho a la autodeterminación informativa.

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 a través de Internet que identifican o hacen identificables a las personas.

Para encontrar esta legislación consultamos fuentes primarias (normas) y secundarias (reportes, artículos) de los tres países. A partir de allí notamos que todas eran muy similares en varios aspectos, pero con ciertas diferencias en términos de desarrollo e institucionalidad. Entre las características comunes estaba que los tres países recogían en sus Constituciones tanto el derecho a la intimidad como la autodeterminación informativa. También que todos contemplaban la acción de “Hábeas Data” como mecanismo para exigir la protección de derechos relativos a la privacidad. Finalmente, todos tenían leyes específicas sobre protección de datos personales.

En cuanto a las diferencias, la principal era que solo Argentina y Perú contemplaban un régimen de protección de datos que permitía reclamarlos en sede administrativa, mientras que en Chile esto solo era posible en sede judicial a través de la acción de Hábeas Data. También que solo los dos primeros contaban con Autoridades de Protección de Datos Personales, que eran las instancias encargadas de resolver los casos en sede administrativa, pudiendo ordenar el cumplimiento y sancionar las infracciones.

La conclusión a la que arribamos luego de recopilar esta normativa fue que solo en el caso de las normas de protección de datos personales había obligaciones concretas y exigibles en materia de privacidad. Por ello, decidimos tomarlas como única referencia para medir el impacto de los programas de e-proctoring. Era una lógica sencilla: Si el uso de alguno de estos softwares incumplía con las obligaciones establecidas por estas normas, podríamos afirmar que existía una posible afectación a la privacidad.

Ahora bien, para determinar el nivel de cumplimiento de las normas de protección de datos en los tres países era necesario valorar principalmente dos elementos: Los sujetos obligados al cumplimiento y los datos personales tratados. El primer elemento estaba atravesado por cuestiones poco claras como la jurisdicción y el nivel de responsabilidad. No obstante, un factor común en todos los casos era que las universidades podían ser consideradas como las obligadas principales, más allá de que hubiera intermediarios en la

recolección y tratamiento de los datos de los estudiantes. El segundo elemento requirió mapear los datos personales que pudieran estar siendo tratados a partir de las diferentes tecnologías empleadas por los programas de e-proctoring.[21]

Pero, ¿cómo saber qué datos trataban? A falta de mayor referencia, empleamos un proceso de verificación de tres niveles. 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 la imagen. También otros datos derivados de la misma como los rasgos faciales o documentos de comparación como el documento 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 opera el software. 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 privacidad como por ejemplo el Reglamento General de Protección de Datos (RGPD) que rige 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 lista 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:

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

[21] Para mayor detalle, consultar la sección 9 de este Reporte, donde se han colocado enlaces hacia las bases de datos.

Luego de obtener estos datos, pasamos a verificar qué obligaciones específicas tenían las universidades en cada país:[22]

5.1 Argentina

En Argentina la norma vigente es la Ley N° 25326 de Protección de Datos Personales, que regula la forma del tratamiento de los datos personales. Como ocurre en todas las legislaciones de este tipo, la norma argentina establece un esquema de principios como: legalidad, consentimiento, calidad, seguridad, a partir de los cuales se derivan obligaciones específicas. Además, se reconocen regímenes diferentes para los datos considerados "sensibles", que son todos aquellos que revelan ámbitos muy íntimos de la vida como la etnia, salud y religión. Debido a criterios interpretativos de la Autoridad de Protección de Datos Personales de este país, se considera que los datos biométricos también pueden ser considerados sensibles en tanto revelen otros datos cuyo uso pueda resultar potencialmente discriminatorio.

En el caso del principio de legalidad, la regla es que el tratamiento de todos los datos personales siempre está permitido, salvo en el caso de los datos sensibles, que solo puede ser llevado a cabo por razones de interés general autorizadas por ley. Esto significa que sin haber ley que lo autorice, aún obteniendo el consentimiento, los datos sensibles no pueden ser tratados de forma lícita en Argentina.

En el caso del principio de consentimiento, en todos los casos quien va a tratar los datos debe requerir el consentimiento de forma previa al tratamiento, salvo excepciones previstas por ley. Además, dicho consentimiento debe cumplir con ser libre, expreso e informado y constar por escrito u otro medio análogo. El contenido de cada una de estas características se define caso por caso cuando existen denuncias de los afectados.

En el caso del principio de calidad, en todos los casos quien va a tratar los datos debe registrar previamente el archivo, registro o banco de datos ante la Agencia de Acceso a la Información Pública (anteriormente era la Dirección 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 u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados, salvo excepciones previstas por ley.

En el caso del 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

[22] Para mayor detalle, consultar la sección 9 de este Reporte, donde se han colocado enlaces hacia las bases de datos.

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).[23]

Finalmente, los derechos reconocidos a los titulares de los datos personales son los de Información, Rectificación, Actualización y Supresión.

[23] Ver RESOL-2018-47-APN-AAIP, “Medidas de seguridad recomendadas para el tratamiento y conservación de los datos personales en medios informáticos”, https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-47-2018-312662/texto

5.2 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. Tal como en Argentina, la norma chilena establece principios similares, desde los cuales se derivan las obligaciones. También se reconoce el régimen especial de los denominados datos sensibles.

En el caso del principio de legalidad, la regla es que el tratamiento de todos los datos personales siempre está permitido. No obstante, en el caso de los datos sensibles se requiere cumplir con alguno de estos supuestos: Que la ley lo autorice, que haya consentimiento del titular, o que sea necesario para la determinación u otorgamiento de beneficios de salud. Al ser esta lista amplia y no excluyente, es posible afirmar que hay amplio margen para tratar cualquier tipo de dato en Chile.

En el caso del principio de consentimiento, en todos los casos quien va a tratar los datos debe requerir el consentimiento de forma previa al tratamiento, salvo excepciones previstas por ley. Además, dicho consentimiento debe cumplir con ser expreso e informado y constar por escrito, salvo excepciones previstas por ley. El contenido de cada una de estas características se define caso por caso cuando existen denuncias de los afectados.

En el caso del principio de calidad, solo en el caso de que quien va a tratar los datos sea una entidad pública, debe registrar previamente el archivo, 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.

En el caso del 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.

Finalmente, los derechos reconocidos a los titulares de los datos personales son los de Información, Modificación, Cancelación o Bloqueo y Oposición.

5.3 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. Tal como en Argentina y Chile, la norma peruana establece principios similares, desde los cuales se derivan las obligaciones. También se reconoce el régimen especial de los denominados datos sensibles.

En el caso del principio de legalidad, la regla es que el tratamiento de todos los datos personales siempre está permitido, incluso cuando se trata de datos sensibles. No obstante, en este último caso concurrirán diferentes requisitos de forma y de fondo.

En el caso del principio de consentimiento, en todos los casos quien va a tratar los datos debe requerir el consentimiento de forma previa al tratamiento, salvo excepciones previstas por ley. Además, dicho consentimiento debe cumplir con ser previo, informado, expreso e inequívoco, salvo excepciones previstas por ley. En el caso de los datos sensibles, el consentimiento debe constar por escrito, un requisito que puede ser cumplido además a través de medios electrónicos.

En el caso del principio de calidad, en todos los casos quien va a tratar los datos debe registrar previamente el archivo, 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.

En el caso del 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 de los datos. 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.[24]

Finalmente, los derechos reconocidos a los titulares de los datos personales son los de Acceso, Rectificación, Cancelación y Oposición.

[24] Ver Resolución Directoral Nº 019-2013-JUS/DGPDP, “Directiva de Seguridad”, https://www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-de-Directiva-de-Seguridad.pdf

6. Análisis de impacto en la privacidad a partir del uso de software de e-proctoring

El siguiente análisis busca señalar de forma específica situaciones que se han producido o que podrían producirse en los tres países estudiados, en las cuales el uso de alguno de los softwares de e-proctoring detectados afectan o podrían afectar la privacidad de los estudiantes. Para ello se ha tomado en consideración la legislación de privacidad recogida en la sección anterior y las capacidades de cada programa detectado.

6.1 Argentina

Salvo un caso en que no se pudo determinar el software de e-proctoring utilizado por parte de la universidad, en todas las demás se utilizaron programas cuyas capacidades incluyen tecnología de reconocimiento facial, monitoreo en tiempo real a través de grabación continua o capturas de imagen y voz, y bloqueo de acciones en los dispositivos de los estudiantes. Además, en la mayoría de casos, era necesario que los estudiantes instalen el software en sus dispositivos.

Asumiendo que todos estos programas se utilizaron en sus máximas capacidades, estamos frente al tratamiento de múltiples datos personales, incluyendo datos sensibles como la imagen y los rasgos faciales, que pueden revelar la etnia o potencialmente ser usados para discriminar al titular. Esto significa que en todos los casos son exigibles las diferentes obligaciones que establece la legislación argentina sobre protección de datos personales. Vamos a desarrollar cada una, en la misma secuencia de principios que la sección anterior:

En el caso del principio de legalidad, aunque para la mayoría de datos bastaba el consentimiento de los estudiantes, respecto de los datos sensibles era necesario también que dicho tratamiento esté autorizado por ley. Ahora bien, es de sentido común asumir que las universidades públicas y privadas ya trataban datos sensibles desde hace mucho tiempo, como por ejemplo los datos de salud con el fin de prestar servicios esenciales como los de enfermería o aseguramiento. ¿Cuál sería pues la base para tratarlos? La respuesta parece ser las normas que regulan el acceso a la educación universitaria.

Pero, ¿esto aplica a los datos sensibles tratados por software de e-proctoring? No está claro cuál es el límite. Por ejemplo, a mediados de 2020, se anunció que las universidades públicas argentinas iban a emplear una plataforma denominada Siu Quechua, con el fin de realizar la validación de identidad de los estudiantes mediante reconocimiento facial. En su momento, organizaciones como la Asociación por los Derechos Civiles (ADC) exigieron saber si se habían realizado estudios de impacto en la privacidad o si se había coordinado esta iniciativa con la Agencia de Acceso a la Información Pública.[25] Esto significa que nuevas formas de tratamiento no suelen pasar sin objeción.

[25] Maximiliano Fernandez, “Las Universidades Públicas Usarán Un Sistema De Reconocimiento Facial Para Evitar Fraudes En Los Exámenes,” Infobae (infobae, 16 de Julio, 2020), https://www.infobae.com/educacion/2020/07/16/las-universidades-publicas-usaran-un-sistema-de-reconocimiento-facial-para-evitar-fraudes-en-los-examenes/

Volviendo al caso concreto, si alguien decidiera reclamar acerca de la legalidad del tratamiento de datos sensibles por parte de las universidades que emplearon programas de e-proctoring, efectivamente estas podrían invocar diferentes normas educativas que ya les permiten tratar datos sensibles de sus estudiantes. No obstante, esta invocación sería genérica, pues no existen actualmente normas que habiliten a ninguna institución educativa en Argentina a tratar datos sensibles como los rasgos faciales con el fin de realizar evaluaciones académicas. La autoridad de protección de datos sería finalmente la encargada de dirimir esta cuestión ante una denuncia.

En el caso del principio de consentimiento, nos encontramos ante dos situaciones, que dependen de si resulta legal o no el tratamiento de datos sensibles por parte de los programas de e-proctoring. Si se considera que las universidades podían tratar datos sensibles bajo el amparo de las normas educativas, por conexión podrían alegar también que no necesitaban pedir el consentimiento de los estudiantes para tratar dicho datos. Si este fuera el caso, nuevamente se estaría apelando a normas genéricas, cuya validez tendría que ser cuestionada ante la autoridad.

Si por el contrario, resultaba ilegal tratar datos sensibles a partir del uso de softwares de e-proctoring, las universidades habrían infringido la normativa argentina de protección de datos, afectando así la privacidad de sus estudiantes. Esto habría ocurrido, aún si las universidades hubieran recabado su consentimiento, ya sea directamente o a través de la aceptación de términos y condiciones de los programas pues hemos dicho que el tratamiento de datos sensibles en Argentina requiere la existencia de ley habilitante.

Yendo más allá de la aplicación normativa, está también el hecho de que Argentina vivió y vive actualmente circunstancias excepcionales a raíz de la pandemia de COVID-19. Estas circunstancias hicieron que muchas de las actividades, incluidas las clases universitarias, tuvieran que pasar de presenciales a virtuales. Teniendo esto en cuenta, ¿es posible que las normas de protección de datos pudieran relajarse debido a este evento? Estrictamente hablando, hacerlo habría requerido la expedición de una norma de alcance nacional que regule este supuesto. Sin embargo, no encontramos ninguna regulación de este tipo.

Ahora bien, si asumimos que aún sin una ley habilitante, las circunstancias justificaban estos “tratamientos excepcionales”, queda por determinar si por lo menos se debió requerir el consentimiento de los estudiantes para tratar sus datos. Si la respuesta es afirmativa, habría que detenernos a pensar también cómo debería haberse otorgado dicho consentimiento. Por ejemplo, la normativa argentina señala que el consentimiento debe ser libre. ¿Esto significa que el estudiante debió tener la posibilidad de escoger no ser evaluado utilizando los programas de e-proctoring? ¿Se le debió otorgar alternativas a su uso? Estas y otras preguntas solo podrían ser valoradas por la autoridad ante una denuncia.

En el caso del principio de calidad, tanto las universidades públicas como privadas tenían la obligación legal de registrar sus ficheros o bancos de datos personales ante la Autoridad Nacional de Protección de Datos. Este requisito incluso aplica a aquellas universidades a las que no se les detectó el uso de software de e-proctoring. En todos los casos, se esperaría

que todas ellas tuvieran por lo menos un registro ante la autoridad con el banco de datos de sus estudiantes. ¿Pero, esto fue así?

Habiendo consultado mediante el "Buscador del Registro Nacional de Bases de Datos Personales" del sitio web del Gobierno de Argentina, pudimos corroborar que solo 2 de las 10 universidades mapeadas en este país contaban con un registro ante la autoridad de protección de datos. Estas fueron: la Universidad Argentina de la Empresa[26] y la Universidad de Palermo,[27] ambas universidades privadas. Ahora bien, este resultado tiene dos posibles lecturas.

La primera es que las universidades que no inscribieron sus ficheros consideran que no están afectas a las obligaciones de registro. Esto parece probable, sobre todo si detrás de dicha lógica subyace la idea de que las normas educativas las habilitan para tratar datos sensibles, lo que incluso podrían hacer sin tener que solicitar el consentimiento a sus estudiantes. La segunda es que, aún considerando que están afectas a esta obligación, deciden no cumplirla, ya sea porque no temen ser fiscalizadas o porque han decidido deliberadamente infringir la ley.[28]

No hay forma de saber qué situación corresponde a cada universidad y cualquier generalización resultaría injusta. No obstante, eso no impide mencionar algunos detalles que hacen que la primera lectura no sea totalmente consistente: hay por lo menos una veintena de universidades que consignan registros en el buscador, de las cuales por lo menos cuatro son universidades públicas. Si fuera generalizada la idea de que estas instituciones no están obligadas a presentar sus registros de datos personales ante la autoridad, ¿por qué otras sí lo han hecho?

En el caso del principio de seguridad, resultó imposible corroborar qué tipo de medidas de seguridad implementaron las universidades o las empresas proveedoras de software de e-proctoring. Tampoco se logró obtener información sobre brechas de seguridad o problemas de funcionamiento, al menos de fuentes de acceso público. No obstante, es de notar que la mayoría de empresas están domiciliadas fuera de Argentina, lo que significa que al momento de tratar los datos de los estudiantes posiblemente realizan flujo transfronterizo. La normativa argentina de protección de datos prohíbe el flujo hacia países sin protección adecuada o equivalente. Siendo esto así, ¿qué ocurre en los casos en que las empresas están domiciliadas en Estados Unidos y posiblemente transfieren los datos

[26] Fuente: https://www.argentina.gob.ar/aaip/datospersonales/reclama/30539187658--RL-2019-89077500-APN-DNPDP#AAIP

[27] Fuente: https://www.argentina.gob.ar/aaip/datospersonales/reclama/33620101449--RL-2019-95298681-APN-DNPDP#AAIP

[28] Dentro de nuestra investigación hemos encontrado evidencia que sugiere la existencia de "bases de datos" inscritas de algunas de las universidades mapeadas, pero que no han sido ubicadas a través de la herramienta de búsqueda oficial. La mayoría de estas evidencias han sido recabadas de este estudio de 2013 sobre bases de datos de universidades públicas: http://oiprodat.com/2013/07/11/gestion-de-datos-personales-en-las-universidades-nacionales-de-argentina/

personales a servidores ubicados en este país? ¿Se estaría vulnerando la privacidad de los estudiantes al ser este un destino con un menor nivel de protección?

Finalmente, existe un caso que amerita ser mencionado, el de Klarway. La empresa que comercializa este programa de e-proctoring consigna en su sitio web que está domiciliada en territorio argentino. Esto significa que, mientras que en los otros casos decidimos asumir que las universidades eran los principales obligados para evitar el dilema de la jurisdicción, en este caso todas las obligaciones hasta aquí abordadas le resultan aplicables también a dicha empresa. Ahora bien, al menos hasta donde es posible verificar, Klarway parece cumplir con la mayoría de obligaciones. Dejando de lado el tema de la legalidad de tratar datos sensibles a través del e-proctoring, la empresa cuenta con políticas de privacidad sobre sus productos, lo que incluye información sobre la forma y fines del tratamiento de los datos. Además, cuenta con un banco de datos registrado ante la autoridad de protección de datos argentina.

6.2 Chile

Salvo dos casos en los que no se pudo determinar con precisión el software de e-proctoring utilizado por parte de las universidades, en todas las demás se utilizaron programas cuyas capacidades incluyen tecnología de reconocimiento facial, monitoreo en tiempo real a través de grabación continua o capturas de imagen y voz, y bloqueo de acciones en los dispositivos de los estudiantes. Además, en la mayoría de casos, era necesario que los estudiantes instalen el software en sus dispositivos.

También asumiendo que todos ellos se utilizaron en sus máximas capacidades, estamos frente al tratamiento de múltiples datos personales, incluyendo datos sensibles (imagen, rasgos faciales). Esto significa que en todos los casos son exigibles las diferentes obligaciones que establece la legislación chilena sobre protección de datos personales:

En el caso del principio de legalidad, a diferencia de Argentina, en Chile los datos sensibles se pueden tratar incluso solo con el consentimiento del titular. Así pues, para cumplir con las normas chilenas a las universidades les habría bastado con solicitar el consentimiento a los estudiantes para poder emplear los softwares de e-proctoring de forma lícita. No obstante, igual que en Argentina, la norma chilena parece permitir también la interpretación de que las normas educativas pueden ser invocadas para justificar el tratamiento, pudiendo prescindir así del consentimiento.

En el caso del principio de consentimiento, como decíamos, las universidades pueden obviar el consentimiento aplicando la misma lógica que las universidades argentinas. Es decir, amparándose en leyes sobre la educación para afirmar que no necesitan pedir permiso para tratar datos personales. Si bien en este caso también se puede reclamar la validez de estas leyes, al no tener Chile una sede administrativa de queja, parece menos probable obtener un resultado favorable en sede judicial, tal como ha sido señalado varias veces por expertos de este país.[29]

Dado que la normativa chilena es más permisiva que la argentina, no parece necesario siquiera citar las circunstancias producidas por el COVID-19 como una suerte de atenuante para el tratamiento de datos por parte de programas de e-proctoring. En cualquier caso, nuestra búsqueda tampoco halló ninguna disposición legal que buscara “relajar” el estándar de cumplimiento de la protección de datos personales en el país a propósito de la pandemia.

En el caso del principio de calidad, las normas chilenas solo establecen la obligación de inscribir bases de datos a las entidades públicas. Eso significa que dicho registro solo era exigible a la Universidad de Chile, que fue la única universidad pública mapeada en este país. A partir de la búsqueda en el “Registro de Bancos de Datos Personales a cargo de Organismos Públicos” del sitio web del Registro Civil e Identidad pudimos corroborar que esta universidad no registraba ningún banco de datos.[30] Algo que también nos llamó la

[29] Maria Paz Canales, “Chile necesita una regulación de protección de datos con dientes, 12 de Julio, 2019, https://www.derechosdigitales.org/13443/proteccion-de-datos-con-dientes/
[30] Fuente: http://rbdp.srcei.cl/rbdp/html/Consultas/consultas.html

atención mirando otros registros es que solo 2 de un total de 8 universidades públicas cuentan con registros de bases de datos.

Volviendo al caso, aún si la Universidad de Chile no hubiera tratado datos a través del uso de software de e-proctoring, de todos modos habría tenido que cumplir con la obligación de registrar sus bases de datos pues es evidente que trata datos (de estudiantes, trabajadores, etc). ¿Por qué no lo hizo? A diferencia de Argentina, en donde podría ser oponible la inexigibilidad del registro a partir del hecho que existen leyes que habilitan a ciertas entidades a tratar datos sensibles incluso sin consentimiento, en el caso de Chile hay un mandato expreso de que las entidades públicas sí realicen dicho registro. El no haberlo hecho podría configurarse en una afectación a la privacidad de los estudiantes.

En el caso del principio de seguridad, resultó imposible corroborar qué tipo de medidas de seguridad implementaron las universidades o las empresas proveedoras de software de e-proctoring. Tampoco se logró obtener información sobre brechas de seguridad o problemas de funcionamiento, al menos de fuentes de acceso público. En el caso de Chile, todas las empresas están domiciliadas fuera del país, lo que significa que al momento de tratar los datos de los estudiantes posiblemente realizan flujo transfronterizo. No obstante, a diferencia de Argentina, la norma chilena no ha regulado las características de este flujo, por lo tanto este acto no infringe en forma alguna la norma de protección de datos, pese a que algunos destinos como Estados Unidos estén sujetos a una regulación menos segura.

6.3 Perú

El caso de Perú es diferente de los anteriores tanto por la cantidad de universidades mapeadas como por los diferentes tipos de software detectados, así como por ser el país del cual se cuenta con mayor información. Por todo ello, el análisis se va a desarrollar siguiendo la misma línea que los dos anteriores, pero teniendo en cuenta ciertas particularidades. Tal vez la primera de ellas es una cuestión previa sobre la exclusión de uno de los programas de e-proctoring: Safe Exam Browser.

Al momento de elaborar la lista de Perú, este programa fue detectado en dos universidades, una pública y la otra privada. Si bien por su forma de funcionamiento, este se ajusta a la definición de e-proctoring que ofrecimos al inicio de este trabajo, presenta características que nos impiden compararlo con los demás. Según se señala en su sitio web, Safe Exam Browser es un programa de código abierto que se ofrece de forma gratuita a quien desee instalarlo. Además, dado que no es un servicio bajo demanda, quien lo instala es también el encargado de operarlo. En el caso de las universidades que lo utilizaron para controlar la realización de exámenes, estas tuvieron que acoplarlo a través de APIs a sus propias plataformas de evaluación.

El uso más frecuente, sino el único, de Safe Exam Browser es el de bloquear la navegación en el dispositivo del estudiante, con el objetivo de que se mantenga dentro de la plataforma o página donde debe desarrollar la prueba. Para ejecutar esta acción, Safe Exam Browser se conecta al sistema operativo del dispositivo y “desactiva” acciones como los comandos de acceso rápido, hacer clic derecho o acceder a la barrera de inicio. Su funcionamiento no requiere la recolección de datos de ningún tipo y tampoco existe un flujo de datos desde el dispositivo hacia terceros. Es decir, no se produce tratamiento de datos personales. Todo ello, pero especialmente esto último, nos hizo tomar la decisión de excluir de este análisis tanto al programa como a las universidades que lo utilizaron.

Volviendo a los demás, salvo en seis casos en donde no se pudo identificar el software de e-proctoring utilizado, en todos los demás se determinó que los programas utilizados por las universidades poseían tecnologías de reconocimiento facial, monitoreo en tiempo real a través de grabación continua o capturas de imagen y voz, y bloqueo de acciones en los dispositivos de los estudiantes. Además, en la mayoría de casos, era necesario que los estudiantes instalen el software en sus dispositivos.

Igual que con Argentina y Chile, asumiendo que todos estos programas se utilizaron en sus máximas capacidades, estamos frente al tratamiento de múltiples datos personales, incluyendo datos sensibles (imagen, rasgos faciales). Esto significa que en todos los casos son exigibles las diferentes obligaciones que establece la legislación peruana sobre protección de datos personales:

En el caso del principio de legalidad, de forma similar que la normativa chilena, en Perú todos los datos, incluido los sensibles, se pueden tratar siempre que se cumplan con las formalidades establecidas, siendo una de ellas que se cuente con el consentimiento del titular de los datos. Para cumplir con este principio, a las universidades les habría bastado

con solicitar el consentimiento a los estudiantes. No obstante, en su ausencia, también podría haberse invocado la normativa de educación para avalar el tratamiento, igual que en Argentina y Chile. Cualquier discrepancia sobre este punto, tendría que ser dirimida por la autoridad de protección de datos.

En el caso del principio de consentimiento, existen dos escenarios que no necesariamente son excluyentes. En el primer escenario, si las universidades no solicitaron consentimiento de los estudiantes para tratar sus datos a través de los softwares de e-proctoring, podrían argumentar que las normas educativas las habilitaban para ello. Si este fuera el caso, tendrían que ampararse en normas genéricas pues no encontramos ninguna disposición legal que expresamente habilite este tipo de tratamiento.

En el segundo escenario, si solicitaron el consentimiento, debieron cumplir además una formalidad que tiene la normativa de protección de datos peruana respecto del tratamiento de datos sensibles: que el consentimiento se otorgue por escrito. Ahora, esto no significa necesariamente que se tenga que entregar en una hoja de papel y a través de firma manuscrita. La ley peruana señala que se entenderá también por consentimiento escrito al uso de firma electrónica u otros medios análogos. Si las universidades no lo hubieran obtenido de esta forma, podría configurarse una afectación a la privacidad.

En el caso de Perú, vale la pena también referirnos a las circunstancias producidas por el COVID-19. Por la manera en que funciona el sistema de acceso a la educación universitaria en este país, la mayoría de universidades tanto públicas como privadas se ven obligadas a realizar exámenes de ingreso por lo menos dos veces al año, los que suelen tener una concurrencia masiva. Esta situación, sumada a la necesidad de garantizar una evaluación justa sería la causa de que en Perú se hayan detectado más del doble de casos de uso de software de e-proctoring que en Argentina y Chile. ¿Esto podría ser un atenuante si se trataron datos personales de forma indebida? Solo la autoridad podría determinarlo ante una denuncia.

En el caso del principio de calidad, tanto las universidades públicas como privadas tenían la obligación legal de registrar sus ficheros o bancos de datos personales ante la Autoridad Nacional de Protección de Datos. Este requisito incluso aplica a aquellas universidades a las que no se les detectó el uso de software de e-proctoring. En todos los casos, se esperaría que todas ellas tuvieran por lo menos un registro ante la autoridad con el banco de datos de sus estudiantes. ¿Pero, esto fue así?

Habiendo consultado el “Registro Nacional de Protección de Datos Personales” del sitio web del Ministerio de Justicia de Perú,[31] pudimos corroborar que ninguna universidad pública mapeada contaba con registros ante la autoridad, mientras que todas las universidades privadas sí contaban con los mismos, con excepción de la Universidad César Vallejo. Además, cabe resaltar que la mayoría de universidades con registros contaban con dos tipos de bases de datos diferenciadas, una para postulantes y otra para alumnos, lo que da cuenta de un alto nivel de cumplimiento. Es de resaltar también que en todos estos casos,

[31] Fuente: https://prodpe.minjus.gob.pe/prodpe_web/BancoDato_verResultado#

se especificaba el tratamiento de datos como la imagen, nombre y documento de identidad, que son algunos de los que tratan los softwares de e-proctoring.

De forma similar que en Argentina, una primera lectura de estos hallazgos es que las universidades públicas no registran sus bancos de datos porque consideran que existen leyes (por ejemplo, las normas educativas) que les permiten tratar datos sin cumplir con la normativa de protección de datos personales. No obstante, a diferencia de dicho país, en el Perú casi la totalidad de universidades privadas sí realizan el registro de sus bases de datos, lo que lleva a pensar que esta forma de pensamiento no es necesariamente correcta. Así mismo, un hecho que resta consistencia a esta lectura es que hay por lo menos tres universidades públicas que sí tienen sus bases de datos registradas ante la autoridad.

Una segunda lectura es que las universidades públicas sin registros han decidido desacatar directamente las obligaciones de la normativa de protección de datos porque consideran que no les son aplicables en ningún caso. Esto que parece sorprendente, en realidad es una práctica que viene siendo ejecutada por algunas entidades públicas del país, como por ejemplo; el Registro Nacional de Identidad y Estado Civil (RENIEC). En una investigación que realizamos en 2020 sobre identidad digital, detectamos que RENIEC efectivamente no cumple varias de las obligaciones establecidas por la ley de protección de datos personales, negándose a inscribir sus bases de datos y dificultando el ejercicio de diferentes derechos como el acceso, la modificación y la cancelación gratuita de datos personales en su poder.[32]

Independientemente de las razones por las que las universidades públicas no registran sus bancos datos, el hecho de que no lo hagan crea dos estándares de protección para los estudiantes. Por un lado están las universidades privadas que, al emplear software de e-proctoring, deben ceñirse a las obligaciones derivadas del registro que realizan y por el otro las universidades públicas que realizan los mismos actos pero parecen no sentirse afectas a ninguna regulación. En este último caso, estaríamos hablando de varios tipos de afectaciones a la privacidad si resulta que sí les son aplicables las normas de protección de datos.

En el caso del principio de seguridad, resultó imposible corroborar qué tipo de medidas de seguridad implementaron las universidades o las empresas proveedoras de software de e-proctoring. Sin embargo, en dos casos resultó posible acceder a información sobre brechas de seguridad. El primer caso fue el de la Universidad de San Marcos, que recibió amplia cobertura en el país y consistió básicamente en el mal funcionamiento de Smowl durante la realización de su Examen Virtual, lo que ameritó incluso una investigación por parte de la Autoridad de Protección de Datos Personales. El segundo caso es el de la Universidad del Santa, que no fue tan cubierto pero del que se sabe tuvo que cancelar su prueba por un intento de fraude, tras lo cual abandonó el uso del programa de e-proctoring en favor de una prueba presencial.

[32] Carlos Guerrero Argote, “Identidad Digital En Perú: Descifrando Al Leviatán,” 15 de Diciembre, 2020, https://hiperderecho.org/wp-content/uploads/2020/11/guerrero_identidad_digital.pdf

Finalmente, dado que todas las empresas proveedoras de los softwares de e-proctoring están domiciliadas fuera de Perú, ello significa que al momento de tratar los datos de los estudiantes posiblemente realizaron flujo transfronterizo. La normativa peruana es un poco más permisiva que la argentina, pues siempre que se informe acerca del flujo y el país de destino de los datos tenga un nivel de protección equivalente, estos sí se pueden transferir de forma lícita. En la práctica, esto incluye a las empresas que tienen servidores en Estados Unidos por lo que aparentemente no cabría demandar que se produciría una vulneración a la privacidad por este hecho.

7. Conclusiones

Todo lo visto hasta ahora nos permite llegar a varias conclusiones sobre los softwares de e-proctoring, su uso por parte de 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 pasamos a señalar algunas de estas conclusiones:

- El mapeo de universidades en los tres países de estudio arrojó una gran cantidad de instituciones que utilizan software de e-proctoring, especialmente en el caso de Perú. No obstante, 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 8 a 2 y de 10 a 1 respectivamente. Solo en el caso de Perú existe un equilibrio entre universidades públicas y privadas, siendo la relación de 12 a 13.
- Aunque no puede declararse de forma categórica, la información disponible permite concluir que el principal (y a veces único) uso del software de e-proctoring por parte de las universidades es controlar la realización de exámenes para evitar las conductas deshonestas. Esto a pesar de que una gran parte de los programas detectados ofrecen también otro tipo de servicios.
- 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 acciones en los dispositivos de los estudiantes. Finalmente, cinco de ellos son provistos por empresas cuya sede principal está en Estados Unidos.
- 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 normativa de protección de datos en cada uno de los tres países donde operan. 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.
- 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. Esto es especialmente evidente en tres ámbitos: Las restricciones para tratar datos sensibles; las disposiciones sobre registro de banco de datos; y las reglas aplicables al flujo transfronterizo de datos. Además, la inexistencia en Chile de una autoridad de protección de datos y de una vía administrativa para reclamar infracciones parece exacerbar las posibles vulneraciones a la privacidad como consecuencia del uso de software de e-proctoring.

- 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 o bancos de datos personales ante la autoridad, existe poco o nulo cumplimiento de esta obligación tanto de las universidades públicas como las privadas. En el caso de Perú, este incumplimiento se da casi exclusivamente por parte de las públicas. No es posible determinar a qué se debe esta situación, pudiendo esto responder a una misma razón o a diferentes razones de índole legal o cultural en cada país. En Chile, la única universidad obligada que es pública, tampoco cumple estas disposiciones.
- Salvo en Perú, en los otros dos países no fue posible verificar a través de documentos de acceso público que hayan existido fallos o brechas de seguridad a partir del uso de los softwares de e-proctoring. No obstante, aún en los casos documentados de Perú, no existe a la fecha un pronunciamiento de la autoridad de protección de datos sobre los mismos o de cualquier otra entidad llamada a fiscalizar que el uso de estas tecnologías no cause perjuicios a los estudiantes.
- 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 las denuncias de los estudiantes por alguna de las posibles afectaciones a la privacidad expuestas en este trabajo.

8. Recomendaciones

Aunque es evidente la naturaleza emergente de este tema, además de las conclusiones de este estudio, consideramos útil proponer también algunas recomendaciones tanto para las universidades como para los proveedores de software de e-proctoring. Estas recomendaciones no tienen como objetivo alentar el abandono de estas tecnologías, sino promover acciones que prevengan o mitiguen las posibles afectaciones a la privacidad que hemos detectado a partir de su uso.

8.1 Para las Universidades

- La adquisición de cualquier tipo software de e-proctoring debería estar precedida por un diálogo abierto y transparente al interior de la comunidad universitaria con el fin de que se sepa con anticipación qué tecnologías se pretenden utilizar, en qué casos y cuáles son los argumentos para optar por ellas y no por otras soluciones análogas.
- Además de contar con el acuerdo de la comunidad universitaria, las universidades deben considerar prioritario establecer si el uso de software de e-proctoring les acarrea el cumplimiento de nuevas obligaciones legales, especialmente en términos de protección de datos personales. Si fuera así, se debe garantizar su cumplimiento.
- En todos los casos, el uso de software de e-proctoring debe superar un período suficiente de capacitación y de prueba, de manera que los estudiantes conozcan de antemano el proceso de funcionamiento de estas tecnologías, y de esa forma no se vean perjudicados por fallos en el software o en los procesos de evaluación.
- Por lo menos en situaciones críticas de evaluación, ya sea por la cantidad de estudiantes evaluados o por la importancia de las pruebas, debería evitarse el uso de software de e-proctoring. No obstante, si tuviera que usarse, los estudiantes deben tener la opción de escoger ser evaluados de formas alternativas.
- Más allá de sus obligaciones legales, las universidades deberían contar con organismos de seguimiento que evalúen el desempeño del software de e-proctoring a través de la retroalimentación recibida por parte de los estudiantes. Si durante un período sostenido este presentara problemas que afectan la evaluación o causan perjuicios no motivados a los estudiantes, debería considerarse su abandono.

8.2 Para los proveedores de software de e-proctoring

- Todos los proveedores de software de e-proctoring -especialmente los constituidos en la Unión Europea- deberían realizar un examen, aunque sea superficial, evaluando si las universidades que han requerido sus servicios cumplen con las normas de protección de datos que resultarían exigibles a sus pares en sus respectivos países.
- Si no realizan el examen o habiéndolo realizado detectan posibles incumplimientos, podrían tomar un rol más proactivo y hacer pública la relación contractual entre ambos (Por ejemplo, en su sitio web). Esto con el fin de permitir que los posibles

afectados tengan mayor información y, llegado el caso, puedan tomar las acciones que consideren correspondan contras las universidades.

9. Bibliografía

Para la realización de este trabajo consumimos todo tipo de fuentes, todas ellas disponibles en Internet. Aunque es posible entender todo este trabajo con las notas al pie de página y los enlaces que se encuentran en la base de datos donde se mapearon las universidades, recomendamos encarecidamente las siguientes lecturas con el fin de ampliar el horizonte de entendimiento sobre este tema.

Sin ningún orden específico, las fuentes consultadas fueron:

Noticias y artículos de blog sobre e-proctoring

1. "Students Are Pushing Back Against Proctoring Surveillance Apps", Electronic Frontier Foundation (EFF)
2. "Is the fight against cheating during remote instruction worth enlisting third-party student surveillance platforms?", Inside Highered
3. "¿Cómo garantizan estas universidades que no haya fraudes en los exámenes de admisión virtuales?" Diario El Comercio
4. "Respondus, un software de vigilancia para exámenes, desembarca en la Universidad Nacional de Córdoba", La Izquierda Diario
5. "Startups: ¿Es tan fácil copiar en un examen virtual? Esta herramienta vigila a los alumnos", Diario El País
6. "La supervisión inteligente de las evaluaciones en línea", UPC
7. "Tras verse obligadas a dar las clases online, las universidades deberán afrontar un nuevo reto: hacer los exámenes por Internet", Xataka
8. "¿Quién anda ahí? Evitar la suplantación en e-learning", PUCP
9. "Llegan los exámenes virtuales: así se evita que los alumnos hagan trampas", Diario El País
10. "Las universidades públicas usarán un sistema de reconocimiento facial para evitar fraudes en los exámenes", Infobae
11. "La educación virtual es otra cosa", Agencia de Noticias Ciencias de la Comunicación - UBA
12. "Polémica en la Universidad de Granada por el proctoring", Nius Diario
13. "Tecnología y Sociedad: El lado oscuro del software que vigila a los alumnos para que no copien", MIT Technology Review
14. "Reconocimiento facial en exámenes online: ¿es legal que te graben?", UNIR
15. "SUNEDU supervisará educación no presencial de universidades ante las medidas de control y prevención del COVID-19", SUNEDU

Videos con experiencias de uso de e-proctoring

16. Webinar: Herramientas de eProctoring en las Universidades Iberoamericanas, MetaRed
17. SIU-Quechua: uso para evaluaciones y otros procesos, SIU
18. Resumen de la Segunda Jornada Online para Compartición de Experiencias de Modelos de Evaluación Alternativos "Foro Online de Experiencias ante la Suspensión de la Actividad Docente Presencial en Universidades Españolas por el COVID-19, Universidades Españolas

Estudios y otras investigaciones relacionadas

19. Implementation of E-Proctoring in Online Teaching: A Study about Motivational Factors, Varios autores
20. Eyes on Integrity: A Comparative Look at Online Proctoring Models, Software Secure
21. La universidad entre la crisis y la oportunidad: Reflexiones y acciones del sistema universitario argentino ante la pandemia, Paulo Falcón (compilador)
22. Estado de la situación de las tecnologías aplicadas a la enseñanza y el aprendizaje en la educación superior argentina, Universia
23. Proctoring: protocolo de aplicación en CEA Medicina, Universidad de Chile
24. Recomendaciones UMC para el trabajo académico on-line, Universidad de Chile
25. Informe acerca de la compra y de las implicancias de la implementación del software Respondus en la UNC, Universidad Nacional de Córdoba
26. Riesgo de fraude en plataforma Moodle y evaluaciones asincrónicas en la Licenciatura en Lenguas Extranjeras con énfasis en inglés, CEAD José Acevedo y Gómez, (UNAD), Sandra Cáceres
27. Investigación sobre el aparente daño del Respondus LockDown Browser (LDB) en los dispositivos de los estudiantes, Universidad de Puerto Rico
28. El ámbito de aplicación del habeas data en la legislación argentina, Mario Masciotra
29. Desafíos de la biometría para la protección de los datos personales, ADC
30. Régimen Legal nacional de protección de datos personales, Biblioteca del Congreso Nacional de Chile
31. El Estado de la Protección de Datos Personales en Chile, Derechos Digitales

10. Bases de datos

Tal como se señaló en las secciones anteriores, para llevar a cabo el mapeo de universidades, de software de e-proctoring y recopilar la normativa aplicable, procedimos a elaborar bases de datos (¡sin datos personales!). A lo largo de este trabajo hemos presentado algunos cuadros informativos derivados de dichas bases de datos, pero consideramos que bien valía la pena hacerlas de acceso abierto por dos motivos: Para que los datos aquí presentados puedan ser corroborados y para que sean útiles para otros investigadores.

A continuación podrán encontrar enlaces a las siguientes bases de datos:

1. "Mapeando el uso de software de e-proctoring en universidades de Latinoamérica": Base de datos que contiene el mapeo consolidado y por país del uso de software de e-proctoring. También se ha incluido el mapeo inicial de todas las universidades de los tres países analizadas.
2. "Datos tratados por cada tecnología": Base de datos que contiene una compilación de los datos personales tratados por cada tecnología. También las tecnologías identificadas en cada uno de los softwares de e-proctoring.
3. "Legislación de privacidad aplicable al uso de software de e-proctoring": Base de datos que contiene el mapeo de la legislación de privacidad consolidada y por país en relación al tratamiento de cada uno de los datos que tratan los softwares de e-proctoring.