Proyecto
Aspectos Éticos

privacidad y seguridad en la educación

Participantes:

Iván Álvarez
Andrea Siles
Edgar Andrés

Abstract

Este artículo busca exponer tres casos éticos relacionados con el ámbito de la educación, primeramente se introduce el dilema ético para posteriormente analizarlo, por último añadimos nuestra conclusión acerca del análisis.

En cuanto a las temáticas trabajadas en el trabajo se encuentran algunas de especial relevancia en cualquier ámbito de la sociedad contemporánea: Seguridad de la información, Privacidad y Seguridad de las personas.

Mediante el proceso descrito previamente pretendemos aportar líneas generales de interpretación para posteriores análisis éticos, y aportar distintos puntos de vista para que cualquiera con intención de informarse acerca de la educación, entienda los distintos aspectos subyacentes a la problemática.

Llegados a este punto mencionamos nuestro trabajo antecedente sobre la contextualización social de la educación para completar la comprensión acerca de técnicas innovadoras de enseñanza, y sus distintos problemas de despliegue y planificación, esperamos sea de utilidad para entender la educación desde diferentes perspectivas.

Caso 1:

An Ethics Case Study by Irina Raicu

Introducción

Las universidades cada vez analizan y recolectan mayor cantidad de información sobre sus alumnos para diversos propósitos, en la universidad de Arizona por ejemplo, un investigador analizó los giros de las localizaciones de las cartas ID por el campus con el fin de reconocer rutinas y relaciones entre estudiantes, y esto relacionarlo con la probabilidad de que vuelva al campus tras su primer año de estudios.

Resultados:

en la página web de la Universidad, una reseña resaltada muestra la precisión predictiva del modelo y entra en detalles acerca del experimento, el estudio mostró:

En cooperación con UA IT 'University of Arizona Information Technology', el investigador recolectó y analizó información sobre el uso de la carta de acreditación de estudiantes de primer año durante tres años seguidos, se utilizó esta información para generar grandes redes enlazando qué estudiantes han interactuado entre sí y con cuánta frecuencia.

Por ejemplo, si el estudiante A utiliza su tarjeta el la misma localización y tal vez a parecido tiempo que el estudiante B, esto puede sugerir una interacción social entre ambos, asimismo se estudiaron los cambios de interacción a lo largo del tiempo.

Existen gran cantidad de medidas extraíbles de dichas redes como por ejemplo el tamaño de su círculo social, y es analizable si dicho círculo crece o decrece, así como la fuerza de sus lazos con sus compañeros.

Método

El investigador informó que la información utilizada era anónima, también añadió que el estudio sería revelado para mejorar la retención de estudiantes con cuyos consejeros académicos se comparten los resultados. Además se postula la idea de añadir información de los casi 8000 puntos de acceso WIFI del campus para recrear con mayor precisión las rutas y el comportamiento.

el artículo también citó al rector asistente de la UA para investigación institucional el cual explicó que aunque el análisis de las tarjetas de acceso de los estudiantes no se

utilizaba para retener a los actuales estudiantes, se aprovechaban junto a la información de los 800 puntos de información para crear indicadores que informan cómo apoyar al alumnado en los programas lectivos y de prácticas.

Repercusión

El artículo estimulo variedad de conversaciones en los medios y diversos artículos en medios de difusión masivos. Uno de ellos publicado por Arizona Public Media y titulado “La investigación de las tarjetas de acreditación de estudiante genera consternación sobre la privacidad”, en él se cita a un profesor de ciberseguridad de la Universidad el cual explica que imparte clases acerca de la privacidad digital y habló a sus estudiantes sobre ello. Los más ávidos en tecnología piensan que siempre se recolecta información sobre ellos porque están dentro del sistema y eran completamente inconscientes de toda la información que podrían haber sido recolectada sobre ellos.

Posteriormente EDUCAUSE publicaba un artículo titulado “Sobre la mesa: El uso responsable de información sobre estudiantes en educación superior”, en él se detallan las conclusiones de la recolección por parte de académicos, científicos industriales, administradores de universidades, oficiales de gobierno y representantes altruistas, los cuales en 2016 se reunieron para considerar un sistema ético y responsable de uso de información estudiantil en educación superior, uno de sus principios sería la transparencia y los expertos declaran que:

La claridad del proceso y la evaluación es el distintivo de los sistemas de educación humanos y deben ser mantenidos aunque crezcan y se complejizan, los estudiantes tienen el derecho de :

- Conocer claramente la información que los describe así como su naturaleza, esto debe garantizarse en su institución y es relevante para terceros.
- Deben ser notificados de la manera en que son investigados.
- Deben ser capaces de solicitar revisiones de dicha información mediante sistemas de gobierno claramente articulados.

De todas maneras el artículo no insta a que los estudiantes detengan dicha recolección puesto que las organizaciones educacionales tienen la obligación de estudiar la información estudiantil para promover que sus entornos educacionales sean más efectivos y contribuyan mejor al conocimiento general.

Por contra, cuando preguntamos a los reporteros de Arizona Public Media sobre las complicaciones acerca de la privacidad de la información, el Rector de la Universidad para Investigación Institucional sugirió que el uso de la información de las tarjetas de acreditación se convirtió en parte de los esfuerzos para retener el talento, movimiento predecesor a las comunicaciones entre Campus universitarios aunque los estudiantes deberían tener la posibilidad de detener su monitorización si lo deseasen.

Como deberiamos reaccionar ante el uso y la recoleccion de informacion de los estudiantes por partes de Institutos y Universidades como esfuerzos para mejorar la retención del talento y el éxito académico. Cómo pueden estas acciones ser percibidas desde el prisma ético de utilidad, derechos, justicia, virtud y bien común.

Análisis Ético

Para el análisis del caso de estudio presentado previamente se utilizará el artículo 'Summary of the qualities of a good ethical judgment, Michael McFarland, S.J' , según el cual deben rellenarse las siguientes preguntas:

- ¿ Cuales son los hechos?

  El caso nos expone la recolección y uso de datos personales de alumnos por parte de las instituciones educacionales.

- ¿Quién está involucrado?

  El el caso están involucrados : El investigador de los hechos, el rector de investigación institucional, la Universidad de Arizona, las Autoridades Educacionales, los expertos de seguridad y las autoridades legisladoras.

- ¿Cuales son las posibles alternativas?

  Por un lado (A) se puede seguir con la práctica habitual de la recolección y uso de datos como se planteaba hasta el momento, por otro lado (B) se puede modificar dicha práctica para respetar el derecho de los estudiantes, y por último (C) puede cesar la práctica por completo.

- ¿Cuales son los beneficios / costes de cada alternativa?

  En el caso de (A) los beneficios son cantidades ingentes de información y capacidad de investigación lo que supone en grandes avances en los programas de formación y el abaratamiento de costes del sistema informacional a costa de la vulneración de los derechos del estudiante y grandes críticas sociales, por otro lado (B) tiene como beneficios cantidades moderadas de información, una investigación moderada, el respeto de los derechos de la mayoría de partes involucradas y avances moderados o pequeños en los programas de formación a coste de críticas menores por parte de escépticos / contra sistemas y mayores costes para mantener el sistema informacional, por último (C) tiene como beneficios la nula crítica, el respeto de todas las partes involucradas y la inexistencia de sobrecostes por mantenimiento del sistema a costa del nulo o escaso avance en los programas de formación.

- ¿Cuales son los derechos de cada involucrado?

  El investigador de los hechos tiene derecho a trabajar en condiciones razonables y a exponer su ética a sus superiores en cuanto a los temas que investiga, el rector de investigación institucional tiene derecho a la toma de decisiones en ámbito Institucional de Investigación, la Universidad de Arizona tiene el derecho de lograr la excelencia académica mediante su gestión interna, las Autoridades Educacionales tienen el derecho de regular toda actividad educacional, los expertos de seguridad tienen el derecho de ser tenidos en cuenta en todo lo relacionado con su área de expertitud 'expertise' y las autoridades legisladoras tienen el derecho de regular estas prácticas.

- ¿Existen analogías para entender mejor los hechos?

  Apps and Privacy, Irina Raicu, como en este caso la recolección de datos y su tratamiento no fueron transparentes lo que supuso penas elevadas para la empresa y la obligación penal de modificar su sistema, en este caso al ser una institución lo que se ha perdido es el renombre por crítica social y además se ha tenido que modificar el sistema.

- ¿Qué leyes son aplicables?

  En este caso son aplicables las siguientes leyes del estado de Arizona :

  Ariz. Rev. Stat., § 18-551 & 18-552 *Data security breaches.*

  Ariz. Rev. Stat., § 36-3801-3809 *Provisions of health information organizations.*

  Ariz. Rev. Stat., § 44-1373-1373.03 *Restricted use of Personal Identifying Information.*

  Ariz. Rev. Stat., § 44-7012 *Electronic records retention*

  Ariz. Rev. Stat., § 44-7601 *Discarding and disposing of Personal Identifying Information Records.*

  Ariz. Rev. Stat., § 44-7701 *Retention of customer information; transmission to third parties prohibited.*

- ¿Existen estándares y normas aplicables?

  Sí existen estándares como podría ser la ISO:27001 gestión de seguridad y normas a nivel internacional como podría ser la ley RGPD.

- ¿contexto social y como afecta?

  En este caso el contexto se ubica geográficamente en el Estado de Arizona dentro de los Estados Unidos, en ámbito jurídico mediante la OTAN se compromete a cumplir el RGPD y cada estado se responsabiliza de legislar de manera autónoma resultando en las leyes redactadas previamente.

  En cuanto al contexto social EE UU es un país que se caracteriza por su Capitalismo voraz y por tanto una gran competitividad en todos los sectores de la sociedad. Asimismo las desigualdades sociales provocan gran desinformación en estratos menos pudientes cuyos derechos se vulneran con mayor facilidad.

- ¿Cuales son las responsabilidades de los involucrados?

  El investigador de los hechos tiene la responsabilidad de tratar los datos garantizando principios CIDAN, el rector de investigación institucional tiene la responsabilidad de velar por la excelencia de la investigación, la Universidad de Arizona tiene la responsabilidad de velar por los derechos de sus estudiantes, las Autoridades Educacionales tienen la responsabilidad de regular las actividades educacionales, los expertos de seguridad tienen la responsabilidad de velar por la seguridad de la información y las autoridades legisladoras tienen la responsabilidad de legislar de acuerdo a las necesidades sociales.

Conclusión

El tema del tratamiento de datos personales independientemente del ámbito, es delicado, y aquellas empresas / organizaciones que pretendan salvaguardar tanto la ley como los intereses de sus clientes, deben cumplir las recomendaciones de la norma ISO:27001 así como las normas establecidas internacionalmente mediante el RGPD para minimizar los riesgos relacionados con la recolección y tratamiento de la información.

Lo postulado previamente es crucial para el sector privado ya que las regulaciones son más férreas, en el caso del público no solo se deberían cumplir dichas recomendaciones sino que los organismos reguladores deberían tomar parte para cubrir lo antes posible todos los posibles vacíos de la solución propuesta.

Por último destacar que el erróneo o innecesario tratamiento de datos personales en la práctica termina conllevando grandes penas económicas y judiciales para los responsables por tanto el juicio ético de estas actividades resulta crucial para garantizar la sostenibilidad empresarial.

Caso 2:

Privacidad, tecnología y medidas en la escuela: Un estudio de caso de Ética

Introducción

Este articulo esta basado en la efectividad de las tecnologías para la seguridad de los estudiantes en las escuelas ,universidades y en el área de la educación en general y la privacidad de estos.

A raíz de los de los recientes incidentes ,como tiroteos o atentados,que han atemorizado a muchos,algunas escuelas y universidades están implementando medidas técnicas con la meta de reducir tales incidentes.

Se están lanzando por medio de algunas empresas diversos servicios para su uso en entornos educativos .Algunos de ellos incluyen tecnología facial y herramientas de monitoreo en redes sociales que utilizan el análisis de sentimientos para tratar de identificar publicaciones de estudiantes en redes sociales que puedan presagiar acciones violentas.

Un artículo del New York Times ha señalado que más de 100 distritos escolares públicos y universidades ha contratado compañías de monitoreo de medios sociales en los últimos 5 años.Según el articulo los costes que se presenta de dichos servicios varían desde miles de dólares hasta decenas de miles por año, y los programas son implementados por distritos escolares sin notificación previa a los estudiantes y padres o juntas escolares.

Las publicaciones analizadas en redes sociales que son monitoreados y analizados son públicas y las herramientas de monitoreo utilizan algoritmos para analizar las publicaciones.Según la revista Wired las escuelas son publicaciones de medios sociales de estudiantes de minería en busca de signos de problemas.

Se ha demostrado según una investigación que es difícil para los adultos interpretar fácilmente el contenido en las comunidades en línea,y se ha llegado a un problema sobre las nuevas herramientas que utilizan algoritmos que no pueden comprender el contexto de lo que se está viendo.*(Amanda Lenhart)*

También se ha expresado otro problema sobre la efectividad de los programas de monitoreo y sobre el impacto que podría tener en la relación entre los estudiantes y los administradores .

La organizaciones educativas quieren demostrar a sus comunidades que están haciendo todo lo posible por la seguridad de sus estudiantes.

Análisis Ético

- ¿Cuales son los hechos?

  Los hechos son la falta de seguridad a raíz de los recientes tiroteos en colegios y universidades.
  Los distintos programas implementado por distritos escolares sin notificación previa a los estudiantes , padres y juntas escolares.
  Dificultad de los adultos de interpretar fácilmente el contenido en las comunidades en línea.
  El uso que se hace de los datos de estos estudiantes por medio de los administradores de los sistemas tecnológicos.

- ¿Quién está involucrado?

  Están involucrados:
  Colegios,Universidades
  Ministerio de educación
  Compañías de monitorización
  Estudiantes,profesores,padres,juntas escolares
  Administradores

- ¿cuales son los posibles respuestas al hecho?

  Las posibles respuesta a estos hechos son:La Contratación e implantación de sistemas de seguridad,como compañías de monitorización .

- ¿Cuales son los beneficios y costes de cada alternativa?

  Los beneficios de la implantación de herramientas tecnológicas es la seguridad de los estudiantes y la productividad.
  Los costes de esta alternativa vienen en costes económicos de implantación y vulnerabilidad de los datos de los interesados.

- ¿cuales son los derechos de cada involucrado?

  Los derechos para :colegios ,universidades ,estudiantes,profesores ,padres,juntas escolares son:el ser notificados de todos los servicios que se implementan ,la usabilidad ,accesibilidad a sus datos y por supuesto prestar consentimiento para el uso de sus datos.
  Derecho del ministerio de educación:Derecho a establecer parámetros para la seguridad para el bien común de sus estudiantes.
  Derechos de las compañías y administradores de los sistemas tecnológicos:Trabajar con libertad dentro de unos parámetros éticos con los datos recogidos.

- ¿Existen analogías para entender mejor el caso?

  Es análogo al caso de la compañía Apple en la que prevaleció su cliente frente al bien común.

- ¿Qué leyes son aplicables?

  Algunas leyes aplicables de protección de datos en E.E.U.U son :
  HIPAA(Ley de Transferibilidad y Responsabilidad del Seguro Sanitario)
  FACTA(Ley Federal de Transacciones Crediticias Justas y Exactas)
  COPPA(Ley de Protección de la Privacidad de Menores de los Estados Unidos)

8.¿Existen estándares y normas aplicables?

Sí existen estándares como podría ser la ISO:27001 gestión de seguridad y normas a nivel internacional como podría ser la ley RGPD.

9.¿Como es el contexto social y como afecta?

El artículo está basado en un contexto social estadounidense,en la cual cada estado tiene su propia legislación de protección de datos y solo el estado de california se asemeja mucho a la RGPD.
Las normas de protección de datos en E.E.U.U deben estar regidas a las leyes del estado donde se realiza la recogida de datos,en el caso de recopilar datos de ciudadanos europeos se deben regir a la RGPD que entró en vigor en 25 de mayo 2018.

10. ¿Cuáles son las responsabilidades de las implicados?

Enfocarlo en general.

Ministerio de educación

La misión del Departamento de Educación de Estados Unidos es garantizar la igualdad de acceso a la educación, promover la excelencia en la educación en todo el país y mejorar el sistema educativo con el programa “Que Ninguno Se Quede Atrás”.

Compañías de monitoreo:

Las compañías de monitoreo tiene la responsabilidad de prestar sus servicios con calidad, disponibilidad y con la adecuada presentación de contratos de consentimiento para la accesibilidad a los datos de los individuos para evitar fines ilícitos.

Por otro lado los padres,profesores,juntas escolares y estudiantes unas de sus responsabilidades aceptar lo que los organismos proveen, acogerse a la norma,instruirse en la norma.

Conclusión:

Como conclusión se nos presentan distintos escenarios sobre seguridad ,privacidad de datos y eficacia de la tecnologías usadas.
Por un lado observamos en el artículo la falta de privacidad de los datos de los alumnos, de notificación sobre el uso de sus datos y la poca efectividad de los herramientas tecnológicas ,debido a un contenido difícil de interpretar para los administradores de estas tecnologías.

Reflexión personal

Puedo destacar un problema de conflicto ético entre seguridad y privacidad, hasta qué punto es aceptable este uso de tecnología para la seguridad frente a estos acontecimientos y como esta herramientas pueden ser inseguras a la vez por la falta de privacidad de los datos de las personas participantes, en el sentido de que estamos dejando todos nuestros datos a empresas y a personas que pueden utilizarlos con fines ilícitos.

Con respecto a las herramientas tecnológicas, me surge una duda con respecto a su efectividad, a la hora de recoger,trabajar,analizar la información por el contexto en el que se basan, estamos hablando de una época en la que los jóvenes piensan que es bueno,escribir mal, expresarse mal, muchos de los comentarios que podemos ver en distintas redes sociales carecen de un mínimo de sentido.

Caso 3:

Apps and privacy

Introducción

La privacidad de los usuarios en distintas aplicaciones móviles, puede verse gravemente comprometida debido al mal uso y mala gestión de los datos que tanto las empresas desarrolladoras, como grandes corporaciones (Apple, entre otras) hacen, no cumpliendo la normativa vigente, y no realizando un análisis más exhaustivo de las aplicaciones que se encuentran en sus propios mercados de cara a los usuarios.

Por parte de las empresas desarrolladoras, no ofreciendo una transparencia clara del funcionamiento de sus aplicaciones, sobre todo si se acceden a los datos personales de los usuarios.

En este caso, veremos un ejemplo concreto de esto que acabamos de mencionar, así como los efectos a nivel legislativo, y las consecuencias para la empresa, que la falta de miramiento en la información con la que se trata, puede acarrear.

Análisis Ético

Para el análisis del caso de estudio presentado previamente se utilizará el artículo ‘Summary of the qualities of a good ethical judgment, Michael McFarland, S.J’ , según el cual deben rellenarse las siguientes preguntas:

- ¿ Cuales son los hechos?

  El caso que tratamos, expone la necesidad de gestionar de una forma cautelosa y ante todo segura los datos, así como la solicitud de permisos al usuario final, indicando de manera clara y concisa, qué información necesitará , con qué fin, y como se encargará de proteger ésta.

- ¿Quién está involucrado?

  El el caso están involucrados : La propia aplicación “Path”, Apple por no realizar un control exhaustivo de las aplicaciones que ofrece en su Apple Store, el poder judicial Estadounidense, los más de 3000 usuarios finales afectados por la App, la empresa desarrolladora de la aplicación, y el bloggero de Singapur, el cual reportó el uso indebido de los datos que hacía la app.

- ¿Cuales son las posibles alternativas?

  Las alternativas posibles son sencillas e implicaría la no existencia de los hechos que causaron toda la problemática: Por un lado, solicitar el permiso explícito de los usuarios para el acceso a los contactos de su agenda, indicando en todo momento la finalidad del acceso a esa información, y por otro lado, encriptar dicha información, tanto para su envío a los servidores, como para su posterior almacenamiento.

- ¿Cuales son los beneficios / costes de cada alternativa?

  El coste de solicitar permiso explícito de los usuarios, entendemos que tendría un coste ínfimo, y totalmente asequible, puesto que no implicaría ir más allá de redactar unas pocas líneas adicionales en el formulario de conformidad para el uso de la aplicación.
  Por otra parte, el coste de encriptar los datos, indudablemente sería mayor que la solicitud de permisos a los usuarios, sin embargo, estaríamos hablando de un coste muy inferior a la sanción que la empresa obtuvo por no haberlo hecho, y de un proceso totalmente imprescindible para tratar con datos tan delicados como son la agenda de contactos de sus usuarios.

- ¿Cuales son los derechos de cada involucrado?

  En este caso particular, los derechos totalmente violados, han sido los de los usuarios finales, puesto que se estaba obteniendo información que ellos no habían permitido, y que ni siquiera conocían, por tanto, los únicos afectados han sido los usuarios. Ni la empresa, ni Apple, han visto sus derechos vulnerados, puesto que son los únicos culpables de lo ocurrido.

- ¿Existen analogías para entender mejor los hechos?

  Existen muchos casos similares que implican el acceso a datos de usuarios sin permiso, Facebook y Google son algunos ejemplos de grandes corporaciones que se han visto (y se ven) envueltas en grandes escándalos por estos temas, por tanto, no es, ni será ninguna novedad que la privacidad de los usuarios es un tema candente y que necesita de una protección a nivel legal, mucho más estricta.

- ¿Qué leyes son aplicables?

  En el propio artículo, se hace alusión a la ley quebrantada y que impuso una sanción económica de 800.000$: La ley de protección de la privacidad online de los niños, por sus siglas en Inglés (COPPA)

- ¿Existen estándares y normas aplicables?

  Sí, existen estándares como podría ser la ISO:27001 gestión de seguridad y normas a nivel internacional como podría ser la ley RGPD.

- ¿contexto social y como afecta?

  Los hechos como tal, tienen lugar en EEUU, sin embargo, la aplicación generó problemas a miles de usuarios alrededor del mundo, por tanto, el contexto social es a nivel global, y las personas afectadas podrían estar en cualquier país.

- ¿Cuales son las responsabilidades de los involucrados?

  En primer lugar, la empresa desarrolladora de la App, tiene la responsabilidad de garantizar la seguridad de los datos de sus usuarios, respetando la ley vigente, y respetando el contrato de Apple, para colocar su aplicación en la App Store.
  Por parte de Apple, tiene la responsabilidad de asegurar que todas aquellas aplicaciones que se encuentren en la App Store, cumplen con las normas y condiciones exigidas para poder ser puestas de cara al público.

Conclusión

La seguridad de los datos de los usuarios es un tema extremadamente serio, que debe tratarse con extremo cuidado. Los usuarios deben estar protegidos por leyes elaboradas concretamente para estos temas.

Además, es una obligación moral y legal por parte de las empresas desarrolladoras, mostrar un mayor grado de transparencia en cuanto al uso que dan de los datos de los usuarios, y por último, deben ser las grandes corporaciones las que actúen como barrera protectora, para garantizar que las aplicaciones que se encuentren en sus mercados, sean seguras para el uso de todos los tipos de usuarios posibles.

De no cumplirse estas reglas, las sanciones deberán ser ejemplares, siendo así medidas disuasorias que sirvan de ejemplo para futuros casos, donde otras empresas desarrolladoras, se encuentren ante la posible falta de moralidad en el desarrollo de sus aplicaciones.