Mancini Perez, Ian Lihuel Demian
75642/9

El Internet como recurso para hacer frente a la pandemia: un arma de doble filo

Taller de Diseño Multimedial V

Profesor Titular:
Joselevich Puigross, Federico

Ayudantes:
Toledo, Elizabeth
Mata Lastra, Nicolas

Año 2020

Índice

Palabras Clave

Privacidad, COVID-19, trabajo remoto, Internet, phishing, redes sociales, minería de datos, big data, Internet de las Cosas, analíticas web, ciberseguridad, educación a distancia

Hipótesis

Debido a la pandemia por COVID-19, muchas personas están migrando al espacio digital para poder continuar con diferentes actividades que antes llevaban a cabo en el mundo físico, pero por su falta de experiencia con las computadoras, pueden encontrarse fácilemente en situaciones en las que su privacidad vulnerada, pudiendo sufrir diferentes tipos de perjuicios

Problemas específicos

- ¿De que maneras afectó la pandemia a la rutina de las personas, y que grado de importancia cobró Internet en este contexto para personas que antes lo utilizaban de forma tangencial?
- ¿De que maneras y que efectos puede tener la violación de la privacidad en Internet?
- ¿Qué agentes buscan vulnerar la privacidad de las personas en Internet y con qué fines?
- ¿Qué es la minería de datos y qué importancia tiene con respecto protección privacidad?

- ¿Qué herramientas o técnicas se pueden utilizar para pasar a estar en una posición en la que la privacidad se vuelve difícil de vulnerar?

Resumen de 30 palabras

Con la pandemia por COVID-19, muchas personas migraron al espacio digital y suponen un nuevo vector de ataque para hackers y compañías de IT, que pueden vulnerar su privacidad

Resumen

La presente investigación tiene la intención de hacer un repaso sobre el impacto que tuvo y tiene la pandemia de COVID-19 sobre la vida de las personas a nivel global, y sobre el rol fundamental que el Internet pasó a jugar para mitigar los efectos de la pandemia tanto en el plano social como en el económico cuando las medidas de "distanciamiento social" y las cuarentenas entraron en vigencia. Esta situación lleva a que muchas personas que nunca habían tenido que usar computadoras (o que las habían usado tangencialmente) tengan que pasar muchas horas al día frente a una pantalla, ya sea por motivos laborales, educativos o sociales.

Esta nueva ola de usuarias y usuarios supone un vector de ataque para hackers, que pueden abusar de la desinformación y el miedo a la enfermedad para vulnerar sus sistemas informáticos, (y, como consecuencia de esto, otros aspectos de su vida privada), pero también son una nueva fuente de datos por minar por parte de las empresas que son dueñas de los servicios de Internet más utilizados (Google, Facebook, Amazon, Microsoft, Netflix, etc.), que aseguran brindar un amplio abanico de opciones para proteger la privacidad de quienes consumen sus productos, pero que por detrás de ese discurso y, a partir de diversas estrategias como lo son el uso de "Términos y Condiciones de Servicio", son quienes más provecho sacan de la situación. La privacidad es mucho más que un conjunto de interruptores que permiten ocultar que fotos pueden ver nuestras amigas y amigos en las redes sociales. ¿Podemos confiar en que estas compañías no van a usar nuestros datos con intenciones maliciosas con el mero fin de obtener rédito económico? Diferentes ejemplos del pasado indican que este no es el caso, y las analíticas de la web y la minería de datos pueden ser utilizadas como herramientas para controlar a las personas a partir de la personalización de información que se les presenta cuando navegan en Internet.

1. Repercusiones de la pandemia en el mundo y el rol de Internet

Frente a la situación de la pandemia de COVID-19, muchas personas experimentaron un cambio de paradigma radical en sus vidas debido a las medidas adoptadas por los gobiernos de los distintos países, que en muchos casos

desembocaron en cuarentenas estrictas. Frente a este panorama, las trabajadoras y trabajadores que tuvieron más suerte y que asistían todos los días a un lugar para poder llevar a cabo sus tareas, tuvieron que adaptarse modalidad de trabajo remota de forma abrupta, mientras que muchas y muchos más perdieron su trabajo, sin posibilidad de hacer nada al respecto. Estudiantes que participaban de clases presenciales (y que tanto ellas y ellos como sus instituciones educativas disponían de los recursos necesarios) continuaron sus procesos de aprendizaje a través de Internet. Las instituciones que brindaban educación de manera asincrónica en este medio (como Coursera o edX) desde antes de la pandemia vieron un crecimiento vertiginoso en la cantidad de inscripciones en sus plataformas. Algo similar ocurrió con los servicios de videoconferencias (Zoom, Google Meet, etc.), que vieron crecer el número de usuarios hasta diez veces más que el habitual antes de la pandemia (De', Pandey & Pal, 2020). Términos como "la nube", "IoT" (Internet de las Cosas), "big data", "blockchain", "inteligencia artificial", "aprendizaje de máquina" y "aprendizaje profundo" están pasando a formar parte del léxico con el que nos encontramos a diario, ya sea en conversaciones casuales con otras personas, en redes sociales o en noticias, y son parte de las herramientas de las que se pueden usar hacer uso para enfrentar los desafíos que nos presentó la pandemia.

Estos términos corresponden a herramientas que pueden cumplir roles como son el monitoreo, vigilancia, detección y prevención o mitigar el impacto de la pandemia. El Internet de las Cosas, entre otras cosas, permite a agencias de la salud acceder a datos con respecto a la enfermedad que son recolectados constantemente en diferentes lugares del mundo en paralelo. El "Mapa de COVID-19" de la universidad John Hopkins[1], por ejemplo, hace uso de este tipo de tecnología para poder acceder y distribuir los datos procesados en tiempo real. "Big data" se refiere a conjuntos de datos enormes y a la metodología y tecnología que permite trabajar con estos, que en el caso de la pandemia generan oportunidades para realizar estudios que permiten modelar y predecir la propagación del virus o detectar patrones (no obvios) sobre los efectos de la enfermedad. La inteligencia artificial permite mejorar la detección del virus y los diagnósticos, mejorando la precisión de los tests a la vez que los hacen más accesibles (Ting y col., 2020, p. 1)

Así, el Internet es una herramienta fundamental para combatir la amenaza del virus en tanto provee herramientas para hacerle frente, pero también es motor que permite que una gran variedad de actividades económicas y personales de diversa índole que se llevaban de manera presencial puedan continuar, en menor o mayor medida, a la vez que se minimiza el riesgo de contagio del virus. Además, el uso de Internet en diferentes actividades ociosas, puede aliviar algunos males que hoy son comunes, como el estrés, la ansiedad, la falta de certeza con respecto al futuro, la depresión y otros malestares causados por el miedo a la enfermedad y producto del encierro (en soledad o con familiares). Sin embargo, el uso desmedido también puede ser problemático en tanto algunas actividades como apostar, jugar videojuegos, ver series de televisión, el uso de redes sociales y ver pornografía se pueden convertir en

[1]ver COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU) en: https://coronavirus.jhu.edu/map.html

hábitos adictivos de los cuales puede ser difícil de salir (Király y col., 2020). Además el internet promueve ámbitos de trabajo en el que las empleadoras y empleadores pueden hacer un seguimiento mucho más riguroso y constante que en los espacios de trabajo físicos, que en definitiva producen de tecnoestrés en las empleadas y empleados (De', Pandey & Pal, 2020).

Sumado a esto, la información incorrecta y las noticias falsas que se difunden en las redes sociales, con respecto a la etiología, prevención, secuelas y curas de la enfermedad de COVID-19 ponen trabas a la difusión de información científicamente correcta sobre prácticas que reducen el riesgo de contagio y, a su vez, promueven prácticas que, paradójicamente, pueden incrementar los contagios (Tasnim, Hossain & Mazumder, 2020). El pánico causado por este tipo de desinformación en las redes sociales provocó que las personas hagan compras masivas para prepararse para la cuarentena, dejando afuera a las personas con menos capital que no pueden comprar reservas, entre otras consecuencias como sobredosificaciones de drogas que no están probadas científicamente como curas para la enfermedad, o que las personas con síntomas que se asocian a la enfermedad no se aíslen y terminen contagiando a otras personas.

Más allá de los usos incorrectos que se le pueden dar al Internet, es y seguirá siendo una herramienta valiosa y un pilar fundamental de la sociedad del siglo XXI, pero tampoco hay que caer en la trampa y tomarlo a la ligera como si fuera la panacea, ya que muchas personas no tienen acceso al medio por razones socioeconómicas o culturales, e incluso hay quienes deciden no usarlo voluntariamente, como suele ser en el caso de las pelonas mayores, que tienen dificultad con la curva de aprendizaje que la tecnología conlleva y el ritmo acelerado en el que esta cambia. Una encuesta llevada a cabo en suiza y 16 países de la unión euro pera demostró que el 49 % de las personas mayores de 50 años utiliza Internet, lo que puede desembocar en una doble exclusión hacia ellos, que son aislados por precaución por ser más frágiles y vulnerables al virus que las personas más jóvenes (Seifert, 2020).

Muchas personas que trabajan en condiciones no formales (sin un contrato), como aquellos que lo hacían a través de Uber o Airbnb vieron sus ingresos fuertemente reducidos (De', Pandey & Pal, 2020), y muchas instituciones que dependían casi exclusivamente de su espacio físico y que tuvieron que cerrar sus puertas se vieron en una situación en la su única opción fue generar estrategias para seguir funcionando en el espacio virtual de Internet, diseñando nuevas estrategias para poder seguir cumpliendo con sus tareas, como es el caso de los museos, que al igual que las universidades se movieron al modelo de enseñanza a través de internet o concentraron sus esfuerzos en canales de difusión como las redes sociales (Agostino, Arnaboldi & Lema, 2020).

2. La importancia de privacidad y la seguridad en Internet

Más allá de las posibles implicancias de un uso desmedido de Internet y de la desconexión que se pueda producir con las personas que no lo usan (mencionado en la sección 1), existe otra serie de problemas que son tan antiguos como el Internet mismo y que se pueden asociar con la esfera de la privacidad.

Antes de continuar, sería prudente definir la noción (o nociones) de privacidad y explicar cuál es su importancia. En *Ethics and technology : controversies, questions, and strategies for ethical computing*, Tavani (2013) hace una excelente introducción poniéndola en relación con la cibertecnología. En primer lugar, menciona algunas metáforas que se suelen usar, según las cuales la privacidad es algo que se puede "reducir, sugiriendo que la privacidad se puede entender en términos de un repositorio de información personal que puede ser disminuida completamente o erosionada gradualmente". Esto se puede contrastar con "descripciones de la privacidad como algo que puede ser invadido, donde la privacidad se entiende en términos de una metáfora espacial, una zona, que merece protección". También sugiere que la privacidad "se entiende como algo que puede ser violado cuando se lo piensa en términos de un derecho o de un interés que merece protección legal" (Tavani, 2013, p. 134).

En la página siguiente, Tavani (2013, p. 135) explica cómo la noción de privacidad evolucionó desde el siglo XVIII:

> Inicialmente, la privacidad se entendía en términos de libertad con respecto a la intrusión (física). Más adelante se la empezó a asociar con la libertad con respecto a la interferencia en los asuntos personales, incluyendo la capacidad de tomar decisiones libremente. Más recientemente, la privacidad se ha identificado estrechamente con las preocupaciones que afectan el acceso y el control de la información personal, un punto de vista que también se conoce como "privacidad de la información"

Según Moor, "un individuo tiene privacidad en una situación con respecto a otros solo si en esa situación el individuo es protegido de otros de la intrusión, interferencia y acceso a la información por otros" (Moor, 2000, como se citó en Tavani, 2013, p. 136). Nissenbaum amplía esta noción, dándole un sentido más específico al término "situación" en su modelo de privacidad como "integridad contextual". Ella adecúa la protección de la privacidad a "normas de contextos específicos". Todo lo que ocurre en nuestras vidas pasa por un contexto o "esfera de la vida", como la educación, política, etc. Las normas que afectan estos contextos se dividen en dos categorías: normas de propiedad y normas de distribución: las primeras definen si es apropiado divulgar cierta información en un contexto, mientras que las de distribución limitan el flujo de información dentro de un contexto particular (Nissenbaum, 2004, como se citó en Tavani, 2013, pp. 137-138)

Las preocupaciones en torno a la privacidad no encuentran su origen en el advenimiento de las computadoras, pero es cierto que desde que existen aumentó la cantidad de información que se puede recolectar, la velocidad a la que esta se recolecta, la cantidad de tiempo que esta se puede almacenar y los tipos de información que se pueden recolectar e intercambiar (Tavani, 2013, p. 133)

La privacidad es necesaria para poder alcanzar ciertos fines humanos necesarios, como la confianza y la amistad (Tavani, 2013). Para Moor, la privacidad es importante porque es la articulación o expresión del valor central de la seguridad. Según Johnson, es un bien social importante, porque cuando las personas son observadas todo el tiempo toman la perspectiva de quien las observa, que empieza a influenciar sus decisiones. Esto provoca que piensen antes de actuar, y este proceso de pensamiento erosiona la libertad de las personas. A su vez, esto afecta la democracia (Johnson, 2001, como se citó en Al-Saggaf y Islam, 2012, p. 3). La privacidad también es importante para el amor, el respeto y la dignidad, la libertad de expresión, la autonomía, la soledad, el anonimato y la discreción, la protección de datos y el autoestima (Al-Saggaf & Islam, 2012).

Según la cultura o la nación que se observe, la privacidad tiene diferentes valores: suele tener más valor en las sociedades más democráticas occidentales que en las menos democráticas, como la República de China, en la que se le da más importancia a valores sociales más amplios, que son percibidos como beneficiosos para la sociedad en conjunto. Hay sociedades como la de Israel que es democrática pero en la que la idea de “seguridad nacional” es más importante que la de la privacidad, por lo que no se le puede asignar un valor universal a esta (Tavani, 2013, p. 140).

Volviendo a los tiempos que corren, en Internet y los medios de comunicación masivos podemos encontrar noticias sobre las aplicaciones para celulares que están desarrollando los gobiernos de los diferentes países que, por un lado, son una herramienta valiosa para poder aislar a las personas que estuvieron en contacto con otras personas, pero, en muchos casos, también son polémicas por la cantidad de datos que solicitan y el tipo de datos que solicitan (De’, Pandey & Pal, 2020), además de falta de transparencia con respecto a cómo esos datos son usados y almacenados.

Otro caso que es controversial es el de la telesalud a través de tecnologías de monitoreo de salud remotas (dispositivos físicos o software), que recolectan información sensible sobre el estado de las personas, como lo puede ser un registro de ritmo cardíaco.

La comisión de la Unión Europea desarrolló un conjunto de herramientas para indicar requisitos y brindar guías prácticas para el desarrollo de aplicaciones de seguimiento de contactos y alertas. Estas aplicaciones tienen que cumplir con las normas de privacidad y protección de datos de la UE y tienen que ser instaladas voluntariamente. Además, deben utilizar Bluetooth (preferiblemente) en vez de, por ejemplo, localización por GPS, y deben trabajar con datos anónimos (Gerke y col., 2020, p. 5).

En contraste con las políticas de la UE, en Estados Unidos la Ley de Responsabilidad y Portabilidad del Seguro de Salud (HIPPA) regula el uso y divulgación de la información de salud de las y los individuos, pero solo en el caso de que esa información sea generada por "entidades cubiertas" (Gerke y col., 2020, p. 5). En un contexto en el que la creación de nuevas herramientas para hacer frente a la pandemia tiene un ritmo acelerado, es peligroso que la responsabilidad con respecto a la privacidad de las personas escape a la ley, recayendo esta en los valores éticos de las compañías que manufacturan estos dispositivos o desarrollan software, que fácilmente pueden aprovechar esa área gris para comercializar los datos recolectados, pudiendo dañar a las personas que sus productos deberían resguardar.

3. Analíticas en la web, minería de datos y su riesgo

Esta nueva ola de usuarias y usuarios de computadoras son potenciales participantes de las redes sociales, donde se conduce la actividad de minería de datos más grande.

Las personas utilizan las redes sociales para mantener relaciones existentes, para establecer nuevas relaciones y para comunicarse con personas conocidas con las que ya no tenían trato, y para hacer eso comparten información personal, fotos, videos, pensamientos y sentimientos.

Revelar información privada en las redes sociales es común: se comparten visiones políticas, direcciones residenciales, fechas de nacimiento, libros leídos, películas vistas, escuelas a las que se asistió, orientaciones sexuales, pensamientos sobre sus conocidas/os, vecinas/os, colegas, empleadoras/os. Esta autorrevelación puede ser perjudicial para su privacidad informacional, e incluso puede extenderse a otras esferas como la financiera y física (Al-Saggaf & Islam, 2012)

La minería de datos se lleva a cabo a través de una serie de tareas, como lo son la recolección de datos, el preprocesamiento de esos datos y su posterior transformación a un formato plano, la limpieza de datos corruptos y, finalmente, la extracción de patrones a través de diferentes técnicas o uso de algoritmos.

Esta práctica puede tener un amplio rango de aplicaciones, como en análisis de redes sociales, a partir del cual se pueden extraer patrones que no son obvios sobre los comportamientos de las usuarias y usuarios, segmentación de mercado, agrupamiento de resultados de búsqueda en la web. También se puede usar para realizar marketing directo, en el que se presentan anuncios únicamente a potenciales compradoras/es, y diferentes tipos de análisis de negocios. Por ejemplo, una cadena de supermercados puede utilizar "minería de reglas de asociación", donde parten de un conjunto de transacciones enorme, como podría ser una serie de productos que son vendidos en conjunto (una misma compra llevada a cabo por clientes). La cadena puede analizar ese tipo

de datos (cruzando los datos de diferentes sucursales), para diseñar un supermercado de forma tal que los productos que se compran habitualmente a la vez estén cerca entre sí, para que las personas compren más productos que se suelen comprar en conjunto (Al-Saggaf & Islam, 2012, [34-35).

El caso más controversial y masivo sobre el uso malicioso de la minería de datos en los últimos años fue el de Cambridge Analytica, en el que esta compañía accedió a información de identificación personal de más de 87 millones de personas que se encontraban en Facebook y otros sitios de Internet.

En el 2013, investigadoras/es de la Universidad de Cambridge analizaron el perfil psicológico de voluntarios que tomaron un test llamado “OCEAN” y lo correlacionaron con su actividad en Facebook, lo que les permitió descubrir que el perfil de generado por el test se podía deducir para otras personas a partir de las interacciones en la red social únicamente, sin la necesidad de que se tomen el test. Posteriormente, Global Science Research (GSR) llevó a cabo junto con Cambridge Analytica otro proyecto de investigación que fue el que les permitió acceder a los datos de las personas a través de la interfaz de programación de aplicaciones (API) de Facebook. Cambdrige Analyitica combinó la información de los perfiles “OCEAN” con una serie de datos de diferentes plataformas de redes sociales, navegadores, resultados de votaciones, etc. para poder generar contenido diseñado específicamente para votantes o consumidores con mensajes para modificar su comportamiento. El “Proyecto Álamo” utilizado durante la campaña de Trump en 2016 se basó en el uso de estos mensajes para convencer a las personas de no votar a su oponente. Las personas sin cuentas de Facebook no estaban protegidas, porque el seguimiento de Facebook funciona en cualquier sitio que tenga un botón de “login social” con la red social. Hay muchas formas adicionales de hacer seguimiento de las personas, como son el uso de cookies. Con el monitoreo en tiempo real de anuncios, incluido el reemplazo en tiempo real de contenido para comprobar que los cebos (“click bait”) funcionaban, la campaña de Cambridge Analytica fue capaz de maximizar su impacto y detectar tendencias invisibles en una escala macro (Isaak & Hanna, 2018).

La personalización de experiencias y la búsqueda por la obtención del máximo retorno posible, están teniendo un efecto disruptivo en la economía global, en la estructura de la sociedad, en el flujo de ideas y el acceso a la información. Esta situación es empeorada por los dispositivos del Internet de las Cosas, que cada vez son más ubicuos (Isaak & Hanna, 2018).

4. Conclusión

Es de fundamental importancia preparar a las personas para que entiendan la importancia de la privacidad y sus datos, para que puedan defenderse y que el tener que utilizar la tecnología no se convierta en una causa adicional de malestar que se suma a problemas que la pandemia trae consigo.

El cibercrimen hace uso de ataques de "phishing"[2] destinados a usuarias/os inexpertas/os de computadoras para ocasionar robo o destrucción de datos. Si estas personas son educadas para identificar cuando un correo electrónico o un anuncio en Internet es falso, pueden evitar problemas serios.

El sitio "eeskiri-COVID-19.chm" es un ejemplo puntual de un sitio malicioso que se hizo pasar por un sitio de ayuda sobre COVID-19, que en realidad capturaba todas las pulsaciones del teclado (software conocido como "keylogger") y las enviaba a otro servidor, para poder extraer las contraseñas de las/los visitantes del sitio (Ahmad, 2020).

Además de educar a las personas para que sean capaces de identificar cuando alguien o algo (en el caso de un programa que envíe correos electrónicos automáticamente, por ejemplo) tiene intenciones maliciosas, es importante educar a las personas sobre diferentes herramientas que pueden ayudarlas a proteger su privacidad. Si bien es difícil tomar medidas en ciertas situaciones, por ejemplo, en el caso de gobiernos autoritarios que obligan a utilizar aplicaciones para un rastreo constante, existen una serie de herramientas llamadas Tecnologías de Mejoramiento de la Privacidad[3] que pueden ser utilizadas para combatir el seguimiento en diferentes lugares del Internet (Tavani, 2013, p. 162). Por ejemplo, TrackMeNot[4] es una extensión del navegador que envía falsos positivos y oculta las búsquedas reales de los motores de búsqueda para hacer más difícil la creación de perfiles a través de la minería de datos. HTTPS everywhere[5] es una extensión creada por la Electronic Frontier Foundation (EFF), una ONG que tiene el fin de defender las libertades civiles en Internet, fuerza al navegador a hacer peticiones sobre el protocolo HTTPS, para que los datos enviados desde la computadora hacia el sitio web y viceversa estén encriptados.

Otras prácticas para mejorar la seguridad en Internet son los sistemas de autenticación con contraseñas de doble factor, en el que se debe proveer una contraseña normalmente y un "factor adicional" para demostrar que se es la persona que se dice ser (este sistema es común en los sistemas de "homebanking", mediante el uso de aplicaciones secundarias que generan "tokens") y actualizar el software de las computadoras a las últimas versiones. En el caso de que se esté trabajando remotamente con una computadora ajena (por ejemplo, de una empresa), se pueden utilizar VPNs (Ahmad, 2020), que son redes virtuales que pueden su tráfico encriptado o limitado (para reducir la superficie de ataque). Con respecto a la comunicación por chats, se pueden utilizar servicios que provean cifrado extremo-a-extremo (en la que los mensajes son encriptados por quien los envía y solo quien los recibe puede descifrarlos), para que ningún tercero pueda leerlos criptográficamente seguros, como

[2] En este tipo de ataque, se suelen enviar mensajes a nombre de personas o empresas desde direcciones falsas, para intentar convencer a las personas de que brinden información privada voluntariamente o involuntariamente (por ejemplo, con un enlace que lleva a un sitio falso, que luce igual que uno real, para que la persona introduzca su contraseña)

[3] (en inglés: "PET" o "Privacy Enhancing Technologies")

[4] Sitio web: https://cs.nyu.edu/trackmenot

[5] Sitio web: https://www.eff.org/https-everywhere

Signal[6] o qTOX[7].

En el caso de las redes sociales, un requisito para usarlas es ceder el derecho a la privacidad (al aceptar los términos y condiciones de servicio), pero existen servicios alternativos, muchos de los cuales son federales, personalizables y que son autoalojables [8]. Redes sociales como Mastodon [9], pixelfed [10] y PeerTube[11], que son alternativas (similares) a Twitter, Instagram y YouTube respectivamente, son parte de un conjunto de servidores que usan protocolos para poder comunicar a diferentes instancias entre sí. Por ejemplo, esto permite que una familia tenga un servidor de la red social Mastodon en una de sus computadoras, al cual se conectan diferentes personas de esa familia, pero si algún día decidieran que quieren interactuar con personas que no están registradas en el servidor, pueden conectarse con personas que estén en otra instancia (por ejemplo, de otra familia), van a poder hacerlo sin ningún requisito técnico que no esté cubierto de antemano, y la experiencia sería identica a la de las redes sociales comerciales monóliticas (que tienen un "único servidor", o una sola URL y donde todas las personas pueden interactuar con el resto de las personas).

Otra forma de proteger a las personas es a través de leyes. La visión de la EFF es que estas leyes deberían ser transparentes, en el sentido de que deberían comunicar que tipo de datos y mediante que mecanismos se recolectan los datos, y en el caso de que se muestre algún anuncio (u otro contenido personalizado) explicar qué datos se utilizaron para mostrarlo. Además, las personas deberían poder acceder a los datos que se recolectaron, y tener control eliminar los datos recolectados, o en el caso de dispositivos móviles, tener el control para desinstalar aplicaciones que vienen "preinstaladas" (como suele ser el caso de la aplicación de Facebook, en algunos dispositivos). Adicionalmente, las personas deberían ser notificadas inmediatamente si su información se pierde o si se usa malintencionadamente (Isaak & Hanna, 2018).

Finalmente, me gustaría cerrar remarcando la importancia de que quienes somos más afines con la tecnología deberíamos hacer lo posible por acercar los medios necesarios para que quienes están mas desprotegidas/os en Internet pasen a estar en una posición donde no sean fáciles de vulnerar. El contexto de la pandemia incrementó el caudal de ataques que aprovechan la carencia de alfabetización tecnológica y que juegan con las emociones de las personas que se vieron forzadas a migrar al espacio digital. La situación del cibercrimen y los abusos de poder no van a cambiar (o, por lo menos, no va a pasar en un día) pero lo que podemos hacer es compartir información sobre las prácticas que protegen la privacidad para darle una mano a quienes la necesitan.

[6] sitio web: https://signal.org/

[7] sitio web: https://qtox.github.io/

[8] Esto quiere decir que podemos descargare el software y ejecutarlo en la computadora propia, teniendo control de donde y como se almacenan los datos, a diferencia de usar un servicio que se ejecuta en computadoras ajenas

[9] sitio web: https://joinmastodon.org/

[10] sitio web: https://pixelfed.org/

[11] https://joinpeertube.org/en

A. Obra: museo.red

Este anexo contiene la descripción de la obra que diseñé y desarrollé acompañar las ideas expuestas en este escrito y que será exhibida en la muestra de Artimañas 2020.

Figura 1: Logo de museo.red

La obra consiste de una aplicación web en la que los usuarios se registran con sus cuentas de redes sociales para posteriormente acceder a un espacio tridimensional en el que se encuentra un museo y sus alrededores. Su exposición (llamada “Artificios 2020”) consta de adaptaciones de las obras de Artimañas 2020 (construidas a partir de modelos 3D, imágenes, videos y sonidos según el caso), y de material complementario sobre éstas, como podría ser arte conceptual previo o textos de las investigaciones correspondientes. En cada una de las salas que contienen las obras también hay una computadora con la que se puede interactuar para obtener información sobre la obra a la que corresponde esa sala y un link para navegar hacia el sitio real de la muestra.

El espacio tridimensional se puede recorrer con los controles típicos de un videojuego en primera persona. La idea principal del museo es presentar una suerte de navegación alternativa/experimental al sitio web oficial, pero que acerque más a las personas entre sí en pleno contexto de pandemia, que nos obliga a estar aisladas/os físicamente.

Figura 2: Museo visto por fuera

Cada persona controlará un avatar fantasmal para recorrer el museo. Esto es así para intentar comunicar dos ideas: en primer lugar, el fantasma es intangible, lo cual nos permite pensar en la distancia social (dos fantasmas no pueden tocarse) y, por otro lado, el fantasma no tiene rasgos que lo distingan de otros fantasmas, lo que funciona como una metáfora del anonimato en Internet. Durante su recorrido podrá encontrar fantasmas de otras personas que estén al mismo tiempo recorriendo el museo.

Este museo tiene una arquitectura, por un lado, reminiscente de la de los museos de arte contemporáneo (con características de arquitectura moderna), pero sin intentar representar ninguno en particular; y por otro, de un poliedro geodésico (similar a una esfera, compuesto por triángulos), donde las caras son ventanas y las aristas los marcos que unen a las ventanas. Esto es así por dos razones: busca ser similar al típico símbolo de la World Wide Web, en el que hay un globo con líneas que conectan los polos y líneas paralelas al ecuador (planeta Tierra), y además es una arquitectura que permite que todas sus salas se pueden conectar con un hall común y que estas no estén conectadas entre sí. En el centro de este edificio hay un pilar y una escalera, que permite subir al primer piso, pero también sirve como un punto desde el cual se pueden ver todas las salas, lo que permite pensarlo como una suerte de panóptico.

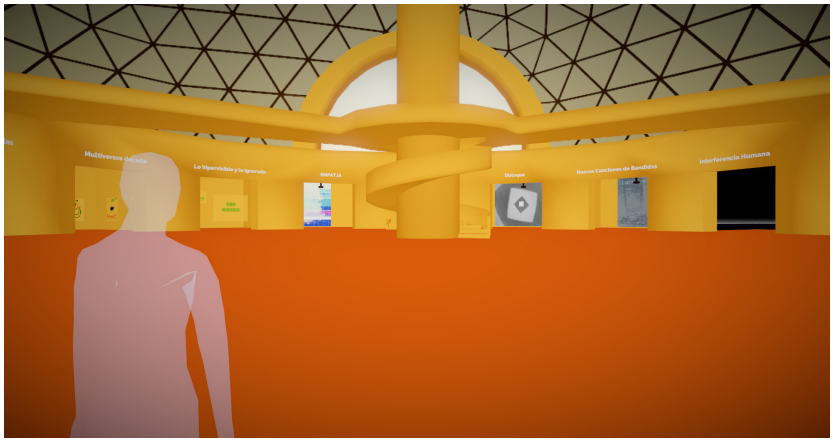

Figura 3: Interior del museo y avatar fantasmal

Estas decisiones arquitectónicas (el panóptico dentro del globo que representa Internet) tienen que ver con la segunda intención de la obra: además de intentar acercar a las personas, busca generar conciencia sobre la importancia de la privacidad en Internet, en vista de que hay muchas personas que últimamente se vieron forzadas a migrar a este espacio. En Internet estamos bajo un escrutinio constante, y en el museo se llevan a cabo diferentes formas de seguimiento de las personas para ilustrar esto:

- Número de visitas
- Número de interacciones

- Cantidad de tiempo pasado en el museo
- Obras con las que mas se interactuó
- Recorrido llevado a cabo (mapa)

Todos estos datos se recolectan y se almacenan por persona, pero también se almacena la suma total de los datos recolectados sobre todas las personas por día, y la suma de todos los datos desde que se abrió el museo.

En el museo hay una pintura que es intangible: si alguien decide saltar en esta, puede llegar a un pasillo escondido que está detrás, y luego de descender por unas escaleras, puede llegar a una habitación repleta de monitores. En estos monitores se mostraría la información listada anteriormente, junto con la dirección de IP de la persona que está viendo los monitores y otros datos personales extraídos de la red social con la que se accedió museo.red:

- Nombre
- Foto de perfil
- Dirección de correo electrónico

Nuestra privacidad se ve comprometida en Internet de formas que son invisibles al ojo inexperto, y la intención de la obra es poner en evidencia esto de una forma sutil y a través de la metáfora, pero ilustrando un caso lo más cercano posible a la realidad de las analíticas de la web.

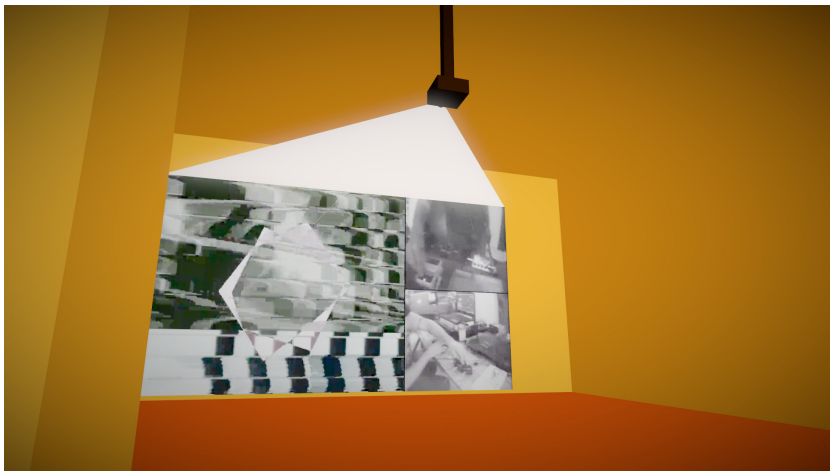

Figura 4: Video-proyección de “Disloque”, una de las obras de Artimañas 2020

Una vez que se accedió a la habitación de los monitores, la persona puede volver al museo y continuar recorriendo el resto de las salas, y podrá regresar cuando quiera a la habitación de monitoreo. La obra no tiene un fin explícito

(como suele suceder en videojuegos convencionales), pero se enviará un correo electrónico a las personas que hayan llegado a la habitación de monitoreo apuntando a diferentes herramientas y recursos para proteger su privacidad en Internet. A su vez, si las personas no llegan a la habitación de monitoreo y se desconectan, a las horas recibirán un correo electrónico con una foto de la pintura a través de la que se accede a esta y un mensaje con formato de adivinanza, invitándolos a volver y que busquen la otra cara del museo. Si logran encontrar la habitación posteriormente, recibirán el correo electrónico informativo mencionado previamente. A su vez, si la muestra termina y no encuentran la habitación, también recibirán el correo electrónico informativo, acompañado de una explicación de cuál era la cara oculta del museo.

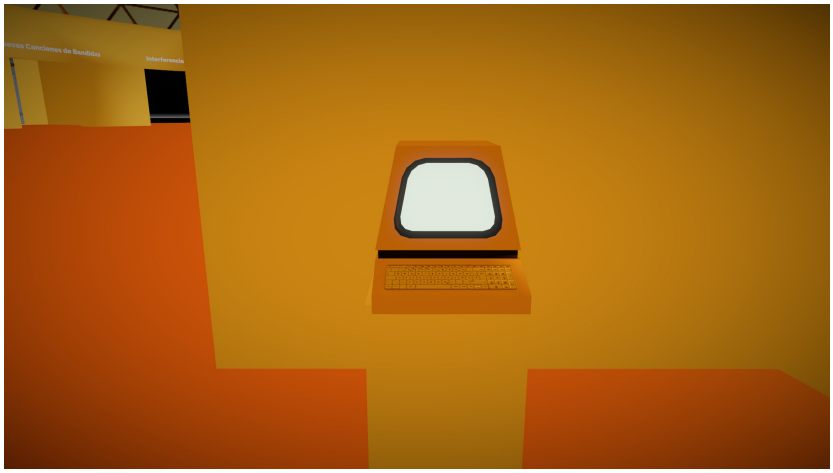

Figura 5: Computadora con la que se puede interactuar para obtener información sobre las obras

B. Inspiración (obras)

Las siguientes obras sirvieron de inspiración en el desarrollo de esta investigación y de la obra (museo.red).

- Newstweek. Julian Oliver (2011). https://julianoliver.com/output/newstweek.html
- Mont-réel. Eva Clouard (2015). http://www.artandsurveillance.com/?portfolio=mont-reel
- Watched and Measured (2000), Guardian Angel (2001). David Rokeby. http://www.davidrokeby.com/
- The Big Plot. Paolo Cirio (2009). https://www.paolocirio.net/work/the_big_plot/the_big_plot.php

- Listen and Repeat. Rachel Knoll (2013). https://rachelknoll.com/portfolio/listen-and-repeat
- F'BOOK, WHAT MY FRIENDS ARE DOING ON FACEBOOK. Lee Walton (2009). http://www.leewalton.com/art/fbook-what-my-friends-are-doing-on-facebook
- Rachel Is. Rachel Perry Welty (2009). http://magazine.art21.org/2009/10/29/rachel-is-an-interview-with-rachel-perry-welty/
- Emoji Nation. Nastya Ptichek (2014). https://www.behance.net/ptichek
- Project Face. Rina Dweck (2012). https://www.huffpost.com/entry/project-face-artist-rina-_n_2119318
- Public Access. David Horvitz (2011). http://media.rhizome.org/blog/7949/Public-Access-PDF.pdf
- Hansel & Gretel. Ai Weiwei (2017). https://www.engadget.com/2017-06-16-ai-weiwei-hansel-and-grete
html
- Tinder Project. Jiyeon Kim (2017). http://jiyeonkim.de/albums/tinder-project-1/
- Tinder Diaries. Audrey Jones (2017). http://www.audreyjones.net/tinder-diaries
- The Artist Is Kinda Present. An Xiao (2010). http://memestomovements.com/art/artistiskindapresent.html
- The Stanley Parable. Galactic Cafe (2011) http://www.stanleyparable.com/

Referencias

Agostino, D., Arnaboldi, M. & Lema, M. D. (2020). New Development: Covid-19 As an Accelerator of Digital Transformation in Public Service Delivery. *Public Money & Management*, *nil*(nil), 1-4. https://doi.org/10.1080/09540962.2020.1764206 (vid. pág. 5)

Ahmad, T. (2020). Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3568830 (vid. pág. 10)

Al-Saggaf, Y. & Islam, M. (2012). Privacy in Social Network Sites (SNS): the threats from Data Mining [Imported on 12 Apr 2017 - DigiTool details were: Journal title (773t) = Ethical Space: the international journal of communication ethics. ISSNs: 1742-0105;]. *Ethical Space: the international journal of communication ethics*, *9*(4), 32-40 (vid. págs. 7-9).

De', R., Pandey, N. & Pal, A. (2020). Impact of Digital Surge During Covid-19 Pandemic: a Viewpoint on Research and Practice. *International Journal of Information Management*, *nil*(nil), 102171. https://doi.org/10.1016/j.ijinfomgt.2020.102171 (vid. págs. 4, 5, 7)

Gerke, S., Shachar, C., Chai, P. R. & Cohen, I. G. (2020). Regulatory, Safety, and Privacy Concerns of Home Monitoring Technologies During Covid-19. *Nature Medicine*, *26*(8), 1176-1182. https://doi.org/10.1038/s41591-020-0994-1 (vid. págs. 7, 8)

Isaak, J. & Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*, *51*(8), 56-59 (vid. págs. 9, 11).

Johnson, D. (2001). *Computer ethics*. Prentice Hall. (Vid. pág. 7).

Király, O., Potenza, M. N., Stein, D. J., King, D. L., Hodgins, D. C., Saunders, J. B., Griffiths, M. D., Gjoneska, B., Billieux, J., Brand, M., Abbott, M. W., Chamberlain, S. R., Corazza, O., Burkauskas, J., Sales, C. M., Montag, C., Lochner, C., Grünblatt, E., Wegmann, E., ... Demetrovics, Z. (2020). Preventing Problematic Internet Use During the Covid-19 Pandemic: Consensus Guidance. *Comprehensive Psychiatry*, *100*, 152180. https://doi.org/10.1016/j.comppsych.2020.152180 (vid. pág. 5)

Moor, J. H. (2000). Cyberethics: Social & Moral Issues in the Computer Age. En R. Baird, R. Ramsower & S. Rosenbaum (Eds.). Prometheus Books. https://books.google.com.ar/books?id=tJnuAAAAMAAJ. (Vid. pág. 6)

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*(1), 119-157 (vid. pág. 6).

Seifert, A. (2020). The Digital Exclusion of Older Adults During the Covid-19 Pandemic. *Journal of Gerontological Social Work*, *nil*(nil), 1-3. https://doi.org/10.1080/01634372.2020.1764687 (vid. pág. 5)

Tasnim, S., Hossain, M. M. & Mazumder, H. (2020). Impact of Rumors and Misinformation on Covid-19 in Social Media. *Journal of Preventive Medicine and Public Health*, *53*(3), 171-174. https://doi.org/10.3961/jpmph.20.094 (vid. pág. 5)

Tavani, H. (2013). *Ethics and technology : controversies, questions, and strategies for ethical computing*. Wiley. (Vid. págs. 6, 7, 10).

Ting, D. S. W., Carin, L., Dzau, V. & Wong, T. Y. (2020). Digital Technology and Covid-19. *Nature Medicine*, *26*(4), 459-461. https://doi.org/10.1038/s41591-020-0824-5 (vid. pág. 4)