CONFLUÊNCIAS | Entrevista

ISSN: 1678-7145 | E-ISSN: 2318-4558

Sección Entrevistas

Volumen 26, Número 2, agosto de 2024
Enviado el: 21/08/2024
Aprobado el: 03/10/2024

ENTREVISTA CON LA PROFESORA MÓNICA ARENAS RAMIRO, profesora de la Universidad de Alcalá

Mónica ARENAS RAMIRO[1]
Universidad de Alcalá (UAH)

Eder Fernandes MONICA (Eder van PELT)[2]
Universidade Federal Fluminense (UFF)

Hilbert REIS[3]
Universidade Federal Fluminense (UFF)

Prof.ª Mónica Arenas Ramiro

Entrevista hecha por correo electrónico en mayo de 2024.

[1] Profesora de Derecho Constitucional de la Universidad de Alcalá (UAH) – España. Doctora en Derecho por la Universidad de Alcalá (UAH). Delegada de Protección de Datos de la Universidad de Alcalá (UAH). – E-mail: monica.arenas@uah.es – Orcid: https://orcid.org/0000-0002-9329-2246.
[2] Profesor adjunto da la Facultad de Derecho e Profesor permanente del Programa de Posgrado en Sociología y Derecho de la Universidade Federal Fluminense. (UFF). Doctor en Ciencias Jurídicas y Sociales por la Universidad Federal Fluminense (UFF). – E-mail: ederfm@id.uff.br – Orcid: https://orcid.org/0009-0000-5666-6491.
[3] Profesor de Derecho de la Escuela Técnica Estadual "José Martimiano da Silva" (ETEC – Ribeirão Preto). Cursa doctorado en Sociología y Derecho pela Universidade Federal Fluminense (UFF) – E-mail: hilberts@id.uff.br – Orcid: https://orcid.org/0000-0002-9539-4844.

Estimada Profesora Mónica Arenas Ramiro. Inicialmente, nos gustaría agradecerle su participación en esta entrevista. Hacemos mención muy brevemente de sus trabajos más destacados y los más recientes, especialmente los relacionados con el consentimiento en las redes sociales (2010), las brechas digitales de género (2021), la transparencia y los partidos políticos (2017 y 2021), aplicaciones de rastreo de contactos y el pasaporte COVID (2021), y partidos políticos e Internet (2019). Así, nos gustaría ampliar un poco esta presentación, preguntando sobre su jornada académica y sus proyectos de investigación.

Eder Monica; Hilbert Reis: ¿Qué le motivó a combinar las clases de Derecho Constitucional con la investigación sobre sociedad digital y protección de datos? ¿Podría contarnos sobre el inicio de esta experiencia y los motivos que la llevaron a abordar estos temas tan sensibles en nuestra contemporaneidad?

Mónica Ramiro: Siempre me han preocupado mucho la protección de la dignidad de las personas y los peligros de los avances tecnológicos y científicos. En el fondo, me planteaba cómo un mal uso de nuestra información personal, que se podía ver incrementado exponencialmente con técnicas informáticas, podía condicionar nuestra forma de vivir en sociedad, de relacionarnos, de comunicarnos y de participar. Pero también me obsesionaba, por otro lado, que estos mismos miedos o temores a los avances tecnológicos supusieran un freno al avance digital de nuestras sociedades y a la investigación o a la innovación. Desde Hipatia de Alejandría, cuántos y cuántas investigadores y científicos no habrán sido martirizados por sus ideas y cuántas invenciones no se habrán perdido fruto del temor a lo desconocido.

Cuando mi Director de Tesis -hace ya muchos, demasiados, años- me dijo que pensara en un tema de investigación, lo tuve claro, quería escribir sobre algo que impactara en la vida de los ciudadanos, que tuviera la capacidad disruptiva de transformar personas y Estados. Y por eso elegí analizar la regulación del tratamiento de datos personales.

No es cierto que la información es el petróleo del Siglo XXI. La información siempre ha sido poder. No es algo nuevo. Pero los avances tecnológicos han posibilitado mejores y más potentes formas de recopilarla, almacenarla y distribuirla, entre otras cosas.

No hay que olvidar que el control de esa información debería ser un poder que tenemos los ciudadanos, cada uno de nosotros porque es nuestra información personal, lo que nos identifica y nos define. Es nuestro derecho fundamental. Y por eso la importancia de darle un enfoque constitucional, desde el prisma de los derechos fundamentales. Los datos son el objeto de protección de un derecho fundamental, del derecho fundamental a la protección de datos. Así lo recoge en España nuestro texto constitucional (en su artículo 18.4 -aunque no de forma expresa-) y así se recoge en muchos textos constitucionales, ese habeas data, incluso a nivel internacional con la protección de la vida privada por el Consejo de Europa mediante el Convenio Europeo de Derechos Humanos de 1950, o a nivel europeo de forma expresa en la Carta de Derechos Fundamentales de la Unión Europea. Pero esto lo hemos perdido de vista, hemos monetizado un derecho fundamental y lo hemos dejado en manos de gigantes tecnológicos cuya función principal no es ser servir a la ciudadanía.

Debemos encontrar un equilibrio. Un equilibrio entre tecnología y Derecho, un equilibrio y una necesaria colaboración entre sector público y sector privado, y estoy convencida de que eso sólo lo lograremos si lo hacemos desde el prisma del Derecho constitucional, desde una reinterpretación de la Teoría de los derechos fundamentales y del Estado porque es cierto que estamos ante un cambio de paradigma.

Eder Monica; Hilbert Reis: En “Brecha digital de género: la mujer y las nuevas tecnologías”, de 2011, con una dosis de esperanza sobre las nuevas tecnologías digitales desde una perspectiva de género, concluye que: “Si queremos una sociedad democrática, debemos defender el reconocimiento de las mujeres como sujetos de derechos, como creadores y no meros receptores, y que no sean vistos como una mera manifestación teórica”. (Ramiro, 2011, p. 120). Trece años después, con el continuo avance de las Tecnologías de la Información y Comunicación (TIC) y con el aumento de los temas que involucran la cultura tecnológica desde una perspectiva de género, ¿cuál es su diagnóstico sobre los avances y retrocesos en este tema?

Mónica Ramiro: Dicen que niños pequeños problemas pequeños y niños grandes problemas grandes. No digo que la digitalización sea un problema, pero si un gran reto, un enorme reto. Y a grandes retos, grandes respuestas. Y la respuesta no sólo debe tener un enfoque internacional,

más allá de fronteras porque la digitalización rompe barreras, sino que debe tener un enfoque de género.

Debemos aplicar la perspectiva de género también a los avances tecnológicos. Estoy convencida de que la tecnología es neutra, pero no así las personas que las diseñan ni las que las aplican. Por eso, si tenemos sociedades que discriminan, nuestra tecnología, nuestra sociedad digital discriminará. Las herramientas de IA se nutren de datos, de información personal. Si alimentamos a "la bestia" con datos en mal estado, con algoritmos discriminatorios, nuestra IA será machista o xenófoba. Si tenemos sociedades que discriminan, tendremos tecnología y herramientas tecnológicas que discriminen. No nos puede sorprender que una IA que aprende de Twitter se vuelva machista o racista porque no podría ser de otra forma.

En cuestión de género el problema se produce en el caso de las mujeres porque el acceso, uso, diseño y control de las nuevas herramientas tecnológicas e Internet viene marcado por unos fuertes estereotipos sociales. Es ilusorio e irreal mantener que en la actualidad no existen diferencias de trato injustificadas y que éstas no se perpetúan a través de odiosos estereotipos reproducidos en la Red y por los algoritmos e inteligencias artificiales que se programan para tomar decisiones que afectan a la ciudadanía.

Por eso, estoy convencida de que estamos en un punto, en un momento de la historia que podemos revertir el orden establecido y aprovechar ese cambio de paradigma para romper los odiosos estereotipos que siguen anclados en nuestras sociedades. La tecnología lo permite, nos permite ser más participativos sin importar el género, pero, a la vez, permite emplear la información personal para tener en cuenta las necesidades específicas de un género en concreto.

Las posibilidades que se abren para crear sociedades más justas e igualitarias son incuestionables, de la misma forma que es innegable que el entorno digital no va a hacer otra cosa que reproducir los odiosos estereotipos discriminatorios, no sólo de género, que existen en nuestras sociedades actuales si no lo evitamos.

Debemos partir del hecho de que la tecnología es un instrumento más en manos de las personas, una herramienta neutra que favorece la integración de las personas en la sociedad y que la misma tendrá los efectos positivos o negativos que nosotros mismos les demos, aunque cargado, como no puede ser de otra forma con nuestro equipaje social. El problema, por lo tanto, no lo

serán los instrumentos o tecnología utilizados, sino el tipo de sociedad que hemos construido, donde se maneja la citada información y al servicio de la cual se ponen dichos instrumentos.

De ahí la importancia, como acabamos de señalar, de que un diseño y uso de algoritmos o herramientas como la Inteligencia artificial sea respetuoso con los derechos fundamentales y desde una perspectiva de género, teniendo en cuenta los roles que tradicionalmente se han venido asignando a las mujeres y han condicionado su acceso y uso a la tecnología, con el fin de erradicar las diferencias existentes, adaptándolos a un entorno digital. Todo ello, al mismo tiempo que los poderes públicos y el sector tecnológico toman las medidas necesarias para reconocer a las mujeres como sujetos de derechos en igualdad de oportunidades que los hombres. Por ese mismo motivo, hay que eliminar no sólo las barreras de acceso, sino la exclusión de la toma de decisiones y de diseño en el terreno de las TICs.

Eder Monica; Hilbert Reis: En los últimos años, muchos países, entidades y personas pueden haber sido víctimas de espionaje a través de programas informáticos. En 2021, con el apoyo de Amnistía Internacional y la ONG francesa *Forbidden Stories*, se estimó que más de 50.000 periodistas, empresarios, defensores de derechos humanos, líderes religiosos y jefes de Estado de diferentes países pudieron haber sido víctimas de espionaje mediante el programa informático de espionaje llamado 'Pegasus', desarrollado por la empresa israelí *NSO Group*. Al año siguiente, un comunicado del Gobierno de España, de 2 de mayo de 2022 (MENÉNDEZ, 2022), informó sobre el uso de Pegasus para espiar al presidente del Gobierno y la ministra de Defensa. En 2024, la policía federal brasileña inició la Operación "*Vigilância Aproximada*" para investigar el uso indebido del programa *FirstMile*, de la empresa israelí, *Cognyte* (antes llamada *Verint*) (CNN, 2024).

En este caso se investiga situaciones de espionaje ilegal a algunas importantes autoridades de Brasil. Ante estos casos de espionaje a través de programas informáticos, que involucran a Estados democráticos, ¿cuáles son los reales riesgos del uso de estos programas para las democracias, especialmente en relación con los Estados democráticos?

Mónica Ramiro: Es evidente que, si los ciudadanos se saben observados o, incluso, aunque no lo estén siendo, pero existe una sospecha, no actuarán con la misma libertad que si controlaran qué es lo que se sabe o conoce de ellos.

Ésto ya nos lo advirtió, a finales del siglo XVIII, el filósofo inglés Jeremy Bentham con la idea del panóptico (modelo de estructura carcelaria consistente en la existencia de una torre de vigilancia central rodeada de celdas, pero desde las cuales los reclusos no pudieran saber nunca si en la torre existía o no alguien vigilando). Así las cosas, si los ciudadanos no controlan lo que se sabe o conoce de ellos, no participarán libremente en la sociedad de la que forman parte, afectando ésto, directamente, al principio democrático.

Pero la cuestión no sólo es ésta, sino que el verdadero problema es el uso ilícito que se está haciendo de este tipo de herramientas, esto es, la finalidad para la que se utilizan estos programas, que es, esencialmente, controlar a los ciudadanos y, más concretamente, a los ciudadanos que tienen poder de representación o de decisión a nivel estatal y desestabilizar así los Estados; o vigilar a potenciales elementos subversivos contra el poder establecido, aunque sin las garantías propias de un Estado de Derecho.

En este sentido, se intenta justificar el uso ilícito de estos programas bajo el pretexto de la seguridad nacional. El eterno y falso debate: proteger derechos o garantizar la seguridad nacional. Pero en un Estado de Derecho, el fin no justifica los medios.

La idea de la democracia no implica exclusivamente la idea de la participación, que sólo puede darse en condiciones de libertad, sino también la rendición de cuentas, y ésto solo se puede producir a la luz del sol, esto es, a la luz de la transparencia y de la responsabilidad de los poderes públicos. La democracia sólo puede ejercerse en condiciones de transparencia, que conlleva la rendición de cuentas de los poderes públicos. De ahí que el uso de este tipo de sistemas debe ser transparente en lo que, a su existencia, condiciones de uso y garantías se refiere.

Estamos configurando los parámetros de la privacidad en un mundo digitalizado y abierto a nuevas amenazas que hacen tambalear la estabilidad de nuestros Estados, pero debemos evitar convertir nuestros Estados democráticos en Estados policiales. De lo contrario, como ya sentenció el TEDH en el asunto Klass, corremos el riesgo de "destruir la democracia con el motivo de defenderla" (§ 49).

Eder Monica; Hilbert Reis: Ante el problema jurídico de si los Estados pueden o no vigilar de forma tan sensible a sus ciudadanos bajo el pretexto de la seguridad nacional, ¿podría

compartir su impresión sobre las actuales soluciones jurídicas disponibles en España y Europa para casos de esta naturaleza?

Mónica Ramiro: El lado negativo, o más negativo, de la tecnología nos va a enseñar casos de espionaje masivo de personas extranjeras o nacionales por servicios de inteligencia no sometidos al principio del Estado de Derecho, el control total de la población mediante reconocimiento facial, la alteración de la voluntad democrática mediante técnicas de manipulación neuroemocional en las redes, la falsificación de la realidad mediante estrategias de desinformación y noticias falsas, o el efecto discriminador mediante el uso de algoritmos basados en el perfilado de sujetos a través del conocimiento de sus datos personales. Todo ello son buenos ejemplos de los riesgos, aunque no los únicos.

Todas estas amenazas afectan, de una u otra forma, en mayor o menor intensidad, a todos los derechos y libertades que conocemos, desde las libertades informativas, expresión e información, a los derechos de participación, a la privacidad y a la igualdad, entre otros, y, en último término, a la dignidad y al libre desarrollo personal.

De ahí que se hace necesario adaptar las garantías existentes para que esto no suceda. La tecnología debe estar al servicio de la humanidad. Y de ahí su configuración conforme a Derecho y, de forma imprescindible, conforme a unos principios y valores éticos.

Si bien la seguridad nacional es un objetivo legítimo que permite utilizar programas espía y limitar nuestros derechos fundamentales, en un Estado democrático y de Derecho toda limitación de derechos debe estar contenida en una norma clara y previsible y debe ser, además, necesaria en una sociedad democrática, lo que implica superar un estricto test de proporcionalidad, por lo que, ante mecanismos menos lesivos para conseguir un fin legítimo, son éstos los que deben ser empleados. Así nos lo vienen indicando no sólo los Tribunales, sino las Autoridades de protección de datos, como el Supervisor Europeo de Protección de Datos (SEPD).

Ya en 1978, el Tribunal Europeo de Derechos Humanos (TEDH) se pronunció sobre el tema en el caso Klass y, cuarenta años más tarde, en 2021, en el asunto *Big Brother Watch*, el TEDH concluyó que, aunque estos sistemas en sí mismos no contravienen el Convenio Europeo de Derechos Humanos (CEDH), es necesario que “se limiten a casos estrictamente necesarios para

salvaguardar las instituciones democráticas" y que cuenten con las "garantías adecuadas y afectivas contra el abuso".

Igualmente, el Tribunal de Justicia de la Unión Europea (TJUE), en 2020, en el asunto *Quadruture Du Net*, señaló que las restricciones a la protección de datos personales se deben establecer sin sobrepasar los límites de lo estrictamente necesario, para lo que será esencial realizar la correspondiente ponderación.

Más contundente fue el SEPD quien, en unas Observaciones publicadas en febrero de 2022, con referencia expresa a Pegasus, reconoce su potencial y la dificultad de su control y -dudando de que su uso pudiera considerarse proporcionado incluso con la finalidad legítima de prevenir la delincuencia o mantener la seguridad nacional, por el elevado nivel de injerencia en la vida privada- recomienda su prohibición. Esto es, como ya hemos dicho, que el fin no justifica los medios. Y en esta misma línea se pronunció el Parlamento europeo en una Recomendación, de junio de 2023, sobre el uso de este tipo de programas espía de vigilancia. Su adquisición y uso debería ser algo excepcional y previsto legalmente.

Eder Monica; Hilbert Reis: Como Profesora de Derecho Constitucional de la Universidad de Alcalá desde 1999, ¿cree que es posible armonizar, desde una perspectiva jurídica, la garantía de los derechos fundamentales y el uso de sistemas de vigilancia por parte de los Estados?

Mónica Ramiro: Dado que parece innegable que los sistemas de vigilancia son necesarios para garantizar la estabilidad de los Estados, y que no podemos tapar el sol con un dedo, si finalmente deciden emplearse, sólo nos quedan las garantías.

Entre las garantías a reforzar, citadas en las Observaciones del SEPD de 2022 y en la Recomendación de junio de 2023 del Parlamento Europeo, destacamos: fortalecer su supervisión eficaz a través de las autoridades de protección de datos y de controles judiciales antes y después de su uso; aplicar de forma estricta la normativa de protección de datos; reducir el riesgo de que los datos obtenidos con estos programas lleguen a bases de datos ubicadas en la Unión Europea; y, por último, empoderar a la sociedad civil para que conozca del uso de estos sistemas.

Se confunde muchas veces la idea del secreto y la reserva que deben rodear a estos sistemas de vigilancia con la necesidad de que no se rijan por los principios de transparencia y rendición de cuentas. Evidentemente, no se va a comunicar a los sujetos investigados que lo están siendo para que puedan evadir cualquier tipo de responsabilidad, pero los ciudadanos, incluso los investigados, sí que deben conocer la existencia de estas herramientas y de las garantías que van a rodear su uso, así como de las responsabilidades derivadas de un uso ilícito de las mismas.

Estoy convencida de la posibilidad y, sobre todo, de la necesidad de emplear este tipo de herramientas de vigilancia y poder respetar, a la vez, los derechos fundamentales de los ciudadanos. La delincuencia emplea cada vez formas más perfeccionadas para delinquir y hace uso de las ventajas que le ofrecen las herramientas tecnológicas e Internet para evitar el cumplimiento de las normas.

Pero, es cierto, que para conseguir dicho equilibrio hace falta crear una cultura y una voluntad no sólo en la ciudadanía -generando confianza en los poderes públicos-, sino en los poderes públicos, que son los que deben emplearlos. Se debe capacitar a los empleados públicos, formándoles en una cultura de la privacidad, que entiendan la necesidad de respetar y garantizar derechos incluso en situaciones complejas donde la seguridad nacional está en juego.

Eder Monica; Hilbert Reis: Profesora, olvidemos un poco de la perspectiva de la vigilancia por parte del Estado y avancemos hacia la temática de la protección de los datos personales y de la privacidad de los ciudadanos. Sabemos que muchos aeropuertos, centros comerciales e incluso hospitales utilizan tecnología de *Wi-Fi tracking*. ¿Podría comentarnos brevemente sobre los riesgos de esta tecnología para nosotros, los usuarios habituales de la Internet?

Mónica Ramiro: Hoy en día vivimos apegados a la tecnología, a nuestros dispositivos móviles y éstos están configurados, por defecto, para poder localizarnos.

Como venimos comentando, el uso de la tecnología al servicio de la humanidad debería ser el objetivo. El objetivo debería poder ser utilizar herramientas y tecnologías que nos llevaran a localizar a personas en situaciones de vulnerabilidad o peligro y que garantizaran la seguridad y la integridad de los ciudadanos. Esa debería ser la finalidad de estas tecnologías *WI-FI*

tracking. Y todo aquello que excediera de esa finalidad legítima y que no contara con las garantías adecuadas, debería estar prohibido.

Las ventajas que ofrecen estas tecnologías son muchas, pero los peligros o riesgos que llevan aparejados también, pues el *WI-FI tracking* implica el tratamiento de datos personales, ofreciendo información no sólo de presencia en un determinado lugar, sino de localización o de trazabilidad de la movilidad de una persona. Y cuando esto se hace sin el control del titular de dichos datos, sin su conocimiento, esa pérdida de control ya es en sí un problema para nuestra privacidad.

Eder Monica; Hilbert Reis: Recientemente, la Agencia Española de Protección de Datos, el Consejo de Protección de Datos y Transparencia de Andalucía, la Autoridad Vasca de Protección de Datos y la Autoridad Catalana de Protección de Datos desarrollaron unas directrices para el uso de tecnologías de *Wi-Fi tracking* (AEPD *et al*., 2024). ¿Cómo evalúa la implementación de directrices y orientaciones de agencias y autoridades sobre transparencia y protección de datos para el uso de seguimiento Wi-Fi (*Wi-fi tracking*)? ¿Está esto previsto en el RGPD?

Mónica Ramiro: Las Autoridades de protección de datos, ya sea la estatal, las autonómicas y, de la misma forma, a nivel europeo, están llevando a cabo una gran labor a pesar de estar realizando su trabajo "predicando en el desierto", en una sociedad donde han cambiado los paradigmas y los ciudadanos, a pesar de valorar su privacidad, deciden compartir su información personal a través de las redes sociales por un minuto de gloria o fama. A ello se suma un alto grado de desconfianza ciudadana y una escasez de recursos, que hace todavía más encomiable la labor que llevan a cabo.

En este terreno de las tecnologías de *WI-FI tracking*, como las propias Autoridades de control indican expresamente en las Directrices mencionadas, "todas las personas deben tener derecho a moverse libremente sin "sentirse espiados". Enlazamos esta idea con nuestra respuesta a los programas espia. Es cierto que la finalidad inicial es diferente, pero la percepción ciudadana de sentirse observados es la misma. Y es esa expectativa de privacidad que tenemos los seres humanos la que debe respetarse, la que debe garantizarse porque es, en ese contexto, en el que

nos desarrollaremos libremente, participaremos libremente y tomaremos decisiones de forma libre.

Ahora bien, una cosa es la labor de las Autoridades de control y otra, muy diferente, el cumplimiento y la implementación de sus Directrices y Orientaciones porque esto último depende, como también se ha dicho, de la voluntad del sector público y del sector privado, de convencerles de la necesidad de garantizar derechos de los ciudadanos, de garantizar su privacidad a la vez que se están llevando a cabo medidas que pueden suponer una limitación de esta privacidad. Debemos recordar que los derechos no son ilimitados. No hay derechos ilimitados. Lo que sucede es que dichas limitaciones, en un Estado de Derecho, deben estar sometidas a restricciones y a la existencia de unas necesarias garantías previstas legalmente.

El RGPD ha sido calificado como un mecanismo normativo neutro, tecnológicamente neutro, por lo que no hay referencia a una herramienta o tecnología específica, y por lo tanto, no se refiere a las herramientas de *WI-FI tracking* como tampoco lo hace a los sistemas de biometría o de reconocimiento facial de forma explícita.

El RGPD sólo hace referencia al hecho de que determinados tratamientos de datos personales, entre los que pueden incluirse los datos especialmente protegidos o categorías especiales de datos, deben garantizarse y adoptarse bajo una previsión legal, ya sea previsto en del Derecho de la Unión Europea o en la normativa estatal correspondiente.

Eder Monica; Hilbert Reis: Recientemente, en una consulta hecha por nosotros a un sitio web español, ha sido exigido una contraprestación [económica] para ejercer el derecho al anonimato (si quieres el acceso gratuito, debes aceptar los *cookies*; si no, debes pagar por el acceso). ¿Cómo piensa este tipo de cobro por parte de sitios web y redes sociales? Para el RGPD, ¿es posible este tipo de contraprestación para hacer efectivo el derecho al anonimato en internet?

Mónica Ramiro: No, esto no es lo normal. Debemos ser conscientes de que se ha avanzado mucho, especialmente en los últimos años, a la hora de implementar la normativa de protección de datos, pero todavía queda camino por recorrer.

Así, es cierto que en lo relativo al uso de *cookies*, las instrucciones o Directrices de las Autoridades de control han venido siendo un poco dispares (de hecho, nuestra Agencia Española de Protección de Datos, tuvo que adaptar, en julio de 2023, su Guía sobre el uso de las cookies). Pero el Comité Europeo de Derechos Humanos lo ha dejado claro en febrero de 2023, en sus Directrices 03/2022 sobre patrones engañosos en redes sociales. Los usuarios de Internet deben aceptar o rechazar expresamente el uso de cookies que, además, deben presentarse en un lugar y en un formato destacados. El objetivo del RGPD y de las propias Autoridades de control, encargadas de hacerlo cumplir y vigilar su cumplimiento, no es otro que empoderar a los ciudadanos. De ahí la exigencia de aceptar o rechazar la *cookies* de forma expresa, sin que su no aceptación implique la falta de prestación del servicio solicitado.

Más aún, este criterio ya venía siendo evidente para el TJUE. Y así el TJUE lo dejó todavía aún más claro, al condenar el tipo de actuaciones como las descritas en la pregunta. De ahí que el uso de cookies obligue a abrir pantallas en las que se nos pregunten qué tipo de cookies deseamos que se nos instalen en nuestro dispositivo. Pero en ningún caso, y bajo ningún concepto se permitirá, y esto fue lo que condenó el TJUE, el tener que aceptar las cookies para que se nos preste un determinado servicio. Esto se ha repetido desde el conocido asunto Planet49 (asunto C-673/17), de octubre de 2019.

Eder Monica; Hilbert Reis: Profesora, sobre la IA: Para concluir, ¿Qué medidas deberían ser adoptadas por el Estado para proteger los derechos fundamentales y la privacidad de las personas, especialmente en lo que respecta a la IA?

Mónica Ramiro: Tanto sector público como sector privado -especialmente desde la declaración mundial de pandemia por coronavirus en el 2020- aceleraron su proceso de transformación digital y desencadenaron la aparición, el desarrollo y la evolución de todo un conjunto de tecnologías disruptivas que trajeron ventajas, pero que también provocaron nuevas amenazas para los derechos y libertades de las personas. Estamos ante un conjunto de retos a los que debemos darles una respuesta desde el mundo del Derecho.

Asimismo, no podemos perder de vista que lo que está en juego son derechos, y esto es fundamental para focalizar nuestro objetivo y legislar en un sentido correcto donde lo que protejamos sean personas y no otros intereses geopolíticos, sociales o económicos. Esto implica

adoptar una visión "antropocéntrica" y "antropogénica", donde "la dignidad personal sea el impulso de las obligaciones jurídicas", y donde todos los actores implicados en la transformación se sometan a las mismas reglas de una forma proactiva, transparente, auditable, y con una serie de valores éticos.

Más allá de normas claras y precisas -y éticas- y un estricto cumplimiento del test de proporcionalidad, se requiere de forma previa a la puesta en marcha de cualquier nueva invención una evaluación del impacto en la vida de los sujetos atendiendo a valores éticos y no discriminatorios. En esta línea se dirigen los esfuerzos europeos y no solo el recientemente aprobado Reglamento sobre Inteligencia Artificial, sino con las conocidas "Directrices éticas para una IA fiable" ("*Ethics guidelines for trustworthy AI*"), del Grupo de Expertos de Alto nivel de la UE para IA, publicadas ya en abril de 2019, y que se centran en tres componentes: que la Inteligencia Artificial sea licita, que sea ética y que sea robusta desde el punto de vista técnico y social. Estas orientaciones pivotan alrededor de la transparencia con las exigencias de facilitar la trazabilidad y la auditabilidad de los sistemas de Inteligencia Artificial, o la promoción y formación y la educación con el fin de conocer una Inteligencia Artificial fiable. Estoy convencida de que todo ello se puede trasladar a cualquier nuevo desarrollo o avance tecnológico.

Eder Monica; Hilbert Reis: Finalmente, nos gustaría finalizar la entrevista hablando un poco de la importancia del intercambio de conocimientos entre investigadores de Brasil y España. En 2021, la Revista Confluencias, vinculada al Programa de Posgrado en Sociología y Derecho (PPGSD), organizó un dosier titulado "Diálogos entre la Unión Europea y América Latina: desafíos y perspectivas para la sociedad internacional en el siglo XXI". Fue el resultado de un intercambio científico entre las Universidades Complutense de Madrid (España) y la Universidad Federal Fluminense (Brasil). Sus 16 (dieciséis) artículos involucraron temas sobre el trabajo; comunicación y tecnología digitales; movimientos migratorios; medio ambiente; Comercio internacional; y, los derechos humanos, desde una perspectiva interdisciplinaria entre la sociología y el derecho. En este dosier tuvimos la grata oportunidad de contar con un artículo suyo: "Nuevas tecnologías y objetivos para la protección de datos personales en Europa: rastreo de contactos durante la pandemia de COVID-19".

Además, el PPGSD organizó, junto con la Universidad Complutense de Madrid, en 2021, el "IV Congreso Internacional sobre Globalización, Ética y Derecho", en el que tuvimos su participación como una de las coordinadoras de un grupo de trabajo. En 2023, ahora en un convenio entre el PPGSD y la Universidad de Vigo, en Galicia, usted fue la conferencista inaugural del Congreso. ¿Qué opina de nuestras alianzas interinstitucionales y los diálogos académicos internacionales que venimos produciendo entre Brasil y España? ¿Qué impacto tiene esto en un debate sobre una sociedad digital globalizada? ¿Cómo puede colaborar la universidad en este proceso de instauración de una sociedad del siglo XXI efectivamente democrática y plural?

Mónica Ramiro: Brasil es un Estado puntero en reconocimiento de derechos en Internet y de derechos digitales. De hecho, fue uno de los primeros Estados en el mundo en tener una "Constitución de Internet". Tenemos mucho que aprender de esto. Pero España también tiene mucho que ofrecer. Tenemos grandes expertos en protección de datos personales y en tecnología y somos también uno de los primeros Estados a nivel mundial en reconocer, de forma vinculante, la existencia, en la Ley Orgánica 3/2018, de derecho digitales (también reconocidos, aunque sin efecto vinculante, en la Carta de Derechos Digitales aprobada por el Gobierno en julio de 2021).

Las sinergias entre Brasil y España son muchas y la tecnología imparable, así que hay mucho camino por recorrer, y mejor hacerlo en buena compañía.

No se puede hablar de una sociedad digital globalizada si no hacemos un estudio comparado, si no miramos a nuestro alrededor y aprendemos de lo que se está haciendo en otros Estados. Europa debe mirar hacia Estados Unidos, hacia Latinoamérica e incluso, aunque parezca curioso porque los sistemas de respeto de derechos fundamentales pueden ser cuestionables, hacia China. La regulación de la tecnología debería tener un carácter universal, internacional. De ahí la importancia del Tratado Internacional sobre IA aprobado por el Consejo de Europa en junio de 2024.

Y es en este proceso de aprendizaje y de difusión de ideas y de conocimiento, donde las Universidades son un elemento central. Las Universidades siempre han sido fuente de generación y de transmisión de conocimiento. Nuestro futuro dependerá de la formación de las

personas que ahora mismo están en nuestras Universidades. Los y las estudiantes deben ser formados y capacitados para un mundo digital, pero no sólo les debemos alfabetizar digitalmente, sino dotarles de los valores éticos necesarios para crear sociedades más igualitarias y justas.

Es obligación de todos los que formamos partes de Universidades, públicas o privadas, contribuir a la formación de nuestros y nuestras estudiantes, transmitirles valores y conocimientos para que salgán preparados para la sociedad de la que formarán parte y de la que, pueden, llegar a tener puestos de toma de decisiones en la misma, afectando a la vida de muchas otras personas. Si decíamos que la información es poder, mucho más la educación. Los docentes somos afortunados de poder formar parte del proceso de formación de nuestro futuro, por lo que es indispensable que nosotros mismos nos formemos y seamos conscientes de lo que el proceso de transformación digital significa y de la necesidad de transmitir no solo conocimientos, sino también valores. Sólo así aseguraremos un futuro más justo para todos.

Referencias

Agência Espanhola de Proteção de Dados; Autoridade Catalã de Proteção de Dados; Autoridade Basca de Proteção de dados; Conselho de Transparência e Proteção de Dados da Andaluzia. **Tecnologias de rastreamento de Wi-Fi**: Orientações para controladores de dados. Maio de 2024. Disponível em: https://www.avpd.euskadi.eus/contenidos/informacion/publicaciones_avpd/es_def/adjuntos/guia_wifi_tracking-es.pdf. Acesso em: 08/05/2024.

ARENAS RAMIRO, Mónica. Brecha digital de género: la mujer y las nuevas tecnologías. **Anuario de la Facultad de Derecho**, v. 4, 2011, p. 97-125.

_____. El consentimiento en las redes sociales on line. **Derecho y redes sociales, Civitas**, 2010, p. 117-44.

_____. Nuevas Tecnologías y retos para la protección de datos personales en Europa: El rastreo de contactos durante la pandemia por covid-19. **Confluências - Revista Interdisciplinar de Sociologia e Direito**, v. 23, n. 2, p. 99-17. Disponível em: https://doi.org/10.22409/conflu.v23i2.50519. Acesso em: 07/05/2024.

_____. Pasaporte COVID, ¿libertad de circulación de forma segura o discriminación y privacidad en juego? **La Ley privacidad**, v. 8, 2021.

_____. Transparencia y partidos políticos: Las insuficiencias de la Ley 19/2013. Estudios sobre la función y el estatuto constitucional de los partidos políticos. **Marcial Pons**, 2022, pp. 361-89.

CNN Brasil. **FirstMile**: como funciona ou o software espião que vinha sendo utilizado pela Abin de Ramagem. 25 de janeiro de 2024. Disponível em: https://www.cnnbrasil.com.br/politica/firstmile-como-funciona-o-software-espiao-que-teria-sido-usado-pela-abin-de-ramagem/. Acesso em: 07/05/2024.

MENÉNDEZ, María. Espionaje Pegasus. El Gobierno denuncia que Sánchez y Robles fueron espiados por Pegasus: "Son escuchas ilícitas y externas". **RTVE**, 2 de mayo de 2022. Disponible en: https://www.rtve.es/noticias/20220502/gobierno-anuncia-sanchez-robles-espiados-pegasus/2345960.shtml. Acceso el: 07/05/2024.

★