Arturo Ribagorda y sus experimentados conceptos

"La única opción sensata —si no queremos retroceder varias décadas en la historia— es conocer los riesgos de la tecnología que nos ocupa para aprender a minimizarlos, pero sin rechazarla", advierte enfático.

Sara Gallardo M.

A Arturo Ribagorda Garnacho, nacido en Madrid, España, doctor en informática y catedrático de la universidad Carlos III en su ciudad natal, le encanta la historia y se declara un apasionado lector de novelas y ensayos. "También me considero melómano y disfruto mucho paseando, principalmente por el campo. En todo caso mi afición primera, desde muy pequeño, ha sido la astronomía", agrega con cierta nostalgia porque la academia lo atrapó desde sus primeros pasos profesionales.

Muchas cosas dejó aplazadas por no privarse del contacto permanente con sus alumnos, que dice "me permiten envejecer –o esa ilusión tengo-, con más lentitud".

Pero el mundo empresarial también lo atrajo y desde hace cuatro años optó por guardar en la memoria los múltiples cargos desempeñados como docente, para dirigir lo que él denomina su grupo de seguridad de las Tecnologías de la Información, cuya composición y trabajos se pueden consultar en www.seg.inf.uc3m.es.

Con la satisfacción a cuestas valora lo adquirido en los espacios por los que ha transitado. "El conocimiento de dos mundos tan distintos como el académico y el empresarial -también este imprescindible para no terminar investigando sobre el sexo de los ángeles, tentación extendida entre algunos académicos-".

De ahí que recurramos a su vasta experiencia para nutrir a nuestros lectores con sus opiniones en torno a la seguridad, la privacidad y los sistemas de información, asuntos determinados por el uso de los nuevos desarrollos tecnológicos.

Revista Sistemas: Las nuevas tecnologías informáticas y su permanente evolución han generado cambios en el ser humano, sobre su forma de actuar y de pensar dentro de la sociedad. De ahí la necesidad de crear un espectro que contemple el alcance de tales desarrollos, dentro de unos códigos éticos encaminados a proteger la seguridad, la privacidad y los sistemas de

información, además de regular el saber y la práctica informáticas. ¿Cuáles son sus consideraciones al respecto?

Arturo Ribagorda Garnacho: Creo que el mayor problema es la rapidez del cambio impuesto por estas tecnologías. Las grandes transformaciones técnicas, llamadas revoluciones, experimentadas por la humanidad, tuvieron un ritmo de expansión mucho más lento (miles de años en el caso de la revolución agrícola, cientos en la industrial), mientras que ahora la transformación se mide en años Esta velocidad de propagación no permite su asimilación y consiguiente adaptación por la sociedad, que se ve a menudo desbordada por el empuje de estas nuevas técnicas y sin tiempo de reflexionar sobre ellas y su impacto en nuestro presente y futuro. De otro modo dicho, necesitaríamos de un respiro —que no nos dan— para así poderlas reconducir de manera que nos ayudasen a conseguir un mundo mejor y más justo. Ahora sin embargo, somos un sujeto pasivo del cambio sin poder actuar sobre el mismo.

RS: ¿Cuáles son los deberes de las empresas que las manejan, frente a la responsabilidad que deben asumir con sus clientes y usuarios? ¿Qué no pueden hacer las empresas que manejan información personal de clientes y usuarios? ¿En qué no se pueden equivocar en el tratamiento de los datos personales?

ARG*:* Las empresas deben tener siempre presente que no son dueños de los datos personales que manejan, sino sólo sus depositarios y custodios. Así pues, nunca debieran hacer nada que su legítimo propietario, es decir las personas físicas (naturales) a las que conciernen no les haya autorizado, salvo que una ley lo imponga. Por ello, el principio del consentimiento del interesado se constituye en la piedra angular de las leyes de protección de datos y debe guiar el tratamiento de estos datos por parte de las empresas.

Pero más aún, este consentimiento debe ser un consentimiento informado (el interesado debe saber para que se le solicitan los datos), no genérico (no se pueden solicitar para una pluralidad indeterminada de usos) y revocable (deben poderse retirar cuando el interesado lo solicite).

RS: ¿Cuáles son los lineamientos fundamentales para garantizar a los clientes y usuarios la seguridad y protección de su información personal?

ARG: Desde luego, ceñirse a las prescripciones legales respecto a cómo manejar las informaciones de los individuos, manteniendo en todo momento las medidas de seguridad actualizadas según el estado del arte.

Así mismo, aunque algunas leyes no lo contemplen, las empresas debieran garantizar a las personas físicas los denominados (en España) derechos ARCO, es decir los derechos de acceso, rectificación, cancelación y oposición.

RS: La comunicación móvil ha cambiado las relaciones profesionales y personales y, más aún, las redes sociales; los seres humanos usuarios de tales tecnologías están permanentemente expuestos, ¿cómo analiza usted ese contexto dentro del marco de la seguridad y la privacidad?

ARG: Con preocupación creciente, pues no hemos asumido los riesgos inherentes a las redes. Así como hoy en día, cualquiera es consciente de las amenazas que conlleva conectarse al servidor de su banco, de hacer un pago por internet, de

pulsar un enlace que recibe en un correo electrónico, etc., y adopta precauciones para minimizar el riesgo, ello no sucede cuando se ingresa en una red social. Parece que la percepción de hallarnos entre amigos (aunque a muchos no los conozcamos directamente), nos hace relajarnos y perder todo recelo a subir fotos inapropiadas (para nosotros o para otros), hacer comentarios comprometidos (por ejemplo sobre nuestro jefe), o expresar ideas sindicales o políticas. Todo ello sin considerar que no tenemos certeza de quiénes pueden estar en esa red y de que internet no olvida. Por ejemplo, es cada vez más habitual que las empresas busquen en Internet rastros de los candidatos a un puesto de trabajo, por más que pueda ser ilícito.

Aquí, sobre todo, cabe aplicarse la frase que Shakespeare pone en boca de Gonerila en El Rey Lear: "Es más prudente exagerar los temores que la confianza".

RS: Considerando la tendencia en movilidad, ¿cuáles serían los retos propios de los datos personales en este tipo de dispositivos? ¿Cómo protegerlos?

ARG: Tomando como paradigma de los sistemas móviles a los teléfonos celulares, nos encontramos con la paradoja de que acostumbrados a usarlos desde décadas como un instrumento pasivo de simple comunicación, los seguimos viendo y usando con la misma despreocupación que hace unos pocos años.

Sin embargo, estos dispositivos se han convertido súbitamente en pequeños ordenadores, que almacenan una enorme cantidad de datos: fotos (quizás comprometidas, recuérdese el reciente caso de la actriz Scarlett Johansson), contraseñas de acceso a nuestro banco, empresa, correo corporativo o personal, etc. Igualmente, tenemos allí nuestra agenda, contactos, y en general todo tipo de datos privados, algunos de ellos íntimos. Y además, estos dispositivos se conectan a internet desde cualquier lugar (incluso inadvertidamente a través de redes *wi-fi* abiertas) o a otros dispositivos mediante *bluetooth*.

Y no obstante, su capacidad de proceso es aún escasa en comparación con cualquier ordenador, incluso portátil. Esto les impide tener los mismos sistemas de protección que tenemos en estos últimos equipos citados. No disponemos aún en ellos de cortafuegos, IDS, ni de antivirus equiparables a los de un ordenador convencional.

Todo lo anterior (almacén de datos personales, conectable a internet, escasa capacidad de protección) es una mezcla peligrosa que requiere, de nuevo, una actitud precavida, más que la que adoptamos al trabajar con nuestros ordenadores.

Y lo mismo cabe decir de otro dispositivo móvil de rápida expansión: los dispositivos RFID, que en poco tiempo nos acompañarán permanentemente, sea insertados en nuestra ropa o en cualquier otro objeto que portemos o adquiramos, permitiendo nuestro rastreo y delatando nuestros gustos, actitudes y comportamientos. Estos dispositivos constituyen así una creciente amenaza para nuestra intimidad y ya han sido objeto de varias recomendaciones por parte de la Comisión Europea.

Pero, al igual que sucede con los celulares, las etiquetas RFID pasivas (las más comunes) apenas superan unos pocos miles de puertas lógicas, lo que impide programar en ellos cualquier algoritmo de cifrado de uso común, debiendo llevar algoritmos criptográficos ligeros, mucho menos robustos, lo que expone en gran medida los datos que almacenan.

RS: Los clientes y usuarios tienen el derecho a que su información personal, debidamente recolectada, sea protegida. ¿Cómo hacen valer tal derecho? ¿Existen los mecanismos para lograrlo?

ARG: Técnicamente existen los suficientes mecanismos como para que, de ser correctamente aplicados, nos sintamos seguros. El problema va más por la escasa o insuficiente normativa legal en muchos países. Sin unas leyes que sancionen duramente el uso ilícito de nuestros datos seguirá habiendo un lucrativo campo de negocio, que será aprovechado por delincuentes de "guante blanco". Pero además, las leyes deben prever las denominadas en Europa, Autoridades de Control (en España, Agencias de Protección de Datos), que tutelan el uso que se hace de nuestros datos y puedan de oficio o a instancia de parte sancionar administrativamente conductas ilícitas con nuestros datos y que en el caso español puede imponer sanciones de hasta 600.000 euros.

Además, ciertos ilícitos de este tipo deben estar sancionados también penalmente —no sólo administrativamente—, conformándose así un marco legal integral de protección, que debiera limitar (obviamente erradicar es imposible) el uso fraudulento de nuestros datos.

RS: Los creadores de las redes sociales y profesionales, para quienes ponerlas en funcionamiento y mantenerlas es su negocio, ¿tienen alguna responsabilidad jurídica y/o ética frente al manejo y uso de la información personal de los usuarios que a ellas acceden?

ARG: Al menos en la Unión Europea tiene responsabilidad jurídica: tratan datos personales y por tanto les afectan las leyes de protección de estos datos. El problema es que en ocasiones se amparan en que sus sedes sociales y sistemas de información no radican en el país que les pide cuentas (en el caso europeo, a estos efectos todos los países son como si fuesen uno solo), con lo que tratan de eludir, o al menos de dilatar, sus responsabilidades. Tratándose de empresas gigantescas, económicamente hablando, esta táctica les permite en ocasiones evadirse, sobre todo si enfrente tienen a países con escaso poder de resistencia.

RS: ¿Cómo balancear la libertad de expresión, los datos personales y la forma de compartir información a través de las redes sociales? ¿Cuál debería ser la posición de las empresas en este sentido?

ARG: El problema tiene un gran calado. Vivimos en la sociedad de la información, que precisa y demanda manejar grandes volúmenes de datos, pero por otro lado el derecho a la intimidad personal está recogido en la Declaración Universal de los Derechos Humanos e incorporada a las constituciones de numerosos países. Balancear estos dos principios es legalmente complejo y constituye un problema de primer orden en nuestro mundo.

Bajo el punto de vista empresarial yo diría que debiera primar el habeas data, aunque sea una tentación muy fuerte no explotar todos los datos personales a los que pueda tener acceso la empresa. En cualquier caso, el cumplimiento estricto de la Ley debe ser el límite a imponerse en caso de duda.

RS: La seguridad, la privacidad y el manejo de los sistemas de información ¿son más una cuestión de tecnología? O, por el contrario, ¿tienen más que ver con formas de actuar de las empresas, o con relación a una legislación sobre

el alcance de tales temas y su aplicación?

ARG: Durante un tiempo se pensó por muchos que las soluciones de seguridad eran cuestiones meramente técnicas. Empero, hoy es comúnmente aceptado que por exhaustivas que sean las medidas técnicas sin adecuadas medidas organizativas y administrativas —o sea sin una adecuada gestión— no sólo es inútil sino que puede ser contraproducente, pues está comprobado que producen en muchos una sensación, obviamente falsa, de seguridad absoluta. Actualmente, valoramos más la formación en seguridad, los planes de contingencia, el análisis y gestión de riesgos, los planes de seguridad, etc., que las medidas exclusivamente técnicas. Lamentablemente, mientras que la técnica se puede conseguir con meras inversiones económicas, los aspectos citados tienen dimensiones que sobrepasan estas inversiones, siendo por tanto mucho más difíciles de llevar a cabo.

Al margen de lo anterior, la información es un bien más, pero su protección tiene una dificultad adicional: su carácter inmaterial. Así pues, debe tener la protección general de cualquier tipo de recurso, pero además la específica correspondiente a este carácter inmaterial. Y es así como estamos procediendo en todos los países.

RS: Teniendo en cuenta su experiencia en el desarrollo e implementación de la Ley Orgánica de Protección de Datos Personales española, ¿cuáles son los aspectos claves que un país debe considerar, para que una regulación sobre estos temas sea útil y procure la protección de los derechos de las personas frente a su información personal?

ARG: Bajo el supuesto de que el país tenga regulado mediante una ley este derecho, el aspecto más importante, en mi opinión, es complementar dicha ley con instrumentos ágiles que determinen lo más detalladamente posible los aspectos técnicos que requiere la protección de datos. Las leyes, por su naturaleza, tienen un desarrollo muy lento, por lo que tienen vocación de permanencia. Por ello, entre otros motivos, no entran a definir si para transmitir ciertos datos es obligado el cifrado, o si se deben mantener registros de auditoría o la política de identificación o control de accesos, etc. Y sin estos detalles, las leyes se quedan en los principios generales de la protección del derecho que nos ocupa, y las empresas en la incertidumbre (que puede venirles muy bien a algunas) acerca de las medidas concretas a adoptar para ajustarse a los principios contenidos en la ley. En España, y en otros países europeos (pocos), se ha optado por complementar la ley con otros desarrollos también legales, pero de menor rango (en España, un reglamento) que no exigen la participación del Parlamento. En España, por ejemplo, un reglamento es elaborado por uno o varios Ministerios y aprobado por el Consejo de Ministros. De este modo, este Reglamento puede entrar en los aspectos técnicos y organizativos y amoldarse más ágilmente a los rápidos avances tecnológicos al poderse cambiar con más facilidad que una ley.

RS: Desde su perspectiva, ¿cuáles son las tendencias procedimentales y técnicas en el tratamiento de los datos personales? ¿Habrá un resurgimiento de la seguridad de la información?

ARG: En cuanto a procedimientos, la tendencia más importante es el seguimiento de los estándares internacionales. Esto ha sido posible gracias al liderazgo asumido en esta materia por el SC27 del CTN71 del JTC1 de ISO/IEC, que está desarrollando la serie 27000, conjunto de normas técnicas de extraordinaria importancia, pues detallan

o detallarán (muchas están aún en proceso de elaboración) todo tipo de procedimientos de seguridad.

En cuanto a las tendencias técnicas, y sólo por citar las más relevantes, se están imponiendo las llamadas PET (*Privacy enhanced technology*) y el principio conocido como *privacy by design*, que impone la consideración de la privacidad (y por extensión de la seguridad) como un requisito más desde el diseño del producto, en vez de ser algo que sólo al final, y ya con difícil arreglo, se contemplaba.

RS: Y Arturo Ribagorda Garnacho se despidió con la siguiente reflexión.

ARG: Como complemento de mis respuestas, me gustaría hacer una reflexión acerca de cómo tomar los riesgos que he venido exponiendo. A menudo, cuando hablo en público o para algún medio de difusión, tengo la sensación de que ciertas personas pueden pensar que, siendo tantos los riesgos, estas tecno-logías no merecen la pena. Haríamos un flaco favor a la sociedad si alguien se quedase sólo con esta sensación. Las tecnologías de la información son un instrumento único en la historia de la Humanidad para crear un mundo más justo, próspero y longevo, y no podemos en absoluto renunciar a las mismas por temor a los riesgos que conllevan, que por otra parte son inmensamente menores que el que comportan otras tecnologías, como la nuclear, la química o, si se excede, la biotecnología. La única opción sensata —si no queremos retroceder varias décadas en la historia— es conocer los riesgos de la tecnología que nos ocupa para aprender a minimizarlos, pero sin rechazarla. En definitiva, vivimos en la sociedad del riesgo, certeramente teorizada por Ulrich Beck, pero no podemos vivir en la sociedad del miedo (y menos a las tecnologías de las que tratamos), pues como acertadamente afirmó Franklin D. Roosevelt: “A la única cosa que debemos tener miedo es al miedo mismo.”

Sara Gallardo M. *Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas “Uno y Cero”, “Gestión Gerencial” y “Acuc Noticias”. Editora de Aló Computadores del diario El Tiempo. Redactora en las revistas Cambio 16, Cambio y Clase Empresarial. Ha sido corresponsal de la revista Infochannel de México y de los diarios “La Prensa” de Panamá y “La Prensa Gráfica” de El Salvador. Autora del libro “Lo que cuesta el abuso del poder”. Investigadora en publicaciones culturales. Fue gerente de Comunicaciones y Servicio al Comensal en Andrés Carne de Res. Es corresponsal de la revista IN de Lanchile y editora de esta publicación.*