novática
CEPIS UPGRADE Revista de la Asociación de Técnicos de Informática

Novática, revista fundada en 1975 y decana de la prensa informática española, es el órgano oficial de expresión y formación continua de **ATI** (Asociación de Técnicos de Informática), organización que edita también la revista **REICIS** (Revista Española de Innovación, Calidad e Ingeniería del Software). ***Novática*** co-edita asimismo **UP**GRADE, revista digital de **CEPIS** (*Council of European Professional Informatics Societies*), en lengua inglesa, y es miembro fundador de **UP**ENET (**UP**GRADE ***E**uropean **NET**work*).

<http://www.ati.es/novatica/>
<http://www.ati.es/reicis/>
<http://www.upgrade-cepis.org/>

ATI es miembro fundador de **CEPIS** (*Council of European Professional Informatics Societies*) y es representante de España en **IFIP** (*International Federation for Information Processing*); tiene un acuerdo de colaboración con **ACM** (*Association for Computing Machinery*), así como acuerdos de vinculación o colaboración con **AdaSpain**, **AI2, ASTIC, RITSI** e **Hispalinux**, junto a la que participa en **ProInnova**.

Coordinación Editorial, Redacción Central y Redacción ATI Madrid
Padilla 66, 3º, dcha., 28006 Madrid
Tlfn.914029391; fax.913093685 <novatica@ati.es>
Composición, Edición y Redacción ATI Valencia
Av. del Reino de Valencia 23, 46005 Valencia
Tlfn./fax 963330392 <secreval@ati.es>
Administración y Redacción ATI Cataluña
Vía Laietana 46, ppal. 1ª, 08003 Barcelona
Tlfn.934125235; fax.934127713 <secregen@ati.es>
Redacción ATI Aragón
Lagasca 9, 3-B, 50006 Zaragoza.
Tlfn./fax 976235181 <secreara@ati.es>
Redacción ATI Andalucía <secreand@ati.es>
Redacción ATI Galicia <secregal@ati.es>
Suscripción y Ventas <http://www.ati.es/novatica/interes.html>, ATI Cataluña, ATI Madrid
Publicidad
Padilla 66, 3º, dcha., 28006 Madrid
Tlnf.914029391; fax.913093685 <novatica@ati.es>
Imprenta: Derra S.A., Juan de Austria 66, 08005 Barcelona.
Depósito legal: B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
Portada: Graffiti luminoso - Concha Arias Pérez / © ATI
Diseño: Fernando Agresta / © ATI 2003

Nº 207, septiembre-octubre 2010, año XXXVI

sumario

Monografía del próximo número: "*Visión por computador*"

RISEPTIS, Advisory Board of the Think-Trust Project

Confianza en la Sociedad de la Información: el informe RISEPTIS

Síntesis y traducción: Alonso Álvarez García (coordinador de la Sección Técnica "Tendencias Tecnológicas" de ***Novática***)

Resumen: este artículo contiene una versión abreviada del informe del mismo nombre elaborado por RISEPTIS (Research and Innovation in Security, Privacy and Trustworthiness in the Information Society, Investigación y Desarrrollo en Seguridad, Privacidad y Confianza en la Sociedad de la Información), el consejo consultivo del proyecto Think-Trust de la Unión Europa. El informe aborda cuestiones muy importantes (privacidad, seguridad, confianza…), sobre la base de que la Sociedad de la Información europea debe ajustarse a los principios que han dirigido a Europa desde sus orígenes, ya que los valores e instituciones democráticas, la libertad y el respeto de la intimidad son esenciales para la confianza en nuestra sociedad. También lo es el cumplimiento de la ley, la transparencia y el control públicos. La confianza social creada así es esencial. La versión completa de este informe está disponible en <http://www.think-trust.eu/downloads/public-documents/riseptis-report/download.html>.

Palabras clave: *confianza, informe, Internet, RISEPTIS, Sociedad de la Información, Think-Trust, Web.*

Autor

RISEPTIS, el Consejo consultivo para la investigación y el desarrollo en seguridad, privacidad y confianza en la sociedad de la información del proyecto europeo Think-Trust es el autor de este informe.

En abril de 2008 se estableció RISEPTIS con el objetivo de proporcionar orientación y visión sobre los retos políticos en la investigación en el ámbito de la seguridad y la confianza en la Sociedad de la Información. RISEPTIS ha sido apoyado con el proyecto Think-Trust financiado bajo la figura "Coordination Action" por la UE, cuyo objetivo es desarrollar un programa de investigación sobre la confianza en las TIC (Tecnologías de la Información y las Comunicaciones). RISEPTIS ha recibido el apoyo de más de 30 expertos en dos Grupos de Trabajo: (1) La seguridad, confiabilidad y confianza en la Internet del Futuro, (2) Privacidad y Confianza en la Sociedad de la Información. "Think-Trust" (FP7-216890) es un proyecto financiado por la Comisión Europea en el Séptimo Programa Marco (IST), dentro de la Unidad TIC F5 para la Confianza y Seguridad. <http://www.think-trust.eu/>

Resumen ejecutivo

La confianza es la esencia del orden social y la prosperidad económica. Es la base para las transacciones económicas y la comunicación entre las personas. Internet y la World Wide Web están transformando decisivamente la sociedad. La comprensión de cómo se pueden mantener los mecanismos de confianza a través de esta transformación es de crucial importancia.

Es evidente que algunos temas no son simplemente tecnológicos, ni puramente sociales. Sus complejas interacciones significan que la promoción de la confianza en la Sociedad de la Información requiere un enfoque interdisciplinario coordinado, que está muy en consonancia con la emergente ciencia de la web (*Web Science*).

RISEPTIS tiene la firme convicción de que los desarrollos tecnológicos en sistemas confiables serán más eficaces si se implementan a través de una fuerte interacción con las perspectivas sociales y empresariales, así como con la política y la regulación. Del mismo modo, estos últimos aspectos también pueden beneficiarse del conocimiento tecnológico. Los gobiernos quedarán en mejores condiciones para asumir la responsabilidad de dirigir este proceso de interacción.

Este informe hace algunas recomendaciones preliminares que pueden abrir perspectivas e iniciar las actividades en la dirección correcta. Las recomendaciones no sólo se refieren a la investigación, la innovación y el desarrollo de infraestructuras, sino también al marco jurídico, la aceptación social y la necesidad de cooperación internacional, para demostrar la interdependencia en la búsqueda de una Sociedad de la Información libre, democrática, y segura para los ciudadanos.

1. Introducción

La integración de las TIC (Tecnologías de la Información y las Comunicaciones) en nuestras vidas es un hecho transformacional.

Actúa como un catalizador para nuevas formas de creatividad, colaboración e innovación. Por otra parte, plantea cuestiones fundamentales respecto a la propiedad, la confianza, la privacidad, la identidad y la economía. Al mismo tiempo, nuestra creciente dependencia de las infraestructuras y servicios digitales ha oscurecido el manejo de nuestros datos personales y ha aumentado nuestra exposición a nuevas amenazas y malas prácticas en una escala alarmante.

2. La confianza en juego

En este capítulo vamos a discutir los conceptos de confianza, confiabilidad, identidad y privacidad. Estos se desarrollan en el contexto del marco jurídico de la Unión Europea sobre protección de datos y privacidad, y la evolución prevista de la tecnología.

2.1. Conceptos

Vemos la **confianza** como una relación entre tres partes (A confía en B para hacer X). Las partes A y B pueden, a este respecto, ser seres humanos, organizaciones, máquinas, sistemas, servicios o entidades virtuales. La evaluación de la confianza que A tiene en B para hacer X juega un papel importante en la decisión de A para participar en cualquier transacción, intercambio o comunicación entre ellos. Al reducir el riesgo, la confianza facilita efectivamente la actividad económica, creatividad e innovación. La confianza es muy dependiente del contexto. La confianza es más fácil de establecer cuando la identidad y/o cualquier otra información de autenticación (credenciales) sobre una tercera parte se conocen.

La confiabilidad se relaciona con el nivel de confianza que se puede asignar a una parte (B) por otra parte (A) para hacer algo (X) en el contexto de una relación. Es un atributo o propiedad asignado por la parte A a la parte B, que influye en la relación de confianza según la percepción de A. En este sentido, no es un valor absoluto y es dependiente del contexto. Los sistemas digitales deben dar al menos, y en la medida de lo posible, garantías cuantificables e información sobre los riesgos relacionados en materia de calidad de servicio, seguridad y persistencia, transparencia de las acciones y protección de datos, y privacidad de los usuarios, de conformidad con políticas predefinidas y reconocibles. Llamamos a los sistemas que satisfacen estas características: sistemas dignos de confianza (*Trustworthy Systems*).

Para una discusión más detallada sobre estos dos conceptos relacionados, pueden consultarse las referencias a Russell Hardin [1], Kieran O'Hara [2] y la *Trustguide* [3].

Identidad e **identificación** son conceptos difíciles de captar formalmente. En la identidad digital, en un sentido general, se incluyen todo tipo de atributos: los necesarios para nuestra identificación, los datos personales facilitados a través de los sistemas Web, información sobre todo tipo de páginas web que registran nuestras vidas profesionales; en general, toda nuestra huella digital.

El **anonimato** se refiere a la falta de información de identificación asociada a una persona física. Pseudoanonimato es la situación en la que se proveen ciertas credenciales pero que no pueden ser usadas para obtener directamente una identificación; sin embargo, la persona real sigue siendo identificable, si fuera necesario.

3. La tecnología en el contexto social

Para situar el debate y los conceptos presentados en el contexto de la vida cotidiana en este capítulo se discute el atractivo de determinados escenarios de servicios futuros y los peligros de la recopilación de datos cuando no está bien controlada, o en el mejor de los casos, no está suficientemente controlada por el interesado.

Antes de mostrar los escenarios, en primer lugar vamos a analizar brevemente dos de los problemas que afrontamos hoy en día a medida que avanzamos hacia la Sociedad Digital:

3.1. Los peligros de nuestra huella digital

Mucha gente deja datos personales en toda clase de sitios web. Del mismo modo, los usuarios publican todo tipo de información sensible y reveladora en las redes sociales. Ni la persona que sin darse cuenta revela su identidad y estilo de vida, ni el amigo de Facebook, a quien no parece importarle la revelación de datos de identificación a más personas de las que imagina, parecen estar preocupados por la huella digital que están creando.

3.2. Los eslabones más débiles de la cadena de almacenamiento de datos

Por su propia naturaleza, el proceso de transferencia y procesamiento de datos es un problema. Este procedimiento expone al atacante los datos en su forma más vulnerable. Por lo tanto, a pesar de medios sofisticados y recursos considerables desplegados para proteger la información sensible cuando está almacenada en forma digital, lo cierto es que la transferencia de estos datos significa que la cadena de confianza de datos no está completamente asegurada.

La percepción humana es uno de los factores que debe tomarse en consideración cuando se plantea la forma de informar sobre brechas en la seguridad de grandes empresas y gobiernos. Se argumenta que la confianza pública en la organización afectada caerá a medida que se conozcan los informes sobre sus vulnerabilidades. Si esa disminución de confianza está justificada o no, es algo que todavía está por verse. De cualquier manera, la percepción pública y la confianza de los usuarios es un problema importante en el mundo digital.

3.3. La vida en la Sociedad de la Información del futuro

3.3.1. Prólogo: descripción de un escenario práctico

Jorge es un estudiante de 23 años de edad. Vive en Londres con Teresa, su novia de 21 años. Teresa es una licenciada en Económicas que está ocupada actualmente a tiempo parcial en varios "trabajitos", mientras busca un puesto a tiempo completo. La abuela de Teresa, Elena, vive en Londres también, en una zona residencial tranquila.

Como la mayoría de sus amigos, Jorge y Teresa desean generar la menor "huella de carbono" posible por medio del uso de servicios en línea.

3.3.2. La visita "inteligente" de Jorge al dentista

Es viernes por la mañana y después de recordar a Jorge que debería renovar su tarjeta de identificación que caduca hoy, Teresa sale de su apartamento hacia un cercano despacho de abogados donde cada semana trabaja llevando la contabilidad financiera.

Cuando ha terminado de revisar un trabajo en curso, Jorge se conecta y accede a la página web del Gobierno sobre tarjetas de identidad. Aunque no es algo que él haya considerado anteriormente (o incluso haya creído posible), selecciona una tarjeta de identificación electrónica ó e-ID que tiene la capacidad para almacenar su perfil seguro de salud y una clave para acceder a su historial de salud si así lo precisa. Lo hace porque se da cuenta de que tener su información médica fácilmente a la mano puede ser útil y un ahorro de tiempo para más adelante.

Después de confirmar su elección de e-ID (dentro de una gama de opciones a su disposición), Jorge establece una cita con la Administración Nacional de Salud y más tarde va a la oficina más cercana dentro de su área. En el mostrador entrega su antigua tarjeta de identificación y el número de referencia de su reserva *online*. En cuestión de minutos, recibe su nueva tarjeta de identificación electrónica e-ID. No hay que esperar semanas, ni largas colas, y se hace sin rellenar papeleo.

Ahora que tiene su nueva tarjeta inteligente e-ID, Jorge piensa que puede ser el momento para hacer una largamente demorada visita al dentista. Gracias a una de las aplicaciones cargadas en su tarjeta, Jorge inserta el dispositivo en el lector de su PC y, a través del navegador web, selecciona el Dr. Malcolm Bond, un dentista cercano, para su segunda cita del día.

Cuando la cita se confirma, Jorge hace clic en los registros dentales dentro de una lista de opciones que le permite decidir qué parte de su información médica es compartida con el proveedor de servicios web del dentista. Esto le ahorrará al Dr. Bond los inconvenientes de hacer de nuevo un nuevo conjunto de radiografías, lo que significa menos tiempo en la silla del dentista para Jorge. ¡Y quizá también una factura menor! Jorge está un poco preocupado, sin embargo, sobre la transferencia de sus registros dentales a través de Internet. También se pregunta si una copia de sus registros dentales quedará ahora almacenada permanentemente en la web del dentista. Tiene la intención de preguntar al Dr. Bond sobre esto, aunque no es muy optimista acerca del conocimiento que tenga el dentista sobre la transferencia o el almacenamiento de datos "Una explicación del dentista, de la gente de las tarjetas o del portal web sería útil", piensa Jorge, "pero este sistema es muy cómodo y supongo que mi información va a estar bien", concluye.

3.3.3. La inolvidable tarde de compras de Teresa

Después de terminar su trabajo en el bufete, Teresa se decide por una "terapia" de compras en el centro comercial local. Su abuela, Elena, les visitará para comer el próximo domingo y a Teresa le gustaría comprarse un nuevo traje para impresionar a su abuela. La etiqueta RFID en la chaqueta es captada por un lector en el exterior de unos grandes almacenes. El lector envía el número de serie de la etiqueta a un Servicio de Localización, el cual transmite estos datos a un sistema centralizado que gestiona los datos relacionados con el consumo de esa área en particular.

Teresa es ajena a todas estas acciones, lo que implica su ropa, su ubicación y su número de teléfono móvil. Así, cuando el sistema reconoce a Teresa y examina sus preferencias antes de presentarse, lo primero que recibe de este sistema es un mensaje de texto en su teléfono móvil, ofreciéndole un descuento del 20% en la tienda.

Después de hacer su selección, Teresa usa la tarjeta de crédito que comparte con Jorge para pagar. El cajero le pregunta por una identificación para verificar su identidad, bien sea un pasaporte o la tarjeta de identificación. Sin embargo, Teresa no tiene su tarjeta de identificación con ella y mantiene su pasaporte en la caja fuerte de su apartamento. Su antigua tarjeta de identificación de estudiante no es aceptable para esta transacción y por lo

tanto, el cajero registra el suceso como un "fraude potencial" en el sistema de pago de la tienda. Sin medios para identificarse a sí misma y, por tanto, para verificar la propiedad de la tarjeta de crédito que acaba de presentar al cajero, Teresa descubre que está empezando a sentirse muy avergonzada delante de los otros compradores en la tienda. No se da cuenta que este incidente con la autenticación está a punto empeorar.

Por razones de seguridad, se envía una alerta a la agencia emisora de tarjetas de crédito para que verifique el número de tarjeta de crédito frente a otras actividades potencialmente fraudulentas. Por desgracia para Teresa, el exceso de celo del sistema afirma que ha habido otra posible acción fraudulenta con esta tarjeta de crédito recientemente, y la agencia informa a la policía. El sistema de gestión de la Policía accede al Servicio de Localización para obtener la ubicación del consumidor y enviar a dos policías desde la comisaría más cercana para hablar con una abrumada Teresa. Al ser co-responsable de la tarjeta de crédito, Jorge también emprende camino a la tienda, tras haber recibido un mensaje SMS informándole de la posible actividad criminal generado por la infraestructura de la agencia emisora de la tarjeta crédito.

3.3.4. Unas vacaciones muy modernas

Por suerte, aunque fuera del conocimiento de Teresa y Jorge, la tarjeta de crédito no fue utilizada de ninguna forma sospechosa recientemente. Al contrario, cuando la tarjeta se utilizó mientras ella y Jorge estaban en unas breves vacaciones en Italia hace unas semanas, la agencia agregó automáticamente esta actividad como "potencialmente fraudulenta". Esto se debió a que el restaurante donde cenaron Jorge y Teresa mientras estaba de vacaciones había tenido varias denuncias por fraude con tarjetas de crédito.

Este fue el único inconveniente del viaje de la pareja a Italia, ya que todo lo demás fue perfecto durante sus vacaciones. Jorge había decidido repentinamente ofrecer a Teresa un pequeño descanso y reservó sus vuelos en el último minuto, a través de una web de vacaciones. Sin embargo, no tuvo tiempo de reservar alojamiento por adelantado –sólo tuvieron tiempo de hacer las maletas y dirigirse al aeropuerto. Mientras esperaba para embarcar, Jorge recibió un formulario de preferencias de hotel en su teléfono móvil enviado desde una cadena hotelera. Jorge se preguntó por un instante cómo llegó este mensaje a su teléfono móvil, pero en realidad no lo consideró una invasión de su privacidad. "Debe haber algún tipo de leyes para que las grandes empresas no puedan aprovecharse de ti de este modo" le comentó alguien una vez en la cafetería de la Universidad. "A pesar de todo merece la pena probar", pensó. Después de consultar con Teresa cumplimentó el formulario, incluyendo la parte dedicada a las preferencias de alimentación.

Al aterrizar en la terminal del aeropuerto en Roma, el teléfono móvil de Jorge recibió un mensaje SMS y él quedó muy contento al ver que le enviaban una lista de hoteles y restaurantes que coincidían con su lista de preferencias.

A través de la misma interfaz en el teléfono móvil, la joven pareja eligió lo que parecía ser un hotel romántico, y posteriormente recibió otro SMS informándoles de que un vehículo de cortesía del hotel estaba en camino para recogerlos en el aeropuerto. Después de llegar a "Casa Della Rosa", Jorge y Teresa recibieron un menú a medida, que sólo incluía platos que se adaptaban a las preferencias que había cumplimentado mientras esperaban su vuelo en Londres.

Como le volvería a ocurrir unas semanas más tarde al permitir el envío de información médica al dentista, Jorge se pregunta si sus preferencias se almacenan de forma insegura e incluso si pueden robarse, pero asume ingenuamente que sus datos (ahora almacenados en algún lugar de Italia) no formarán parte de cualquier estudio de mercado en Londres.

3.3.5. Nos preocupamos por usted

La abuela de Teresa, Elena, se siente un poco sola. Desde que tiene todo tipo de sensores de "salud y bienestar" instalados en su apartamento, su familia sabe que va a recibir una alerta si algo le ocurre; por lo tanto, no la llaman para verificar cómo se encuentra con la frecuencia de antes. Elena les echa de menos, pero el intercambio de videos y fotos y llamadas multimedia la ayudan a llenar los vacíos entre las visitas.

Además de los detectores de movimiento instalados en cada habitación de su apartamento y del sensor de ritmo cardíaco en su bañera, tiene una serie de sensores en su cocina que pueden detectar fugas de gas, humo y exceso de agua en el suelo. Elena tiene un botón de pánico que está enlazado con la oficina de salud local. Ella cree que los escáneres RFID en su nevera y armarios son de gran utilidad para la gestión de sus compras de comestibles. Su suscripción al servicio de entrega a domicilio de un supermercado cercano significa que recibe un envío semanal con todas sus necesidades, sin tener que afrontar las inclemencias del tiempo.

A Elena también le gusta hacer su revisión de bienestar regular, a través de su portal de servicios de salud. Además de observar qué alimentos está consumiendo, estos exámenes también toman datos de los sensores de ritmo cardíaco y de otros sensores instalados en su casa. Sin embargo, a pesar de esta atención mediante la última tecnología que recibe, Elena se siente un poco incómoda por el hecho de que su proveedor de servicios de salud esté recogiendo tanta información acerca de ella. Recientemente, éste le informó de que ahora va a comparar los resultados de sus exámenes médicos con los de otras mujeres de su edad de todo el país.

El proveedor de servicios de salud dice que este trabajo de elaboración de perfiles les ayudará a decidir sobre factores de riesgo, por ejemplo, predecir con mayor precisión posibles ataques de corazón. Como resultado, van a ofrecer a Elena un asesoramiento sobre su dieta personalizado. Pero esa recopilación de información personal, junto con las frecuentes noticias en periódicos y televisión sobre la pérdida o robo de CDs que contienen datos personales, hace que Elena esté preocupada. Teresa, su nieta, también le ha dicho que su proveedor de servicios de salud recibe importantes ofertas económicas de compañías de seguros para acceder a la información recogida. En el entorno financiero actual, Elena piensa que estas ofertas deben ser cada vez más tentadoras y está ansiosa por conocer los efectos reales a largo plazo de tener su hogar "a la última".

Elena piensa en cambiar de proveedor de servicios de salud. Esto significaría transferir y compartir todos sus datos (incluyendo los financieros) con un nuevo proveedor. Lo que ella no sabe, sin embargo, es que esto sólo será posible si los sistemas de intercambio y almacenamiento de datos de ambos proveedores son compatibles. Tampoco se sabe quién controla realmente sus datos ahora o exactamente cómo se van a utilizar. Llamó por teléfono a su actual proveedor de servicios de salud y fue puesta en contacto con la llamada irónicamente "Línea de ayuda", pero sólo oyó ofertas de nuevos servicios por medio de voces automatizadas.

3.3.6. La oficina invisible

Pocos días después del problema con la tarjeta de crédito y la policía en el centro comercial, Teresa recibe un correo electrónico pidiéndole que presente su currículum para un puesto temporal en una empresa recién creada, llamada *CEANNAIM*. Antes de decidir si optará al trabajo, Teresa investiga un poco en Internet sobre esta empresa.

Descubre que *CEANNAIM* es una compañía que trabaja "en la Nube" (*Cloud*). Cuenta con una red de empleados distribuidos por toda Europa. Los empleados son esencialmente subcontratistas, y cada uno recibe un contrato personalizado que están obligados a firmar digitalmente antes de remitirlo a la central de la compañía. La ubicación geográfica declarada por el empleado en el contrato

determina la jurisdicción legal y financiera para cualquier acción emprendida por la empresa o el empleado.

Siendo reacia a volar, Teresa se siente atraída por el hecho de que la organización no tiene oficina física y, por tanto, las reuniones de empresa se llevan a cabo mediante el uso de herramientas de conferencia online en la Nube. Los empleados de CEANNAIM usan almacenamiento *online* para los documentos de la compañía; lo mismo ocurre con el sistema de gestión de relaciones con el cliente (CRM) y el software financiero.

También descubre que el empleo en la empresa es muy dinámico, es decir, que las personas se incorporan y salen continuamente. Cuando se requiere un perfil determinado dentro de la empresa, su área de recursos humanos (RRHH) explora varias comunidades de Internet en busca de las personas idóneas. Una vez que se ha seleccionado un cierto número de posibles candidatos, RRHH procede a recabar información en distintas redes sociales con el fin de obtener una imagen más completa de sus futuros empleados.

Teresa no es consciente de esta práctica invasiva en la búsqueda de información y sabe que puede formar parte de la compañía por un corto período. Sin embargo, el trabajo es escaso y necesita el dinero. Por lo tanto, decide solicitar el trabajo. A medida que introduce los datos solicitados a través del portal recursos humanos de la empresa, no advierte que sus nuevos empleadores ya han creado un perfil, y que ella sabe muy poco acerca de las condiciones y expectativas de trabajo de sus nuevos compañeros distribuidos por toda Europa.

3.3.7 Los anuncios gratuitos de Jorge

Unas semanas después de volver de sus cortas vacaciones en Italia, Jorge empieza a recibir mensajes de texto en su teléfono móvil desde *SEIRBHIS*, una empresa de publicidad, ofreciéndole descuentos en varios restaurantes en Londres. Al principio, simplemente los ignora, pero a los pocos días de recibir este "*spam*", se pone en contacto con su proveedor de red para tratar de averiguar de dónde vienen estos mensajes.

A través de su centro de atención telefónico, el proveedor le informa que, aunque los mensajes son originarios del Reino Unido, no es posible revelar el número de teléfono de origen. Le preguntan a Jorge si se ha suscrito a algún servicio nuevo recientemente y Jorge dice que no, pero afirma que él ha respondido recientemente a una encuesta sobre los hoteles y comida que había sido enviado mientras estaba en el aeropuerto. "¡Ajá!", dice el operador, quien explica a Jorge que la información sobre preferencias de hotel o comida habrá sido enviada a una empresa de marketing desde un país destino (Italia, en este caso) y que la utilizan para sugerir servicios personalizados a los visitantes. Si bien la empresa de marketing cumplió con la declaración de privacidad suministrada a Jorge de no distribuir sus datos de preferencias a cualquier empresa hotelera italiana, no hizo ninguna referencia a no compartir sus datos con empresas asociadas en toda Europa, incluyendo SEIRBHIS en el Reino Unido. "Esta es probablemente la forma en la que consiguió su número", concluye el operador.

Jorge podría continuar ahondando en el asunto y presentar una queja a "alguien", pero en este momento ni siquiera sabe en qué país se almacenan sus datos y los de Teresa. Jorge decide dejar inmediatamente al proveedor de red que facilitó esta intrusión y jura no volver a visitar el hotel y el restaurante que él y Teresa escogieron en sus vacaciones ya que los considera cómplices.

3.3.8. Epilogo: la huella digital es alargada

En estos escenarios e historias, los tres personajes se apoyan mucho en las posibilidades del mundo digital que tienen a su alrededor. Por lo tanto, si un atacante monitorizara la información transferida y compartida desde sus PCs y teléfonos, podría obtener una cantidad significativa de datos sobre ellos.

Por ejemplo, si alguien puede acceder a la actividad de Jorge *online*, podría ver que:
1) Reservó vuelos desde Londres a Italia recientemente;
2) Ha solicitado una nueva tarjeta de identificación que contendrá sus datos médicos;
3) Había dos citas en el mismo día en distintas direcciones (la administración de Salud y la consulta del dentista).

El atacante también puede descubrir los registros dentales de Jorge e información de sus antecedentes médicos. Si el atacante es capaz de violar los registros del teléfono móvil de Jorge, podría obtener información acerca de la comida favorita de Jorge y Teresa, y el tipo de hotel en el que desean alojarse, así como la dirección exacta de su ubicación elegida en Italia.

Lo que también podría ser fácilmente descubierto acerca de la pareja es que tienen un amigo cercano o familiar con el hablan de forma regular, ya que, si alguien estaba vigilando el tráfico de Internet, se daría cuenta de que hay una serie de llamadas de vídeo entre la pareja y un usuario en particular. Sería razonable deducir que existe una relación estrecha entre los dos interlocutores, especialmente si las llamadas se llevaron a cabo fuera de las horas normales de oficina. La abuela Elena quedaría expuesta si un atacante tuviera acceso a sus comunicaciones con el servicio de entrega a domicilio del supermercado. Por no hablar de la vulnerabilidad en el caso de que alguien penetrara en los sistemas de su proveedor de servicios de salud. Si un atacante intercepta tanto las sugerencias de dieta que recibe, como la lista de alimentos generada automáticamente por su cocina inteligente, entonces podría ver si ella sigue o no estos consejos (su seguro de salud podría estar interesado en esta información).

La naturaleza *online* de *CEANNAIM*, la empresa que invita a Teresa a presentar su CV, significa que hay muchas violaciones potenciales de protección de datos. Debido a que CEANNAIM emplea trabajadores en diversos estados de Europa, es posible que necesite proporcionar los datos de todos sus trabajadores en cada uno de esos países, con el fin de establecer los medios para reclamaciones legales y financieras. Los datos facilitados por Teresa, así como el perfil elaborado por *CEANNAIM*, a partir de su discutible búsqueda en redes sociales, puede acabar almacenada en diversos países de toda Europa. El control de Teresa sobre la propiedad de sus propios datos está, por tanto, comprometido. Y eso sin que se haya producido aún un fallo de seguridad en la empresa que pueda comprometer los datos de las herramientas de conferencias y almacenamiento on-line.

3.3.9. Deducciones de super-detective

Si uno de los posibles atacantes pudiera obtener acceso a todos los datos en bruto disponibles, tanto de forma deliberada como inadvertidamente, de los personajes de las historias anteriores, también podría deducir más información contextual de esas personas, sus movimientos y las relaciones entre ellos; con ello podría constituir un perfil rico y potencialmente lucrativo. Entre otros detalles, podría suponer que:

- Jorge y Teresa mantienen una relación;
- Una mujer mayor llamada Elena es la abuela de uno de ellos;
- La relación entre la joven pareja y Elena es estrecha y se llevan bien;
- Elena no siempre sigue los consejos dietéticos que recibe;
- A Jorge y Teresa les gusta viajar por Italia;
- Teresa está en paro, pero está buscando activamente trabajo;

4. Hacia una Sociedad de la Información merecedora de nuestra confianza

En los capítulos anteriores hemos expuesto distintos problemas que nos esperan en el desarrollo futuro de una Sociedad de la Información, donde las comunicaciones, capacidad de procesamiento y la prestación de servicios ubicuos se están convirtiendo en una parte integral de nuestra vida física y social, es decir de la vida real.

Vemos el riesgo de que el péndulo oscile demasiado en la dirección de perder la con-

fianza en la forma de organizar y gestionar nuestra sociedad debido a la falta de control y transparencia, y a una delincuencia que no pueda ser controlada por la policía debido a su carácter mundial.

Nuestras recomendaciones pretenden ser positivas. La confianza futura en la Sociedad de la Información se basará en un ecosistema de comunicaciones, capacidad de proceso de datos y prestación de servicios que deberá respetar los valores humanos, sociales y culturales. En las recomendaciones que hacemos a continuación nos centraremos en algunas de las cuestiones básicas que facilitan o estimulan el desarrollo de ese ecosistema.

4.1. Investigación y Desarrollo tecnológicos

Nuestra primera recomendación se centra en el desarrollo de una agenda de investigación sobre la Confianza en las TIC. Cabe señalar que existe una clara continuidad aquí con el vigente programa de trabajo 2009-2010 para las TIC del 7º Programa Marco. Ya se han realizado importantes actividades de investigación, pero ahora hay que considerar su extensión y una reorientación de su foco. Los grupos de trabajo que apoyan a RISEPTIS proponen cuatro áreas principales donde fijar la atención:

1) Seguridad en entornos de red, servicios y computación (heterogéneos)
Debe incluirse la elaboración de retos de seguridad para el diseño de arquitecturas, protocolos y entornos que definan el futuro de los sistemas TIC a gran escala y en red a nivel mundial. En concreto, éstos se centran en la Internet del futuro; el *Cloud Computing*; la "Internet de las Cosas", con su mezcla de entornos y modos de computación; componentes de comunicaciones y almacenamiento; e infraestructuras globales de servicios.

El polimórfico futuro de la confianza en Internet es una cuestión importante, que requiere seguridad en el núcleo de la red principal y en los nodos críticos a través de protocolos y arquitecturas a gran escala y con una alta velocidad de transferencia de datos.

La confianza en la computación global requerirá seguridad contextual con servicios inteligentes en la Nube para compartir información, así como entornos cooperativos que ganen aceptación social, con el fin de transmitir la sensación de control del entorno digital. También se requieren nuevas infraestructuras, utilizando las TIC como una herramienta para hacer los objetos del mundo real más dignos de confianza en los distintos entornos de aplicación.

2) Infraestructuras de confianza, privacidad y gestión de reclamaciones (meta-sistemas)
Las *infraestructuras de confianza* públicas y privadas deben ser proporcionadas por nuevos actores confiables que ofrezcan garantías bajo varios modelos de confianza. Requerirán: arquitecturas de confianza y nuevos protocolos para delegar la confianza total y parcialmente; instrumentación de la confianza y herramientas de alto nivel para el usuario final; instrumentos cognitivos y de aprendizaje para la confianza; y los servicios gestores de perfiles y comunidades.

3) Principios básicos de ingeniería
Dedicados a establecer la confianza, la privacidad y la seguridad en el espacio digital y desarrollar medidas o modelos de calificación para ello; implementar las propiedades de transparencia, responsabilidad y privacidad para las principales entidades y modelos informáticos; desarrollar indicadores y herramientas para la evaluación cuantitativa de la protección y la seguridad predictivas en un entorno complejo; y la composición y evaluación de los sistemas a gran escala.

4) Políticas de datos, gobernanza y aspectos socioeconómicos
Deben incluirse las cuestiones de política y de gobierno relacionados con la informática en la Web y en la Nube ubicua. Esto estimulará el desarrollo de conceptos tecnológicos de seguridad, así como responsabilidad y compensación.

Con el fin de hacer frente a los problemas globales de la Internet del futuro, tenemos que abordar la gobernanza multipolar y las políticas de seguridad entre un gran número de participantes y competidores.

Recomendación 1: La UE debería estimular la investigación interdisciplinaria y el desarrollo y despliegue de tecnología que responda a las necesidades de confianza y seguridad en la Sociedad de la Información. Las áreas prioritarias son:
· Seguridad en entornos (heterogéneos) de red, servicio y computación, incluyendo una Internet del Futuro confiable.
· Marcos de gestión de la confianza, privacidad e identidad, incluyendo estándares y garantías de seguridad compatibles con la interoperabilidad TIC.
· Principios de ingeniería y arquitecturas para la confianza, la privacidad, la transparencia y la fiabilidad, incluyendo métricas y tecnologías de apoyo (por ejemplo, la criptografía). · Gobernanza de políticas y datos y sus aspectos socio-económicos relacionados, incluida la responsabilidad, la compensación y la multipolaridad de la gobernanza y de su gestión.

4.2. La interacción de la tecnología, la política, el derecho y la socioeconomía

Las palabras clave de una visión para el futuro de la Sociedad de la Información deben ser *confianza* y *fiabilidad*. Ellas forman la base de nuestras comunicaciones, las operaciones y el comportamiento económico y social en el espacio privado, público y privatizado.

Las propiedades relacionales y contextuales de la confianza hacen que sea imposible una aproximación completamente ingenieril a la confianza en la vida digital. Siempre dependerá de las emociones, circunstancias y estados de ánimo personal, y cambia entre culturas y entornos sociales.

Sin embargo, hay elementos que pueden ayudar a establecer la confianza, algunos basados en las leyes y reglamentos existentes que con cambios relativamente pequeños podrán ser aplicados plenamente.

También ayudará al establecimiento de la confianza la construcción de nuevos mecanismos y herramientas que ayuden a los ciudadanos, empresas y organismos públicos a controlar sus activos y flujos de acciones.

Recomendación 2: La UE deberá apoyar iniciativas concretas que reúnan tecnología, política, y a actores jurídicos y socioeconómicos en el desarrollo de una Sociedad de la Información confiable (la organización "*Partnership for Trust in Digital Life*" [4] podría ser un primer paso).

4.3. Un marco común europeo para la gestión de identidades

Un elemento esencial para garantizar una sociedad de la información confiable es un marco para la gestión de la autenticación que incluya los sistemas de identificación electrónica gubernamentales. En cualquier relación, la confianza se construye principalmente sobre la información acerca de la otra parte. Este marco es necesario para el control, no repudio y la transparencia. Europa necesita un marco común que permita la federación y la interoperabilidad entre todos estos sistemas. Al mismo tiempo, tenemos que contar con instrumentos para el análisis forense.

La Comisión ha propuesto el desarrollo de acciones europeas a gran escala en identidad electrónica y comunicaciones [5]. Los miembros de RISEPTIS han desarrollado un plan de trabajo con las acciones detalladas que deben adoptarse para lograr un marco común europeo.

Recomendación 3: La UE, junto con los Estados miembro y las partes interesadas del sector, deberán dar mayor prioridad al desarrollo de un marco común de la UE para la gestión de identidades y autenticación que garantice el encaje con el marco jurídico sobre protección de datos personales y privacidad, y que permita un

amplio espectro de actividades que vayan desde la administración pública o la banca, con autenticación fuerte cuando sea precisa, hasta actividades web sencillas llevadas a cabo bajo anonimato.

4.4. Desarrollo ulterior del marco jurídico de la UE para la protección de datos y privacidad

Hay discusiones en curso para un mayor desarrollo del marco jurídico de la UE para protección de datos y privacidad. En la Directiva propuesta [6] se ha establecido la notificación obligatoria de violaciones de seguridad. Algunos investigadores [7] han cuestionado la completitud de la definición de datos personales en relación a la información basada en ubicación y perfil. Los desarrollos tecnológicos en tratamiento y vinculación de datos sugieren que en el futuro todos los datos serán susceptibles de ser considerados datos personales en algún momento.

El desarrollo de los aspectos legales debe ser parte de una política integral que debe estar estrechamente relacionada con el progreso tecnológico. Esto permitirá una reacción más eficiente.

Recomendación 4: La UE deberá favorecer el desarrollo de la protección de datos y privacidad en el marco jurídico de la UE como parte de un ecosistema global y coherente que incluya legislación y tecnología, así como otros marcos, instrumentos y políticas relevantes. Debe hacerlo de manera conjunta con la investigación y desarrollo tecnológicos.

4.5. Proyectos de innovación a gran escala

Se ha afirmado que Europa está en una posición destacada para tomar la iniciativa en la innovación y el desarrollo tecnológico de la confianza y la seguridad. Sin embargo, hay que promover proyectos europeos a gran escala que saquen el máximo provecho de estos puntos fuertes de Europa.

Europa debe desarrollar un ecosistema tecnolegal para la confianza, la seguridad y privacidad que debe someterse a la cooperación global, fomentar el crecimiento europeo y proporcionar una base sólida para la cooperación internacional.

Recomendación 5: La UE, junto con los agentes públicos y sectoriales deben lanzar acciones a gran escala para construir una Sociedad de la Información confiable que saque partido de las fortalezas europeas en la comunicación, la investigación, las estructuras jurídicas y los valores sociales; por ejemplo, con una Nube que se ajuste a la legislación europea .

4.6. La cooperación internacional

Internet y la Web forman una infraestructura global para la comunicación, el procesamiento de datos y la prestación de servicios. Se deben emprender pasos para llegar a acuerdos de cooperación e interoperabilidad internacionales, y para trabajar en medidas y estándares internacionales sobre la gobernanza, la lucha contra la delincuencia, la gestión de identidades, la seguridad y otros temas relevantes.

Recomendación 6: La UE debería reconocer que, para ser eficaz, debe abordar la dimensión mundial y el compromiso de fomentar en los debates internacionales, con carácter de urgencia, la promoción del desarrollo de estándares abiertos y marcos federados de cooperación en el desarrollo de una Sociedad de la Información global.

Notas

[1] R. Hardin. *Trust & Trustworthiness*, Russell Sage Foundation, New York 2002.

[2] K. O'Hara. *Trust: From Socrates to Spin*, Icon Books, Cambridge 2004. ISBN-10: 184046531X.

[3] H. Lacohee, S. Crane, A. Phippen. *Trustguide: Final report*, <http://www.trustguide.org.uk/>.

[4] Trust in Digital Life Consortium. <http://trustindigitallife.eu/Home%20Page.html>.

[5] Comisión Europea. COM (2009)116: A Strategy for ICT R&D and Innovation in Europe: Raising the Game. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0116:FIN:EN:PDF>.

[6] Parlamento Europeo. Propuesta para un marco regulatorio para las redes y servicios de comunicaciones electrónicas (*Proposal for a Regulatory framework for Electronic communication networks and services*).

[7] K. Rannenberg, D. Royer, A. Deuker. *The Future of Identity in the Information Society*, Springer 2009. ISBN-13: 978-3-540-88480-4.