Ecuador y la Privacidad en Internet: Una Aproximación Inicial

Estrada J. A.*; Estrada J. C.; Rodríguez A.*; Tipantuña C.***

**Escuela Politécnica Nacional, Facultad de Ingeniería Eléctrica y Electrónica, Quito, Ecuador*
e-mail: {jose.estrada; ana.rodriguez; christian.tipantuna}@epn.edu.ec
*** e-mail: jancoej@gmail.com*

Resumen: La privacidad es un concepto muy relativo y sujeto al sentimiento de seguridad que tenga un usuario. Aunque es común estudiar la percepción de privacidad de los usuarios de Internet, casi nada se ha discutido sobre este derecho en Ecuador. Por ello, tampoco se han puesto de manifiesto algunos riesgos a la privacidad de los usuarios que están latentes en el contexto nacional. Ya que la administración pública en Ecuador experimenta una explosiva integración al "gobierno en línea" en la que se gestiona información de los ciudadanos, resulta crucial estudiar la privacidad de estos datos desde su perspectiva local y en el marco de los riesgos latentes que dicha privacidad enfrenta. Se realizó un estudio de percepción de privacidad mediante una encuesta para determinar, entre otras cosas, qué información es considerada sensible por los usuarios. Además, se hizo un análisis experimental no intrusivo de algunos servicios de información ecuatorianos en Internet, para determinar si la percepción de los usuarios concurre con los riesgos de su privacidad en Internet. Se encontró que los usuarios están claramente conscientes de las amenazas a su intimidad en línea. Lamentablemente, la información que consideran "no sensible" podría permitirle a un atacante obtener información que los usuarios consideran "muy sensible", con lo que la conciencia inicial que muestran no resultaría suficiente para proteger su privacidad.

Palabras clave: Privacidad, Ecuador, percepción, seguridad, Internet, riesgos

Abstract: Privacy is a very relative concept subject to the user's feeling about security. Although it is common to study the privacy perception of Internet users, little has been discussed about that in Ecuador. Thus, the risks of user privacy in the local context have not been highlighted. Since public administration in Ecuador suffers an explosive integration into the e-government where information on citizens is managed, it is crucial to study these data privacy from a local view and within the framework of the underlying risks that such privacy faces. We performed a study of privacy perception by means of a poll which helped us to determine how concerned users are about some types of information. Moreover, we did an experimental nonintrusive analysis of some Ecuadorian information services available on Internet in order to find if the users' perceptions match their privacy risk on Internet. We found that users are aware of the threats to their privacy online. Sadly, the data they find "non sensible" could allow an attacker to get information that users find "very sensible", so the initial awareness they show may not be enough to protect their privacy.

Keywords: Privacy, Ecuador, perception, security, Internet, risks

1. INTRODUCCIÓN

Desde hace casi una década, el Ecuador (y el mundo con anterioridad a eso) sufre una revolución en la gestión de la información, catalizada por la masificación del acceso a Internet y la integración de una gran cantidad de procesos cotidianos en esta red global.

La virtualización de las interacciones entre usuarios, ciudadanos, consumidores y autoridades o proveedores, a través de la infraestructura que ofrece Internet (en lo que se conoce como gobierno en línea), representa una tendencia que no se detiene [21] debido a las ventajas que supone su aplicación [18]. En ese contexto, una serie de iniciativas de gobierno en línea promovidas los últimos años se han llevado a cabo en Ecuador, orientadas, entre otras cosas, a la transparencia de la gestión pública, la consolidación de la información pública de los ciudadanos y a la realización electrónica de trámites.

A pesar de la eficiencia, la reducción de costos y la transparencia que promueven los mecanismos de gobierno en línea, existen en estos contextos algunos inconvenientes que podrían poner en riesgo la seguridad de la información de los ciudadanos. Esto se debe a que dichos mecanismos concentran grandes cantidades de información en servicios informáticos accesibles públicamente desde Internet.

Aquellos datos no son necesariamente privados (sino personales) pero, al combinarse los que se obtienen de distintas fuentes públicas, se podría vulnerar la privacidad de un individuo, al utilizar esos datos para inferir información privada.

No obstante, poco se conoce en Ecuador sobre los riesgos relativos a la privacidad, causados por la exposición indiscriminada de información personal. Menos todavía se ha investigado acerca de la percepción que existe sobre estos tópicos, y muy superficialmente se ha discutido acerca de la necesidad de legislación orientada a la protección de los datos. En este artículo hacemos una aproximación inicial para medir esta percepción de los usuarios sobre los riesgos a su privacidad. De manera complementaria, hacemos un trabajo exploratorio para obtener una primera impresión de los problemas de privacidad (datos personales expuestos) que podrían derivarse de la información contenida en ciertos servicios públicos en línea en Ecuador (Seguridad Social, Servicio de Rentas Internas, Registro Civil, etc.). Así, se intenta evaluar el impacto que podría generar el aprovechamiento de estos riesgos manifiestos en la privacidad de los ciudadanos, considerando la percepción medida de estos ciudadanos sobre dichos riesgos.

El resto del artículo está organizado como sigue: en la Sección 2 se presenta un análisis del estado actual de la privacidad en el Ecuador desde el punto de vista jurídico y cultural. En la Sección 3 se describe el escenario y metodología utilizados para realizar el presente estudio, tanto en cuanto a la medición de la percepción como al análisis exploratorio de la privacidad en línea en el Ecuador. En las secciones 4 y 5 se plantean los resultados obtenidos al determinar la percepción de los usuarios sobre su privacidad en Internet en Ecuador y al investigar las amenazas presentes a dicha privacidad en los sistemas de información dispuestos para el ciudadano. En la Sección 6 se plantea una discusión sobre un escenario de riesgo a la privacidad de un usuario puntual. Finalmente, en la Sección 7 se presentan las conclusiones de este trabajo.

2. LA PRIVACIDAD EN EL ECUADOR DE HOY

Ecuador es un país con casi 16 millones de habitantes, en el que la penetración de Internet en los últimos 7 años ha crecido exponencialmente, tal como puede observarse en la Fig. 1. Este incremento se debe, en primera instancia, a la reducción de los costos de acceso a Internet y en gran medida, también, a la intensa promoción del uso de canales electrónicos para la interacción con la empresa pública y privada (trámites en línea). De acuerdo al último censo de TICs realizado por el INEC (Instituto Nacional de Estadísticas y Censos) [5] en 2013, es evidente el incremento de los índices de uso de tecnología de comunicaciones. Seguramente por la tardía expansión del servicio de Internet en Ecuador (comparar con la evolución de la penetración de Internet en EEUU en Fig. 1), la preocupación sobre temas de privacidad en línea no ha sido discutida aún con profundidad en el país.

2.1 Legislación Ecuatoriana sobre Privacidad

La privacidad está consagrada como un derecho en la Declaración Universal de los Derechos Humanos de las Naciones Unidas [12]. Sin embargo, es común pensar que la

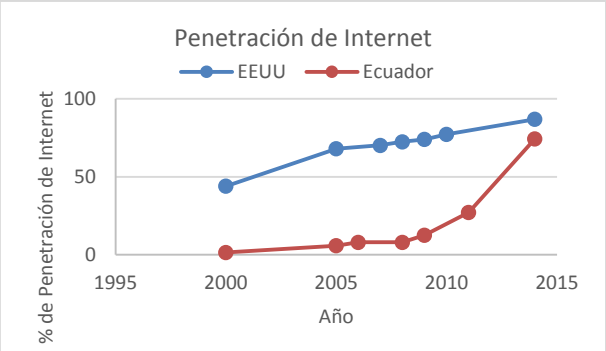

Figura 1. Tendencias de penetración de Internet de Ecuador y EEUU *(Internet World Stats, 2014)*

privacidad está ligada solamente al ámbito "físico" de la vida personal de un individuo. El contexto virtual en el que la gente se desenvuelve mediante Internet, al hacer búsquedas o usar redes sociales, usualmente es relegado a un segundo plano (al parecer inconscientemente) por preocupaciones individuales más tangibles (delincuencia, economía, etc.). Pese a ello, y a raíz de los constantes escándalos [11] motivados por el espionaje que realizan ciertas organizaciones a los ciudadanos, varios países han expedido normativa referente a la protección de los datos personales [16].

En Ecuador; sin embargo, muy poco se ha avanzado en legislación para la protección de datos personales. Históricamente, la Constitución política de 1998 hacía una tibia referencia al derecho a la intimidad, y al secreto de la correspondencia. En concordancia con este texto constitucional, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, emitida en 2002, le dedica el artículo 9 a la protección de datos, pero se concentra solamente en determinar que los datos personales podrán ser usados o transferidos únicamente con autorización del titular o la orden de autoridad competente.

Posteriormente, en la Constitución ecuatoriana vigente desde 2008, también se determina la acción jurisdiccional del *habeas data*, en el artículo 92. Este derecho permite a una persona (o institución) conocer, autorizar y rectificar la información que sobre ella se almacene en bases de datos públicas o privadas. Sin embargo, el recurso de *habeas data* sólo permite reparar un daño ya consumado (*a posteriori*) y no dispone la existencia de una autoridad de protección de datos que pueda actuar de oficio. Esto resulta muy poco efectivo en la protección de la información personal que se recopila indiscriminadamente a través de Internet [17].

Finalmente, en 2010 se expidió la Ley del Sistema Nacional de Registro de Datos Públicos (LSNRDP) que regula la forma en la que se registra y accede a los datos públicos, con el fin de transparentar y organizar el acceso a la información que las instituciones públicas y privadas almacenan de una persona. Aunque en su artículo 6 se definen los datos que se consideran confidenciales y se dispone que el acceso a ellos podrá ser autorizado por el titular o por mandato de la ley,

esta normativa no promueve mecanismos que garanticen o protejan los datos personales. Es así que, aunque otros países (Argentina y Uruguay) están a la vanguardia de la legislación sobre protección de datos y privacidad, muy poca atención se le ha dado a estos temas a nivel jurídico en Ecuador, aunque sí se han hecho propuestas desde la academia [15, 1].

2.2 La cultura de privacidad en Ecuador

La actitud de un grupo humano frente a la privacidad y a los problemas de seguridad en Internet se define en la literatura en función de sus valores culturales [8, 14]. Para ello se suele utilizar el Modelo de las Dimensiones Culturales de Hofstede [4], que define cinco agrupaciones de valores que sirven para identificar patrones culturales de un conjunto de personas. En cuanto a la postura frente a la privacidad, las dimensiones que podrían dar una idea sobre el comportamiento de la gente se encuentran: la distancia al poder, y el individualismo/colectivismo. De acuerdo al análisis de Hofstede, Ecuador es un país extremadamente colectivista [9] lo que, según otros análisis [19], supone que los ecuatorianos tienen mucha más confianza en otras personas que la que tendrían ciudadanos de EE.UU., España, México o Argentina, que son culturas más individualistas. Aunque este análisis no es determinante, es curioso observar, por ejemplo, que con cierta regularidad los países más individualistas (menos "confiados") son aquellos (EE.UU., España, México, Argentina, Costa Rica, Uruguay) que poseen una legislación sobre protección de los datos desde hace varios años.

Por otro lado, cabe resaltar la actitud generalizada que se tiene frente a la vigilancia (monitorización indiscriminada) en Internet, en el sentido de que si "uno no tiene nada que esconder", entonces el derecho a la privacidad puede rescindirse. Esta postura peligrosa normalmente sirve de justificación a quienes tienen el poder sobre los datos (gobiernos o mega corporaciones en Internet) para realizar actividades de *profiling* o *targeting* que podrían estar rebasando los límites de la intimidad de las personas. Con referencia a esto, a finales de 2013, durante la discusión del nuevo Código Integral Penal en Ecuador, se promovió (aunque finalmente no prosperó), la inclusión de un artículo que disponía a los proveedores de servicios de telecomunicaciones, e incluso a quienes compartiesen su servicio de acceso a Internet, conservar los datos de los usuarios de dichos servicios, con el fin de que pudiesen servir como evidencia probatoria en investigaciones penales (de ser necesario), lo que generó mucha preocupación en ciertos sectores de la sociedad ecuatoriana [3].

Finalmente, es común que aunque mucha gente está medianamente informada sobre los riesgos a los que se enfrenta su privacidad en Internet, ésta decide de todos modos entregar información personal privada (nombres completos, ubicación geográfica, números de tarjetas de crédito, etc.) a cambio de ciertos servicios (relaciones sociales, acceso a información, etc.) en una suerte de transacción que se torna inevitable si se quiere aprovechar los recursos tecnológicos modernos de comunicaciones.

3. ESCENARIO DE ANÁLISIS

Con el fin de hacer un análisis preliminar del estado de la privacidad en el Ecuador, que de ninguna manera intenta ser exhaustivo, se ha enfocado este trabajo a tres elementos: (1) un sondeo inicial de la percepción sobre la privacidad en Internet en Ecuador, (2) una exploración breve y no intrusiva de los riesgos de privacidad en varios sistemas de información en Ecuador (en general públicos), y (3) una discusión concluyente donde se vinculen los componentes de los dos primeros elementos. A continuación se describe el procedimiento utilizado para realizar este análisis.

Es necesario notar que muchos de los sistemas de información abajo descritos representan una evolución trascendental en el contacto entre las instituciones del Estado y los ciudadanos. Concordantemente, el objetivo de este análisis es destacar cómo, al igual que sucede con la tecnología en general, la integración en la sociedad de la información envuelve ciertos riesgos (muchas veces imperceptibles) a la privacidad de los usuarios.

3.1 Encuesta de Percepción de Privacidad en Internet

Aunque muchos esfuerzos se han puesto en medir técnicamente el riesgo de privacidad en Internet [7, 2], así como en implementar mecanismos de protección en distintos contextos [6, 22], la actitud que tiene un usuario frente a estos riesgos dependerá siempre de su situación particular (laboral, política, económica y hasta sentimental), y con relación a ella tendrá que estimarse el riesgo. Además, esta actitud se revela también como la sensación que tiene un usuario frente a las amenazas a su privacidad en Internet [10]; es decir, lo que conozca, las reflexiones que manifieste, y las acciones que tome frente a ellas.

Con el fin de medir esta descrita percepción, se realizó una encuesta a 120 estudiantes universitarios de Carreras de Ingeniería, con conocimientos técnicos avanzados sobre el funcionamiento y uso de Internet, aunque no entrenados en los mecanismos de protección de los servicios que se despliegan en la red.

Si bien las conclusiones que de las preguntas se obtengan no son en ningún caso extrapolables a toda la población ecuatoriana, vale la pena notar que son un interesante punto de partida, ya que la muestra sobre la que se aplican podría decirnos algo sobre los grupos con reducido conocimiento técnico acerca de Internet.

3.2 Riesgos Directos para la Privacidad en Internet

Comúnmente, los riesgos para la privacidad de un usuario en Internet son estudiados conforme a un modelo de ataque indirecto en el que el atacante identifica o clasifica a dicho usuario en función de un conjunto de datos que, aunque aparentemente desagregados (etiquetas, palabras de búsquedas, intereses, sitios visitados, y en general un disperso rastro digital), podrían permitir a un atacante

identificar a su víctima y posteriormente vulnerar su privacidad al inferir información crítica de ella.

Estos estudios, sin embargo, dejan de lado la información manifiestamente personal o privada de los usuarios que se encuentra accesible a través de Internet. Es de suponerse que esta información se debería conservar más segura que otra información aparentemente no tan privada (como la descrita en el párrafo anterior). Sin embargo, hay deficiencias en el manejo mismo de la información en Internet desde distintas instancias públicas y privadas, lo que podría facilitar significativamente el trabajo de los atacantes. Además, mucha de la información personal de los individuos ya está disponible en línea (en muchos casos es provista por el mismo titular) evitando que dichos atacantes tengan que hacer un trabajo muy sofisticado para vulnerar la privacidad de sus víctimas.

Con el fin de poner de manifiesto estos riesgos directos a la privacidad de la información de los usuarios en Ecuador, se analizaron varios sitios web que alojan información personal de los ciudadanos y que podría ser utilizada para vulnerar la intimidad de los dueños de esos datos. Luego, mediante un sencillo ejercicio deductivo, se ilustra cómo la información disponible en Internet sobre un usuario permitiría intuir, con relativa facilidad, detalles sensibles (de acuerdo a la percepción medida) sobre la intimidad de éste.

3.3 Ilustración de los Riesgos de Privacidad en línea en Ecuador

Para determinar el impacto de los riesgos a la privacidad de los ciudadanos ecuatorianos en Internet, se correlaciona la percepción de los usuarios acerca de la privacidad y la sensibilidad de sus datos con las amenazas directas existentes en el Ecuador y que son producto del despliegue de servicios de información en línea. Se ilustra un posible escenario de ataque a la privacidad de un usuario, para demostrar la preocupante facilidad con la que se podría recopilar sus datos personales en línea, a partir de elementos de información que los mismos usuarios consideran como "no sensibles".

4. PERCEPCIÓN SOBRE LA PRIVACIDAD EN ECUADOR

Luego de una vorágine de escándalos de espionaje atribuidos a la Agencia de Seguridad Nacional de los EEUU (NSA, por sus siglas en inglés) [18] a partir de las revelaciones que hiciera el ex agente Edward Snowden [21], se evidencia que la conciencia que tiene la gente sobre su privacidad en Internet (y los graves riesgos que la amenazan) se ha modificado significativamente. Esto, sin duda, es también consecuencia del nivel de formación y de contacto con la tecnología que adquiere la gente. Este fenómeno se manifiesta en los resultados de la encuesta realizada y, aunque muestran en general que hay una marcada preocupación sobre la privacidad de los datos en Internet, esta preocupación no se lleva a la práctica en acciones que deriven en la protección de este derecho individual.

En primera instancia, al pedir a los encuestados que definan la palabra "privacidad", se observa que se la relaciona

íntimamente con la información personal y con la idea de derecho individual. En menor medida, se asocia la privacidad a la palabra espacio, lo que quizás sugiere una referencia a la dimensión "física" de la privacidad (intimidad). En la Fig. 2 se ilustra esta interpretación, que ya denota una visión moderna del término, seguramente determinada por la edad (18-24 años) y el nivel de educación de los encuestados.

Por otro lado, si bien la gran mayoría de encuestados (97 %) está de acuerdo en que los usuarios pierden el control de la información personal al ser recopilada por las compañías de Internet, más del 90 % ha escuchado poco o nada sobre la posibilidad de que los gobiernos recopilen información de llamadas telefónicas, mensajes de correo y otras comunicaciones en línea. Estos resultados se obtienen a pesar de la enorme inquietud causada por las actividades de espionaje imputadas a EEUU, incluso a grandes potencias europeas.

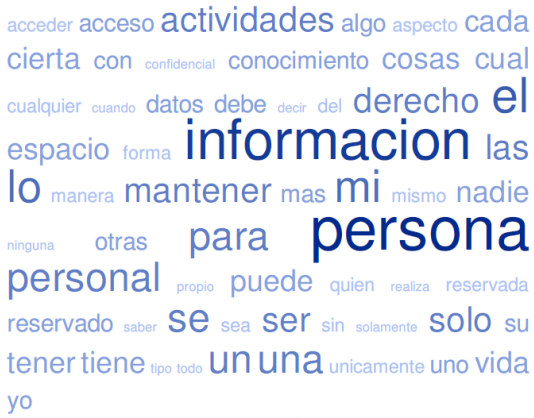

Figura 2. Nube de palabras que ilustra la frecuencia con la que se mencionan las palabras en la definición de *privacidad* de los usuarios

A casi el 80 % de encuestados le preocupa que autoridades en la jerarquía laboral (o de estudios) accedan a la información que los primeros comparten en redes sociales. Considerando que un porcentaje similar está de acuerdo en que es muy difícil o imposible borrar información inexacta sobre un individuo en Internet, se puede pensar que entre los encuestados hay una muy sólida percepción de los riesgos que, al menos en el ámbito laboral, podría acarrear la pérdida de la privacidad.

Otra contradicción interesante muestra que el 96 % de los encuestados espera tener los mismos derechos legales sobre sus datos en línea que los que tiene sobre los datos en su computador personal; sin embargo, el 62 % de ellos nunca (o casi nunca) lee las políticas de privacidad de los sitios que visita en Internet, como normalmente sí lo haría al firmar un contrato en la "vida real".

Al consultar a las personas sobre la información privada que no desearían compartir en Internet, se encontró que los datos económicos individuales (detalles de tarjeta de crédito,

cuenta bancaria e ingresos) son los más sensibles, tal como se ilustra en la Fig. 3.

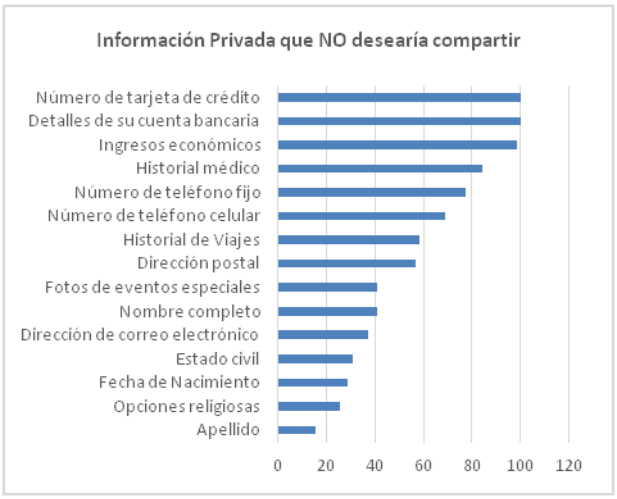

Figura 3. Tabulación de los tipos de información y la sensación de los encuestados sobre compartirlos. Indica el número de personas no quisiera compartir cada tipo de información.

El número de identificación (cédula de ciudadanía) es considerado también un parámetro sensible para la privacidad. Curiosamente, el nombre completo no está entre los datos considerados más privados, así como tampoco la fecha de nacimiento y el estado civil. Se puede observar también que el historial médico, el de viajes y la dirección postal están en una región intermedia, concebidos como sensibles por al menos la mitad de la muestra consultada.

Al ser consultados sobre la sensibilidad que se asigna (individualmente) a varios tipos de datos, se observó que se considera sensible y muy sensible al número de cédula, historial de salud y medicinas consumidas, contenido de conversaciones telefónicas, mensajes de correo, ubicación física en el tiempo, historial de llamadas, historial sentimental, historial de navegación, relaciones de amistad y lugar de votación. Por otro lado, los encuestados asignaron un nivel de sensibilidad bajo o inexistente a sus hábitos alimenticios, su fecha de nacimiento, y a sus puntos de vista religiosos y políticos.

Finalmente, pese a que se reconoce a casi toda la información como sensible, la mayoría de las respuestas apuntan a que la restricción del uso de los computadores o del servicio de acceso a Internet no es la solución.

5. EXPLORACIÓN PRELIMINAR SOBRE LA PRIVACIDAD DE LOS DATOS EN ECUADOR

Durante los últimos años, el Estado ecuatoriano ha venido promoviendo profundas medidas para la constitución de una plataforma de gobierno electrónico. En esa línea, se han puesto en marcha varias iniciativas en la forma de sistemas informáticos que manejan información de instituciones públicas, empresas y ciudadanos, y cuya disponibilidad y agregación podrían incorporar ciertos riesgos a la privacidad de los agentes previamente mencionados.

5.1 La Ley de Transparencia

Para empezar, en Ecuador en 2004 fue aprobada la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP), con el objetivo de garantizar el acceso a la información pública del estado, en función del artículo 91 de la Constitución vigente. Sin embargo, esta ley define de forma muy general lo que considera como información pública, abarcando todo documento que se encuentre en poder de las instituciones públicas (art. 5). Y, aunque se define (art. 6) lo que en el ámbito anterior se puede considerar como información confidencial, esta confidencialidad se aplicaría sobre la base de los derechos civiles (Constitución de 1998) o de libertad (Constitución vigente) que, en lo que respecta a este estudio, se refieren de forma muy vaga a la intimidad personal. Así, se deja sin acotar la información pública de aquella que, quizás, no debería serlo. Esta ley dispone a las instituciones públicas que publiquen periódicamente cierta información mínima; de lo contrario, los funcionarios responsables podrían ser sancionados incluso con la remoción del cargo.

Entre los datos que esta ley dispone transparentar está la remuneración mensual por puesto y que al momento se publica en el sitio web de (prácticamente) todas las instituciones públicas en cumplimiento del literal c del artículo 7 de la LOTAIP. Aunque este artículo no dispone que al publicar esta información cada puesto esté asociado a la identidad de quien lo ocupa, en prácticamente todas las instituciones públicas esta información salarial se pone en línea junto con el nombre completo de los servidores públicos. Considerando que la información financiera individual es la más sensible, según la encuesta analizada previamente, la publicación de esta información parece algo que se podría discutir (o modificar) en beneficio de la seguridad de los servidores públicos.

5.2 La Ley de Contratación Pública

Otra normativa que busca transparencia, en este caso en los procesos de adquisiciones para el sector público, es la Ley Orgánica del Sistema Nacional de Contratación Pública (LOSNCP). Entre otros datos, esta ley dispone publicar los pliegos de contratación, que contienen "información técnica, económica y legal del proceso […] como planos, estudios, especificaciones técnicas […]". En el campo tecnológico, es fácil imaginarse toda la información (cantidad de equipos, marcas, *software* de servicios y sus respectivas versiones) que puede recopilar un atacante sobre la infraestructura tecnológica de una dependencia pública en la fase de reconocimiento de un ataque informático, sin necesidad de hacer ingeniería social o escaneo de red, sólo mediante una pasiva, legal e indetectable recopilación de información públicamente disponible. Luego, este atacante podría utilizar información técnica (versiones de *software*) para intuir vulnerabilidades de una red y reducir significativamente el ámbito de un ataque posterior.

5.3 La Ley del Sistema Nacional de Registro de Datos Públicos (*LSNRDP*)

La LSNRDP (descrita en la Sección 2), en el artículo 31, dispone consolidar, en una base de datos única, todos los registros públicos. Así, la entidad encargada de coordinar el cumplimiento de la ley (DINARDAP) implementó el Sistema Dato Seguro. Este sistema agrupa la información de los ciudadanos obtenida de doce entidades públicas, entre ellas: Servicio de Rentas Internas, Registro de la Propiedad, Instituto Ecuatoriano de Seguridad Social y Registro Civil. Por lo tanto, se almacena información individual de: datos de identidad y de contacto, datos financieros (pago de impuestos, aportaciones de seguridad social), bienes inmuebles, compañías, relaciones laborales, infracciones de tránsito, etc. Mucha de esta información es efectivamente pública y ya está disponible en línea; sin embargo, su consolidación encarna graves riesgos adicionales para la privacidad de las personas, especialmente si los mecanismos de autenticación para acceder a este sistema son débiles (como al final lo llegan a ser todos en Internet, tanto como las personas que los usan). En sus inicios, Dato Seguro mostró ciertas fragilidades (para el registro sólo validaba un par de dígitos de la cédula de identidad) que permitieron el acceso no autorizado a la cuenta del Presidente de la República [13]. Hoy, el mecanismo de registro es un poco más estricto, pero la información de validación que se solicita se podría conseguir con relativa facilidad de otras fuentes, igualmente en línea.

5.4 Los Datos de la Seguridad Social

Con el fin de facilitar algunos trámites y consulta de información, el Instituto Ecuatoriano de Seguridad Social (IESS) mantiene habilitada, desde hace al menos 5 años, una plataforma informática accesible desde Internet que poco a poco ha ido incorporando una gran cantidad de servicios para el afiliado, entre ellos: agendamiento e historial de citas médicas, historial laboral y solicitud de préstamos. Considerando que, según nuestra encuesta, más del 60 % de consultados sugiere que no compartiría la información de su historial médico, es razonable afirmar que este servicio en línea recoge información privada, muy sensible para sus usuarios. El proceso de registro (acceso por primera vez) en el sistema se lo hace en línea y requiere contestar correctamente tres preguntas sobre el historial de afiliación del individuo. Tal como sucede con otros sistemas en los que la primera validación del usuario se la realiza en línea, las preguntas en las que se basa el registro en la plataforma del IESS, tienen respuestas que un atacante podría obtener mediante técnicas de ingeniería social o, si conoce un poco a la víctima, mediante una reflexión deductiva simple. Por otra parte, este proceso de registro resulta tan engorroso para el usuario común, que éste normalmente termina acudiendo a un centro de cómputo donde estos trámites son tan frecuentes que hasta tienen una tarifa definida por el soporte técnico que ofrecen a los afiliados para ingresar al sistema. Esto implica que el afiliado le indique su contraseña al empleado del centro de cómputo, con muy pocas probabilidades de que ésta sea luego cambiada. Justamente ahí radica el riesgo a la privacidad de un usuario que se ve obligado a exponer sus datos personales a cambio de un poco de ayuda para ingresar al sistema.

5.5 Los Datos de Facturación Electrónica

El Servicio de Rentas Internas, en resolución del 6 de mayo de 2013, dispuso la obligación de ciertos contribuyentes (instituciones financieras, empresas públicas, contribuyentes especiales, entre otros) de emitir comprobantes (facturas, retenciones, etc.) únicamente a través de mensajes de datos y firmados electrónicamente; proceso que en términos coloquiales se conoce simplemente como facturación electrónica. El problema radica en que muchos de los contribuyentes especiales que ahora facturan electrónicamente, lo hacen a través de sistemas informáticos, la mayoría de ellos tercerizados (alojados en empresas de terceros), accesibles desde Internet (para que un consumidor pueda consultar su factura), y con inexistentes (o débiles) mecanismos de autenticación o autorización para el acceso a dicha información. Del análisis exploratorio realizado, esto básicamente significa que un atacante podría encontrar estos sistemas en Internet (usando un motor de búsqueda, o en la página del contribuyente) porque son públicos y, usando solamente el número de cédula de su víctima, sería capaz de obtener detalles de las facturas (y por tanto consumos) que se han emitido a dicha víctima.

Esto es posible ya que algunos de estos sistemas publican estos documentos personales incluso masivamente, otros no tienen mecanismos de autenticación (sólo piden el número cédula para acceder a la lista de facturas) o, si lo tienen, el mecanismo de registro (la primera vez) es deficiente. Entre los problemas observados que podrían derivar en amenazas a la privacidad de los usuarios (cuya gravedad podría variar dependiendo del tipo de consumos) se encuentran los siguientes:

a) Almacenamiento y despliegue público de todos los documentos de facturación emitidos en una sola página web, sin restricción alguna.

b) Acceso a los documentos con autenticación basada solamente en el número de cédula o parte de éste, o en su uso como nombre de usuario y contraseña.

c) Utilización de una misma contraseña sencilla para el acceso de todos los usuarios (1234, por ejemplo) al sistema de consulta de facturas emitidas.

d) Proceso de registro y creación de cuenta basados en número de cédula y sin validación de identidad.

e) Utilización del número de documento (número de factura) como contraseña para el acceso al documento de facturación.

Adicionalmente, en la Tabla 1, se resumen algunos de los tipos de contribuyentes cuyos sistemas se analizaron. Cabe destacar que, para la obtención de esta información se realizó una observación simple de los mecanismos de autenticación utilizados, luego de haber adquirido un producto y de recibir acceso a nuestra factura electrónica en el sistema respectivo. Por tanto no se utilizó ninguna técnica intrusiva, ni se vulneró la privacidad de ningún usuario.

5.6 El número de cédula de ciudadanía

Vale la pena notar que la cédula en Ecuador es un documento al que se asocia mucha información personal y, en general, privada, a tal punto que contiene datos (no sólo el número sino también otros datos de este documento) que se utilizan como contraseña o mecanismo de validación de registro en los sistemas de información antes mencionados.

Consecuentemente, para evidenciar el riesgo que corre la privacidad de un usuario en Internet (en Ecuador) sólo hay que recordar lo fácil que resulta obtener el número de cédula de los cientos de copias de cédula que entregamos en algún trámite, o de las decenas de hojas de vida (donde colocamos este número) que presentamos para conseguir empleo. Por lo tanto, la sola divulgación del número de cédula es, al menos, un parámetro generador de riesgo a la privacidad de los usuarios en el contexto en el que ahora se desenvuelve la sociedad ecuatoriana, tal como se puede ilustrar en la siguiente sección.

Tabla 1. Deficiencias de seguridad (riestos de privacidad) encontrados en los sistemas de gestión de facturación electrponica de varios tipos de contribuyentes. Las deficiencas están codificadas de acuerdo a la sección 5.5

Tipo de Contribuyente	Cantidad	Deficiencias
Farmacia	2	b), d
Alimentos	9	b), c), d)
Empresa Pública	3	a)
Ropa	1	e)
Entretenimiento	2	b), d)
Deportes	1	a)

6. DISCUSIÓN SOBRE UN ESCENARIO DE RIESGO DE LA PRIVACIDAD EN ECUADOR

Se ha realizado un análisis preliminar de la privacidad en Ecuador: ciertas percepciones de los ciudadanos y algunos de los riesgos de la privacidad en Internet. Para medir la percepción de los usuarios se realizó una encuesta y, para detectar los riesgos de la información personal pública en el país, se ejecutó una exploración no intrusiva de la información disponible en sistemas de información en Internet. Se evaluó el impacto que podría tener esta información públicamente accesible en función de la percepción medida de los usuarios sobre su privacidad en línea.

De la encuesta, está claro que los usuarios están conscientes de los riesgos a su privacidad en Internet y que estos se concentran en la información. Sin embargo, parecen no percibir que información aparentemente no sensible puede correlacionarse para encontrar información muy sensible ya que las huellas que dejamos en Internet son casi imposibles de borrar. Lo curioso es que los mismos encuestados reconocen la pérdida de control sobre los datos que sobre sí mismos se encuentra en Internet, pero no alcanzan a percibir el impacto negativo que podría tener el procesamiento de esos datos para obtener información privada.

La mayor preocupación percibida se centra en los datos financieros individuales, el historial médico, los datos de contacto telefónico, y el número de cédula. Estos son, sin duda, datos de carácter privado cuya difusión podría afectar significativamente a su dueño. Sin embargo, como ya se sugirió, según la percepción de los usuarios y varios de los escenarios analizados de información expuesta, algunos de los datos considerados menos sensibles podrían facilitar enormemente un ataque a la privacidad de estos usuarios.

Entre los datos no tan sensibles para los encuestados tenemos: el nombre completo (o parte de él), la fecha de nacimiento, el grado académico, y hasta el estado civil. Esto indicaría que la muestra de encuestados estaría dispuesta a aligerar su preocupación por este tipo de datos por considerarlos menos críticos. Sin embargo, si un atacante desea empezar a indagar sobre su víctima, le basta conocer su nombre y su alma máter. Si el atacante no conociera el nombre completo de su víctima, y si ésta posee un grado académico de tercer nivel, seguramente su tesis de grado será pública y en ésta se podrá encontrar el nombre completo de la víctima, así como información adicional (probablemente en la dedicatoria). Para averiguar el número de cédula, es suficiente consultar el sistema de verificación de títulos de la Secretaría de Educación, Ciencia y Tecnología que entrega información de los títulos de un ciudadano (y el número de cédula) solo con pasarle el nombre (o parte de éste). Tal como se notó en la sección anterior, el número de cédula ya podría ser la puerta de entrada hacia algunos sistemas de información del usuario (a los de facturación electrónica especialmente). Si el atacante no está satisfecho, y si la víctima no ha activado su cuenta de Dato Seguro, éste podría animarse a realizar el registro por la víctima, suplantando la identidad de la víctima (lo cual podría configurar un delito).

Al intentarlo, el sistema le pide validar su identidad mediante la respuesta a tres preguntas. Para el registro, el sistema solicita tres datos: fecha límite de declaración del impuesto al valor agregado, provincia de sufragio, y cantón del matrimonio civil (si se es casado y, si no, se debe indicar que se es soltero). Los tres datos, conociendo el número de cédula del individuo, son públicos en línea en respectivos sistemas del SRI, Consejo Nacional Electoral y Registro Civil (un par de meses luego de la versión inicial de este artículo, ya no es posible obtener información de estado civil).

Considerando que los datos financieros son los percibidos como más sensibles por los encuestados, resulta preocupante

que sea posible encontrar tanta información pública de los ciudadanos en esa categoría. Una vez que un atacante ha logrado obtener datos de identificación de sus víctimas, podría intentar perfilarlas en función de sus ingresos económicos. Esto es perfectamente posible mediante la información del impuesto a la renta causado que es pública en el sitio web del Servicio de Rentas Internas, o a través de la remuneración mensual por puestos que publican todas las entidades públicas (si la víctima es empleado público).

Al tener el nombre de la víctima o su número de identificación, un atacante podría también indagar sobre los bienes inmuebles que posee la víctima al consultar el sistema en línea del respectivo municipio pues, en ciertas ciudades en el país, esta información también es pública y fácilmente accesible.

Tomando en cuenta que el historial de salud es otra de las categorías sensibles para la privacidad de los encuestados, es interesante notar cómo un atacante podría acceder a información de los medicamentos consumidos por su víctima explotando las vulnerabilidades de autenticación (Tabla 1., ítem Farmacia) de los sistemas de facturación electrónica. Lo más preocupante es que, en ciertos casos, para ello, el atacante solo necesita conocer el número de cédula de su víctima, que previamente obtuvo a partir del nombre de ésta, y que este parámetro (nombre completo) no es percibido como sensible por lo que no hay interés de protegerlo.

Pero los riesgos a la privacidad en Ecuador no solamente se enfocan solamente a los individuos sino también a las organizaciones, y en particular a las entidades públicas. Tal como se indicó en la sección 5, la Ley de Contratación Pública dispone, en la mayoría de casos, publicar los documentos de contratación de toda entidad pública. Esto implica poner en línea información minuciosamente detallada de equipos y procesos que necesita dicha entidad. Imaginemos solamente un proceso en el que una dependencia pública llama a concurso para contratar los servicios de mantenimiento de sus equipos de red y seguridad.

De los documentos del proceso, un atacante podría inferir, sin mucho esfuerzo, el tipo de infraestructura de red de la organización, la marca de los equipos, y las versiones de *software* con que funcionan. Al contratar servicios de mantenimiento, la organización podría necesitar publicar incluso algún detalle de los problemas o inconvenientes que tiene la infraestructura de red y que podrían ser aprovechados por el atacante para vulnerar los sistemas de comunicaciones.

Así, un atacante de la privacidad de un usuario o de una organización (no solo en Ecuador) sería capaz de obtener una radiografía muy completa de su víctima (en términos de información personal o técnica), en la comodidad de su escondite, sin arriesgarse y (peor aún) sin despertar la más mínima sospecha, pues estamos hablando de un análisis no intrusivo, prácticamente imposible de detectar.

7. CONCLUSIONES

En este artículo se ha intentado hacer una modesta aproximación preliminar sobre el estado de la privacidad en Ecuador, en el contexto de la información personal pública de los ciudadanos que se gestiona en sistemas de información en Internet. Existe una actitud de preocupación frente a los riesgos de privacidad en línea que se manifiesta en una encuesta de percepción. Sin embargo, esta actitud no se expresa en un criterio más reflexivo y activo sobre la información pública de los ciudadanos en Internet, pues no se comprende aún la magnitud de la cantidad de información de usuario que se encuentra en línea. Por otro lado, la migración en Ecuador de servicios y trámites (públicos y privados) a plataformas en la Web plantea varios riesgos a la privacidad de los ciudadanos que las emplean, pues abundante información "no sensible" podría correlacionarse para obtener información "sensible".

Además, los mecanismos de seguridad para el acceso a plataformas con información personal y la cultura misma de manejo de información de los usuarios son deficientes y esto facilitaría enormemente la recopilación de datos personales. Lo más grave es que, para obtener información personal crítica (datos financieros, por ejemplo, según la percepción medida), un atacante sólo necesitaría partir de ciertos datos considerados no críticos (como el nombre de una persona) y, ya que estos datos no se perciben como sensibles por los usuarios, existirá mayor probabilidad de que no sean protegidos adecuadamente.

Aunque es deseable la transparencia en la gestión pública y especialmente en el manejo económico, sería importante evaluar el impacto de publicar cierta información personal (y no necesariamente privada) en ciertas garantías individuales de los ciudadanos.

Ya que se trata de un trabajo inicial, no se pretendió ser exhaustivos (la muestra de la encuesta es pequeña) ni obtener un diagnóstico definitivo, pero sí dar una pauta para la investigación de la privacidad de la información en el país, desde el punto de vista técnico y cultural (multidisciplinario). En trabajos futuros, se podría plantear una muestra más amplia y representativa de la población ecuatoriana para la medición de las percepciones de los ciudadanos sobre su privacidad. También sería interesante comparar los niveles de conciencia y preocupación (sobre la privacidad) con los de otros países, y determinar las divergencias existentes, así como sus posibles causas. Esta investigación podría hacerse de manera periódica para determinar, con cierta certeza, tendencias en la evolución del comportamiento de los usuarios y de los gestores de información frente a la protección de la privacidad de los ciudadanos. De hecho, del lado de las instituciones, se podría analizar también las políticas de privacidad que publican en sus sitios web para el manejo seguro de la información del usuario, y si efectivamente se implementan o están adecuadamente definidas.

REFERENCIAS

[1] B. Torres Espinoza (2010). Proyecto de ley orgánica de protección de datos personales.

[2] D. Rebollo-Monedero, J. Parra-Arnau, C. Diaz, & J Forné (2013). On the measurement of privacy as an attacker's estimation error. International journal of information security, 12(2), 129-149.

[3] Ecuadorinmediato (2013), Asociaciones digitales señalan preocupación sobre privacidad en Internet tras aprobación del COIP en Ecuador. [En línea] Recuperado de: http://goo.gl/ZHPWaI. Última visita: 15 de junio de 2015.

[4] G. Hofstede (1984). Cultural dimensions in management and planning. Asia Pacific journal of management, 1(2), 81-99.

[5] INEC (Instituto Nacional de Estadísticas y Censos), Censo TIC 2013. [En línea] Recuperado de: http://www.ecuadorencifras.gob.ec/tecnologias-de-la-informacion-y-comunicacion-tic/. Última visita: 15 de junio de 2015.

[6] J. A. Estrada, & A. Rodríguez (2014). Evaluación de Protección de Privacidad de una Herramienta de Navegador Web. Revista Politécnica, 33(1).

[7] J. Parra-Arnau, D. Rebollo-Monedero, & J. Forné, (2014). Measuring the privacy of user profiles in personalized information systems. Future Generation Computer Systems, 33, 53-63.

[8] P. Kumaraguru, & L. Cranor (2006, January). Privacy in India: Attitudes and awareness. In Privacy Enhancing Technologies (pp. 243-258). Springer Berlin Heidelberg.

[9] G. Hofstede (2013). The Hofstede Centre. [En línea] Recuperado de: http://geert-hofstede.com/ecuador.html. Última visita: 15 de junio de 2015.

[10] D. Malandrino, V. Scarano, & R. Spinelli (2013). Impact of Privacy Awareness on Attitudes and Behaviors Online. SCIENCE, 2(2), pp-65.

[11] D. Schiller (2014). Geopolítica del espionaje: las ramificaciones del caso Snowden. Le Monde diplomatique en español, (229), 1-9.

[12] D. U. de los Derechos Humanos (1948). Asamblea General de las Naciones Unidas. París: ONU: http://www. un. org/spanish/aboutun/hrights.htm.

[13] Ecuadorinmediato (2012), Director Informática de Fiscalía: bloguero acceso de manera no consentida a registro del Presidente Correa en Dato Seguro [En línea] Recuperado de: http://goo.gl/391i0d. Última visita: 15 de junio de 2015.

[14] G. Cecere, F. Le Guel, & N. Soulié (2015). Perceived internet privacy concerns on social networks in Europe. Technological Forecasting and Social Change.

[15] J. CIESPAL (2014). Conferencia: Protección de datos y privacidad en procesos electorales, hacia la Declaración de Ecuador y unificación de criterios.

[16] M. F. C. Ronderos (2014). Legislación informática y protección de datos en Colombia, comparada con otros países. Revista Inventum, (17).

[17] M. H. Birnbaum (2004). Human research and data collection via the Internet. Annu. Rev. Psychol., 55, 803-832.

[18] M. Kassen (2014), Globalization of e-government: open government as a global agenda; benefits, limitations and ways forward. Information Development, 30(1), 51-58.

[19] R. Goldfarb, D. Cole, E. Wasserman, T. Blanton, H. Carter, J. Mills, & B. Siegel (2015). After Snowden: Privacy, Secrecy, and Security in the Information Age. Macmillan.

[20] R. Warner, & R. H. Sloan (2015). The Self, the Stasi, the NSA: Privacy, Knowledge, and Complicity in the Surveillance State. ExpressO.

[21] UN Public Administration Programme, 2014 UN E-Government Survey and E-Government Indicators, Bangkok, Thailand, Octubre, 2015.

[22] V. Toubiana, A. Narayanan, D. Boneh, H. Nissenbaum, & S. Barocas, (2010, March). Adnostic: Privacy preserving targeted advertising. In Proceedings Network and Distributed System Symposium.