2008

Gobernanza de Internet y Privacidad

Dr Gus Hosein

rits nupef rits IDRC CRDI

Gobernanza de Internet y Privacidad

Dr Gus Hosein

CATEDRÁTICO VISITANTE

Grupo de Sistemas de Información e Innovación, Departamento de Gestión

The London School of Economics and Political Science

http://personal.lse.ac.uk/hosein

Después de más de una década de estudios en este campo finalmente llego a la conclusión de que la privacidad es confusa. Quizá "confusa" no sea el término más correcto pero ciertamente no es un dominio que esté bien definido. A diferencia de otros dominios como la regulación de contenido en línea, la brecha digital o incluso la política ambiental, el campo de la privacidad está conformado por un conjunto de actores e instituciones en permanente cambio, tecnologías y oportunidades, alineaciones y coaliciones y, por supuesto, amenazas.

Como académico se supone que use estos niveles de procesos analíticos para describir la complejidad de un campo de políticas, aunque como alguien que se ha desempeñado como defensor en el mundo de la privacidad puedo asimismo deducir que el derecho a la privacidad también confunde a muchos y algunas veces hasta a mí.

Pensemos en las últimas controversias que mis colegas y yo en Privacy International tuvimos que considerar en las dos semanas dedicadas a la redacción de este trabajo:

- Entablamos una demanda ante el comisionado de privacidad de Ontario afirmando que los planes de la ciudad de Toronto de instalar más de 10 mil cámaras en su red de tránsito no había pasado en forma suficiente la "prueba de la necesidad". Le proveímos al regulador de privacidad los resultados de estudios del Reino Unido y de Berlín demostrando que la efectividad de las cámaras de Televisión de Circuito Cerrado (Closed Circuit Television - CCTV) no era tan efectiva como se había prometido. Se alzó un torbellino alrededor de la historia en los medios de comunicación, lo cual fue ciertamente un resultado agradable en particular porque la financiación para este plan de vigilancia fue aprobada con escaso debate público. Sin embargo y pese a todo esto, hemos estado recibiendo un gran número de coléricos correos electrónicos de canadienses enfurecidos reclamando que su derecho a la seguridad es más importante que el derecho egoísta a la privacidad.

- En el Reino Unido hemos estado trabajando con varias organizaciones tratando de efectuar un cambio en las

actuales prácticas respecto de la recolección de muestras de ADN de presuntos criminales. El Reino Unido tiene la base de datos más grande de ADN en el mundo, en la cual se retira una muestra de cualquier persona arrestada por haber cometido un delito para luego añadir esta información a la base de datos de ADN. Durante mucho tiempo hemos sostenido que ésta es una práctica problemática ya que aunque a alguien se le declare inocente, el perfil de su ADN permanece en la base de datos. Además, el perfil de una persona puede usarse para identificar a otras personas debido a la "búsqueda familiar" que, como resultado, hace que se agreguen millones de personas a esta base de datos. En el mes de octubre de 2007, las noticias dijeron que un violador enmascarado había sido finalmente rastreado 14 años después de haber cometido el crimen, no porque su ADN estaba en la base de datos (él había llevado una vida con una ficha limpia sin antecedentes policiales) sino porque el ADN de un miembro de su familia se encontraba en la base de datos.

- En Estados Unidos (EEUU), el Gobierno de Bush logró llevar a buen término una ley a través de un Congreso que en general obra de forma hostil, que permitía a la Agencia Nacional de Seguridad interceptar comunicaciones que pasaban por EEUU. Debido a la historia y diseño de las telecomunicaciones globales, gran parte del tráfico a nivel mundial en verdad pasa por redes de propiedad de compañías de Estados Unidos que también las gestionan. La ley permite que la Agencia Nacional de Seguridad, cuya sigla en inglés es NSA, obtenga acceso a los registros sin que sea necesario contar con una orden judicial. Muchos comentaristas en EEUU consideran esto como una solución práctica porque sostienen que los derechos constitucionales de Estados Unidos se aplican sólo a los residentes y ciudadanos de dicho país y a las comunicaciones de los ciudadanos de otros países que pasan a través de EEUU y están bajo la jurisdicción de instituciones para la aplicación de la ley de Estados Unidos. Es perfectamente factible que la mayor parte de las comunicaciones de Latinoamérica a Europa o África pasen por "redes norteamericanas". Es muy probable que correos electrónicos de un ciudadano francés dirigidos a otro, brasileño a otro brasileño, etcétera, pasen por redes de Estados Unidos porque pasan por los servidores norteamericanos de compañías como Google y Microsoft. Pero la conciencia sobre este desarrollo legal fuera de EEUU es bastante baja y no es como si los gobiernos extranjeros o autoridades oficiales tuviesen alguna jurisdicción sobre redes de Estados Unidos. Mientras tanto hay un intenso y puntual debate en los círculos políticos norteamericanos, pero una dinámica altamente política redunda en que el Congreso haya aprobado la legislación.

Frente a probabilidades y a hechos como estos, es de esperar que los defensores de la privacidad apoyen un enfoque consecuente sobre un tema tan controversial y complicado. Y en todas estas historias, el defensor de la privacidad termina apareciendo como el malhechor. Mi propósito en este trabajo no es el de encontrar alguna simpatía o solidaridad hacia el defensor de la privacidad. Más bien, mi meta es mostrar que aunque la privacidad sea un campo altamente controversial y complicado, son su complejidad y las controversias las que hacen que tenga tanta importancia.

De hecho, el punto que deseo recalcar es que éste es un ambiente fértil de política que merece mayor atención de parte de investigadores, estudiantes y legisladores en materia de gobernanza de Internet.

La riqueza del dinamismo de este campo deriva no sólo de las historias de terror sobre la privacidad. Comenzamos a ver lo que ocurre cuando a la privacidad no se le da el debido peso o cuando el debate público y las deliberaciones sobre políticas se ven reprimidos en nombre de la seguridad. Hemos visto esto en el amplio panorama de las políticas públicas.

No resulta sorprendente constatar que han habido saltos y rebotes en estos últimos años en relación al avance del tema de la seguridad. El ambiente de políticas ha promovido adelantos en lo que atañe a la leyes de vigilancia, políticas y tecnologías. Finalmente también comenzamos a vislumbrar también los fracasos de estas políticas. Una inmensa cantidad de fondos y recursos ha sido dedicada a las nuevas tecnologías con la promesa de que funcionarían y ahora nos percatamos de que tal vez no sea así. Volviendo a los casos antes mencionados:

- Numerosos estudios demuestran que hay serios problemas con las infraestructuras de CCTV y, de hecho, la creación de políticas CCTV tiende a ser inducida por el virtuosismo político en vez de la necesidad. Por ejemplo, en el caso canadiense, un gobierno federal recién instaurado quiso mostrar su determinación sobre la seguridad tras tomar posesión del cargo y prontamente se apresuró a proveer financiación para garantizar las redes de tránsito a lo largo de Canadá sin detenerse a considerar el uso apropiado de dichos fondos.
- La colecta y retención de ADN ha hecho que el 75 por ciento de la población masculina joven afrodescendiente esté incluida en la base de datos; hasta un niño tan pequeño como de 9 meses de edad y casi 10 mil niños están registrados en esta base de datos con perfil delictivo, haciendo que los políticos de todas las tendencias y partidos pongan esta política en tela de juicio. De hecho, la anterior política del gobierno fue buscar una base de datos nacional de ADN a hurtadillas para lentamente ingresar a todas las personas en la base de datos; pero ahora se ve forzado a apartarse de esta posición debido a la creciente preocupación pública.
- El gobierno de Bush ahora admite que le dio demasiado vuelo a esta causa en pro del cambio en la política de Estados Unidos sobre la intercepción cuando intentó señalar que los arrestos recientes en Europa se lograron solo gracias a las intercepciones de EEUU, cuando en verdad no fue así.

El mundo hoy en día no es el mismo después de la carrera a enmiendas legislativas que hemos atestiguado y actualmente las políticas están siendo discutidas de manera más plena y concienzuda. Ya no se toman los hechos literalmente y nosotros ahora cuestionamos la efectividad de una política.

A pesar de este giro en los acontecimientos en otras esferas políticas, los debates sobre gobernanza de Internet continúan sin tomar en cuenta la privacidad. Los debates en las cumbres de Naciones Unidas contienen lenguaje

sobre terrorismo, crimen y seguridad, siempre ignoran los problemas en las políticas emergentes y raramente consideran los desafíos de asegurar la privacidad. Esto es sorprendente considerando el número de opciones de políticas y de alternativas que podríamos estar discutiendo, si tan solo hubiera un debate en primer lugar. Por supuesto que la privacidad es complicada y controversial. Pero aún sin comprometernos con estos asuntos no logramos siquiera llevar a cabo el necesario debate.

Hay una serie de probables respuestas a este interrogante en lo que se refiere a por qué las cumbres sobre gobernanza de Internet ignoran la privacidad. Estas incluyen:

1. La geopolítica de obligar a países a que estén de acuerdo sobre la privacidad cuando puede aducirse que es un fenómeno puramente occidental

2. Menos prioridad dada a la privacidad en aras de la seguridad

3. Falta de instrumentos de políticas disponibles para incidir sobre el problema

El resto de este trabajo demostrará que éstos son meramente pretextos para no tomar la privacidad con la debida seriedad.

I. La privacidad como valor occidental

En convenciones y reuniones realizadas en todo el mundo a las cuales asisto, a menudo alguien que no es occidental me lleva a un lado para tratar de explicarme por qué yo soy un ingenuo por creer que la privacidad es un derecho universal y me explica cómo su sociedad no considera a la privacidad como un asunto importante y que dicha privacidad es un derecho egoísta que no tiene cabida en las sociedades comunitarias fuera de occidente. Hasta la fecha he oído ese mismo discurso de ciudadanos de: China, Egipto, India, Irán, Japón, Corea del Sur, Tailandia y Zimbabwe. No listo estos países como forma de sondeo de algún tipo de representación global, sino más bien para mostrar los puntos en común en este sentimiento expresado sobre la privacidad a pesar de las diferencias entre estas naciones, estados y sociedades. Hablando en nombre de su gente, me dijeron que estos países no tienen necesidad ni interés en derecho de privacidad.

Suelo sentirme sumamente frustrado ante estas situaciones. Encuentro incomprensible, como varón nacido y criado en occidente, cómo uno podría no interesarse en la privacidad. Ya sea la privacidad de los padres y los amigos de nuestra juventud, la revelación selectiva de información personal a amigos a medida que construimos relaciones de confianza, el desarrollo de la sexualidad de uno y la torpeza y la evolución que rodea esta etapa o, en términos más generales, la necesidad psicológica de recluirse de vez en cuando; se tan poco sobre el mundo que no logro comprender sociedades enteras que no necesitan de estos procesos. Pero deben

1 Rhoda Howard y Jack Donnelly, en Micheline Ishay's The Human Rights Reader: Major Political Writings, Essays, Speeches, and Documents from the Bible to the Present. Londres: Routledge, 1997.

perdonarme por mis suposiciones respecto del estado de la humanidad pues no soy sociólogo ni antropólogo.

Soy, sin embargo, un estudioso de políticas y tecnología. Hasta una mente política clásica al observar estas sociedades y estados singulares se preguntaría cómo puede sobrevivir un sistema político sin derecho a la privacidad. Los derechos a organizarse o sindicarse para dirigirle una petición al gobierno dependen de la habilidad de esos peticionarios a organizarse en contra de un posible estado antagónico. Este es el motivo por el cual, por ejemplo, en EEUU el derecho a la privacidad dio un salto gigantesco durante el movimiento de los derechos civiles en 1960 cuando el estado de Alabama exigió que todas las organizaciones, incluyendo la Asociación Nacional para el Progreso de Gente de Color (organización del Reverendo Martin Luther King Jr.), revelasen sus listas de miembros ante el gobierno; la Corte Suprema de Estados Unidos reconoció que los movimientos políticos precisan de algún tipo de privacidad y rechazó el pedido de Alabama de estar enterado sobre las afiliaciones y preferencias políticas de sus ciudadanos.

Todos los sistemas políticos, incluso los que cuentan con un único partido, habrán de enfrentarse a los peticionarios y éstos necesitan espacio y autonomía para organizarse y actuar sin estar bajo constante vigilancia. Grupos de estudiantes en Irán, partidos de oposición en India, Egipto y Zimbabwe, emigrantes en Tailandia e instituciones religiosas (o cultos) en China pueden sentir alguna necesidad de privacidad.

Tal necesidad de autonomía es un factor endémico en la política, aunque no lo sea para la cultura. Este es el motivo por el cual la privacidad está recogida en el artículo 12 de la Declaración Universal de Derechos Humanos, documento redactado por personas de diferentes partes del mundo y firmada por estados de todos los tipos de culturas. Rhoda Howard y Jack Donnelly declaran el propósito por el cual se ha incorporado a la Declaración:

"El derecho a la privacidad (artículo 12) más explícitamente aún tiene por objeto garantizar la capacidad para elaborar una visión personal de lo que significa una vida digna de un ser humano" .

No estoy tratando de ser imperialista sosteniendo que el hecho de que esté plasmado en el documento signifique que deba ser implementado a rajatabla en todos lados. Más bien, simplemente estoy manifestando que consta pues ha sido reconocido como necesario por personas de todos los rincones del mundo.

Me inclino a aceptar que aún no he podido salir airoso en este debate ya que cada país y cultura debe poder escoger sus propios caminos. Pero como ya mencioné antes, soy también un estudioso de la tecnología. Mientras que las culturas pueden variar vemos cada vez más que las tecnologías no. Las mismas tecnologías que son implementadas en EEUU y en Europa Occidental se implementan en África, Asia y Europa Central. Sin embargo, los riesgos que existen al implementar estas tecnologías en occidente no desaparecen solamente porque estén siendo implementados en culturas diferentes. Las brechas y distorsiones en términos de datos, la poca deliberación sobre política y el desperdicio

2 Alan F. Westin, Privacy and Freedom, Nueva York: Atheneum, 1967.

resultante de recursos son factores presentes por doquier. Así fue cuando EEUU implementó vastos regímenes de acusación en sus fronteras sin una adecuada deliberación sobre políticas y después se dio cuenta de que una inmensa cantidad de fondos había sido desperdiciada en un plan que no funcionó de manera eficaz y que además resultó inseguro; ¿estamos afirmando que estos mismos problemas no aquejarán a Japón a medida que emprende el camino siguiéndole los pasos a Estados Unidos usando la misma retórica política de proteger las fronteras contra elementos terroristas?

Pero más allá del mero proceso de política tecnológica, ¿qué pasa con los temas humanos y culturales que subyacen a la transferencia de tecnología? Nuevamente sostendría que como estamos viendo la misma tecnología en una serie de contextos y culturas, los riesgos de ignorar los riesgos para la privacidad con estas tecnologías crearán problemas a través de todos estos mismos contextos y culturas, sin tener en cuenta sus diferencias. En 1960, con la amenaza del incremento del procesamiento de datos y el almacenamiento de información personal en "bancos de datos", Alan Westin definió de manera memorable la privacidad y autodeterminación informativa como:

"El clamor de las personas, grupos o instituciones a determinar ellos mismos cuando, cómo y hasta qué punto la información sobre ellos habrá de ser comunicada a otros (...) Las personas desean poder escoger libremente bajo qué circunstancias y hasta qué punto se expondrán ante los otros, así como su actitud y su comportamiento" .
Es decir, las personas deben tener la libertad de escoger qué tipo de información personal estará accesible a otros y bajo qué circunstancias. Westin percibió que las tecnologías ponían en peligro este principio. Afirmar que este es meramente un derecho al alcance tan solo de los que viven en occidente es negarle a todos los demás el derecho a decidir en el sentido más básico.

Adonde sea que esta tecnología se explaye vemos retos similares. La necesidad de proteger la identidad de un blogger en EEUU en infracción de derechos de autor es similar a la necesidad de proteger el nombre de un blogger en China (donde hay una base de datos nacional con todos los bloggers) o en Egipto (donde el nombre de un blogger homosexual fue revelado al gobierno). Cualquiera que me enfrente y argumente que lo que alguien diga públicamente sobre sus preferencias políticas o sexuales en un país debería ser ilegal en otro debido a diferencias culturales, está nuevamente atacando los cimientos de lo que significa el concepto de ser humano y lo que es tener alguna autonomía.

Ahora, volviendo a la falta de acción en términos de privacidad y gobernanza de Internet, no basta con decir que la privacidad es un concepto occidental que no merece discusión ni reconocimiento especial a nivel internacional. Las Naciones Unidas, en particular, no pueden ignorar este asunto porque sus piedras angulares residen en documentos que aluden a la importancia de la privacidad y a un concepto universal. Pero más allá de esto, surge un caso tras otro sobre abuso de los procesos políticos en países de todo el mundo, en el oeste, este, norte y sur. Con tecnologías extendiéndose a través de las fronteras vemos métodos similares y familiares de represión

y opresión y no podemos simplemente quedarnos de brazos cruzados y decir que cada país tiene una cultura diferente.

2. Yendo más allá de la seguridad

Pese a todas estas preocupaciones culturales que hay alrededor del mundo me resulta asombroso observar con qué facilidad los líderes hablan públicamente sobre cómo los países deben aprender a cooperar en materia de seguridad. El proceso de Naciones Unidas está colmado de tales declaraciones a medida que todos los años en la Reunión General oímos un discurso atrás del otro de diplomáticos y jefes de estado sobre la necesidad de enarbolar y avanzar en la causa de la seguridad.

Esta fue también la situación que se presentó en las cumbres de Naciones Unidas sobre la sociedad de la información donde, en el campo de la gobernanza de Internet, se puso mucho más énfasis en los debates sobre seguridad que en otros terrenos de políticas.

Claro, hoy en día hablar de seguridad es entretenido, es como si uno estuviese del lado de los bienaventurados al hacerlo. Antiguamente se decía que nunca ningún gerente de TI había sido despedido por comprar computadoras de IBM. Ahora los políticos creen que la mentalidad que prevalece es la de que a ningún político o burócrata se le ha llamado la atención para votar o autorizar nuevas normas de actuación sobre seguridad y tecnologías.
Pero estas son todas posturas excesivamente simplistas incluso en las sociedades de hoy.

Primero, obtener consenso internacional sobre políticas de seguridad es sumamente difícil aún para países que están de acuerdo en muchas otras cosas. Hemos visto que las negociaciones sobre las políticas de seguridad fracasan en muchos sectores. A pesar de toda la retórica sobre el terrorismo la ONU, por ejemplo, ha sido incapaz de convenir en una definición de terrorismo o grupo terrorista. Hay diferentes listas de terroristas y grupos terroristas en cada país. Este problema no se limita al terrorismo. Las definiciones de crímenes difieren de un país al otro, lo cual a menudo entorpece la cooperación y el establecimiento de un único régimen legal hasta en países vecinos.

Aunque haya cooperación, esta suele conducir a problemas. Durante años el Consejo de Europa se dedicó a trabajar para elaborar una convención para los crímenes cibernéticos. Fue enarbolado en todo el mundo como un paso crucial hacia la gobernanza de la seguridad e Internet. Bajo esta premisa varios países no pertenecientes al Consejo de Europa están ahora tratando de implementar la convención en su legislación nacional a pesar de que, habiendo transcurrido cinco años, la mayoría de países del Consejo de Europa aún no han logrado llegar a un acuerdo.

También oímos frecuentes llamados a que se establezca una cooperación entre la industria y el gobierno en esta materia. A menudo se presume que ambos sectores tienen preocupaciones comunes. Tampoco esto podría estar más lejos de la realidad. Durante años el G8 realizó reuniones con autoridades de la industria del mundo entero que versaban sobre la seguridad en Internet pero con el paso del tiempo la iniciativa fue liquidada por falta de acuerdo. Aún dentro de

la industria podemos encontrar varios puntos de vista sobre lo que es la seguridad, por ejemplo, ¿es la protección de sistemas computacionales incluso de piratería informática legítima con fines de investigación? ¿el sistema incluye algún esquema de protección de derechos de autor? Sin embargo continuamos dedicando gran parte del tiempo a escuchar la retórica sobre gobernanza de Internet dentro de los procesos de la ONU diciendo que la cooperación es necesaria, casi como que la ONU no le ha estado prestando la debida atención a todos los procesos de política fallidos en el mundo.

En segundo lugar, la mecánica de las políticas de seguridad está cambiando. Estamos adquiriendo más conocimientos sobre los sistemas que fueron desarrollados e implementados con gran prisa en nombre de la seguridad. Las vastas infraestructuras nacionales para promover la seguridad y evitar los ataques terroristas ahora están siendo cuestionadas. A los políticos y autoridades se les vincula con sistemas específicos y no están más encabezando las encuestas. Podemos ahora constatar que las compañías cuentan con amplios proyectos de vigilancia desarrollados a instancias de planes del gobierno y están siendo castigadas por reguladores y por clientes.

Por ejemplo, en el mes de junio de 2006 las organizaciones de los medios de comunicación descubrieron que la Sociedad para la Telecomunicación Financiera Interbancaria Mundial (SWIFT) estaba revelando un gran caudal de datos respecto de transferencias bancarias al Ministerio de Hacienda de Estados Unidos. SWIFT es una cooperativa de instituciones financieras; aunque los particulares usen su servicio, sus verdaderos clientes son los bancos. En este caso, los reguladores de privacidad alrededor del mundo se percataron de que SWIFT estaba quebrantando la ley. Más inquietante aún, lo que se suscitó fueron asuntos geopolíticos (¿qué pasaría si el gobierno de China tuviese acceso a esta misma información?) y los clientes de SWIFT, o sea los bancos, comenzaron a ejercer presión sobre esta para que cambiase sus metodologías. El director general de SWIFT tuvo que jubilarse antes de tiempo y la organización tuvo que rediseñar su infraestructura de red y llevar sus operaciones a Suiza para evitar controversias.

Sin embargo, todavía dedicamos tanto de nuestro tiempo a hablar sobre la necesidad de seguridad y política de seguridad. ¿Cuánto tiempo más deberemos dedicar durante las reuniones sobre gobernanza de Internet a pedir cooperación en el tema de seguridad al mismo tiempo que ignoramos las complejidades de hacerlo y continuamos haciendo caso omiso de la privacidad como si fuese un concepto demasiado difícil de manejar? Entre tanto, las encuestas generales y las de consumidor continúan recordándoles a los legisladores que la privacidad es un tema que preocupa a las personas. La confianza en el comercio electrónico y la participación en la sociedad de información dependen de la confianza que las personas tengan en otros interesados en comunicaciones y transacciones. Las políticas de seguridad y privacidad son facilitadoras clave de la confianza, aunque muy poco se hace a favor del tema de privacidad mientras que nuestros procesos de política continúan enfocándose tan solo en percepciones fallidas de seguridad.

3. La falta de opciones de política

Puesto que es tan difícil llegar a un acuerdo sobre la seguridad en el campo de los actuales instrumentos internacionales y el lenguaje de política, solemos inferir que la privacidad es igualmente difícil de implementar. Esto no es necesariamente veraz. Hay un elocuente consenso que secunda la noción sobre la necesidad de proteger la privacidad y hay un consenso general sobre la manera de hacerlo. Desde 1960 hemos utilizado un sistema de regulación para administrar la información personal. Dicho sistema de regulación fue recogido en convenios internacionales a través de organismos como el Consejo de Europa en la Convención de 1981 sobre la Protección de Individuos en relación al Procesamiento Automático de Datos Personales y la Organización para la Cooperación y el Desarrollo Económico (OCDE) y sus directrices de 1980 que rigen la Protección de la Privacidad y los Flujos Transfronterizos de Datos Personales. Ambos estipulan reglas específicas que abordan la gestión de los datos electrónicos. Estas reglas describen la información personal como datos a los que se les concede protección a cada paso, desde la colecta hasta el almacenamiento y diseminación.

La obligación afirmativa de proteger la privacidad y la información personal se ha plasmado bajo lo que se denomina como "protección de datos" y suele utilizarse para proteger la privacidad individual en contra del abuso de los organismos públicos y empresas particulares. La primera ley moderna de protección de datos del mundo fue promulgada en la Land de Hesse en Alemania en 1970. Esto fue seguido por leyes nacionales en Suecia (1973), Alemania (1977) y Francia (1978). Estas cláusulas legislativas condujeron eventualmente a la proclamación de una directiva de la Unión Europea (UE) de 1995, la Directiva de Protección de Datos de la Unión Europea, 95/46/EU.

Las reglas de protección de datos dependen de las Prácticas Justas y Razonables para la Información, las cuales fueron desarrolladas a finales de los años 60 en respuesta a la amenaza de bancos de datos secretos que contenían grandes cantidades de informaciones personales. Traduciéndolo en términos sencillos, las prácticas justas de información obligan a los "controladores" (administradores de información personal) a ceñirse a ciertas pautas, de forma que:

- los datos personales deben ser recolectados únicamente para propósitos específicos, explícitos y legítimos
- las personas concernidas deben estar al tanto de tales propósitos y conocer la identidad del controlador
- cualquier ciudadano concernido debe tener acceso a sus datos, así como el derecho a cambiar o suprimir datos que no sean fidedignos y
- debe haber medidas correctivas disponibles para poder subsanar cualquier equívoco, incluyendo resarcimiento en caso de daños a través de los tribunales nacionales competentes.

En esencia, para recolectar datos se precisaría de un consentimiento informado expedido por la persona en cuestión; procesados conforme al derecho y de manera justa

para propósitos y uso limitados y guardados por un lapso determinado de tiempo.

Esto no significa que la seguridad sea ignorada. Puede haber leyes que interfieran con la legislación sobre la privacidad de datos. Cuando las cláusulas legislativas nacionales y las tecnologías se combinan de manera concertada para interferir con el derecho a la privacidad en nombre de la seguridad nacional, seguridad pública, bienestar económico, prevención del crimen y la anarquía, la protección de la salud y los principios y la protección de derechos y libertades de otros, el panorama se vuelve más complejo. Sabemos que esto sucede en cualquier sistema político moderno: las leyes que regulan los derechos individuales son sofisticadas y están actualizadas y las leyes que regulan la potestad del estado a interferir en estos derechos deben ser elaboradas con sumo cuidado, además de ser sofisticadas y estar actualizadas.

La Directiva de Protección de Datos de la Unión Europea 95/46 UE es el instrumento de protección de datos más moderno. Asegura que los datos puedan fluir a través y fuera de la UE siempre y cuando se cumpla con ciertos requisitos:

- los datos deben ser procesados de manera justa y en consonancia con la ley.
- deben ser recolectados para propósitos explícitos y legítimos y usados consecuentemente.
- los datos deben ser pertinentes y no desmesurados en relación al propósito para el cual se procesen.
- los datos deben ser precisos y puestos al día cuando fuera necesario.
- los controladores de datos están obligados a proveer medidas razonables para que los sujetos de los datos puedan rectificar, borrar o bloquear incorrecciones al respecto.
- los datos que identifican a individuos no deben ser mantenidos más tiempo que el necesario.

La Directiva también manifiesta que cada Estado Miembro debe proveer una o más autoridades supervisoras para monitorear la aplicación de la Directiva. Finalmente, la Directiva también exige garantías cuando los datos deban ser transferidos a una jurisdicción fuera de la UE para asegurar que existan las protecciones adecuadas. Esto evita que una compañía pueda recolectar datos en Francia y enviar esta información a otro país donde dichos datos puedan ser usados sin respetar las leyes francesas. Más bien, debe haber garantías de que los datos se transmiten a una jurisdicción donde hay adecuadas tutelas legales.

Mientras que OCDE, el Consejo de Europa y la Unión Europea juntos cubren muchos países con sus directrices, convenciones y directivas, todavía subsisten muchos países que carecen de leyes de privacidad de datos. Hay nuevas iniciativas en curso que se ocupan de esta situación. Una iniciativa proviene del subgrupo de privacidad de la Cooperación Económica del Asia-Pacífico (APEC). Han estado desarrollando un conjunto de principios que las economías en vías de desarrollo de la

región pueden adoptar para al menos establecer medidas básicas de protección para la información personal.

Este dominio no está desprovisto de complejidades y diferencias políticas. Hay grandes diferencias entre el modelo europeo y los modelos implementados en otros países. Por ejemplo, EEUU se rehúsa a implementar una ley de privacidad que regule el quehacer del sector privado. Hay cierta inquietud de que EEUU use los principios APEC como una norma global en vez del propósito pretendido, o sea, un conjunto de principios básicos. Esta situación es una traba al surgimiento de una norma global basada en una regulación amplia y fuerte. Algunos representantes de este sector de actividad también han expresado abiertamente sus preocupaciones sobre la ley de protección de datos. En septiembre de 2007 Google demandó una norma global de privacidad pero desechó el modelo europeo más abarcativo y, en su lugar, se plegó a los principios más débiles de APEC (¡lo que tomó a APEC de sorpresa!) para que se implantasen en todo el mundo, incluso en Europa.

Esto no refleja una falta de consenso sobre la necesidad de una política, sino más bien demuestra que se debe entablar un debate sobre los méritos de cada sistema regulador. Dicho debate está en marcha y ha probado ser enriquecedor e interesante. Sin embargo y como siempre, el proceso político de la gobernanza de Internet ignora por completo este dominio pues quizás continúe creyendo que la privacidad es un infranqueable dominio de regulaciones a pesar de los progresos alcanzados en casi medio siglo.

Replanteando la causa de la privacidad

La privacidad es un campo rico y complicado al mismo tiempo. No hay respuestas evidentes para ninguno de los problemas que representa. Pienso que esto también sea valedero en todos los interesantes campos de la política.

Pero el proceso de gobernanza de Internet continúa sin tomar en cuenta como debería a la privacidad. La falta de un examen más minucioso sobre la privacidad y el excesivo énfasis que se le da a una visión simplista de la seguridad nos está engañando a todos. La privacidad es un derecho humano y a la vez un interés de los consumidores. ¿Cuántas áreas de la política pueden afirmar eso de sí mismas? Y pese a todo, el silencio continúa.

Aunque algunas veces me sienta titubeante, otras estremecido por los retos al defender la privacidad, no puedo entender por qué no discutirla al menos en conjunto con todos los otros temas apremiantes de política actual. Este debate se está llevando a cabo en otros lugares y los resultados son fascinantes. Al limitar el debate sobre el tema limitamos asimismo nuestras opciones de política y nos veremos obligados, como hemos visto suceder, a enfrentarnos con las consecuencias de nuestras decisiones equivocadas en el futuro.