Vacío útil

El arte del olvido en la era de la computación ubicua

Por Viktor Mayer-Schönberger (*)

En marzo de 2007, Google confirmó que desde su inicio ha almacenado cada búsqueda que cada usuario ha hecho y cada resultado de la búsqueda sobre la que hizo clic. Google recuerda para siempre.

“хранитьвечно“ (ser preservado por siempre) estampaba la KGB en los expedientes en sus presos políticos. El estado comunista nunca olvidaría la identidad, las creencias, las acciones y las palabras de los opositores.

Como el estado soviético, Google no olvida. Pero a diferencia de la Unión Soviética que dejó de existir hace quince años, Google se ha convertido en una herramienta imprescindible para centenares de millones de personas en todo el mundo, quienes la utilizan cada día. Parece que tenemos que aceptar que nuestra sociedad digital puede perdonar pero no olvidar.

En este artículo sugiero que restablezcamos la capacidad de nuestra sociedad para olvidar. La primera parte describe cómo hemos olvidado olvidar, debido a una combinación de innovaciones tecnológicas y la consiguiente economía cambiante de la tecnología de la información. En la segunda parte critico tres respuestas convencionales a nuestra inhabilidad digital de olvidar. La tercera parte repasa una respuesta no tradicional de combinar la ley y el software propuestos por Lawrence Lessig. En contraste, sugiero una propuesta más modesta de invertir la retención de los datos por defecto, describo cómo tal propuesta trabajaría, y porqué es superior a sus alternativas. (Para los lectores interesados en mi propuesta solamente, salte por favor directamente a la Parte 4).

1. La defunción del olvido

Como seres humanos tenemos la habilidad de recordar. Con todo, a pesar de la capacidad notable de nuestro cerebro, la mayor parte de nuestras memorias se diluyen en un cierto plazo. Nosotros olvidamos. Afortunadamente, tendemos a recordar cosas importantes, y a olvidar las menos significativas. No sólo nuestra memoria individual se pierde. Debido a que somos mortales la memoria colectiva de cada generación desaparecería si falláramos en pasarla a tiempo.

Por miles de años, los seres humanos han intentado preservar sus memorias más allá de la vida de cada generación. Nuestros antepasados han transmitido su saber a

sus niños, a fin de guardar su memoria social viva. Comenzaron a pintar y a escribir. La prensa hizo la retención más barata y la difusión más fácil. Así se difundió la alfabetización. Más tarde, agregamos el fonógrafo, la fotografía y las películas. Así como el equipamiento para registrar y almacenar llegó a estar ampliamente disponible, la gente comenzó a utilizarlo. Más y más de lo que decimos y hacemos se preserva.

Con todo, hasta hace poco tiempo la conservación seguía siendo costosa, la búsqueda era difícil y el acceso limitado. Los costos de la continua preservación nos forzaron a considerar cuidadosamente los beneficios de la retención y del borrado. Solamente los expedientes vistos como importantes y valiosos fueron guardados. Las bibliotecas eran emprendimientos costosos, requiriendo de expertos para mantener los libros en el orden correcto. Nuestros abuelos tenían sus fotos tomadas solamente en las ocasiones especiales, y nuestros padres nos filmarían con Súper 8 en tomas cortas solamente, debido al precio de la película.

Buscar nuestros artefactos culturales de libros y grabaciones, de fotos y películas, era una tarea aburrida y que llevaba tiempo. Acceder y armar un mosaico de las palabras y de las acciones de una persona para armar un registro biográfico, por ejemplo, requería entrenamiento, dedicación y maestría. Los legos raras veces se ocupaban de tales empresas, dejándolo a profesionales para proveer de resúmenes sucintos. Donde el gobierno intentó crear un depósito de datos enorme -como el

Stasi lo intentó en Alemania del Este- a menudo (pero no siempre) falló debido a las limitaciones inherentes para preservar, estructurar, y recuperar la información análoga. Por siglos, nuestra mirada de nuestro pasado había sido formada por las realidades técnicas y económicas de la retención, el acceso y la recuperación de la información.

La tecnología digital ha cambiado esto. El código digital ha hecho el procesamiento así como el almacenamiento de la información no sólo más fácil sino también más barato. La capacidad de almacenamiento magnético se ha duplicado cada año a un valor constante. Incrementos similares en el poder de procesamiento han hecho posible indexar nuestro contenido digital almacenado, así como ofrecer la recuperación casi instantánea de grandes cantidades de información almacenada. Finalmente, a través de las redes digitales –Internet en particular- podemos tener acceso a estos tesoros de la información en todo el mundo desde nuestros ordenadores personales, teléfonos celulares y otros dispositivos digitales.

Esto ha dado lugar a un cambio drástico en nuestro comportamiento en cuanto a la retención de los datos. Durante milenios fue difícil y costoso preservar. Lo hacíamos solamente en circunstancias excepcionales, y frecuentemente solo por un periodo de tiempo limitado. Por casi toda la historia humana, la mayor parte de lo que los humanos experimentaron fue olvidado rápidamente. Hoy, sin embargo, la retención de datos digitales es (relativamente) fácil y barata. Como consecuencia, y

sin otras consideraciones, guardamos en vez de borrar. Éste es el punto central: en nuestro pasado análogo, el valor por omisión era desechar algo antes que preservarlo; hoy el valor por omisión es retener.

Las Compañías de Crédito –en los EE.UU.- almacenan gran cantidad de información sobre cientos de millones de ciudadanos de los EE.UU. Daniel Solove escribió que el proveedor más grande de información de mercadeo en los EE.UU ofrece más de 1000 datos de referencias de cada uno de los 215 millones de individuos en su base de datos. Podemos ver la combinación de fuentes de datos antes dispares. Solove menciona una compañía que provee una vista consolidada de datos de 20.000 diferentes fuentes de todo el mundo. Esta retiene los datos, él escribe, incluso si los individuos disputan su exactitud.

Las compañías guardan nuestras reservas en el transporte aéreo en archivo incluso cuando decidimos no comprar el boleto, junto con rica información sobre nosotros y nuestros patrones de viaje anteriores. Millones de cámaras en lugares públicos -el Reino Unido, solamente, dice operar entre 2 y 3 millones- produce registros de nuestros movimientos que son guardados. Agencias policiales guardan la información biométrica de alrededor de diez de millones de individuos incluso si éstos nunca han sido acusados de un crimen. Los motores de búsqueda conservan cada una de nuestras búsquedas, y mantienen copias archivadas de nuestras páginas web mucho tiempo después de que las hayamos puesto off-line.

Éste es solamente el principio. Con el advenimiento de la computación ubicua, de chips GPS baratos en nuestros teléfonos celulares, cámaras y coches; de etiquetas RFID en objetos diarios, y de sensores minúsculos conectados entre sí alrededor nuestro, un rastro más completo que nunca de nuestras acciones será recolectado. Dado el bajo costo de almacenamiento, la facilidad de recuperación y el potencial valor del acceso a la información, muchos de los datos que se están recogiendo serán guardados por meses, sino años, así como nuestro valor por omisión social ha cambiado de eliminación a retención.

Esto tiene consecuencias drásticas más allá de la capacidad obvia de saber mucho más sobre las preferencias, comportamientos, acciones y opiniones de otra gente que en el mundo análogo de olvido incremental. La vida en un mundo en el cual nuestras vidas están siendo registradas y los registros se están conservando, en el cuál el olvido social ha sido sustituido por un recordar preciso, influenciará profundamente la forma en que vemos nuestro mundo, y cómo nos comportamos en él.

Si lo que hacemos se puede sostener contra nosotros más adelante, si se preservan todos nuestros comentarios impulsivos, estos pueden ser combinados fácilmente en una imagen compuesta de nosotros mismos. Asustados por cómo nuestras palabras

y acciones se puedan percibir años después sacadas de contexto, la falta de olvido puede incitarnos hablar menos libremente y abiertamente.

Ésta es la versión temporal de una sociedad panóptica, en la que todo está siendo observado; es esta una sociedad en la cual la mayor parte se está registrando y recogiendo se está preservando. Independientemente de otras preocupaciones que podemos tener, es difícil de ver como un mundo que no olvida podría ofrecernos la sociedad abierta a la que estamos acostumbrados hoy.

2. Tres respuestas convencionales

Aquellos que tienen acceso y control sobre nuestros datos personales disfrutan de poder informacional. Los intereses por tal poder (y su abuso potencial) han generado tres tipos de reacciones: la respuesta legislativa integral, la reinterpretación de la respuesta constitucional y la respuesta nula.

a. Legislación integral de privacidad:

Muchos defensores de la privacidad sostienen que el rastro integral de la información personal digitalizada que se conservan requiere una reacción legislativa igualmente integral.

Mientras la retención de datos sea obligada el objetivo de tal acción legislativa es mucho más amplio. Mientras que obliga la retención de los datos la meta de tal acción legislativa es mucho más amplia. Solamente los estatutos de privacidad que cubran tanto el sector privado como el público y que abarquen todas las etapas del uso de la información personal -desde la recolección y el procesamiento a la retención y transferencia- se ven como capaces de contener y atenuar el peligro a nuestra privacidad. La así llamada protección de datos ómnibus es a menudo sostenida con revisión rigurosa y procedimientos de ejecución. El resultado es un régimen legal complejo con los cuales los usuarios del sector privado y público de la información personal tienen que conformarse.

En muchas naciones industriales y post-industriales en todo el mundo, desde Canadá, Argentina y Chile a Hong Kong, Australia y Nueva Zelanda, tal legislación ha sido promulgada, parcialmente en respuesta a los miedos públicos en cuanto a la recolección y retención de datos a gran escala; en Europa, la Directiva sobre la Protección de Datos de la Unión Europea (UE), aprobada en 1995, obliga a las veintisiete naciones miembro de la UE a aprobar leyes ómnibus de privacidad rigurosas.

En naciones donde están todavía ausentes tales regímenes integrales de protección de datos, como los Estados Unidos, los defensores de la privacidad esperan que los reportes periodísticos y la inquietud general ciudadana sobre la amenaza a la

intimidad de la información en última instancia produzcan el fermento para la acción política y legislativa.

En el mismo sentido, tal respuesta está cargada con dos problemas substanciales: la inercia política debida a las barreras de acción colectiva, y el potencial estructural rebasado combinado con un impacto real limitado.

La promulgación de legislación sobre la privacidad siempre será difícil de alcanzar políticamente. Un relativamente pequeño grupo de usuarios de datos personales, que están en contra de perder cualquier iniciativa legislativa que restrinja sus actividades, tiene el incentivo para organizar la oposición política. Mientras tanto, millones de individuos quienes son beneficiarios potenciales de tal legislación de privacidad son demasiado difusos y raramente enérgicos como para ejercer presión sobre a las legislaturas para que actúen.

En gran medida, esto es similar a los debates públicos y la acción legislativa resultante sobre la propiedad intelectual.

Allí, también, un relativamente pequeño grupo bien organizado de sostenedores de los derechos ha sido capaz de movilizarse contra el debilitamiento legislativo y a favor de la consolidación legislativa de los derechos de propiedad intelectual,

mientras que el grupo difuso de millones de consumidores de la propiedad intelectual ha fallado en movilizarse.

Dado el registro histórico de los debates sobre la privacidad en los Estados Unidos así como la trayectoria comparable de los debates sobre la propiedad intelectual (con una estructura algo similar de actores en ambos lados) es poco probable pero no imposible un acontecimiento que remueva lo suficiente el apoyo público para que un acta integral de privacidad consiga ser promulgada.

El segundo problema con una respuesta legislativa convencional es estructural. Las leyes son compromisos sociales congelados en el tiempo. Fueron promulgadas bajo circunstancias particulares y dentro de un contexto histórico específico. Así como emergen las nuevas tecnologías, la economía cambia, y la sociedad desarrolla el equilibrio delicado de los valores implícitos en reglas legales que pueden desquiciarse. Al grado tal que un desequilibrio energiza y moviliza a los ciudadanos, y puede llevar a un ajuste de la ley. El objetivo fundamental de tal acción correctiva es restablecer el equilibrio original.

Claramente el cambio en la retención de los datos personales causados por tecnología digital puede requerir un ajuste legislativo. Con todo, lo que los defensores de la privacidad sugieren –legislación ómnibus de protección de datos- no es un simple ajuste. Los estatutos integrales de la privacidad crean derechos

complejos y de gran envergadura, estructuras y procesos, y alteran fundamentalmente la manera en que los datos personales pueden ser utilizados.

Por ejemplo, bajo leyes europeas de la protección de datos, los datos personales generalmente pueden solamente se recolectados, procesados y almacenados con consentimiento -y solamente para un propósito particular. Cualquier cambio de propósito personal requiere obtener el consentimiento del individuo. Los individuos pueden requerir que se les informe qué datos personales se almacenan acerca de ellos, para qué propósito y de qué fuente, y qué información personal se ha pasado a terceros (eventualmente).

Mientras se crea un complejo régimen de nuevos derechos, en realidad estos derechos raramente se practican. Pocos peticionan el acceso a sus datos, e incluso menos hacen cumplir sus derechos a través de una demanda legal. En efecto, durante un período de diez años en Alemania, ningún proceso legal fue traído por un individuo demandando por derechos de privacidad infringidos, aun cuando la ley de protección de datos de Alemania cambia la carga de la prueba en la afirmación de daño a potenciales demandantes por parte de quienes procesan esos datos personales.

En suma, el acta ómnibus de protección de datos crea estructuras, procesos, instituciones, y derechos completamente nuevos que raramente se utilizan.

Introducen un fundamentalmente nuevo régimen para manejar demandas de privacidad, reemplazando de este modo un compromiso de valor social existente por un nuevo. Esto no significa que tal salto hacia un régimen integral de privacidad de la información no debe ser dado, sino que debe ser el resultado de una renegociación social de los valores subyacentes. Dada la inercia legislativa que he descrito, no está claro que nuestra sociedad esté lista y deseosa por tal renegociación en un tiempo cercano.

b. Reinterpretación constitucional:

Hemos entendido algunos valores son demasiado importantes para ser negados por el simple gobierno de la mayoría. Los protegemos con las normas constitucionales, haciéndolos difíciles de alterar. Nuestras cortes son llamadas a interpretar el significado de las cláusulas constitucionales que protegen los valores fundamentales a la luz del cambio social. Esto requiere cuidado, como derechos constitucionalmente protegidos son ellos mismos compromisos sociales minuciosamente balanceados sobre los valores fundamentales congelados en el tiempo.

Uno puede sugerir que el cambio desde el olvido hacia recordar (y la resultante retención de los datos personales que he descrito) significa exactamente una situación en la cual la Suprema Corte deba reinterpretar ciertos derechos

constitucionales, especialmente si las legislaturas, quizás debido a las vallas de la acción colectiva que he mencionado, fallan en actuar y dejan la protección constitucional minada por nuestra realidad social.

Los argumentos que sugieren un ajuste constitucional sobre la base de la Primera Enmienda se basan en la noción de que los seres humanos deben tener el derecho de acordar en un debate público robusto. La retención ilimitada de nuestras observaciones puede imposibilitar a individuos a decir que tienen en mente y empobrecer el debate público. Esta es la idea de que el panóptico causa un efecto glacial que sofoca el discurso libre.

En Laird vs. Tatum, se le requiere a la Corte Suprema que juzgue si los archivos del ejército que contienen actividades pacifistas de demandantes violan su libertad de expresión. Al fracasar en identificar el daño concreto, la corte desestimó el caso. Recientemente, la corte ha atemperado un poco el efecto paralizante del argumento, pero indicó que solo la acción que intenta atemorizar podría violar la Primera Enmienda. Esto, sin embargo, será difícil de demostrar en la mayoría de los casos en los que los datos personales de los individuos están siendo registrados y conservados.

Christopher Slobogin ha sugerido otro potencial argumento de la Primera Enmienda, a saber, la capacidad de expresarse uno mismo anónimamente. Durante las últimas

décadas, la Corte Suprema ha atacado leyes que requerían a los individuos se identificaran a sí mismos o sus afiliaciones antes de participar en una disertación pública. Julie Cohen han sostenido que el anonimato debe ser protegido más allá de la protección en disertaciones públicas. Mientras la Corte Suprema aún no ha decidido un caso de recolección y retención de datos personal a través de la lente del anonimato, uno puede concebir casos que pueden impulsar a la corte a hacerlo en el futuro. Por ejemplo, el registro de individuos a través de las cámaras de vigilancia públicas -especialmente cuando están ligados a la acción comunicativa-, identificándolos automáticamente con reconocimiento de rostro, es la clase de exposición involuntaria del anonimato sobre el que la Suprema Corte estuvo interesada en el pasado.

Las discusiones de la Cuarta Enmienda se centran en el acto de recoger datos personales. Una vez que la recolección de datos pueda ser caracterizada como “búsqueda” de la Cuarta Enmienda, tal recolección requeriría la adhesión a salvaguardas procesales rigurosas. En Katz vs. Los Estados Unidos, la Corte Suprema indicó que en principio la implantación de micrófonos ocultos de una cabina de teléfono público era un tipo "de búsqueda", lo cual indica que el argumento no es sin mérito. Pero en el mismo caso la Corte sostuvo también que si uno “a sabiendas expone al público” la información, no puede reclamar la protección de la Cuarta Enmienda. Por consiguiente la Corte enfatizó que ve que la mera observación sin la intrusión no viola la Cuarta Enmienda. Por lo tanto, solamente cuando los datos

personales se recogen sin que el individuo asuma que sus palabras y acciones son públicas, es esto una "búsqueda" potencial que provoca los apremios de la Cuarta Enmienda. Algunos han sostenido que la Corte Suprema puede necesitar re-conceptualizar más ampliamente su interpretación de la Cuarta Enmienda para responder a las amenazas emergentes a la privacidad, pero la Corte ha sido hasta ahora renuente a hacerlo.

Un tercer argumento constitucional podría ser hecho directamente en base al derecho a la intimidad. Mientras que ésta puede parecer la avenida más obvia, los expertos constitucionales son renuentes. El derecho a la intimidad no se menciona explícitamente en la Constitución; antes, "se ha encontrado" implícito en la Primera, Tercera, Cuarta, Quinta, Novena y Catorceava Enmiendas. Incluso después cuatro décadas de antecedentes sus contornos siguen siendo vagos, y la Corte ha sido muy renuente ampliar su alcance más allá de sus (estrechos) confines originales.

Hay otra coacción importante que limita la utilidad práctica del acercamiento a la reinterpretación constitucional: las garantías constitucionales, con muy pocas excepciones, obligan solamente al gobierno, no la acción privada. En el mejor de los casos, entonces, la reinterpretación constitucional puede restringir la recolección y retención gubernamental de datos personales, pero no tendrá ningún impacto en las prácticas del sector privado. Esto quizás puede aliviar a los libertarios

únicamente preocupados por el poder del estado, pero deja temores infundados hacia un Google panóptico.

c. La respuesta nula:

La tercera respuesta posible es inacción legal, basada en consideraciones procesales y normativas. Procesales, si los ciudadanos están suficientemente preocupados acerca de la retención comprensiva de los datos, ejercerán presión sobre las legislaturas para aprobar la legislación sobre privacidad. El hecho de que (en los EE.UU. al menos) no haya sucedido, indica nuestra sociedad no está lo suficientemente preocupada en desear que se tomen medidas legislativas. Mientras que aquellos en minoría pueden lamentar el resultado, los defensores de la respuesta nula pueden verlo como democracia trabajando. Por otra parte, el mecanismo apropiado que obligue el ajuste constitucional para tratar las preocupaciones de la minoría es el juicio constitucional. Incluso los expertos constitucionales conceden que no hay derecho constitucional al olvido social. Es improbable por lo tanto que la Suprema Corte actual encuentre el cambio general de olvidar a recordar violando una garantía constitucional particular.

Si no hay buena voluntad de la mayoría de legislar, ni caso normativo convincente hecho por la institución que juzga reclamaciones constitucionales de intervenir, la inacción puede ser la mayor parte de respuesta apropiada y eficiente comparada

tanto a un nuevo régimen regulador costoso como a la incertidumbre legal causada por la reinterpretación Constitucional.

La respuesta nula parece que obliga, pero la discusión contiene una potencial debilidad. La respuesta nula de las preferencias de los ciudadanos que están reflejadas adecuadamente en resultados legislativos se basa en una vista idealizada de cómo las democracias modernas trabajan. Los teóricos de las Ciencias políticas han expuesto y explorado largamente la importancia de los intereses bien organizados que pueden capturar la agenda legislativa, especialmente cuando estos intereses se oponen a una relativa y difusa, mayoría activa. “Capturar”, problemas en el accionar colectivo, asuntos de agencia y el interés político disminuyen la habilidad de la mayoría para transformar su voluntad en ley. Asumir que estas barreras están ausentes en el contexto de la retención de los datos es ingenuo, y el cambio social del olvido a recordar puede no ser legitimado por el proceso democrático.

Además, la respuesta nula no es necesariamente la menos costosa. Por ejemplo, dada la trayectoria evolutiva de la tecnología, un pequeño ajuste en el marco jurídico hecho hoy puede ser más económico que adoptar un acta ómnibus más costosa en el futuro.

Parece que estamos enfrentados con tres respuestas subóptimas: acción legislativa que introduzca un marco comprensivo de privacidad mucho más amplio que la aplicación específica de la retención de los datos personales; una interpretación constitucional limitada que cubra solamente las actividades del gobierno; o la inacción a pesar de un cambio social ilegítimo lejos del olvido.

3. Combinando la ley y el código – La respuesta de Lessig:

Lawrence Lessig ha ofrecido una razón de por qué las medidas legislativas convencionales están fallando a menudo en nuestro mundo digital. Él sugiere que la conducta humana se pueda obligar a través diversos mecanismos. La ley, que él apoda "El código de la Costa Este", es uno de ellos; las normas culturales y el mercado son las otras dos. En nuestra era digital, un cuarto mecanismo surge como importante: las reglas incorporadas a nuestras tecnologías de información y de comunicación a través del software. A esto Lessig llama el "Código de la Costa Oeste". Así como nuestras tecnologías digitales ganan importancia en nuestra vida diaria, él sostiene, el software torna mucho más útil el mecanismo para influenciar y obligar nuestro comportamiento que la ley. Lessig propone así que la regulación eficaz de nuestro espacio digital no se pueda alcanzar con ley solamente, sino que requiere la combinación múltiples mecanismos de obligación.

Lessig incluso aplica su teoría a la privacidad de la información. Él es consciente de la respuesta legislativa, el estatuto ómnibus sobre la privacidad. Pero también reconoce las debilidades significativas inherentes en un marco tan complejo, incluyendo su falta de eficacia. En este lugar Lessig sugiere un mecanismo mixto: decretar legislación que garantice a los individuos alguna clase de derechos sobre su información personal, provea una infraestructura técnica para negociar información personal a bajo costo, y facilite mercados en los cuales los individuos pueden decidir para sí mismos si, bajo qué condiciones, y a qué precio permiten que otros utilicen sus datos personales. Esencialmente, Lessig sugiere que creemos ley y software - Código de la Costa Este y de la Costa Oeste - para proporcionar la protección eficaz y eficiente para la información personal.

Lessig toca un aspecto importante que los defensores de las actas ómnibus de privacidad desatienden a menudo: Las restricciones a nuestro comportamiento trabajan mejor cuando no cargan indebidamente comportamiento legítimo.

Esto lo lleva a sugerir un sistema en el cual la ley proteja demandas sobre los datos personales, pero deja al mercado negociar su uso - como Coase ha sugerido para el espectro de la radio.

La tecnología permite estas transacciones de mercado bajando el costo implicado en la transacción de modo que el mercado funcione eficientemente. La tecnología

también ayuda en hacer cumplir, haciendo el comportamiento ilegal relativamente más difícil que el legal. Comparado con las leyes ómnibus de la protección de datos, la propuesta de Lessig tiene la ventaja de la eficacia relativa.

La idea de Lessig de combinar ley y software para regular no es tan radical como puede sonar al principio. De hecho, el congreso ha regulado en forma semejante en por lo menos dos dominios de la información y del reino de la comunicación: la medición de los contenidos de la televisión y los derechos de autor.

En el contexto de medición de los contenidos de la televisión, el Congreso mandó cada que cada receptor de televisión construido desde el 2000 en adelante contenga un chip especial (el así llamado V-Chip), que descifre la información especial enviada con la señal ordinaria de televisión. Esta información contiene una medición del contenido emitido en ese canal, basado en siete dimensiones (violencia, lenguaje, situaciones sexuales, diálogos, fantasía violenta, drama, y humor crudo) y seis niveles. Los espectadores (particularmente padres) pueden fijar su TV para que sólo muestre programas de cierto contenido. Este sistema combina leyes convencionales con una infraestructura tecnológica (el V-Chip, etc.), asegurando de tal modo que los padres puedan utilizar (voluntariamente) las pautas parentales de la TV con eficacia y a bajo costo.

La legislación de los derechos reservados ofrece un segundo caso. La ley de Derechos de Autor convencional prohíbe el uso no autorizado del material con derechos de autor excepto en ciertas circunstancias relativamente excepcionales. Debido a los avances en tecnología digital, el copiado y la distribución de trabajos no autorizados llegó a ser más fácil y más barata que obteniendo una licencia apropiada. Para remediar esta situación, el congreso facilitó una infraestructura del mercado que permita la autorización a mucho menor costo -similar a la idea de Lessig de que tecnología apoye a los mercados eficientes para la información personal.

En su lugar, el congreso en el Acta del Milenio del Derecho de Autor Digital (DMCA) decidió hacer del copiado y distribución no autorizados más difícil prohibiendo el intento de forzar, mediante mecanismos técnicos que protegen trabajos con derechos de autor. Esto restringe un poco el tipo de software que ser desarrollado y ofrecido en el mercado. Quienes quieran violar ley de Derechos de Autor tendrán más dificultad en la obtención de las herramientas técnicas para hacerlo. La conducta ilegal se está convirtiendo en algo mucho más costoso que la legal, y de allí que cambia el modo en que los usuarios se comportan.

En suma, la propuesta de privacidad de Lessig para combinar ley y software es útil en teoría y aplicable en la práctica.

Con todo, en el contexto de este artículo - concebir de una respuesta útil al cambio social del olvido a recordar -su propuesta sufre de una debilidad no disímil a la legislación de la protección de datos ómnibus. Es demasiado amplia. Sugiere que creemos un mercado hecho y derecho para la información personal con la infraestructura técnica, legal, y social necesaria. Asume que la gente se comprometerá y comportará racionalmente en estos mercados.

Es una propuesta compleja y de gran envergadura responder cuál es el límite: la necesidad de nuestra sociedad de recordar el olvidar. Como las Actas de protección de datos ómnibus, la propuesta de Lessig puede ser demasiado substancial para los responsables políticos y los ciudadanos por igual. (En su defensa, Lessig hizo su propuesta como una respuesta comprensiva a la amenaza a la privacidad en el ciberespacio, no como una reacción al asunto de la retención de los datos.)

¿Qué podemos aprender de la propuesta de Lessig para nuestro caso? Necesitamos enfocarnos, responder eficazmente a nuestra inhabilidad social de olvidar. Esto no requiere la disposición de un régimen de privacidad comprensivo, mientras que combinar ley y software puede ayudar a hacer nuestra respuesta eficaz.

4. Reinventado el valor por omisión – Reintroduciendo el olvido en nuestra sociedad:

Donde olvidábamos en un cierto plazo, ahora tenemos la capacidad de recordar perfectamente.

El cambio tecnológico nos ha permitido, antes que borrar datos retenerlos como valor por omisión, a menudo por un tiempo muy largo. Esto es particularmente preocupante cuando estos datos nos pertenecen a nosotros, a nuestras vidas, acciones, creencia, y preferencias.

Propongo que cambiemos el valor por omisión cuando almacenamos información personal de nuevo a donde ha estado por milenios, de recordar por siempre al olvido en un cierto plazo. Sugiero que alcancemos esta revocación con una combinación de ley y de software. El rol primario de la ley en mi propuesta es el de mandar a quienes que crean el software que recoge y almacena estructura de los datos en su código, no sólo la habilidad de olvidar con el tiempo, sino de hacer de tal olvido el valor por omisión.

El principio técnico es similarmente simple: Los datos se asocian a metadatos que definen cuánto tiempo la información personal subyacente debe ser almacenada. Una vez que los datos han alcanzado su fecha de vencimiento, serán suprimidos automáticamente por el software, por el Código de la Costa Oeste de Lessig.

Esto puede sonar simplista o radical (o ambos), pero creo no es ni uno ni otro, como espero que usted convenga cuando entienda cómo lo preveo para trabajar, y cuando explico su ventajas y defectos.

a. Los funcionamientos del olvido:

La propuesta técnica es absolutamente modesta. Manejamos y almacenamos una cantidad cada vez mayor de metadatos sobre nuestra información. Una abundancia de metadatos maneja mucho de lo que nosotros llamamos la Web 2.0. Los sistemas de archivos de nuestros sistemas operativos modernos manejan metadatos en todos nuestros archivos. Las aplicaciones y dispositivos agregan metadatos sin mucha intervención: las cámaras digitales almacenan una abundancia de metadatos con cada foto tomada, nuestro programa de manejo las fotos agrega otro conjunto de ellos. Nuestro software de biblioteca de música maneja los metadatos para nuestra música, de vínculos a las letras y arte del álbum y la lista de reproducción, a nuestras propias etiquetas y preferencias. Y sí, la Administración de los Derechos Digitales (DRM) proporciona (y hace cumplir) metadatos de las derechos para muchos de los trabajos digitales con derechos de autor que hemos almacenado en nuestro dispositivo. Pronto, veremos metadatos geográficos ser agregados a nuestros medios y utilizados para visualizar nuestros viajes y permitirnos conectar con otros en nuestra vecindad geográfica. Mi propuesta agrega simplemente otro tipo de metadato: la información sobre la expectativa de vida de los datos.

En la mayoría de las instancias de uso individual, poco cambiaría el mundo que conocemos. Configuramos nuestro software de procesamiento de textos y de hoja de cálculos una vez, de modo que nuestros documentos son automáticamente etiquetados para tener una vida casi infinita (aunque habría maneras fáciles de cambiar la fecha de expiración).

La situación comenzaría a lucir diferentemente para el software de manejo de webcams y cámaras de vigilancia. Allí el mandato legal requeriría código de software para fijar un valor por omisión relativamente corto para el almacenamiento, quizás un par de días o semanas.

Mi propuesta también alteraría el cómo las cookies de Internet trabajarían. Las cookies tienen ya la fecha de vencimiento, pero esa fecha se fija a menudo décadas en el futuro, creando en efecto datos que nuestros navegadores de Internet nunca olvidarán. Cuando la codifican la ingeniería de software de las cookies deberían preguntar en serio cuánto tiempo los datos de la cookie deben persistir realmente, y fijarlo de acuerdo a eso.

Google y otros motores de búsqueda pueden tener que cambiar sus prácticas también. No podrían almacenar más las preguntas de las búsquedas por siempre. Tendrían que ser suprimidas -olvidadas - en un cierto plazo. Amazon tendría que

ajustarse cambiando su software a “olvidar” automáticamente qué libros usted readquirió en los años anteriores (como resultado los clientes pueden quizás experimentar mayor exactitud en las recomendaciones de Amazon. Después de todo, ¿cuales preferencias literarias permanecen constantes durante años?)

El cambio también afectaría a los teléfonos celulares. El software del teléfono celular almacena actualmente a menudo los datos del tráfico - por ejemplo las diez últimas llamadas hechas - por siempre. Propongo que los datos almacenados del tráfico en teléfonos celulares sean marcados también con una fecha de vencimiento de, digamos, una semana o dos, después de lo cual el teléfono celular automáticamente borraría esa porción de datos sobre el tráfico de la memoria del teléfono celular. Lo mismo se aplicaría a las fotos y a los vídeos en los teléfonos celulares, así como la información personal adentro agendas del teléfono celular, tal vez con un marco de un tiempo mucho más largo quizás de meses o de años.

No me malinterprete: No sugiero que su teléfono celular borre su memoria al día siguiente. Lo qué sugiero es que por omisión la información personal digital no se guarde por siempre. Piense en ella como el análogo a nuestro mundo no-digital, donde escribimos notas temporales rápidamente sobre pequeños trozos de papel, que son fáciles de tirar (o perder). En el mundo de los post-it y las servilletas, el valor por omisión de olvido (o por lo menos perder acceso a) se incorpora obviamente.

Mi propuesta también afectaría la trayectoria y el uso de las tecnologías futuras, especialmente en las áreas de redes de detección. Mucho se ha escrito sobre la amenaza potencial de los sensores digitales dominantes. Limitando la duración que tales datos del sensor que se pueden conservar, podríamos tratar partes significativas del desafío.

Para algunas compañías, los cambios técnicos demandados por mi propuesta pueden requerir trabajo, incluso ajuste de las prácticas empresariales. Para otros puede reflejar sus convicciones sobre la privacidad. Tome Microsoft, por ejemplo. Sus propias "Pautas de Privacidad para Productos y Servicios de Software" indican que "Cualquier dato de usuario almacenado por una compañía debe tener una cláusula de retención que indique cuánto tiempo los datos deben ser guardados, y la manera en que deben ser removidos de todos los medios de almacenamiento de datos."

Mi propuesta apunta reintroducir el concepto del olvido en un cierto plazo en nuestro reino digital. Mi meta es cambiar el valor por omisión de retener para siempre por la supresión después de cierto tiempo. El núcleo de mi propuesta no prevé que los usuarios no pueden cambiar las fechas de vencimiento si quieren - el equivalente digital de escribir la dirección de alguien en una servilleta y ponerla

cuidadosamente en un archivo para preservarla. En cierto modo, hemos tenido la capacidad de hacer eso casi por siempre.

Pero esto requiere un acto deliberado; y eso es lo que sugiero que nuestros dispositivos digitales requieran de nosotros, también.

b. Un espectro de opciones:

Las legislaturas podrían - si quisieran ir más allá del mínimo de lo que sugiero – mandar que las organizaciones que almacenan información personal sólo usen software que pueda manejar meta datos de vencimiento (probablemente en un registro antes que a nivel de archivo) y que mantenga el dato de expiración hasta la fecha.

Esto puede forzar a las Oficinas de Crédito y a vendedores de bases de datos marketing directo a pensar un poco más en sus políticas de retención de datos. Esto puede forzar a los operadores de los sistemas de reservación automatizada en la industria del turismo a suprimir sus registros después de que la reservación fuera cancelada, y a no conservarlos durante mucho más tiempo como usualmente es su práctica. Puede forzar a las agencias de gobierno a ponderar si y cuando borrar datos de los ciudadanos, antes que guardarlos, por caso. Quienes elaboran las políticas seriamente preocupados por la privacidad de los ciudadanos en la era

digital podrían incluso ir un paso más adelante. Podrían obligar las organizaciones y a las compañías que procesan información particularmente sensible a firmar digitalmente los metadatos del vencimiento y – tomando una página de la legislación anti-incumplimiento de DMCA- prohibir la alteración no autorizada o forzada de tales metadatos. Esto podría hacer que un cambio desautorizado en los datos del vencimiento - por ejemplo por terceros – sea más difícil. No estoy proponiendo una medida legislativa, pero sería completamente consistente con mi propuesta.

Esto podría incluso ser aplicado a las fotos y a los vídeos. La provisión de pequeños "dispositivos del permiso", que llevaríamos con nosotros como anillos claves. Podrían ser establecidos como "permitir" o "negar", y transmitiría esa respuesta en forma inalámbrica cuando sea requerido. Una nueva generación de cámaras digitales podría obtener los dispositivos del permiso de la persona registrada. La cámara entonces fijaría los metadatos de vencimiento conforme a eso, dando un par de días o semanas en caso de que el dispositivo de alguien estuviera establecido en "negar", mucho más largo si todos los dispositivos de permiso estuvieran fijados en "permitir". La cámara podría incluso proporcionar una señal visual si el dispositivo de alguien dice "negar".

Mi propuesta ofrece una gama de opciones a los legisladores, un espectro desde la idea central a más complejas, y versiones de mayor envergadura. Donde los

hacedores de las políticas encuentren su específico punto legislativo corre por su cuenta. Por otra parte, ninguna opción promete la perfección. Las salidas - metadata que es cambiada para evitar la cancelación - persistirán, no obstante la variación de grados. Pero la perfección no es mi tema, el cambio de la opción por defecto lo es.

c. Ventajas y debilidades:

Mi propuesta es moderada en por lo menos tres dimensiones:

• Tecnológicamente, como he descrito, utiliza mucha de las ideas, las infraestructuras, y los mecanismos que ya existen. En la mayoría de los casos, requiere solamente modificadas modificaciones técnicas.
• Legalmente, introduce en el reino digital la opción por omisión contra la retención que nos es tan familiar en nuestro mundo análogo, y refleja así el valor fundamental que es la base de nuestra constitución. No crea nuevos derechos, o nuevas instituciones. En su lugar, establece simplemente la opción por omisión donde nosotros como una sociedad negociemos que está. La propuesta es también moderada en combinar ley y software. Como lo ha explicado, esto tampoco es nada nuevo o radical.
• Políticamente, es menos polémico que el acta ómnibus de privacidad. Como otras combinaciones de ley y privacidad de tecnología mejorada (PET) su idea general se entiende bien.

Enfocados en un asunto bien definido y específico esto no es más amplio. No carga excesivamente a los sectores empresariales enteros, pero cambiará cómo percibimos la privacidad en nuestra sociedad. Y nos equipa también para un mundo de computación ubicua y sensores dominantes.

Esta propuesta también tiene la ventaja de la factibilidad eminente sobre otras alternativas. Sabemos que el acta ómnibus de protección de los datos personales no ha incitado a individuos ejercitar los nuevos derechos de privacidad que fueron dados. La reinterpretación constitucional es desigualmente inverosímil, mientras que la respuesta nula puede hacer una eventual reacción legislativa extremadamente costosa. Finalmente, a diferencia de la infraestructura global de la privacidad de Lessig, mi propuesta no requiere que emerjan mercados de privacidad personal y no descansa en la racionalidad de seres humanos como participantes del mercado.

A algunos puede desagradarle la propuesta tener porque no soluciona todos los desafíos de la privacidad de la información. Esto es verdad. Pero no es lo que se procura. La propuesta se centra en una cuestión muy específica: la opción por omisión en la retención de los datos. El cambio de esa opción tendrá efectos positivos significativos sobre la privacidad, pero no de la privacidad general.

Otros pueden criticar mi uso de la teoría de Lessig del Código de la Costa Este y Oeste, y marcarán la dificultad inherente de formar a la sociedad formando la tecnología. Este punto es bien tomado. No sugiero prever cómo los usuarios responderán al cambio en la opción por omisión en la retención y el borrado, cómo quizás pueden socavar la intención legislativa, o pervertirla. Soy completamente consciente de que la tecnología no es una fuerza exógena que se imprime en la sociedad, sino antes implica una delicada danza con la sociedad, en la cual cada lado está influenciando al otro. Por lo tanto, las tentativas de influenciar el comportamiento social formado la tecnología pueden fallar.

Lo que estoy sugiriendo es un mandato legislativo para que la tecnología se ajuste a nuestras prácticas del mundo real, antes que conformar la sociedad de una manera totalmente nueva. Las herramientas tecnológicas necesarias están mayormente desarrolladas, y no se requieren innovación a un nivel que pueda estimular un imprevisto con la sociedad. En suma, las oportunidades de éxito de mi propuesta moderada, mientras que seguramente son no seguras, son perceptiblemente más altas que otras ofertas de la ley que forman tecnología para influenciar a la sociedad.

En un aspecto importante, pienso, mi propuesta es radical: es radical en su deseo de cambiar cuando, qué y cómo recordamos y olvidamos en el reino digital. En este

aspecto y a largo plazo puede tener consecuencias significativas en cómo nuestros espacios digitales son delineados.

5. Conclusiones:

Por milenios, los seres humanos han tenido que deliberadamente elegir qué recordar. La opción por omisión era olvidar. En la era digital, esta opción por omisión del olvido ha cambiado en una opción por omisión de recordar. Así como estas memorias digitales hacen posible una reconstrucción comprensiva de nuestras palabras y hechos incluso si son del pasado lejano, puede obligar a nuestra buena voluntad a llegar más lejos en nuestra sociedad abierta. Tres reacciones convencionales a esta amenaza percibida se han propuesto: las respuestas legislativa, constitucional y nula. Cada uno de ellos tiene debilidades estructurales significativas, limitando su valor. Lawrence Lessig ha sugerido combinar la ley y el software para crear una respuesta nueva a las amenazas nuevas en la era digital, incluyendo amenazas para nuestra privacidad informacional. Su premisa es buena, pero su propuesta sobre la privacidad puede ser demasiado amplia.

En este artículo he sugerido una propuesta alternativa: reintroducir el concepto de olvido en un cierto plazo en nuestro reino digital. Mi objetivo es cambiar el valor por omisión detrás de la retención por siempre a la supresión después de cierto rato. He descrito los componentes legales y técnicos de mi propuesta y cómo trabajarían

juntos. He sugerido una implementación espectro basada en hasta dónde los responsables de las políticas el público quieren asegurar el olvido.

Evaluando mi propuesta relativa a las alternativas he sostenido que es relativamente moderada, en un número de dimensiones de su implementación, haciéndola comparativamente fácil de ser adoptada. Aun así es bastante radical facilitar el cambio fundamental de recordar a olvidar, que es tan central a los valores fundamentales de nuestra sociedad.

(*) Profesor Asociado de Políticas Públicas, The John F. Kennedy School of Government, Harvard University.

Traducción: Enrique A. Quagliano - Revisión y corrección: Stella Toval