FACILITANDO "THE CLOUD": LA REGULACIÓN DE LA PROTECCIÓN DE DATOS COMO MOTOR DE LA COMPETITIVIDAD NACIONAL EN AMÉRICA LATINA

HORACIO E. GUTIÉRREZ*
DANIEL KORN**

Las inversiones en infraestructura de Internet a lo largo de América Latina están comenzando a generar retorno, particularmente a medida que los consumidores, negocios, agencias gubernamentales, proveedores de servicios de salud e instituciones educativas utilizan conexiones a Internet para acceder a los innovadores servicios del cómputo en la nube[1]. En efecto, se espera que el mercado del cómputo en la nube en América Latina crezca a una tasa anual del 70% entre el año 2012 y el 2016[2]. Esto no resulta sorprendente, ya que el cómputo en la nube permite a los usuarios con conexión a Internet acceder en forma asequible a un nivel de poder de computación que hasta hace poco solo estaba disponible para las empresas que contaban con grandes presupuestos de tecnologías de información (TI) y profesionales

* Vicepresidente Corporativo y Consejero General Adjunto de Microsoft Corporation. Fue nombrado "Abogado de las Américas 2013" por la revista publicada por la Universidad de Miami, *Inter-American Law Review.* Este artículo es una versión en español del artículo originalmente publicado por *Inter-American Law Review* como "*Facilitando* the Cloud: Data protection regulation as a driver of national competitiveness in Latin America" (vol. 45, n.º I, 2013).

** Director de Asuntos Corporativos de Microsoft Latin America. Fecha de recepción: 15 de agosto de 2014. Fecha de aceptación: 11 de septiembre de 2014. Para citar el artículo: GUTIÉRREZ, H.E. y D. KORN, "Facilitando *the Cloud*: la regulación de la protección de datos como motor de la competitividad nacional en América Latina", *Revista La Propiedad Inmaterial* n.º 18, Universidad Externado de Colombia, noviembre de 2014, pp. 85-118.

1. "Cómputo en la Nube" (Cloud Computing) puede definirse como un modelo conveniente de acceso de red (*on-demand*) a los recursos de computación que se encuentran en un lugar compartido y que pueden ser ofrecidos rápidamente con poco esfuerzo administrativo o mínima interacción con el proveedor del servicio. Ver *The NIST Definition of Cloud Computing*, [http://csrc.nist.gov/publications/nistpubs/800-15/SP800-145.pdf].

2. Ver *Latin American cloud computing worth US $280mn in 2012, says IDC*, Start Up in Brazil (Sept. 4, 2012), [http://startupbrazil.co.uk/latin-american-cloud-computing-worth-us280mn-2012-idc/].

capacitados[3]. Pero lo más importante es que esta tecnología tiene un potencial enorme para crear nuevos empleos, reducir costos y promover la inclusión social[4].

No obstante lo anterior, la adopción del cómputo en la nube en América Latina está aún en una etapa inicial, y las decisiones que se tomen hoy en día por creadores de políticas públicas y otros participantes influenciará el grado en que los ciudadanos de países particulares, y de la región en general, se beneficiarán de esta tecnología en el corto y el mediano plazo. Las reglas y políticas para la protección de datos en el siglo XXI, y la pregunta de si las mismas están diseñadas con la flexibilidad para acomodar esta tecnología transformadora, jugarán un papel importante para facilitar la adopción del cómputo en la nube y los beneficios que la misma produce para la *competitividad nacional*, es decir, para el crecimiento económico y la mejoría a largo plazo de los estándares de vida de la sociedad, que son el resultado de mejoras en la productividad y eficiencia nacional[5]. Los creadores de políticas públicas a lo largo de la región deben evitar seguir el camino más fácil y, por el contrario, estar preparados para tomar decisiones políticamente difíciles, necesarias para desarrollar reglas de protección de datos que harán posible que sus países asuman el liderazgo en la era que ahora comienza del cómputo en la nube para el beneficio de sus ciudadanos.

Este artículo examina la forma en que los gobiernos y la industria en la región pueden conquistar la confianza de los consumidores en la nube mediante reglas balanceadas y consistentes de protección de datos, incrementando así la competitividad nacional. En la Parte I se analiza cómo las reglas sobre privacidad de datos pueden potenciar el cómputo en la nube. En la Parte II se exploran los grandes beneficios que el cómputo en la nube ofrece para la competitividad nacional. En la Parte III se resaltan los desafíos regulatorios presentados por el cómputo en la nube, incluyendo la experiencia inicial de la regulación de la nube y el rol que juega la industria para establecer la confianza de los clientes en la misma, concluyendo específicamente con una descripción de la posición de Microsoft frente a estos temas.

I. El cómputo en la nube está aumentando la importancia de tener reglas balanceadas de privacidad de datos

La preocupación por la privacidad ha existido desde mucho antes de que existieran la nube, Internet, o incluso las computadoras. Durante siglos, las personas han

3. Ver en general Alexa Huth & James Cebula, *The Basics of Cloud Computing,* U.S. Computer Emergency Readiness Team, disponible en: [www.us-cert.gov/sites/default/files/publications/CloudComputingHuthCebula.pdf]. (que explica cómo la computación en la nube es un recurso fácilmente accessible para individuos y empresas).

4. Ver Joe McKendrick, *Cloud Will Generate 14 Million Jobs by 2015: That's a Good Start*, *Forbes* (Mar. 5, 2012, 8:21 PM), [www.forbes.com/sites/joemckendrick/2012/03/05/cloud-will-generate-14-million-jobs-by-2015-thats-a-good-start/].

5. Orlando Ayala, *Defining National Competitiveness*, Future Gov (May 20, 2011), [www.futuregov.asia/articles/2011/may/20/defining-national-competitiveness/].

buscado tener control sobre el uso y la revelación de sus detalles personales[6]. En la actualidad, muchos gobiernos alrededor del mundo están evaluando la necesidad de leyes para acompañar las nuevas exigencias y realidades del cómputo en la nube, al tiempo que obtienen los mismos beneficios que han impulsado desde hace tiempo la legislación de privacidad: potenciar las decisiones individuales con relación a la privacidad, mantener la seguridad de la información, y desarrollar la confianza en un avance tecnológico importante que promete transformar la sociedad para bien si se maneja correctamente. En Europa, el representante oficial de la Agenda Digital, Neelie Kroes, ha urgido la adopción de "reglas claras y amigables para la nube (…) [porque] una 'nube' sin protección de datos fuerte y transparente no es el tipo de nube que necesitamos"[7]. Asimismo, el Departamento de Comercio de Estados Unidos observó recientemente que la habilidad para "aprovechar en forma segura todo el potencial de los servicios tales como el correo electrónico y el almacenamiento de archivos basado en la nube depende de protecciones a la privacidad que sean consistentes con otros modelos de computación"[8]. Estamos de acuerdo. En pocas palabras, el interés colectivo es que todos los usuarios de la nube tengan una confianza sólidamente establecida en la nube.

En América Latina, el interés en la protección de datos también se está incrementando[9]. Desde los años ochenta, muchos gobiernos de la región han consagrado un derecho constitucional para que los individuos tengan acceso y puedan corregir sus datos personales. Conocida también como "*habeas data*", esta protección tiene el propósito de "proteger la libertad individual contra los abusos en la era de la información"[10]. El *habeas data* garantiza "un control real sobre los datos personales confidenciales, frenando el abuso de tal información, que será perjudicial para el individuo"[11]. En vista de que estas disposiciones de *habeas data* normalmente forman parte de las constituciones nacionales, las mismas reciben "el mayor nivel de protección posible, acompañado de un procedimiento más expedito y mejores tribunales"[12]. Por ejemplo, el artículo 43(3) de la Constitución argentina consagra un sólido derecho al *habeas data*:

6. Ver, por ej., Robert Ellis Smith, "Ben Franklin's Website: Privacy and Curiosity from Plymouth Rock to the Internet" (*Privacy Journal*, 2004) (donde se discute el deseo de los estadounidenses de privacidad a lo largo de la historia de Estados Unidos).

7. Neelie Kroes, Vicepresidente de la Agenda Digital, Comisionado Europeo, Discurso en la conferencia Les Assises du Numérique: *Cloud Computing and Data Protection* (Nov. 25, 2010), disponible en: [http://europa.eu/rapid/press-release_SPEECH-10-686_en.htm].

8. Ver The Department of Commerce Internet Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (Dec. 2010), http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf.

9. Ver Aldo M. Leiva, *Data Protection Law in Spain and Latin America: Survey of Legal Approaches*, 41 *Int'l Law News* 4 (2012), disponible en: [www.americanbar.org/publications/International_Law_News/2012/fall/data_protection_law_spain_latin_america_survey_legal_approaches.html].

10. Enrique Falcón, *Habeas Data: concepto y procedimiento* 28 (1996).

11. Andrés Guadamuz, *Habeas Data vs. the European Data Protection Directive*, 3 *J. Int'L* T. 5 (2001).

12. Ibíd.

> Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o en registros o bancos de datos privados destinados a proveer informes, y en caso de falsedad o discriminación, para la supresión, rectificación, confidencialidad o actualización de los mismos. La naturaleza secreta de las fuentes de información periodística no debe ser perjudicada[13].

Desde el año 2000, los países de América Latina han promulgado leyes exhaustivas de protección de datos basadas en el modelo de la Directiva de Protección de Datos de la Unión Europea de 1995[14]. Estas leyes varían ampliamente, pero por lo general contienen restricciones pre-nube sobre el uso y transferencia de datos, requieren el consentimiento expreso del titular de los datos antes de su tratamiento, permiten a los individuos acceder y corregir cualquier iteración posible de sus datos personales, y requieren medidas de protección para la seguridad de datos. En el año 2000, Argentina promulgó la primera ley comprensiva de protección de datos de la región, que compartía muchos elementos con la Directiva de 1995 de la Unión Europea previa a la nube[15]. Uruguay adoptó una ley de protección de datos similar años más tarde[16]. Comenzando con la adopción de la ley de México, que marcó un precedente en 2010, la consideración, y a menudo la adopción, de leyes comprensivas de protección de datos se ha convertido en la norma en América Latina, como se ilustra en el siguiente cuadro[17].

País	Puntos clave
Argentina	Argentina adoptó una ley del estilo de la Unión Europea en 2000 y recibió una determinación de adecuación de la CE en 2003. En general, las transferencias internacionales de datos desde Argentina están prohibidas, a menos que los titulares de los datos concedan autorización previa y expresa, si el país de destino no tiene lo que el legislador argentino ha estimado como leyes "adecuadas". Ningún *safe harbor* ("puerto seguro") fue creado para facilitar la transferencia de datos a países que no hayan sido considerados como "adecuados".

13. Constitución de Argentina, disponible en: [www.senado.gov.ar/web/interes/constitucion/cuerpo1.php].

14. Leiva, nota 11 anterior ("El enfoque español y latinoamericano frente a la protección de la información personal tiene sus raíces en el concepto europeo de los derechos de privacidad personal que se han desarrollado a través de Europa por varias décadas, y que han culminado por medio de la integración regional con la adopción de la Directiva de Protección de Datos de la Unión Europea (…) en 1995").

15. Ley 25326, 30 de octubre 30, 2000 (Arg.).

16. Ley 18.331, 11 de agosto, 2008, *Diario Oficial* (Urug.).

17. Esta tabla fue preparada por Matt DelNero, de Covington & Burling LLP, el 8 de noviembre de 2013.

Brasil	Brasil no tiene una ley comprensiva de protección de datos, a pesar de que, al igual que en muchos países de la región, existe un derecho constitucional a la privacidad en general. El Ministerio de Justicia elaboró un proyecto de ley y pidió comentarios acerca del mismo de parte del público en 2011. Más recientemente, el Congreso de Brasil está considerando un proyecto de ley que le permitiría al Presidente exigir que los datos personales de los ciudadanos brasileños se mantengan dentro del país.
Chile	Chile adoptó una ley de protección de datos en 1999, pero no se considera que sea de naturaleza comprensiva. En enero de 2012, el Poder Ejecutivo presentó una propuesta de proyecto de ley al Congreso, buscando crear una ley de protección de datos comprensiva. En noviembre de 2013 el proyecto de ley seguía bajo análisis en una comisión del Congreso.
Colombia	Colombia aprobó una ley comprensiva de privacidad de datos con acción final en octubre de 2012 cuando fue promulgada la Ley 1581. Similar a lo que ocurre con las leyes de Argentina y Uruguay, la nueva ley prohíbe la transferencia internacional de datos a países que no tengan regímenes de protección de datos "adecuados", según lo determinado por el legislador colombiano, salvo que los titulares de los datos concedan consentimiento expreso previo. El Decreto 1377, una legislación de carácter secundario, fue expedido en junio de 2013.
Costa Rica	Costa Rica adoptó una ley comprensiva de privacidad de datos en septiembre de 2011. Entre otros requisitos, los datos personales en general no pueden ser tratados sin el consentimiento expreso de la persona en cuestión. En marzo de 2013, el Ministerio de Justicia y Paz publicó las reglamentaciones de la nueva ley. Resulta inusual que las reglamentaciones requerirían que los controladores de datos provean a la autoridad de protección de datos una cuenta de "Súper Usuario", con acceso total. Una circular presidencial expedida el 15 de mayo de 2013 específicamente promueve la compra de cómputo en la nube en el sector público.
República Dominicana	El 22 de abril de 2013, el Senado de República Dominicana aprobó un proyecto de ley de Protección de Datos en línea con el artículo 44.2 de la Constitución de la República Dominicana. El proyecto de ley aguarda votación en la Cámara de Diputados. El proyecto de ley sigue muchos de los principios y conceptos que se encuentran en la Directiva de Protección de Datos de la Unión Europea, tales como las limitaciones a la transferencia de datos, protecciones especiales para datos confidenciales, y la creación de una autoridad independiente de protección de datos. La misma requiere también el consentimiento de los padres para el tratamiento de datos de niños menores de 16 años.

México	México adoptó una ley de privacidad de datos en 2010, que marcó un precedente. Las reglamentaciones de la ley fueron publicadas en diciembre de 2011. La ley mexicana puede proveer un "tercer camino" entre el enfoque *ad hoc* que prevalece en Estados Unidos y el enfoque más prescriptivo que se estila en Europa y, cada vez más, en muchos países de América Latina. Por ejemplo, la ley provee mayor flexibilidad en la transferencia internacional de datos. Adicionalmente, la ley acoge el principio del consentimiento, pero deja en claro que en muchos casos el consentimiento puede ser obtenido tácitamente a través de una divulgación apropiada en un aviso de privacidad. México ha acogido los principios de protección de datos establecidos por el Foro de Cooperación Económica Asia-Pacífico (APEC), en lugar del marco de protección de datos más restrictivo de la Unión Europea. En adición a los elementos de la APEC que se encuentran en la ley, desde enero de 2013, México se convirtió en el segundo participante formal (luego de Estados Unidos) en el marco de Reglas de Privacidad Transnacional de la APEC. Los nuevos lineamientos sobre avisos de privacidad entraron en vigor el 17 de abril de 2013. Similar a lo que sucede con las reglas de la Unión Europea, los nuevos lineamientos requieren que los controladores provean aviso suficiente y obtengan consentimiento del titular de los datos personales antes que sean recolectados por medio de *cookies*, *beacons de web* y otros medios automatizados.
Nicaragua	Nicaragua adoptó una ley comprensiva de protección de datos en marzo de 2012. La nueva ley sigue en gran medida el modelo de la Unión Europea. La misma incluye conceptos tales como el "derecho a ser olvidado", que hace referencia al derecho de que todos los rastros de los datos de una persona sean eliminados de los registros de una compañía.
Perú	La ley de protección de datos de Perú, adoptada en 2011, sigue en gran medida el modelo de la Unión Europea, pero con medios un poco más modernos para facilitar el flujo de datos que es crucial para el cómputo en la nube. Específicamente, mientras que la regla requiere el consentimiento para la transferencia de datos a países sin una ley de protección de datos "adecuada", el controlador puede superar este obstáculo si toma medidas para hacerse responsable por la protección de los datos una vez que sean transferidos fuera del país. Perú adoptó la reglamentación de la ley de protección de datos mediante el Decreto del 22 de marzo de 2013. El reglamento incluye una provisión sobre el cómputo en la nube (denominada "*tratamiento de datos personales por medios tecnológicos tercerizados*" – redacción cuya intención es proporcionar una descripción tecnológicamente neutral que permita desarrollos tecnológicos futuros aún desconocidos). La provisión permite que

	los controladores utilicen servicios en la nube de terceros, siempre y cuando garanticen que el proveedor de nube cumpla con los requisitos de protección de datos contenidos en la ley. Adicionalmente, el proprio proveedor de servicios de nube deberá ser indicado como responsable bajo el contrato con el controlador.
Uruguay	Uruguay adoptó una ley del estilo de la Unión Europea en 2008 y recibió una determinación de adecuación de la CE el 21 de agosto del 2012. Las transferencias internacionales de datos desde Uruguay están prohibidas si el país de destino no tiene leyes "adecuadas". No obstante, contrario a su contraparte argentina, la DPA uruguaya expidió una resolución reconociendo como "adecuado" cualquier país de destino que sea considerado adecuado por la Unión Europea. Entendemos que esta resolución ha sido interpretada para permitir la transferencia a cualquier organización certificada como "puerto seguro" bajo el *Safe Harbor* de Estados Unidos/Unión Europea.

II. El estímulo del aumento en la competitividad nacional requiere una política regulatoria balanceada de protección de datos para el cómputo en la nube

La nube provee recursos de computación en "*pool*" que están disponibles según la demanda y accesibles en cualquier momento desde cualquier dispositivo conectado a Internet[18]. Los proveedores de servicios de nube operan una red global de centros de datos para proporcionar un servicio continuo a una base de clientes en todo el mundo[19]. Esta sección describe los principales beneficios económicos del cómputo en la nube y los elementos de un marco regulatorio balanceado, que podrían ayudar a promover la adopción por el consumidor y el crecimiento de esta increíble tecnología para el beneficio de la comunidad.

A. Beneficios de la nube

Pocas tecnologías recientes han presentado un mayor potencial de beneficios económicos que la nube. Se espera que para 2014, el mercado global del cómputo en la nube haya crecido a US$150 mil millones[20]. En particular en los mercados emergentes, el cómputo en la nube podría convertirse en un motor de crecimiento económico y de beneficios sociales[21]. La nube ofrece tanto a las economías desarrolladas como

18. Ver Huth, nota 5 anterior.
19. Ibíd.
20. Andrew R. Hickey, *Cloud Computing Services Market To Near $150 Billion in 2014*, CRN (Jun. 22, 2010, 12:46 PM), [www.crn.com/news/managed-services/225700984/cloud-computing-services-market-to-near-150-billion-in-2014.htm].
21. Ver *With Cloud, SMBs Will Lead Emerging Economies Across the Digital Divide*, CISCO (Sep. 2012), [www.cisco.com/web/about/ac79/docs/FastFacts/FastFacts_Cloud-and-Digital-Divide.pdf].

a las emergentes una amplia gama de beneficios. Cada uno de los beneficios que describimos a continuación debería ser de particular interés para las pequeñas y medianas empresas (PyMEs), las cuales, se estima, emplean el 67% de su fuerza laboral en América Latina, y las que, en muchos casos, no han sido capaces de apalancar el poder de la computación de una forma significativa hasta hoy en día[22].

1. Creación de empleo a través de la innovación

El cómputo en la nube tiene el potencial de crear empleos a través de la innovación local. Esto se debe en gran medida a que el cómputo en la nube está reduciendo los costos de mantenimiento continuo de infraestructura y aplicaciones legadas, así como la necesidad de hacer grandes inversiones en tecnología, lo que libera el presupuesto de la compañía para dedicarlo a *nuevos mercados* y *nuevos productos*, dos factores que conducen al crecimiento del empleo[23]. En efecto, particularmente con respecto al sector de tecnologías de información, los expertos esperan que el cómputo en la nube sea el motor del crecimiento del empleo en la próxima década. Según un estudio de IDC de noviembre de 2012, patrocinado por Microsoft, la demanda mundial de empleos relacionados con la nube crecerá en un 26% anual hasta el año 2015, creando aproximadamente 7 millones de empleos relacionados con la nube a nivel global[24]. Hasta 2015, el número de empleos relacionados con la nube crecerá a una tasa anual del 22% en Norteamérica y del 24% en Europa, mientras que los mercados emergentes de América Latina, Europa Central y del Este, Medio Oriente y Asia Pacífico tendrán la mayor tasa de crecimiento de empleo relacionado con la nube: 34% anual[25].

Millones de estos nuevos empleos son altamente cualificados y ofrecen los altos salarios que los gobiernos están tan ansiosos por atraer. Por ejemplo, en un estudio publicado por la Comisión Económica para América Latina y el Caribe (CEPAL), el análisis realizado por los economistas Andrea Colciago y Federico Etro concluyó que la adopción del cómputo en la nube por las empresas en Brasil puede resultar en la creación de 900.000 nuevos empleos[26]. En forma similar, el Instituto Mexicano para la Competitividad (IMCO) encontró recientemente que con

22. Angel Gurría, *Latin American Economic Outlook 2013: SME Policies for Structural Change*, OECD (2012), disponible en: [www.keepeek.com/Digital-Asset-Management/oecd/development/latin-american-economic-outlook-2013_leo-2013-en].

23. Ver, por ej., Mohana Ravindranath, *Analysts expect growth in cloud jobs*, WASH. POST (Aug. 15, 2013, 8:00 AM), [www.washingtonpost.com/business/on-it/analysts-expect-growth-in-cloud-jobs/2013/08/14/56d5715a-04fb-11e3-a07f-49ddc7417125_story.html]. ("*Across industries, cost-saving associated with switching to cloud computing has translated not into job loss, but more available resources to invest in other aspects of the business*").

24. Cushing Anderson & John F. Gantz, *Climate Change: Cloud's Impact on IT Organizations and Staffing*, IDC 1, 3 (Nov. 2012), [www.microsoft.com/en-us/news/download/presskits/learning/docs/idc.pdf].

25. Ibíd., pp. 4-5.

26. Ver Valeria Jordán et al., *Banda Ancha en América Latina: Más allá de la Conectividad,* CEPAL 1, 29 (Feb. 2013), [www.cepal.org/publicaciones/xml/2/49262/BandaAnchaenAL.pdf.pdf].

la tecnología de la nube México puede crear 1.800 nuevas pequeñas y medianas empresas, que emplearían, en conjunto, un estimado de 63.400 personas. Y esto con base en un estimado conservador de ahorros, de tan solo el 1% de los costos fijos de las compañías debido a los beneficios de la nube[27].

2. Reducción de costos

Además de la creación de empleos altamente cualificados, el cómputo en la nube impulsa la economía proporcionando a las empresas y agencias de gobierno ahorros significativos en los costos de servicios e infraestructura de tecnologías de información[28]. Datos recientes sugieren que la instalación de nube híbrida podría reducir el gasto total de TI aproximadamente entre un 20 y un 30%[29]. Dado que cualquier empresa u organización se puede conectar a todos los beneficios de la nube con una simple conexión a Internet, hay una necesidad mínima de hacer inversiones de capital por adelantado. Las generaciones anteriores de tecnología requerían inversiones significativas en servidores y otros equipos físicos, pero este capital ya no es necesario con el cómputo en la nube. Al agregar la demanda de computación, la nube hace posible que las tasas de utilización de servidores se incrementen. IMCO estima que el sector público en México puede ahorrar un 1,7% de su gasto anual migrando a la nube[30]. Vale resaltar que estos ahorros de costos sirven para incrementar la democratización de la computación, lo que conduce a una mayor inclusión social, como se discute en la próxima sección.

Es más, los centros de datos de gran escala pueden dar como resultado menores costos por servidor, porque requieren menos electricidad para operar[31]. En la medida que aumenta el número de clientes, se reduce el costo de servidor por inquilino y la gerenciamiento de aplicaciones. En una empresa tradicional sin nube, un solo administrador de sistemas puede atender aproximadamente 140 servidores[32]. En contraste, un centro de nube normalmente administra miles de servidores simultáneamente,

27. *"Computo en la Nube": Nuevo detonador para la competitividad de México*, Instituto Mexicano para la Competitividad A.C. (IMCO), "Computo en la Nube": Nuevo detonador para la competitividad de México, at) 1, 31 (mayo de 2012), [http://imco.org.mx/images/pdf/Computo_en_la_Nube-detonador_de_competitividad_doc.pdf], [en adelante, el Reporte de nube IMCO].

28. Ver HILARY KRAMER, *Washington Moves Into the Cloud: Saving Money and Securing Data*, *Forbes* (8 de julio de 2013, 6:45 AM), [www.forbes.com/sites/hilarykramer/2013/07/08/washington-moves-into-the-cloud-saving-money-and-securing-data/].

29. *Business Agility and the True Economics of Cloud Computing*, VMWARE 1, 6 (2011), [www.vmware.com/files/pdf/accelerate/VMware_Business_Agility_and_the_True_Economics_of_Cloud_Computing_White_Paper.pdf].

30. Reporte de nube IMCO, nota 29 anterior, p. 34.

31. Ver, por ej., Yuan Yao et al., *Data Centers Power Reduction: A Two Time Scale Approach or Delay Tolerant Workloads* (2012), [www.eecs.berkeley.edu/~huang/data-center-power-infocom12.pdf]. (donde se discute cómo los centros de datos de gran escala tienen el potencial de reducir los costos de energía).

32. Ver RICH MILLER, *How Many Servers Can One Admin Manage?*, Data Center Knowledge (Dec. 30, 2009), [www.datacenterknowledge.com/archives/2009/12/ 30/how-many-servers-can-one-admin-manage/].

que son capaces de realizar múltiples tareas al mismo tiempo[33]. Esta eficiencia permite que los profesionales de TI se concentren en actividades de mayor valor agregado, como desarrollar nuevas capacidades y atender los pedidos de los usuarios.

Los ahorros correspondientes de energía pueden traducirse también en una reducción de emisiones de carbono, por lo cual el cómputo en la nube ha sido denominado la "TI Verde"[34]. IMCO estima que la migración a la nube del sector de medianas y grandes empresas de México en forma agregada, podría reducir las emisiones de carbono en forma equivalente a remover 90.000 autos de circulación[35].

3. Democratización de la computación e inclusión social

El cómputo en la nube no solo aumenta la eficiencia; también aumenta la equidad. Al proporcionar acceso a un nivel de computación que anteriormente solo estaba disponible para grandes compañías y economías desarrolladas, la nube es la próxima etapa en la democratización de la computación y en el aumento de la inclusión social[36]. Con el cómputo en la nube, las organizaciones de cualquier tamaño y en prácticamente cualquier lugar del mundo pueden aprovechar el poder de la súper computación y de las aplicaciones de software que antes solo estaban disponibles para las mayores compañías globales[37]. Las personas también pueden utilizar la nube para desarrollar herramientas de computación completamente nuevas. Por ejemplo, el cómputo en la nube permite a los empleados de hospitales rurales consultar con especialistas del mundo entero en tiempo real, proporcionando a los residentes de zonas rurales el cuidado médico que nunca habrían podido recibir antes de la nube[38]. La nube también reduce los costos de los hospitales para el almacenamiento de rayos x y otros archivos voluminosos de salud[39]. En efecto, se espera que el cómputo en la nube en los hospitales crezca a una tasa anual compuesta del 20,5% entre 2012 y 2017[40].

De la misma manera, la nube presenta oportunidades sin precedentes para los distritos escolares rurales y de bajos ingresos[41]. La nube proporciona a las escuelas aplicaciones poderosas basadas en la web, aprendizaje a distancia y almacenamiento

33. Ver Clair Cain Miller & Quentin Hardy, *Google Elbows Into the Cloud*, *N.Y. Times* (Mar. 12, 2013), [www.nytimes.com/2013/03/13/technology/google-takeson-amazon-and-microsoft-for-cloud-computing-services.html?pagewanted=all].

34. Reporte de nube IMCO, nota 29 anterior, p. 40.

35. Ibíd.

36. Joe Mullich, *16 Ways the Cloud Will Change Our Lives*, *Wall St. J.* (Jan. 7, 2011), [http://online.wsj.com/ad/article/cloudcomputing-changelives].

37. Ver, en general, Huth, nota 5 anterior.

38. Pam Belluck, *Nantucket Hospital Uses Telemedicine as Bridge*, *N.Y. Times* (Oct. 8, 2012), [www.nytimes.com/2012/10/09/health/nantucket-hospital-usestelemedicine-as-bridge-to-mainland.html?pagewanted=all].

39. Ken Terry, *Cloud Computing in Healthcare, the Question is Not If, But When*, *FierceHealthIT* (January 9, 2012), [www.fiercehealthit.com/story/cloud-computing-healthcare-question-not-if-when/2012-01-09].

40. Bernie Monegain, 3 *Big Trends for the EHR Cloud*, *Healthcare IT News* (Oct. 8, 2012), [www.healthcareitnews.com/news/3-big-trends-ehr-cloud].

41. Ver Kerri Lee Horan, *Saved by the Cloud*, *District Administration* (Feb. 2010), [www.districtadministration.com/article/saved-cloud].

de bajo costo[42]. También permite a las escuelas pequeñas tener acceso a materiales educativos que de otra forma jamás estarían disponibles. Es más, la nube permite a los gobiernos dar un paso gigante en la oferta de servicios ciudadanos. Por ejemplo, la empresa *Rock Solid*, basada en Puerto Rico, desarrolló una línea de asistencia al ciudadano basada en la nube para el gobierno de Panamá. El servicio permite a los residentes de Panamá marcar 3-1-1 para comunicarse con un servicio centralizado que los conecta directamente con las agencias del gobierno[43]. De la misma manera, el sistema educativo de Colombia ha utilizado la nube para mejorar las pruebas estandarizadas para estudiantes[44]. Sin esta tecnología, el Instituto Colombiano para el Fomento de la Educación Superior (ICFES) hubiera requerido miles de sus propios servidores para poner a disposición de los estudiantes estos resultados dos veces por año[45]. Utilizando el cómputo en la nube, el ICFES aprovechó la escala y la naturaleza *on demand* de la nube, ahorrando en los servidores que necesita para poder satisfacer esta demanda. Esto benefició tanto al gobierno como a los estudiantes, padres y profesores.

Lo que más nos apasiona es que la eficiencia del cómputo en la nube representa la caída de un muro gigante que dividía a nuestras sociedades entre aquellos que *podían* hacer la gran inversión de capital para acceder y actualizar las últimas tecnologías de software, cada vez más necesarias para los negocios, y aquellos que no podían hacer tal inversión. Como el acceso al cómputo en la nube tiene un precio de entrada más bajo, esa infeliz distinción irá desapareciendo, y la interacción regular con la última tecnología se convertirá cada vez más en una realidad de la comunidad en general.

4. Mayor agilidad

El cómputo en la nube también les permite a las empresas y a las organizaciones de gobierno adaptarse a las nuevas demandas y desafíos con mayor agilidad. La capacidad inédita de almacenamiento y el poder computacional disponible hoy en la nube permiten a organizaciones lanzar nuevas aplicaciones y servicios a una velocidad significativamente mayor –y con menor riesgo– que en el pasado[46]. Los servicios que antes hubieran requerido de grandes inversiones de capital e implementaciones demoradas pueden ser lanzados en cuestión de semanas o incluso de

42. Diane Weaver, *Six Advantages of Cloud Computing in Education*, *Pearson* (Apr. 2013), [www.pearsonschoolsystems.com/blog/?p=1507].

43. Ver vídeo en Rock Solid Technologies, *Dynamics CRM & Rock Solid Republic of Panama-311 System,* YouTube (Apr. 6, 2011), [www.youtube.com/watch?v=HVUCALNG2D4].

44. HERNÁN RINCÓN, *This is Latin America's Decade: The Cloud Will Make it Possible*, *Americas Quarterly* (Fall 2011), [www.americasquarterly.org/node/3085].

45. Ibíd.

46. Ver, por ej., REUVEN COHEN, *Build your own Web or Mobile App In Minutes with These Cloud Based Tools*, *Forbes* (Mar. 22, 2013), [www.forbes.com/sites/reuvencohen/2013/03/22/build-your-own-web-or-mobile-app-in-minutes-with-thesecloud-based-tools/]. (explicando cómo la nube puede ser utilizada por las empresas para crear aplicaciones rápidamente).

días. En el pasado, cuando las empresas experimentaban un incremento repentino en popularidad, sus servidores web públicos e internos eran muchas veces incapaces de lidiar con los aumentos en la demanda. Cuando un terremoto devastó a Costa Rica el 5 de septiembre de 2012, tornando inoperables las comunicaciones tradicionales tales como teléfonos, radios y televisores, los residentes pudieron obtener información visitando el sitio web de la estación de televisión nacional (Teletica) dado que el sitio web estaba hospedado en la nube, y la capacidad de Internet del sitio web podía ser escalada para satisfacer el pico en la demanda[47]. Con el cómputo en la nube, las empresas podrían fácilmente ajustarse a tales incrementos en la demanda porque no están limitadas por la capacidad de sus servidores internos. De acuerdo con una encuesta a los tomadores de decisiones corporativos realizada por *AbsolutData* para *VMware* en febrero de 2011, el 65% de los encuestados creen que la nube juega un "rol clave" en el aumento de la agilidad, y que el cómputo en la nube "podría ayudarles a sus organizaciones a mantener una arquitectura flexible para soportar los cambios"[48].

Esta flexibilidad se debe en gran parte a la movilidad de la nube. Esta no solo provee un acceso de un tipo diferente del que teníamos en el pasado; también es un tipo mucho más generalizado de acceso. Más de tres cuartas partes de la población mundial tienen acceso a un teléfono celular[49]. La telefonía móvil es muy diferente a las computadoras personales en nuestros escritorios, o incluso a nuestros *laptops*. Los mismos funcionan como teléfonos, herramientas para envío de textos, cámaras fijas, cámaras de video, computadoras, portales web, plataformas de juegos, y aun así son lo suficientemente pequeños para caber en el bolsillo de la camisa. Podemos llevarlos a donde queramos y tener acceso de doble vía, siempre ligados y siempre conectados al mundo digital. La movilidad está cambiando la manera en que accedemos a los datos y servicios, así como la web cambió la manera como se ofrecen los datos y servicios, y así como el cómputo en la nube está cambiando la manera en que los mismos son procesados y manejados. Por ejemplo, una nueva aplicación móvil llamada "*Agentto*", desarrollada en Brasil, ayuda a hacer que las comunidades sean más seguras, proporcionándoles a los individuos un canal basado en la ubicación en tiempo real, para notificar a la familia, amigos y autoridades durante situaciones críticas tales como accidentes, problemas de salud, violencia doméstica, secuestros y catástrofes[50].

47. Mark Lyndersay, *Microsoft Evangelises the Cloud*, *Trinidad & Tobago Guardian* (Oct. 25, 2012), [www.guardian.co.tt/business-guardian/2012-10-24/microsoft-evangelises-cloud].

48. VMware, *Business Agility and the True Economics of Cloud Computing*, *disponible en* [www.vmware.com/files/pdf/accelerate/VMware_Business_Agility_and_the_True_Economics_of_Cloud_Computing_White_Paper.pdf].

49. *Mobile Phone Access Reaches Three Quarters of Planet's Population*, World Bank (July 17, 2012), [www.worldbank.org/en/news/press-release/2012/07/17/mobile-phone-access-reaches-three-quarters-planets-population].

50. Agentto, [https://agentto.com/About.aspx], (visitado por última vez el 28 de sept. de 2013).

5. Seguridad

Es entendible que muchas organizaciones e individuos están preocupados con la cuestión de seguridad en la nube. En realidad no hay ninguna razón técnica que impida a la nube ser tan o más segura que la computación tradicional. En un estudio de 2012, hecho sobre 70.000 quiebras de seguridad en 1.600 compañías, *AlertLogic* concluyó que los sistemas de computación en las instalaciones de la organización eran más vulnerables a los ataques que las aplicaciones hospedadas en la nube[51]. El 46% de los servidores corporativos fueron afectados por ataques de "fuerza bruta", en comparación con un 39% de los sistemas en la nube[52].

Como ha reconocido la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), "el cómputo en la nube tiene un potencial significativo para mejorar la seguridad y la resiliencia"[53]. Si bien las reglas robustas de privacidad de datos son esenciales para darles a los usuarios la confianza de que sus datos están seguros en la nube, las tecnologías de nube pueden en sí mismas mejorar la seguridad y privacidad de los datos – particularmente para las pequeñas y medianas empresas que disponen de conocimientos y recursos limitados de seguridad de la información. Muchas empresas pequeñas no tienen los recursos necesarios para implementar controles robustos de seguridad física y técnica de forma sistemática, aplicar y examinar los parches de seguridad, implementar soluciones comprensivas de criptografía, o conseguir certificaciones de seguridad y privacidad de la información. El cómputo en la nube le permite a estas organizaciones lograr las mismas protecciones disponibles para organizaciones de gran tamaño con presupuestos considerables para la tecnología de información, personal cualificado e instalaciones[54].

A la luz de todos estos beneficios, no es sorprendente que los usuarios estén entusiasmados con respecto a la nube. Por ejemplo, KPMG encontró que un abrumador 59% de los tomadores de decisiones y líderes de empresas en Holanda están de acuerdo con que "el cómputo en la nube es el modelo futuro de la TI"[55]. La mayoría de los consumidores y empresarios acreditan que estas tecnologías pueden

51. JOE MCKENDRICK, *Cloud Apps Somewhat More Secure Than On-Premises Apps: Survey*, *Forbes*, Sept. 19, 2012, [www.forbes.com/sites/joemckendrick/2012/09/19/cloud-apps-somewhat-more-secure-than-on-premises-apps-survey/].

52. Ibíd.

53. Preguntas y respuestas (FAQ's) del reporte "Cloud Computing: Benefits, risks and recommendations for information security", *European Network and Information Security Agency* (ENISA) (visitado por última vez el 19 de sept. de 2013), [/www.enisa.europa.eu/media/faq-on-enisa/FAQ%20Cloud%20Computing.pdf].

54. Ver TOM KELLY, *SMEs must embrace the cloud to achieve global growth*, THE GUARDIAN (Apr. 26, 2013), [www.theguardian.com/media-network/media-network-blog/2013/apr/26/cloud-services-sme-businesses-growth?guni=Article:in%20body%20link].

55. KPMG, *From hype to future: Kpmg's cloud computing survey* (2010), disponible en: [www.kpmg.com/ES/es/ActualidadyNovedades/ArticulosyPublicaciones/Documents/2010-cloud-Computing-Survey.pdf].

ayudar a los gobiernos a operar de una forma más eficiente y productiva. El desafío para la industria de TI es saber cómo aprovechar este entusiasmo y garantizar a las empresas e individuos que sus datos están seguros en la nube.

B. Un rol importante para una regulación balanceada

Los reguladores pueden ayudar a extender los beneficios del cómputo en la nube a más empresas e individuos, estableciendo la confianza en el cómputo en la nube, garantizando la privacidad y seguridad de los datos, y resolviendo las incertidumbres legales y de política pública. Esta sección describe los elementos generales de un marco regulatorio de privacidad y protección de datos que promueva la competitividad nacional en el cómputo en la nube.

1. Garantizando la protección de la privacidad

La nube no alcanzará todo su potencial si los usuarios no confían en la tecnología. Numerosas encuestas demuestran que las empresas e individuos continúan bastante preocupados acerca de la privacidad y seguridad de la nube. Por ejemplo, una encuesta de 2010 realizada por el Foro Económico Mundial encontró que el 90% de los encuestados en Europa ven la privacidad como una limitación "muy seria" para la adopción del cómputo en la nube[56]. Ya que las personas y organizaciones alrededor del mundo transfieren su información de sus *desktops* a sus dispositivos móviles y hacia la nube, quieren saber si sus datos continuarán estando seguros y protegidos.

Las agencias reguladoras pueden establecer políticas regulatorias claras y justas para ayudar a garantizar que los usuarios, tanto empresas como individuos, no pierdan las protecciones de privacidad al mover sus datos a la nube. En su cargo de Consejero General de Microsoft, Brad Smith declaró durante la 34.ª Conferencia Anual de los Comisionados de Protección de Datos y Privacidad, celebrada en Uruguay en octubre de 2012, que "Necesitamos claridad de manera que todos sepan qué deben hacer, y que las compañías que actúen responsablemente no se vean perjudicadas por compañías que no actúen responsablemente, y es la regulación la que crea el piso que proporciona un campo de juego nivelado"[57]. El marco reglamentario debería enfocarse en los objetivos principales que consisten en garantizar la seguridad de los datos, proteger la privacidad de los consumidores y construir la confianza en la nube.

56. Joanna Gordon et al., *Exploring the Future of Cloud Computing: Riding the Next Wave of Technology-Driven Transformation*, *World Economic Forum* (2010), disponible en: [www3.weforum.org/docs/wef_ittc_FutureCloudComputing_Report_2010.pdf].

57. Brad Smith, General Counsel and Executive Vice President, Microsoft Corp, Keynote Address at the 34th International Conference of Data Protection and Privacy Commissioners: Putting People First: Moving Technology and Privacy Forward (Oct. 23, 2012), disponible en: [www.microsoft.com/en-us/news/download/legal/10-23puttingpeopleplefirst.pdf].

Pero no necesitamos reglas del camino únicamente de los reguladores. La autorregulación por parte de la industria y la innovación basada en el mercado también serán factores clave para garantizar la protección de la privacidad. La autorregulación, en la forma de estándares de la industria, puede hacer avanzar la tecnología más rápidamente y en forma más global que lo que puede lograr la regulación por sí misma. Por ejemplo, las partes interesadas han desarrollado un borrador de estándares internacionales, el ISO/IEC 27018, por medio del cual un proveedor de nube puede demostrarles a los clientes y a los reguladores que maneja los datos personales correctamente y que garantiza la confidencialidad, integridad y disponibilidad de tales datos[58]. De la misma manera, con la innovación basada en el mercado hay la oportunidad para que las empresas experimenten, ensayen cosas nuevas, y vean qué quieren los consumidores; y si los consumidores quieren, en efecto, lo que las empresas están ofreciendo, hay una oportunidad de crecimiento para esas empresas.

2. Promoviendo una mayor transparencia

De la misma manera, el marco regulatorio puede proporcionar a los *clientes* la información que tanto necesitan y buscan sobre la nube. No basta con que los proveedores de servicios en la nube afirmen que sus servicios son privados y seguros. Los clientes deberían estar informados en detalle de por qué esto es así. La regulación de la privacidad y la seguridad de los datos pueden exigir que los proveedores de servicios en la nube mantengan por escrito información comprensiva acerca de sus programas de seguridad y protecciones, que proporcionen resúmenes de estos programas a sus clientes, y que divulguen sus prácticas de privacidad a cualquier cliente cuya información personal sea colectada.

La transparencia es especialmente importante dada la proliferación de los servicios de nube "gratuitos", en los cuales el proveedor de nube lucra con la extracción de datos que le fueron confiados por los usuarios y con la venta de esos datos a los anunciantes u otros terceros. Si bien no hay nada inherentemente errado en estos modelos de negocios basados en anuncios publicitarios, los usuarios necesitan entender la naturaleza de los datos que están siendo recolectados y cómo se están utilizando, para poder tomar una decisión informada antes de aceptar ese convenio. En algunos casos, los consumidores y las pequeñas y medianas empresas pueden decidir no entregar sus datos a un servicio gratuito si la naturaleza de los datos recolectados y la forma en que tal información es revelada a terceros crea un riesgo para su reputación, su privacidad personal o sus intereses económicos. En efecto, los consumidores prestan cada vez más atención a cómo la información que se provee al servicio de nube puede tener consecuencias en otros contextos.

58. Ver Information Technology - Security Techniques - Code of Practice for PII protection in public cloud acting as PII processors, ISO/IEC DIS 27018 (Int'l Org. for Standardization 2013), disponible en: [www.iso.org/iso/catalogue_detail.htm?csnumber=61498].

Por ejemplo, las preocupaciones de que un empleador pueda utilizar las cuentas en medios sociales de un empleado prospecto han llevado a los políticos en Estados Unidos a considerar legislación que limitaría ese uso[59]. En una era en la que los usuarios deben considerar las consecuencias de sus "rastros digitales", la divulgación honesta de las prácticas de uso de datos y privacidad por los proveedores es esencial.

3. Posibilitando y protegiendo el flujo de datos a través de las fronteras

Conseguir migrar los datos entre múltiples áreas geográficas permite a los proveedores del cómputo en la nube hacer un "*pool*" con los recursos de TI, reduciendo sus costos administrativos y aumentando su poder de compra; esto, a su vez, da como resultado beneficios significativos en costos y eficiencia para los consumidores, así como para el medio ambiente, ya que el número de centros de datos utilizados también disminuye[60]. De particular importancia es la escala necesaria para poner a disposición un servicio de nube viable al precio más accesible. Si bien cada nuevo servidor empleado en el servicio de una nube pública conlleva una notable reducción en los costos, hay una reducción de costos aún mayor una vez que se utilizan al menos 10.000 servidores en una nube pública[61]. Desde un punto de vista operativo, los proveedores de computación en la nube transfieren los datos entre centros de datos de manera que puedan ofrecer servicios esenciales a sus clientes, incluyendo soporte técnico y desarrollo de productos 24 horas al día. De la misma manera, la transferencia de datos es esencial para la resiliencia y para los *backups* de datos. Como se menciona en un reporte reciente del mercado de seguros de *Lloyd's*, "El mundo digital es aún susceptible a desastres físicos tales como inundaciones, terremotos y huracanes", y por lo tanto la "concentración geográfica" de datos puede incrementar el riesgo de pérdida[62]. La nube proporciona el vehículo perfecto para garantizar que la información crítica no desaparezca para siempre como resultado de desastres naturales o causados por el hombre, ya que el servicio de nube por naturaleza no concentra el *backup* de datos en el mismo lugar. Por el contrario, distribuye los *backups* de información a lo largo de varias partes del mundo para maximizar la eficiencia y la continuidad del servicio y reducir los costos para el consumidor.

Las reglas que restringen la transferencia de datos e información a través de las fronteras, no obstante, no acompañan a la realidad actual de la computación

59. Ver, por ej., *Employer Access to Social Media Usernames and Passwords 2013*, National Conference of State Legislatures, [www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords-2013.aspx] (visitado por última vez el 23 de sept. de 2013).

60. Ver Niels Soelberg, *The Economics of Cloud Computing for the EU Public Sector*, [www.microsoft.com/eu/transforming-business/article/the-economics-ofcloud-computing-for-the-eu-public-sector.aspx] (visitado por última vez el 23 de sept. de 2013).

61. Federico Etro, *The economic impact of cloud computing on business creation, employment and output in Europe an application of the endogenous market structures approach to a gpt innovation* (Feb. 2009).

62. Lloyd's, Digital Risks - Views of a Changing Risk Landscape, Lloyd's Emerging Risks Team Report (Oct. 2009), disponible en: [www.lloyds.com/~/ media/lloyds/reports/emerging%20risk%20reports/digitalrisksreport_october2009v2.pdf].

basada en el ancho de banda. Si bien no es su intención, estas reglas limitan la innovación y el desarrollo económico que normalmente sería posibilitado por la nube, y a menudo no producen los beneficios correspondientes para la privacidad de los consumidores. Como ha sido reconocido por la Comisión Europea, "existe una necesidad general de mejorar los mecanismos actuales para la transferencia internacional de datos" en vista del vasto aumento de los servicios de entrega en Internet desde que la Directiva de Protección de Datos fue adoptada hace 15 años[63]. La Directiva, en su estado actual, restringe ampliamente la transferencia de datos personales desde Europa a cualquier país cuyas leyes internas no provean el nivel de protección que la Unión Europea considera "adecuado". En la práctica, solo aquellos países que proveen los mismos métodos de protección exactamente iguales a los de la Unión Europea, tales como Argentina y Uruguay, han sido considerados como adecuados[64]. En total, solo siete países son considerados adecuados, junto con cinco micro estados o territorios independientes tales como la Isla de Man[65]. Como resultado, en la práctica, el régimen de adecuación de la Unión Europea ha impuesto amplias limitaciones al movimiento de datos transfronterizo, aun cuando esto compromete la obtención de los beneficios del cómputo en la nube.

La excepción "*Safe Harbor*" adoptada por la Unión Europea para Estados Unidos reconoce que si bien este país no emplea idénticos métodos de protección de privacidad que la Unión Europea, no es necesario negarle a un país el estatus "adecuado" y negar los beneficios de la infraestructura de nube que se encuentran en mercados principales tales como Estados Unidos[66]. Por el contrario, se pueden desarrollar otros mecanismos para permitir el libre pero seguro flujo de datos a través de las fronteras. Bajo el estatus de "*Safe Harbor*", las empresas en Estados Unidos pueden certificar que importarán datos de la Unión Europea únicamente bajo condiciones que concuerdan con las leyes de privacidad de esta[67]. No obstante, no todos los países que limitan la transferencia de datos a aquellos países con leyes de privacidad "adecuadas" han adoptado mecanismos alternativos de cumplimiento, tales como la política de "*Safe Harbor*" adoptada por la Unión Europea. Establecer este tipo de mecanismo en los diversos países de América Latina que han adoptado restricciones para la transferencia de datos según el modelo de la Unión Europea, pudiera ser la clave para el desarrollo de servicios robustos de cómputo en la nube en América Latina[68].

63. Ver *A comprehensive approach to personal data protection in the European Union,* COM (2010) 609 final (Apr. 11, 2010), disponible en: [http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf].

64. *Commission decisions on the adequacy of the protection of personal data in third countries,* European Commission Justice, [http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm] (last updated July 16, 2013).

65. Ibíd.

66. U.S. - E.U Safe Harbor Overview, EXPORT.GOV, [http://export.gov/safeharbor/eu/eg_main_018476.asp] (actualizado por última vez el 1de julio de 2013).

67. Ibíd.

68. La Comisión Europea publicó recientemente ciertas recomendaciones con la intención de mejorar el funcionamiento del mecanismo de protección de salvaguardia ("*Safe*

Con independencia de la naturaleza indebidamente estricta de las restricciones transfronterizas de datos –ya sean resultado de una prohibición expresa en la exportación de datos, de una limitación basada en un requerimiento de "adecuación", o de leyes inconsistentes entre jurisdicciones– la consecuencia involuntaria de colocar una cerca nacional alrededor de una nube del país es disminuir la inversión, reducir el comercio y privar a los consumidores y empresas de los beneficios del cómputo en la nube y otras innovaciones.

Como alternativa, forzar a un proveedor a almacenar los datos localmente en la jurisdicción que impone las restricciones al libre flujo de datos impide que ese proveedor pueda ofrecer a los clientes los beneficios de costos y servicios que se derivan de poder migrar los datos a los sitios con almacenamiento más eficiente. También dejarían de existir los potenciales beneficios ambientales y eficiencia energética que resultan de la consolidación de recursos en menos centros de datos[69]. En pocas palabras, el deseo de tener centros de datos locales entra en conflicto con las eficiencias asociadas con las economías de escala del cómputo en la nube. En la medida en que haya cualquier ganancia de corto plazo en forzar a los proveedores de nube a construir centros de datos locales como condición para hacer negocios, en el largo plazo tales ganancias serán mínimas frente a las oportunidades perdidas, ya que muchos proveedores de nube simplemente decidirán no poner a disposición los servicios de nube en el país. Es más, los mandatos para instalar centros de datos locales producen pocos beneficios económicos dentro del país, ya que la exigencia está basada en la falsa premisa de que los centros de datos físicos –en oposición a los servicios que tales centros de datos facilitan– impulsan el crecimiento del empleo en la nube[70].

4. Armonizando las reglas de protección de datos y la interoperabilidad

La principal característica que define a la nube es la inexistencia de fronteras físicas. Esto permite a los usuarios en cualquier país crear, acceder a datos y compartirlos con otros usuarios en el mundo entero. Infortunadamente, esta inexistencia de fronteras significa que el proveedor de nube está potencialmente sujeto a las leyes de

Harbor"). Si bien los interesados tienen opiniones diversas con respecto a estas recomendaciones, la Comisión reconoció que "la protección de salvaguardia es un componente importante de la relación comercial entre Estados Unidos y la Unión Europea, de la cual dependen varias compañías en ambos lados del Atlántico". Al hacer sus recomendaciones, la Comisión reconoció también que la revocación de la protección de salvaguardia no sería una decisión sabia, mencionando que "afectaría adversamente los intereses de las compañías miembro en la Unión Europea y en los Estados Unidos", y concluyó, por el contrario, que "la protección de salvaguardia debería ser más bien fortalecida". Ver European Commission Justice, Communication from the Commission to the European Parliament and the Council: Rebuilding trust in EU-US data flows 6 (Nov. 27, 2013), disponible en: [http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf].

69. Ver Soelberg, nota 62 anterior.

70. Ver James Heaney, *Yahoo Aims to Expand Data Center in Lockport, Buffalo News* (April 4, 2011, 12:01 AM), [www.buffalonews.com/article/20110404/cityandregion/304049993] ("Data centers are not regarded as significant economic engines, however").

cientos de naciones y miles de jurisdicciones[71]. Las leyes de privacidad y seguridad de datos varían ampliamente[72]. Algunos países imponen requisitos estrictos de aviso y consentimiento, mientras que otros no tienen ninguno[73]. Algunos países limitan la transferencia de datos a otros países, mientras que algunos no restringen el flujo de datos[74]. Algunos países requieren que las compañías custodien cuidadosamente la información personal, mientras que otros no requieren tales protecciones[75].

Las leyes y reglamentaciones de privacidad han variado por décadas. Pero el incremento del cómputo en la nube ha ampliado los problemas causados por estas inconsistencias. Un proveedor de nube verdaderamente global debe asegurarse de cumplir con los requisitos de todas las leyes de privacidad y seguridad de datos, aun si estas leyes entran en conflicto las unas con las otras. Necesitamos reglas que se apliquen cada vez más de modo consistente de un país a otro y de un continente a otro. Sería poco realista esperar que cada país adopte reglas idénticas de protección de datos y privacidad. Pero si los países hicieran un esfuerzo por armonizar ciertos requisitos, reducirían la incertidumbre para los proveedores de nube. Únicamente mediante la colaboración de un gobierno con otro se podrá crear la consistencia entre las políticas regulatorias que son necesarias para que la nube funcione. Los gobiernos podrían comenzar por trabajar para desarrollar reglas que facilitarán el flujo de datos a través de las fronteras nacionales y regionales. En forma alterna, los gobiernos podrían trabajar juntos para desarrollar y acordar principios comunes para determinar cuándo un país tiene jurisdicción sobre los datos almacenados en la nube.

Puede resultar que lo más efectivo sea que los gobiernos, con el paso del tiempo, busquen tener un marco multilateral para estos temas en forma de tratados o instrumentos internacionales similares. Mientras que esta opción indudablemente requeriría un significativo liderazgo diplomático y recursos, ofrece quizás la mejor posibilidad para atender las necesidades legítimas de los gobiernos en una forma coherente, a la vez que garantiza que los intereses de las empresas y de consumidores en la privacidad sean atendidos en una escala global.

Una opción menos formal sería que los países se involucraran en consultar y construir consensos bilaterales o regionales para armonizar en mejor forma sus regímenes respectivos de protección de datos y resolver de mejor manera los problemas de acceso de datos. Tal involucramiento puede incrementar el conocimiento de los problemas y pavimentar el camino para una solución más formal de largo plazo. Por ejemplo, en Asia, el progreso logrado en el Programa de Cooperación para el Desarrollo ASEAN-Australia para armonizar los marcos legales de comercio

71. Ver Juliette Garside, *How global laws protect your data, The Guardian* (Oct.16, 2011, 7:01 PM), [www.theguardian.com/cloud-technology/global-laws-protect-your-data].
72. Ver Constance Gustke, *Which countries are better at protecting privacy,* bbc (June 26, 2013), [www.bbc.com/capital/story/20130625-your-private-data-isshowing].
73. Ibíd.
74. Ibíd.
75. Ibíd.

en línea (*e-commerce*), y en los proyectos de marco de Privacidad de la APEC y el proyecto Pathfinder, provee una plataforma sólida para un desarrollo aún mayor y para atender los enfoques jurisdiccionales divergentes frente a las políticas de tecnología. Asimismo, los estándares voluntarios ISO 27001/27002 garantizan la seguridad de la información en las compañías a nivel mundial. Tales discusiones regionales multipartidarias ofrecen una oportunidad para impulsar el cómputo en la nube y expandir sus beneficios en muchos niveles a lo largo de la región.

A medida que las naciones de América Latina adoptan nuevas leyes y reglamentaciones de protección de datos, deberían también hacer de la interoperabilidad una prioridad. Como punto de partida, los países deberían asegurar que existe un marco interoperable dentro de la región. Por ejemplo, las empresas de cómputo en la nube generalmente deberían poder esperar que si cumplen con las reglas y reglamentos mexicanos sobre privacidad de datos, no tendrían que hacer cambios significativos a sus prácticas para poder cumplir con las reglas y reglamentos de Chile, o viceversa. Un marco interoperable, armonizado, podría proveerle a la región una voz más clara y con mayor peso en el diálogo global respecto a las regulaciones de protección de datos y de nube. El objetivo final debería ser asegurar que las reglas de protección de datos en las naciones de América Latina sean interoperables con aquellas de otras regiones, incluyendo las de Estados Unidos, la Unión Europea y Asia. Como se mencionó, las determinaciones rígidas de "adecuación" crean complicaciones innecesarias para el flujo de datos que hace de la nube una realidad.

5. Fortaleciendo las leyes contra el delito cibernético

Mediante la prevención del delito cibernético, los gobiernos pueden ayudar a construir la confianza del consumidor en la nube. Cuando hablamos de "delito cibernético" nos referimos a una variedad de actividades criminales *online*. Los tres tipos generales de delito cibernético que presentan el mayor riesgo para la nube son: 1) los delitos contra los ciudadanos como individuos, tales como los ataques contra niños, 2) los delitos contra las naciones, tales como el terrorismo, y 3) los delitos económicos, tales como el fraude con tarjetas de crédito[76].

Combatir el delito cibernético siempre ha sido un problema global, pero el cómputo en la nube lo hace aún mayor. Con la víctima a menudo en una jurisdicción, el centro de procesamiento de datos en otra, y el infractor en una tercera, tiene que existir un mecanismo efectivo de cooperación entre las agencias policiales en América Latina, la Unión Europea, Estados Unidos y otras partes. Hay necesidad de contar con estándares claros y consistentes para la producción, retención y pre-

76. Ver, por ej., ELINOR MILLS, *Cybercrime moves to the cloud*, CNET (June 30, 2012, 6:00 AM), [http://news.cnet.com/8301-1009_3-57464177-83/cybercrime-moves-to-thecloud/]. (discussing how the cloud could be targeted by cyber criminals); ver también *Top Threats to Cloud Computing V1.0*, Cloud Security Alliance (March 2010), disponible en: [https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf].

servación de datos en las investigaciones que conciernen a múltiples jurisdicciones, de hacer inversión en conocimiento tecnológico para las agencias policiales locales, y de contar con cooperación en la creación de *clearinghouses* internacionales, a través de los cuales se compartan los datos sobre delitos cibernéticos con un punto central de contacto global que evalúe las tendencias y haga conexiones para ayudar a identificar a los infractores.

En resumen, si se provee un marco de regulación consistente que proteja la privacidad e infunda la confianza del consumidor, el gobierno podrá ayudar a promover la competitividad nacional a través del cómputo en la nube.

III. Desafíos, tendencias y experiencias iniciales de la regulación de la nube

La nube no solo presenta oportunidades sin precedentes; también presenta nuevas preguntas sobre la privacidad y seguridad de datos para la industria, reguladores y consumidores. Todos los participantes deben identificar estos desafíos y determinar la manera más efectiva de abordar estas preguntas, a la vez que aprovechan el potencial completo de la nube para la innovación y la prosperidad económica local.

A. El cómputo en la nube genera preguntas importantes sobre la privacidad y seguridad de datos

La necesidad de una toma de decisiones bien pensadas es especialmente marcada en nuestra era del "*big data*", que es la recopilación, administración y uso de datos a gran escala. Incluso cuando hay piezas individuales de información que por sí solas son relativamente inocuas, estos miles de puntos de datos en su totalidad pueden "comenzar a pintar el retrato de la vida de una persona"[77]. En un ejemplo particularmente vívido, el *New York Times* detallaba cómo una gran tienda minorista era capaz de predecir que una niña adolecente estaba embarazada –y enviarle cupones de descuento– aun antes de que su padre supiera, basada simplemente en su historial de compras[78]. Las redes de publicidad en línea tienen acceso a una variedad mucho más amplia de información. Investigadores de la Universidad de Stanford, por ejemplo, encontraron una red de publicidad que usaba un *script* para determinar los historiales de navegación de los usuarios y relacionar las páginas visitadas con una gran variedad de segmentos de interés, incluyendo temas tan delicados como reparación de crédito y ayuda con deudas[79].

77. Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 *Minn. L. Rev.* 1137, 1141 (2002).

78. Charles Duhigg, *How Companies Learn Your Secrets*, *N.Y. Times Magazine*, Feb. 16, 2012), [www.nytimes.com/2012/02/19/magazine/shopping-habits.html].

79. Jonathan R. Mayer & John C. Mitchell, *Third-Party Web Tracking: Policy and Technology* (2012), disponible en: [https://cyberlaw.stanford.edu/files/publication/files/trackingsurvey12.pdf]; Jonathan Mayer, *Tracking the Trackers: To Catch a History Thief*, *CIS* (July 19, 2011, 4:20 AM), [http://cyberlaw.stanford.edu/node/6695].

Las organizaciones que están migrando a la nube –ya sean empresas, agencias gubernamentales, escuelas u otras instituciones– tienen preocupaciones entendibles acerca de la privacidad y seguridad de su información, el efecto del cumplimiento regulatorio, y las políticas de uso de información por parte de los proveedores de nube. Una encuesta reciente realizada por la "*Cloud Security Alliance*" (Alianza para la Seguridad en la Nube) encontró que los usuarios organizacionales ven la seguridad de la información como la mayor limitación para la adopción de la nube[80].

Los usuarios individuales tienen preocupaciones similares. Ellos necesitan tener la garantía de que sus datos están seguros y a salvo de *hackers*, y que pueden controlar quién accede a su información personal. Establecer la confianza y seguridad es necesario para promover el acceso y fomentar la inversión. Para que la nube pueda realmente tener éxito, los consumidores deben sentirse tan cómodos guardando su información en la nube como se sienten cuando guardan la información en sus discos duros personales.

B. Tendencias regulatorias

Argentina fue pionera en el año 2000 cuando promulgó las primeras reglas comprensivas de protección de datos y privacidad en América Latina[81]. Estas regulaciones desarrollaron la confianza en Internet por parte del consumidor y ayudaron al sector de tecnologías de información del país a prosperar. Pero muchas de estas regulaciones ya no aplican a la nube hoy en día. Infortunadamente, algunos países en la región continúan adoptando leyes que limitan los beneficios de la nube. Las naciones con leyes basadas en modelos desarrollados en los años noventa deben modernizar sus reglas de protección de información y privacidad para desarrollar la confianza en la nube y mantener la competitividad nacional. Vivimos en un mundo digital que ha cambiado radicalmente a lo largo de la última década, y estas leyes pre-nube no atienden de manera adecuada la privacidad y seguridad en la era de la nube, que es ahora una realidad.

Regulaciones de privacidad y protección de datos consistentes pueden establecer un punto de referencia útil para todos los proveedores de nube. Las regulaciones balanceadas pueden establecer la confianza de los consumidores en la nube y ayudar a promover el crecimiento de esta extraordinaria tecnología. En lugar de articular requisitos regulatorios específicos, creemos que es más útil discutir las dos características generales de una regulación de nube efectiva.

80. Joe McKendrick, *Cloud's Full Impact is Still About Three Years Away, Survey Predicts*, *Forbes* (Oct. 12, 2012), [www.forbes.com/sites/joemckendrick/2012/10/03/clouds-full-impact-is-still-about-three-years-away-survey-predicts/].

81. Ver, en general, Maxim Gakh, *Argentina's Protection of Personal Data: Initiation and Response*, 2 I/S: J. L. & Pol'Y for Info. Soc'Y 781 (2006) (donde se discute la Ley de Protección de datos personales de Argentina y los efectos que su promulgación tuvo sobre otros países).

En primer lugar, las regulaciones tienen que permitir que la información fluya libremente a través de las fronteras, en circunstancias en las que haya garantías de que el importador de datos dará los pasos necesarios para proteger y asegurar los datos personales. Así como Internet es global, la nube, que se basa en esta, también debe serlo. Los servicios basados en la nube pueden cruzar docenas o centenares de fronteras nacionales, y a su paso, decenas y centenares de marcos regulatorios. Este mosaico de regulaciones necesita una actualización sustancial.

En segundo lugar, las regulaciones deben proteger la privacidad y asegurar que la nube sea segura para evitar el acceso no autorizado. Como se demostró arriba, la confianza es esencial para el éxito de la nube. La privacidad y la seguridad se citan como los dos impedimentos principales para una adopción más amplia de la nube[82]. Una nube segura y abierta es una nube que está protegida contra *hackers* y ladrones, y que también sirve como un depósito de información que puede ser útil para las personas con servicios asequibles y continuos, a los cuales acceder desde dispositivos siempre conectados.

Los gobiernos, de manera inteligente, han empezado a considerar propuestas que protegerían la privacidad de los consumidores en la nube a través de un régimen orientado hacia los resultados. Por ejemplo, la Comisión Europea sugirió que se incluya expresamente un principio de "responsabilidad" en el régimen de protección de datos de la Unión Europea[83]. Bajo un régimen basado en la responsabilidad, los estándares y requisitos de protección de datos están consagrados en la ley, pero las organizaciones individuales tienen gran parte de la responsabilidad de determinar cuál es la mejor manera de cumplir con esos estándares en la práctica. Es importante, sin embargo, que el beneficio de un enfoque en responsabilidad no se malgaste imponiendo simplemente un requisito según el cual las organizaciones son responsables en adición a la detallada normativa existente de la Unión Europea. Más bien, la responsabilidad debería usarse en lugar de la detallada normativa, un punto que el Comisionado de Información del Reino Unido expuso al inicio de este año, cuando se opuso a aspectos de las reglas de protección de datos propuestas por la Unión Europea[84].

En esa misma línea, el Departamento de Comercio de Estados Unidos recomendó legislación que crearía un puerto seguro contra las acciones legales del gobierno para las compañías que se adhieran voluntariamente a los códigos de conducta apropiados, voluntarios y exigibles, desarrollados a través de procesos con la participación de múltiples interesados. El Departamento de Comercio enfatizó

82. World Economic Forum, *Exploring the future of cloud computing: Riding the next wave of technology-driven transformation* (2010), disponible en: [www.weforum.org/pdf/ip/ittc/Exploring-the-future-of-cloud-computing.pdf].

83. *Data Protection Accountability: The Essential Elements*, The Centre for Information Policy Leadership (Oct. 2009), disponible en: [www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf].

84. Liat Clark, *ICO Commissioner Slams EU Data Protection Directive*, Wired UK (Feb. 7, 2013), [www.wired.co.uk/news/archive/2013-02/07/ico-against-eu-dataprotection]. ("*We want it defined in terms of outcomes rather than regulatory process*").

correctamente que esta posición flexible de puerto seguro no disminuiría las protecciones para los consumidores, al observar que "Incumplir con las provisiones voluntarias y exigibles del código podría conllevar a acciones legales por parte de la Comisión Federal de Comercio (FTC) o de un fiscal general de Estado".

C. La posición de Microsoft

Las reglamentaciones por sí solas no generarán el nivel necesario de confianza en la nube por parte del consumidor. La industria debe tener un diálogo continuo con los clientes acerca de la privacidad en la nube. Microsoft tiene el compromiso de desempeñar un rol proactivo y responsable en esta área. Creemos firmemente que las prácticas de privacidad en la nube se beneficiarían de comunicaciones y servicios que informen a los consumidores y comparen las ofertas. En forma análoga, en la industria automotriz este tipo de diálogo ha sido exitoso impulsando a la industria a innovar en el área de seguridad – a través de iniciativas de gobierno para informar a los consumidores, así como a las revistas de consumidores y sitios web, que califican a los automóviles con base en estándares de seguridad y opiniones de los consumidores. Un diálogo similar en el contexto del cómputo en la nube pudiera facilitar la respuesta de la industria a las necesidades de privacidad.

Microsoft, por ejemplo, obtiene las opiniones de los clientes a través de una variedad de medios, incluyendo evaluaciones de uso, encuestas, grupos de discusión y otros tipos de investigación de campo. Microsoft también ha creado el Programa de Mejora de Experiencia de Usuario (*Customer Experience Improvement Program* - CEIP), a través del cual los clientes pueden compartir voluntariamente información en línea acerca de la manera en que usan los programas de Microsoft y pueden reportar algún problema que encuentren. Esta información le ayuda a Microsoft a innovar y a mejorar la experiencia general del usuario, incluso con respecto a la privacidad y seguridad de sus clientes, privacidad y seguridad que Microsoft se ha comprometido a proteger.

Lo que Microsoft ha aprendido de esta retroalimentación, entre otras cosas, es que los clientes quieren entender mejor qué datos están siendo recolectados y cómo están siendo utilizados. En respuesta a ello, hemos trabajado arduamente para proporcionar información clara y fácil de entender sobre nuestras prácticas de privacidad y seguridad. Por ejemplo, Microsoft creó el Office 365 Trust Center (Centro de Confianza Office 365) para proporcionar un nivel de transparencia líder en la industria, sobre las prácticas de privacidad de datos y seguridad. El Centro de Confianza provee a los clientes y a otras partes interesadas explicaciones claras, fáciles de entender, de lo que Microsoft hace con los datos en la nube – incluyendo cómo se recolectan, las circunstancias bajo las cuales se puede acceder a ellos, hacia dónde fluye la información, y en qué forma puede recibir el cliente información

adicional sobre seguridad, privacidad y auditoría[85]. El Centro de Confianza es único en la industria y ha hecho de Microsoft el líder en materia de transparencia en la nube. En contraste con algunos proveedores de nube que no son completamente transparentes con respecto a sus prácticas de uso de datos, Microsoft hace promesas claras de que utilizará los datos de los clientes empresariales *únicamente* para proporcionar los servicios requeridos por el cliente, y no para beneficiarse comercialmente.

Cuando Microsoft es citada o legalmente obligada por un gobierno a presentar información de un cliente, la posición de Microsoft es clara: creemos que nuestros clientes deben controlar su propia información en la medida posible. Acorde con ello, si una entidad gubernamental se dirige a Microsoft directamente para obtener información que hemos hospedado en nombre de un cliente de Office 365, por ejemplo, Microsoft tratará en primera instancia de redirigir a la entidad al cliente para darle al cliente la oportunidad de decidir cómo responder. Si, no obstante, Microsoft es requerida para responder a una solicitud judicial, únicamente proporcionará la información que le pertenece al cliente de Office 365 cuando haya sido legalmente requerida a hacerlo. Microsoft limitará la entrega únicamente a aquella información que a Microsoft se le exija revelar, utilizando esfuerzos razonables para notificar al cliente con anterioridad a tal revelación, salvo que legalmente se le prohíba hacerlo[86]. Como dijo Brad Smith, *General Counsel* (Jefe del Departamento Legal) de Microsoft, "Microsoft no proporcionará a los gobiernos, en ningún caso, acceso directo o completamente libre de trabas a los datos de clientes o claves criptográficas". Microsoft solo proporcionará y proveerá los datos específicamente requeridos por la solicitud judicial relevante"[87].

Es más, en vista de las recientes acusaciones relacionadas con la vigilancia de datos de clientes por parte de algunos gobiernos, Microsoft está tomando diversas acciones preventivas. Tales acciones incluyen, por ejemplo, fortalecer la criptografía en las redes y servicios de Microsoft (aclarando que los datos de clientes en Office 365 y Outlook.com ya se benefician de la criptografía cuando viajan entre los clientes y Microsoft), y mejorando la transparencia del código del software de Microsoft (esto facilitará la reafirmación de que la ingeniería de software de Microsoft no provee puertas traseras en los productos Microsoft, que los gobiernos pudieran disimuladamente explotar para acceder a datos privados de los clientes). Al mismo tiempo, Microsoft se está uniendo a otras compañías a lo largo de nuestra industria, tales como AOL, Apple, Facebook, Google, LinkedIn, Twitter y Yahoo,

85. *Microsoft Office 365 Trust Center*, Microsoft Corp., [http://office.microsoft .com/en-us/business/office-365-trust-center-cloud-computing-security-FX103030390.aspx] (visitado por última vez el 24 de nov. de 2013).

86. *How we use your data, Microsoft Office 365 Trust Center,* Microsoft Corp., [www.microsoft.com/online/legal/v2/?docid=23] (visitado por última vez el 24 de nov. de 2013).

87. BRAD SMITH, *Responding to Government legal demands for customer data,* Microsoft on the Issues, (July 16, 2013), [http://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/08/30/standing-together-for-greater-transparency.aspx].

para solicitar reformas a las prácticas de vigilancia del gobierno, que exigirán que el gobierno se adhiera a principios específicos con respecto a la vigilancia[88].

En adición a la transparencia, resulta claro que los consumidores también quieren elección y control sobre la forma en que se usan sus datos – en particular por terceras partes comerciales. Una vez más, estamos trabajando arduamente para responder. Internet Explorer proporciona *Tracking Protection* (Protección de Rastreo). En la Internet de hoy en día, cada vez más los sitios web toman el contenido, tal como imágenes y texto, de sitios de terceros. A pesar de que esta es una característica común del diseño web moderno que permite que los proveedores en línea enriquezcan sus sitios web y servicios, los usuarios a veces no son conscientes de que pueden ser rastreados a través de la web por terceros a través del contenido en las páginas. Específicamente, los usuarios podrán crear listas de Protección de Rastreo (*Tracking Protection Lists*) que les permitirán limitar el compartimiento de sus datos con sitios específicos, o con categorías de sitios. Los usuarios podrán incluir los sitios que deseen en estas listas, y esperamos que en el futuro las personas puedan escoger las listas de Protección de Rastreo que sean creadas por todo tipo de empresas y organizaciones – desde defensores de la privacidad hasta empresas de seguridad y grupos publicitarios. Lo que resulta más importante, la Protección de Rastreo da a los usuarios el control, sin emplear mecanismos intrusivos que desvíen la atención de la experiencia en línea, tal como las interrupciones a los usuarios potencialmente cientos de veces, para solicitar su consentimiento expreso cada vez que se implementa un *cookie*[89]. La Asociación Europea de Privacidad alabó recientemente la Protección de Rastreo como una herramienta que contribuye a "la creación de un mercado en línea más enfocado en las necesidades de los consumidores y es atenta a sus preocupaciones de privacidad"[90].

Microsoft les da a los consumidores niveles similares de elección y control a través de nuestras tecnologías y servicios. *Windows Phone 8*, por ejemplo, incluye una característica de "geo-ubicación" que permite que los consumidores aprovechen una gama cada vez mayor de aplicaciones basadas en ubicación y servicios en el mercado. No obstante, ninguna aplicación puede obtener acceso a la información de ubicación a menos que el consumidor lo haya consentido expresamente. Las aplicaciones que usan la ubicación de los consumidores también tienen que permitir a los usuarios desactivar tal acceso posteriormente – y los consumidores tienen la opción de desactivar los servicios de acceso a la ubicación en todas las aplicaciones.

Microsoft también les proporciona a los clientes corporativos herramientas sofisticadas para administrar el uso de información delicada dentro de sus propias

88. Brad Smith, *Protecting Customer Data from Government Snooping,* The Official Microsoft Blog, (Dec. 4, 2013), [http://blogs.technet.com/b/microsoft_blog/archive/2013/12/04/protecting-customer-data-from-government-snooping.aspx].

89. Más información sobre nuestra característica *Tracking Protection* (Protección de Rastreo) está disponible en IE9 y *Privacy: Introducing Tracking Protection*, ieblog (Dec. 7, 2010, 1:10 PM), [http://bit.ly/ietpl].

90. European Privacy Association, *Protection list: on the Right Track*, epa news (Jan. 21, 2011), [www.europeanprivacyassociation.eu/agenda_news.php?function=read&id=36].

organizaciones – utilizando innovaciones tales como *Windows 8 BitLocker* y *BitLocker To Go*, los cuales encriptan los datos en computadores personales y dispositivos USB portátiles, y evitan así el acceso a los datos sensibles de una organización si se pierde el dispositivo de un empleado o si este es robado[91].

En resumen, Microsoft tiene el compromiso de mantener el liderazgo dentro de la industria en la privacidad en la nube. ¿Por qué? En adición a las firmes convicciones de la compañía sobre la privacidad y la seguridad, el modelo de negocios de Microsoft –que está principalmente basado en la generación de ingresos por la venta de software y servicios innovadores– impulsa a Microsoft a proteger la privacidad del usuario. Por el contrario, algunos proveedores de la nube generan ingresos casi exclusivamente de la extracción de datos de los consumidores obtenidos a través de correos electrónicos, búsquedas en línea, etc., para beneficio de los clientes anunciantes de tales compañías (como dice el dicho, "si usted recibe un producto gratuitamente, *usted* es el producto")[92]. Esto conduce a incentivos y enfoques de privacidad muy diferentes. En vista del modelo de negocios de Microsoft, la empresa ve la privacidad con un gran valor comercial para los usuarios, y creemos que Microsoft y otras empresas en la industria deberían competir para proporcionar las mejores protecciones de privacidad disponibles.

Es claro que, si bien las ofertas competitivas producirán muchos beneficios en el ámbito de la privacidad, la colaboración de la industria y la autorregulación son también críticas para promover la privacidad en línea – un punto que la Comisión Europea reconoce en su Agenda Digital para Europa[93]. Esta es la razón por la que Microsoft comparte con socios y competidores los lineamientos de privacidad que Microsoft sigue al desarrollar software y servicios en línea[94]. Desde que Microsoft puso a disposición por primera vez estos lineamientos en el año 2006, los mismos han hecho significativas contribuciones a la certificación profesional de privacidad líder en el sector de TI (Profesional Certificado en Privacidad de la Información para TI, o CIPP/IT), y han ayudado a moldear los estándares de privacidad internacionales.

Vemos una serie de oportunidades para reforzar el diálogo con miembros de la industria acerca de la autorregulación. Por ejemplo, a medida que los datos de

91. Para más información sobre las herramientas de seguridad proporcionadas en Windows 8, cfr. [www.microsoft.com/security/pc-security/windows8.aspx].

Adicionalmente, Microsoft certifica que sus servicios en línea cumplen con los estándares de seguridad de la serie ISO 27000, los cuales, entre otras cosas, establecen los lineamientos y principios generales para iniciar, implementar, mantener y mejorar el manejo de la seguridad de la información al interior de una organización.

92. Bryan Cunningham, *Google's data mining raises questions of national security*, *The Guardian* (Oct. 15, 2012, 11:40 AM), [www.theguardian.com/commentisfree/2012/oct/15/google-data-mining-national-security] ("*The revenue generated by combining and monetizing such data–by mining the mosaic–is the reason 'free' cloud services can afford to be free*").

93. Ver A Digital Agenda for Europe, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions § 2.3 (Trust and Security) (2010).

94. *Privacy Guidelines for Developing Software Products and Services Version 3.1*, Microsoft Corp. (2006), disponible en: [http://go.microsoft.com/?linkid=9746120].

geoubicación son recolectados cada vez más y utilizados para proporcionar una gama de servicios a usuarios, varias organizaciones están liderando esfuerzos para crear códigos de conducta para ayudar a calmar las preocupaciones emergentes de los reguladores en torno a la recolección y uso de tales datos. Microsoft continuará participando activamente y apoyando los esfuerzos para ayudar a crear prácticas coherentes de protección de la privacidad en la industria.

Conclusión

El cómputo en la nube puede estimular las economías mediante la creación de empleos y promoción de la innovación, fomentando una mayor inclusión social y creando estándares de vida más altos, porque se encuentra disponible a un precio que por sí mismo es muy inclusivo. Para viabilizar el crecimiento económico y los beneficios sociales que ofrece el cómputo en la nube, los gobiernos y la industria deben trabajar juntos, tal como lo hicieron en la promoción de eras pasadas de crecimiento impulsado por la innovación. Microsoft está comprometida a hacer su parte, tanto a través de las prácticas líderes del mercado en privacidad y seguridad como a través del apoyo a políticas regulatorias y a la autorregulación de la industria. Ya en América Latina, los Estados Unidos y otras jurisdicciones, los gobiernos han empezado a trazar las medidas necesarias, consultando con una amplia gama de grupos compuestos por diversas partes interesadas. Instamos a los gobiernos a revisar las políticas regulatorias en la medida necesaria para fortalecer sus plataformas de nube, de forma que las más recientes características y servicios puedan ser ofrecidos a los ciudadanos locales a un precio asequible, y para que los innovadores locales puedan compartir sus invenciones con el mundo. En el futuro, al mirar hacia atrás, se dirá que esos marcos regulatorios de protección de datos que facilitaron el cómputo en la nube fueron los que más contribuyeron a las aspiraciones de un país para la competitividad nacional.

Bibliografía

"Computo en la Nube": Nuevo Detonador para la Competitividad de México, Instituto Mexicano para la Competitividad A.C. (IMCO), "Computo en la Nube": Nuevo detonador para la competitividad de México, at) 1, 31 (mayo 2012), [http://imco.org.mx/images/pdf/Computo_en_la_Nube-detonador_de_competitividad_doc.pdf].

A comprehensive approach to personal data protection in the European Union, COM (2010) 609 final (Apr.11, 2010), disponible en: [http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf].

A Digital Agenda for Europe, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions § 2.3 (Trust and Security) (2010).

agentto, [https://agentto.com/About.aspx] (visitado por última vez el 28 de sept. de 2013).

Anderson, Cushing & John F. Gantz, *Climate Change: Cloud's Impact on IT Organizations and Staffing*, IDC 1, 3 (Nov. 2012), [www.microsoft.com/en-us/news/download/presskits/learning/docs/idc.pdf].

Ayala, Orlando, *Defining National Competitiveness*, *Future Gov*. (May 20, 2011), [www.futuregov.asia/articles/2011/may/20/defining-national-competitiveness/].

Belluck, Pam, *Nantucket Hospital Uses Telemedicine as Bridge*, *N.Y. Times* (Oct. 8, 2012), [www.nytimes.com/2012/10/09/health/nantucket-hospital-uses-telemedicine-as-bridge-to-mainland.html?pagewanted=all].

Business Agility and the True Economics of Cloud Computing, vmware 1, 6 (2011), [www.vmware.com/files/pdf/accelerate/VMware_Business_Agility_and_the_True_Economics_of_Cloud_Computing_White_Paper.pdf].

Clark, Liat, *ico Commissioner Slams EU Data Protection Directive*, Wired UK (Feb. 7, 2013), [www.wired.co.uk/news/archive/2013-02/07/ico-against-eu-data-protection].

Cohen, Reuven, *Build Your Own Web or Mobile App In Minutes With These Cloud Based Tools*, *Forbes* (Mar. 22, 2013), [www.forbes.com/sites/reuvencohen/2013/03/22/build-your-own-web-or-mobile-app-in-minutes-with-these-cloud-based-tools/].

Commission decisions on the adequacy of the protection of personal data in third countries, European Commission Justice, http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (actualizado por última vez el 16 de julio de 2013).

Constitución de Argentina

Cunningham, Bryan, *Google's data mining raises questions of national security*, *The Guardian* (Oct. 15, 2012, 11:40 AM), [www.theguardian.com/commentisfree/2012/oct/15/google-data-mining-national-security].

Data Protection Accountability: The Essential Elements, The Centre for Information Policy Leadership (Oct. 2009), disponible en: [www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf].

Duhigg, Charles, *How Companies Learn Your Secrets*, *N.Y. Times*, Feb. 16, 2012), [www.nytimes.com/2012/02/19/magazine/shopping-habits.html].

Employer Access to Social Media Usernames and Passwords 2013, National Conference of State Legislatures, [www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords-2013.aspx]. (visitado por última vez el 23 de sept. de 2013).

Etro, Federico, *The economic impact of cloud computing on business creation, employment and output in Europe an application of the endogenous market structures approach to a gpt innovation* (Feb. 2009).

European Commission Justice, Communication from the Commission to the European Parliament and the Council: Rebuilding Trust in EU-US Data Flows 6 (Nov. 27, 2013), *disponible en* [http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf].

European Privacy Association, *Protection list: on the Right Track*, *EPA News* (Jan. 21, 2011), [www.europeanprivacyassociation.eu/agenda_news.php?function=read&id=36].

Falcón, Enrique, *Habeas data: concepto y procedimiento* 28 (1996).

Gakh, Maxim, *Argentina's Protection of Personal Data: Initiation and Response*, 2 I/S: *J. L. & Pol'Y for Info. Soc'Y* 781 (2006).

Garside, Juliette, *How global laws protect your data, The Guardian* (Oct.16, 2011, 7:01 PM), [www.theguardian.com/cloud-technology/global-laws-protect-your-data].

Gordon, Joanna, et al., *Exploring the Future of Cloud Computing: Riding the Next Wave of Technology-Driven Transformation*, World Economic Forum (2010), disponible en: [www3.weforum.org/docs/WEF_ITTC_FutureCloudComputing_Report_2010.pdf].

Guadamuz, Andrés, *Habeas Data vs. the European Data Protection Directive*, 3 J. *Int'L* t. 5 (2001).

Gurría, Angel, *Latin American Economic Outlook 2013: SME Policies for Structural Change* (OECD 2012), disponible en: [www.keepeek.com/Digital-Asset-Management/oecd/development/latin-american-economic-outlook-2013_leo-2013-en].

Gustke, Constance, *Which countries are better at protecting privacy,* BBC (June 26, 2013), [www.bbc.com/capital/story/20130625-your-private-data-is-showing].

Heaney, James, *Yahoo Aims to Expand Data Center in Lockport, Buffalo News* (April 4, 2011, 12:01 AM), [www.buffalonews.com/article/20110404/CITYANDREGION/304049993].

Hickey, Andrew R., *Cloud Computing Services Market To Near $150 Billion in 2014*, CRN (June 22, 2010, 12:46 PM), [www.crn.com/news/managed-services/225700984/cloud-computing-services-market-to-near-150-billion-in-2014.htm].

Horan, Kerri Lee, *Saved by the Cloud*, *District Administration* (Feb. 2010), [www.districtadministration.com/article/saved-cloud].

How we use your data, Microsoft Office 365 Trust Center, Microsoft Corp., [www.microsoft.com/online/legal/v2/?docid=23] (visitado por última vez el 24 de nov. de 2013).

[http://www.microsoft.com/security/pc-security/windows8.aspx].

Huth, Alexa & James Cebula, *The Basics of Cloud Computing,* U.S. Computer Emergency Readiness Team, disponible en [www.us-cert.gov/sites/default/files/publications/CloudComputingHuthCebula.pdf].

Information Technology - Security Techniques - Code of Practice for PII Protection in Public Cloud Acting as PII Processors, ISO/IEC DIS 27018 (Int'l Org.

for Standardization 2013), disponible en: [www.iso.org/iso/catalogue_detail.htm?csnumber=61498].

JORDÁN, VALERIA et al., "Banda ancha en América Latina: más allá de la conectividad", CEPAL 1, 29 (Feb. 2013), [www.cepal.org/publicaciones/xml/2/49262/BandaAnchaenAL.pdf.pdf].

KELLY, TOM, *SMEs must embrace the cloud to achieve global growth*, *The Guardian* (Apr. 26, 2013), [www.theguardian.com/media-network/media-network-blog/2013/apr/26/cloud-services-sme-businesses-growth?guni=Article:in%20body%20link].

KPMG, *From Hype to Future: KPMG's Cloud Computing Survey* (2010), disponible en: [www.kpmg.com/ES/es/ActualidadyNovedades/ArticulosyPublicaciones/Documents/2010-Cloud-Computing-Survey.pdf].

KRAMER, HILARY, *Washington Moves Into the Cloud: Saving Money and Securing Data*, *Forbes* (July 8, 2013, 6:45 AM), [www.forbes.com/sites/hilarykramer/2013/07/08/washington-moves-into-the-cloud-saving-money-and-securing-data/].

KROES, NEELIE, Vicepresidente de la Agenda Digital, Comisión Europea, Discurso en la conferencia Les Assises du Numérique: *Cloud Computing and Data Protection* (Nov. 25, 2010), *disponible en* [http://europa.eu/rapid/press-release_SPEECH-10-686_en.htm].

Latin American cloud computing worth US $280mn in 2012, says IDC, Start Up in Brazil (Sept. 4, 2012), [http://startupbrazil.co.uk/latin-american-cloud-computing-worth-us280mn-2012-idc/].

LEIVA, ALDO M., *Data Protection Law in Spain and Latin America: Survey of Legal Approaches*, 41 *Int'l Law News* 4 (2012), disponible en: http://www.americanbar.org/publications/international_law_news/2012/fall/data_protection_law_spain_latin_america_survey_legal_approaches.html

Ley 18.331, 11 de agosto, 2008, *Diario Oficial* (Urug.).

Ley 25326, oct. 30, 2000 (Arg.).

Lloyd's, Digital Risks - Views of a Changing Risk Landscape, Lloyd's Emerging Risks Team Report (Oct. 2009), disponible en: [/www.lloyds.com/-/media/lloyds/reports/emerging%20risk%20reports/digitalrisksreport_october2009v2.pdf].

LYNDERSAY, MARK, *Microsoft Evangelises the Cloud*, Trinidad & Tobago Guardian (Oct. 25, 2012), [www.guardian.co.tt/business-guardian/2012-10-24/microsoft-evangelises-cloud].

MAYER, JONATHAN R. & JOHN C. MITCHELL, *Third-Party Web Tracking: Policy and Technology* (2012), disponible en: [https://cyberlaw.stanford.edu/files/publication/files/trackingsurvey12.pdf].

MAYER, JONATHAN R., *Tracking the Trackers: To Catch a History Thief*, *CIS* (July 19, 2011, 4:20 AM), [http://cyberlaw.stanford.edu/node/6695].

MCKENDRICK, JOE, *Cloud Apps Somewhat More Secure than On-Premises Apps: Survey*, *Forbes* (Sept. 19, 2012), [www.forbes.com/sites/joemckendrick/2012/09/19/cloud-apps-somewhat-more-secure-than-on-premises-apps-survey/].

McKendrick, Joe, *Cloud Will Generate 14 Million Jobs by 2015: That's a Good Start*, *Forbes* (Mar. 5, 2012, 8:21 PM), [www.forbes.com/sites/joemckendrick/2012/03/05/cloud-will-generate-14-million-jobs-by-2015-thats-a-good-start/].

McKendrick, Joe, *Cloud's Full Impact is Still About Three Years Away, Survey Predicts*, *Forbes* (Oct. 12, 2012), [www.forbes.com/sites/joemckendrick/2012/10/03/clouds-full-impact-is-still-about-three-years-away-survey-predicts/].

Microsoft Office 365 Trust Center, Microsoft Corp., http://office.microsoft.com/en-us/business/office-365-trust-center-cloud-computing-security-FX103030390.aspx (visitado por última vez el 24 de nov. de 2013).

Miller, Clair Cain & Quentin Hardy, *Google Elbows Into the Cloud*, *N.Y. Times* (Mar. 12, 2013), [www.nytimes.com/2013/03/13/technology/google-takes-on-amazon-and-microsoft-for-cloud-computing-services.html?pagewanted=all].

Miller, Rich, *How Many Servers Can One Admin. Manage?*, Data Center Knowledge (Dec. 30, 2009), [www.datacenterknowledge.com/archives/2009/12/30/how-many-servers-can-one-admin-manage/].

Mills, Elinor, *Cybercrime moves to the cloud*, cnet (June 30, 2012, 6:00 AM), [http://news.cnet.com/8301-1009_3-57464177-83/cybercrime-moves-to-the-cloud/].

Mobile Phone Access Reaches Three Quarters of Planet's Population, World Bank (July 17, 2012), [www.worldbank.org/en/news/press-release/2012/07/17/mobile-phone-access-reaches-three-quarters-planets-population].

Monegain, Bernie, *3 Big Trends for the EHR Cloud*, *Healthcare IT News* (Oct. 8, 2012), [www.healthcareitnews.com/news/3-big-trends-ehr-cloud].

Mullich, Joe, *16 Ways the Cloud Will Change Our Lives*, *Wall St. J.* (Jan. 7, 2011), [http://online.wsj.com/ad/article/cloudcomputing-changelives].

Preguntas y respuestas (faq's) del reporte "Cloud Computing: Benefits, risks and recommendations for information security", European Network and Information Security Agency (enisa) (visitado por última vez el 19 de septiembre de 2013), [www.enisa.europa.eu/media/faq-on-enisa/faq%20Cloud%20Computing.pdf].

Privacy Guidelines for Developing Software Products and Services Version 3.1, Microsoft Corp. (2006), disponible en: http://go.microsoft.com/?linkid=9746120

Privacy: Introducing Tracking Protection, ieblog (Dec. 7, 2010, 1:10 PM), http://bit.ly/ietpl

Ravindranath, Mohana, *Analysts expect growth in cloud jobs*, wash. post (Aug. 15, 2013, 8:00 AM), [www.washingtonpost.com/business/on-it/analysts-expect-growth-in-cloud-jobs/2013/08/14/56d5715a-04fb-11e3-a07f-49ddc7417125_story.html].

Rincón, Hernán, *This is Latin America's Decade: The Cloud Will Make it Possible*, *Americas Quarterly* (Fall 2011), [www.americasquarterly.org/node/3085].

Rock Solid Technologies, *Dynamics CRM & Rock Solid Republic of Panama-311 System,* YouTube (Apr. 6, 2011), [www.youtube.com/watch?v=HVUCALNG2D4].

SMITH, BRAD, General Counsel and Executive Vice President, Microsoft Corp, Keynote Address at the 34th International Conference of Data Protection and Privacy Commissioners: Putting People First: Moving Technology and Privacy Forward (October 23, 2012), disponible en: [www.microsoft.com/en-us/news/download/legal/10-23puttingpeoplefirst.pdf].

SMITH, BRAD, *Protecting Customer Data from Government Snooping,* The Official Microsoft Blog (Dec. 4, 2013), [http://blogs.technet.com/b/microsoft_blog/archive/2013/12/04/protecting-customer-data-from-government-snooping.aspx].

SMITH, BRAD, *Responding to Government Legal Demands for Customer Data,* Microsoft on the Issues (July 16, 2013), [http://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/08/30/standing-together-for-greater-transparency.aspx].

SMITH, ROBERT ELLIS, *Ben Franklin's Website: Privacy and Curiosity from Plymouth Rock to the Internet*, *Privacy Journal*, 2004.

SOELBERG, NIELS, *The Economics of Cloud Computing for the EU Public Sector*, [www.microsoft.com/eu/transforming-business/article/the-economics-of-cloud-computing-for-the-eu-public-sector.aspx]. (visitado por última vez el 23 de sept. de 2013).

SOLOVE, DANIEL J., *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 *MINN. L. REV*. 1137, 1141 (2002).

TERRY, KEN, *Cloud Computing in Healthcare, the Question is Not If, But When*, *FierceHealthIT* (January 9, 2012), [www.fiercehealthit.com/story/cloud-computing-healthcare-question-not-if-when/2012-01-09].

The Department of Commerce Internet Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (December 2010), disponible en: [www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf].

The NIST Definition of Cloud Computing, [http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf].

Top Threats to Cloud Computing V1.0, Cloud Security Alliance (March 2010), disponible en: [https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

U.S. - E.U Safe Harbor Overview, EXPORT.GOV], [http://export.gov/safeharbor/eu/eg_main_018476.asp] (actualizado por última vez el 1 de Julio de 2013).

VMWARE, *Business Agility and the True Economics of Cloud Computing*, disponible en: [www.vmware.com/files/pdf/accelerate/VMware_Business_Agility_and_the_True_Economics_of_Cloud_Computing_White_Paper.pdf].

WEAVER, DIANE, *Six Advantages of Cloud Computing in Education*, PEARSON (Apr. 2013), [www.pearsonschoolsystems.com/blog/?p=1507].

With Cloud, SMBs Will Lead Emerging Economies Across the Digital Divide, CISCO (Sep. 2012), [www.cisco.com/web/about/ac79/docs/FastFacts/FastFacts_Cloud-and-Digital-Divide.pdf].

World Economic Forum, Exploring the Future of Cloud Computing: Riding the Next Wave of Technology-Driven Transformation (2010), disponible en: [www.weforum.org/pdf/ip/ittc/Exploring-the-future-of-cloud-computing.pdf].

Yao, Yuan et al., *Data Centers Power Reduction: A Two Time Scale Approach or Delay Tolerant Workloads* (2012), [www.eecs.berkeley.edu/~huang/data-center-power-infocom12.pdf].