BYOX constituye una tendencia a nivel mundial por la cual las empresas y organizaciones procuran regular el creciente uso de dispositivos móviles personales en ámbitos laborales

BYOX

Observatorio Jurídico

Esc. Dr. Gonzalo Sosa

BRING YOUR OWN …

Las estrategias *BYOD (Bring Your Own Device)* se constituyen en una tendencia a nivel mundial por la cual las empresas y organizaciones procuran regular el creciente uso de dispositivos móviles personales (celulares, tabletas, notebooks) en ámbitos laborales.

BYOD ha sido definido por Gartner como "*una estrategia alternativa que permite a los empleados, socios de negocios y otros usuarios, emplear dispositivos seleccionados y adquiridos personalmente para ejecutar aplicaciones de la empresa y acceder a información. Típicamente abarca celulares inteligentes y tabletas, pero la estrategia también puede ser usada para computadoras personales. Puede incluir un subsidio*."[1].

De la definición referida se desprenden algunas características de *BYOD*:

a) es una estrategia alternativa, enmarcada en consecuencia dentro de una decisión corporativa
b) refiere al uso de dispositivos personales de los empleados para el cumplimiento de sus tareas en el ámbito laboral
c) no se limita a celulares y tabletas
d) puede incluir subsidios

Las tendencias actuales muestran que el crecimiento en el uso de dispositivos móviles interconectados, y permanentemente conectados a internet -objeto también de estudio por parte del Observatorio Jurídico en el informe acerca de *IoT* (*Internet of Things*)- y la consideración de que ese uso en el ámbito laboral se constituye en un "derecho" de los individuos, hace inevitable la conjunción de cuestiones personales y laborales que deben compatibilizarse.

[1] Traducción por el informante. Versión en inglés disponible en http://www.gartner.com/it-glossary/?s=byod Consulta realizada el 30/10/2014.

Ello además plantea una serie de problemáticas vinculadas a la seguridad de la información -tanto personal como de la organización-, los alcances de las normas en materia de privacidad en dispositivos portables -analizado también por el Observatorio Jurídico en el informe sobre Privacidad Móvil-, las compensaciones eventuales por el uso de bienes propios de los empleados en beneficio de la organización o empresa, la compensación por trabajo fuera de horario, entre otros.

Adicionalmente a lo referido, las tendencias actuales también marcan una extensión natural de las estrategias *BYOD* a otros aspectos vinculados a la "portabilidad" que no se limitan a considerar sólo al dispositivo sino que también abarcan las aplicaciones que el mismo contiene, los espacios de almacenamiento empleados por el titular del dispositivo, las redes a las cuáles se conecta, y la tecnología empleada, entre otros.

Así, surgen las estrategias *BYOA (Bring Your Own Application), BYOC (Bring Your Own Cloud), BYON (Bring Your Own Network), BYOT (Bring Your Own Technology o Toolkit)*, cada una de las cuales procura enfocarse en algunos de los aspectos centrales vinculados al uso de los dispositivos móviles personales en el ámbito laboral. Todas ellas se han agrupado en el concepto de *BYOx*.

Señalan Seth EARLEY[2] y colaboradores que se está produciendo una tendencia hacia la "consumerization" (en español "tecnología orientada al consumidor") del ecosistema de servicios de TI, citando a Enrique Castro-León, quien afirma que la "t*ecnología orientada al consumidor*" ha traído una inversión de roles donde los usuarios son quienes imponen la adopción de tecnologías y el cambio. Aducen que ello se debe a una fuerza laboral más joven y adepta a nuevas tecnologías y aplicaciones. Estos nuevos empleados, según los autores, esperan usar sus dispositivos personales y sus aplicaciones en el trabajo, lo que

[2] Información disponible en "*From BYOD to BYOA, Phishing and Botnets*" en IT Pro. Setiembre/Octubre 2014. IEEE CS. Disponible en http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6908910 Consulta realizada el 17/10/2014.

se relaciona con el concepto *de BYOX (Bring Your Own Device, Cloud, App*, y *Network*), que además ha impactado notoriamente en los departamentos de TI que deben decidir cómo protegen sus redes y manejan tecnologías ajenas.

El diseño de estrategias no es de resorte exclusivo del sector privado sino también ha sido incluido en distintos programas gubernamentales en distintos países. El Gobierno de Queensland[3] en Australia, por ejemplo, y en concreto el *"Department of Education, Training and Employment"* creó una página destinada a la estrategia *BYOX* para la educación. Ha definido a la "X" incluida en *BYOX* como "*más que un dispositivo particular, ya que incluye además software, aplicaciones y servicios de conectividad y transmisión de datos"*. Se presenta por el Departamento citado además un completo informe sobre las perspectivas de BYOX en el sistema educacional de Queensland[4].

La multiplicación de estrategias asociadas a esta problemática ha dado lugar por otra parte a un conjunto de herramientas desarrolladas privadamente que tratan de solucionar aspectos puntuales de la gestión de los dispositivos, las aplicaciones, el almacenamiento *(MDM -Mobile Device Management-, MCM -Mobile Content Management-, MAM -Mobile Application Management-),* entre otras. Las diferencias entre unas y otras están en el grado de control que la organización o empresa posee sobre el contenido del dispositivo de sus empleados, lo que impacta en cuestiones de acceso a contenidos, performance, accesibilidad a la red, entre otras.

Las empresas han adoptado multiplicidad de estrategias, desde aquellas que aceptan y regulan el BYOD, hasta aquellas que lo prohíben. Otras han adoptado políticas COPE (Company-Owned, Personally Enabled), facilitándole a sus empleados los dispositivos móviles, y permitiendo su uso para fines laborales.

[3] Información disponible en https://byox.eq.edu.au/Pages/default.aspx Consulta realizada el. 21/10/2014.
[4] "BYOx research project. If you are serious!" Información disponible en https://byox.eq.edu.au/SiteCollectionDocuments/byox-project-research-report.pdf Consulta realizada el 20/10/2014.

Esto último según las predicciones realizadas ha sido una tendencia en el año 2014[5].

La Comisión Europea[6], en referencia al tema ha dicho que BYOD está rediseñando el mundo del trabajo, señalando que tanto expertos como analistas creen que no es una moda pasajera, y citando a Gartner sugieren que el 38% de las empresas esperan dejar de proveer dispositivos a sus trabajadores para el 2016.

No es difícil visualizar que esta tendencia pondrá en jaque el concepto de estrategia "alternativa" propuesta, desde que buena parte de las empresas empiezan entonces a ver la estrategia *BYOD* como la única a seguir.

Distintas organizaciones gubernamentales han comenzado a realizar recomendaciones y sugerencias para atacar esta cuestión.

Recientemente la *CESG*[7] *(National Technical Authority for Information Assurance)* del Reino Unido emitió -con la colaboración de distintos organismos- varias Guías para asegurar políticas exitosas de *BYOD*, incluyendo aspectos tales como privacidad, arquitectura, plataformas, redes, movilidad, entre otras.

En particular se señala por parte del organismo citado que a efectos de implementar una política de *BYOD* efectiva corresponde:

- Limitar la información compartida por los dispositivos.
- Considerar el uso de controles técnicos.
- Comprender las cuestiones legales, y dentro de ello anticipar el incremento en demandas de soporte de los aparatos y promover los acuerdos con el personal.

[5]Información disponible en http://h30499.www3.hp.com/t5/Infraestructura-Convergente-de/Qu%C3%A9-ser%C3%A1-del-BYOD-en-2014/ba-p/6339679#.VFJ0GDSG9uk Consulta realizada el 20/10/2014.
[6]Información disponible en http://ec.europa.eu/digital-agenda/futurium/en/content/bring-your-own-device-byo Consulta realizada el 20/10/2014.
[7]Información disponible en https://www.gov.uk/government/collections/bring-your-own-device-guidance Consulta realizada el 20/10/2014.

- Planificar por potenciales incidentes de seguridad, considerando además modelos de titularidad de dispositivos alternativos.

Estados Unidos por otra parte ha elaborado, a través del *"Digital Services Advisory Group"* y la *"Federal Chief Information Officers Council"* una Guía para promover la implementación de Programas *BYOD* en Agencias Federales. La misma no es obligatoria.

Según esta Guía[8], la tendencia en análisis refiere a proveer a los consumidores de opciones ("tecnología orientada al consumidor"), ofreciéndoles a los empleados una movilidad extendida y una mejor integración de sus vidas laborales y personales. También importa un necesario análisis de costo-beneficio ya que *BYOD* tiende a ser costo-efectivo. Finalmente, la implementación de un programa de *BYOD* presenta a las agencias una serie de desafíos de seguridad, políticos, técnicos y legales, respecto a los cuales hay tres formas de implementación:

- Virtualización: provisión de acceso remoto a recursos para que no se guarden ni procesen datos en dispositivos personales.
- Jardín vallado: guardado o procesamiento de datos en una aplicación segura en el dispositivo personal separado de los datos personales.
- Separación limitada: habilitar procesamiento de datos o guardado compartido de información de la empresa y personal en el dispositivo personal con políticas destinadas a asegurar controles mínimos.

También Estados Unidos ha seguido la tendencia de emplear estrategias BYOD en el ámbito de la educación, promoviendo el uso de dispositivos personales por parte de los estudiantes, y regulando el empleo de los mismos en el ámbito

[8]Información disponible en. http://www.whitehouse.gov/digitalgov/bring-your-own-device Consulta realizada el 21/10/2014.

escolar.[9]

Resulta interesante analizar la evolución de la opinión de los trabajadores respecto de las tendencias en análisis. Desde este punto de vista no se han encontrado a nivel nacional o latinoamericano estudios vinculados a la temática.

En Estados Unidos, la empresa FORTINET ha realizado dos encuestas -en los años 2012 y 2013. En la primera se encuestaron a más de 3.800 trabajadores de entre 20 y 32 años (Generación Y) en más de 15 países de Europa, Asia y Estados Unidos acerca de BYOD procurando evaluar el impacto de BYOD a nivel laboral y personal.

El estudio de 2012[10] revela que más del 55% de los encuestados entiende que usar sus dispositivos personales es un "Derecho laboral" más que un privilegio y más del 74% lo usa regularmente. También mostraba una tendencia preocupante derivada del hecho de que más de un 36% de los encuestados estaba dispuesto a romper las reglas de la empresa en caso de que se le prohibiera usar su propio dispositivo para fines laborales.

El estudio subsiguiente por la misma empresa llevado adelante en el año 2013[11], en 20 países y relevando las opiniones de más de 3.200 empleados de 21 a 32 años, muestra que el 51% de los empleados están dispuestos a romper las reglas de la empresa si se les prohíbe el uso de dispositivos personales con fines laborales. Asimismo, muestra que más del 89% de los empleados tiene una *cloud* personal, y más del 70% de este grupo confiesa haberla usado con fines laborales.

[9] Información disponible en http://www.k12blueprint.com/byod Consulta realizada el 17/10/2014.
[10]Disponible en http://www.fortinet.com/press_releases/120619.html. Consulta realizada el 21/10/2014.
[11]Disponible en http://www.fortinet.com/press_releases/2013/fortinet-global-survey-shows-employees-against-byod-policies.html. Consulta realizada el 20/10/2014.

Por otra parte, y en cuanto a la responsabilidad personal por la información contenida en el dispositivo, a diferencia de en la encuesta de 2012 en la que el 66% de los empleados entendían ser responsables por la seguridad -y el 22% hacían responsable al empleador-, en la encuesta de 2013 el 88% de los encuestados aceptaron su responsabilidad en la seguridad de sus propios dispositivos.

En consonancia con dichos estudios, ya la empresa FORRESTER RESEARCH[12] había encontrado que 53% de los empleados estaba usando su propia tecnología con propósitos laborales en el año 2012, lo que marcaba un 5% de incremento con respecto al mismo estudio realizado el año anterior.

ASPECTOS JURÍDICOS ASOCIADOS A ESTAS TENDENCIAS

Desde el Observatorio Jurídico se ha procurado monitorear cómo afectan las tendencias precitadas la relación laboral, considerado desde la perspectiva de:

a) la privacidad;

b) la seguridad;

c) el desarrollo de la tarea en sí.

Asimismo, debe tenerse presente los diferentes regímenes aplicables a empresas privadas y organismos públicos y a sus trabajadores, ya que las soluciones aplicables en un caso pueden no ser las mismas que las aplicables al otro.

Privacidad

La preocupación respecto a la privacidad y al tratamiento de los datos ha sido una constante en el caso de la implantación de estrategias BYOx. El problema se emparenta con la privacidad móvil, pero incluye otras aristas que deben ser

[12] Información disponible en https://www.forrester.com/home/ Consulta realizada el 22/10/2014.

consideradas, ya que no sólo se trata de información personal del titular del dispositivo sino también de información propiedad de la empresa. La forma de separar ambas, el tratamiento que se le da a una y a otra, la supresión de parte de la información en distintas hipótesis de cese del vínculo laboral, entre otras, son cuestiones a considerar y que no pueden ser soslayadas.

A este respecto, en el Uruguay el marco en materia de protección de datos -tanto de personas físicas como jurídicas- está dado por la Ley Nº 18.331 de 11 de agosto de 2014, modificativas, concordantes y reglamentarias. Esta Ley reconoce el derecho a la protección de datos como un derecho inherente a la persona humana, comprendido en el artículo 72 de la Constitución de la República (Art. 1º).

La cuestión en realidad depende de la alternativa que se adopte en cuanto a la política de provisión de dispositivos y a los mecanismos de almacenamiento de la información de la empresa en ese dispositivo o en la *"cloud".* Una solución alternativa que permitiría conjugar las necesidades de unos y otros es la de promover una política *BYOx* pero con una estrategia de virtualización de la información, evitando de esa manera el almacenamiento de información de la empresa en el dispositivo del trabajador.

En el ámbito de las organizaciones públicas, además, debe tenerse presente la Ley Nº 18.381 de 17 de octubre de 2008. Esta norma tiene por objeto promover la transparencia de la función administrativa de todo órgano público, estatal o no, así como garantizar el acceso de las personas a la información pública. Se define a esta última como toda aquella información que emane o esté en posesión de cualquier organismo público, estatal o no, con algunas excepciones (arts. 1º y 2º).

Finalmente, cabe mencionar la Ley Nº 19.179 de 27 de diciembre de 2013 que establece en su artículo 1º "*Los Poderes Ejecutivo, Legislativo y Judicial, los*

entes autónomos, los organismos descentralizados, las empresas donde el Estado posea mayoría accionaria, los Gobiernos Departamentales, las Juntas Departamentales, el Tribunal de lo Contencioso Administrativo, la Corte Electoral y los organismos de contralor del Estado, deberán distribuir toda información en al menos un formato abierto, estándar y libre. Todo pedido de información deberá ser aceptado en al menos un formato abierto y estándar".

Seguridad

También en este caso dependerá de la política que se adopte en cuanto a la forma de gestionar los dispositivos, las aplicaciones y el almacenamiento. Nuevamente, la política de la empresa puede llevar a emplear mecanismos como el MDM, MAM o MCM a fin de proveer niveles de seguridad más o menos aceptables, siempre evaluando en el caso concreto cómo ello puede afectar la performance de los dispositivos y la disponibilidad de recursos en cuestiones de soporte de los mismos.

A nivel público, la seguridad por la información de la Administración es un tema recurrente, y que ha sido considerado en varias normas como la Ley Nº 18.046 de 17 de octubre de 2006, la Ley Nº 18.362 de 6 de octubre de 2008 y el Decreto Nº 452/009 de 28 de setiembre de 2009, poniendo de cargo de los órganos del Estado el empleo de políticas en materia de seguridad de la información definidas por los órganos competentes (en el caso Cert-Uy). Esas políticas deben ser consideradas también al momento de emplear estrategias BYOD en el Estado.

El desarrollo de las tareas laborales

La vinculación con el tema de "Internet de las cosas" es también en este punto innegable, dada la proliferación y las perspectivas a futuro en cuanto a la cantidad de dispositivos interconectados por persona a nivel global.

Con respecto al empleo de dispositivos y tecnologías personales en la práctica tanto empresas como organizaciones públicas, han optado por proveer a sus empleados y funcionarios de dispositivos adquiridos por la propia empresa u organización, los cuáles deben destinarse en mayor o menor medida a la actividad laboral. De los relevamientos realizados y la jurisprudencia analizada en el punto no surgen otras soluciones diferentes a la planteada.

El uso de dispositivos personales para el cumplimiento de las tareas laborales importa, además de la definición como política de la empresa luego del análisis de aspectos vinculados a la seguridad y privacidad de la información, la determinación de quién asumirá los costos derivados de ese uso, y qué mecanismos se emplearán para cuantificarlos.

Un reciente fallo de la Corte de Apelaciones de California, en el caso *Colin Cochran v. Schwan´s Home Service, Inc*[13]*.* determinó que si los empleados debían usar sus dispositivos personales para realizar llamadas laborales, entonces necesariamente debían ser compensados por ese uso. Lo que la Corte no determinó son los parámetros para la fijación de esa compensación. Este fallo no sólo es relevante por referir al reembolso por llamadas, sino también por sus potenciales implicancias derivadas de los costos por el uso de "clouds" personales o servicios de transmisión de datos o conectividad.

En Uruguay no existen normas -o en su caso antecedentes judiciales- que refieran a la cuestión en estudio, ya que como se explicó previamente, actualmente las políticas de las empresas no están orientadas hacia las estrategias BYOx.

[13] El fallo está disponible en http://www.courts.ca.gov/opinions/documents/B247160.PDF. Consulta realizada el 21/10/2014.

Sin perjuicio de ello, a nivel estatal debe tenerse presente el marco regulatorio de la función pública, y en particular la Ley Nº 19.121 de 20 de agosto de 2013, que en su artículo 29 impone, dentro de la enumeración de deberes y obligaciones de los funcionarios públicos, la de respetar y cumplir la Constitución de la República, las leyes y disposiciones reglamentarias, así como mantener la reserva sobre asuntos e informaciones conocidos en razón de su función, aún después de haber cesado en la relación funcional.

De ello se desprende en consecuencia que en la gestión de la información y datos de la organización a través de dispositivos, “clouds”, tecnologías, etc., personales, los funcionarios deben también cumplir con los deberes funcionales impuestos y considerar las incompatibilidades referidas en la norma mencionada.

CONCLUSIONES

Puede concluirse entonces de las tendencias analizadas que:

a) La proliferación de dispositivos móviles[14] y su empleo en el ámbito laboral es indiscutible e inevitable.
b) Las empresas ya cuentan en buena parte del mundo con políticas BYOD y emplean desarrollos informáticos necesarios para asegurar la privacidad y seguridad en la información de la empresa gestionada a través de dichos dispositivos.
c) Varios Estados han comenzado a tomar en cuenta esta tendencia proponiendo distintas guías o modelos para la aplicación de estrategias exitosas en la materia.

[14] En Uruguay la última Encuesta de uso de tecnologías "EUTIC 2013" muestra que el 83% de la población ha usado un celular y el 25,8% del total de la población urbana emplea teléfonos inteligentes. Además, un tercio del total de usuarios de celulares lo usan para navegar por internet y acceder a redes sociales. Los resultados globales de la encuesta están accesibles en: http://www.agesic.gub.uy/innovaportal/file/4263/1/principales_resultados_eutic_2013.pdf. Consulta realizada el 01/11/2014.

d) Parece conveniente relevar la inserción de estas estrategias en el ámbito laboral uruguayo con el apoyo del Observatorio de la Ciudadanía y generar una Guía con información sobre las tendencias y cuestiones a considerar en los aspectos mencionados, con el apoyo del Observatorio Tecnológico.