# Seguridad y regulación en servicios tipo Máquina-Máquina (eCall, eHealth)

Giuseppe Roa
$TL\ddot{O}N$ (Grupo de investigación
en redes detelecomunicaciones dinámicas y
lenguajes de programación distribuidos
Universidad Nacional de Colombia
Bogotá, Colombia
groao@unal.edu.co

Jorge Eduardo Ortiz
$TL\ddot{O}N$ (Grupo de investigación
en redes detelecomunicaciones dinámicas y
lenguajes de programación distribuidos
Universidad Nacional de Colombia
Bogotá, Colombia
jeortizt@unal.edu.co

## ABSTRACT

Los significativos avances en redes de telecomunicaciones junto con el desarrollo de hardware más potente y económico han permitido considerar como una realidad la masificación de la interconexión entre todo tipo de dispositivos lo cual cambiaría radicalmente las reglas de juego en los mercados e incluso las dinámicas de la sociedad. En este paper se realiza una breve revisión del estado del arte en cuanto a generalidades, aplicaciones, desafíos y principales riesgos que ocasionaría la universalidad del "'Internet de las Cosas"' en términos de seguridad y regulación. Adicionalmente, se proponen recomendaciones regulatorias para que el gobierno Colombiano pueda asegurar privacidad en los nuevos escenarios a los que se enfrentarían los ciudadanos en un mundo con un nivel de interconectividad sin precedentes.

## Keywords

Machine-to-machine, Internet of Things, regulación, ubicuidad, eCall, eHealth, privacidad, operadores móviles.

## 1. INTRODUCTION

El exitoso despliegue de redes inalámbricas tales como Wifi y redes celulares han desencadenado que múltiples tecnologías y aplicaciones sean ahora posibles gracias a las velocidades de transferencia de información y los alcances de cobertura sin precedentes. Entre los nuevos paradigmas que podrían convertirse en realidad se destaca notablemente las comunicaciones máquina-máquina, eje fundamental del popular Internet de las cosas ó *Internet of Things* (IoT).

Pese a que el concepto no es nuevo y que ya existen desarrollos funcionales en industrias específicas, ciertas características en varios flancos hacen viable que IoT sea una realidad [1]: El mercado posee un importante potencial para masificar de manera eficaz y rápida los desarrollos producto de trabajos de innovación. Innovaciones técnicas con respecto al incremento en la capacidad de cómputo de los dispositivos así como la miniaturización y el decremento en el precio de sensores y otros tipos de hardware que permitirían dar "'inteligencia"' a una gran cantidad de objetos cotidianos[2].

La aplicación y masificación de IoT tendría un impacto trascendental en la sociedad y podría representar una importante ventaja competitiva con la que las naciones podrían acelerar su desarrollo.[3]. Estudios actuales evidencian cómo paulatinamente dispositivos distintos a *smartphones* y *laptops* empiezan a tomar partida en el acceso a recursos de Internet y cómo se espera que las diversas tecnologías existentes y emergentes harán frente a los nuevos retos[4].

Entre los servicios más prometederores se destacan $eHealth$ y $eCall$, que a grandes rasgos ofrecerían nuevos mecanismos para que comunidades remotas puedan acceder a servicios de salud de calidad y contar con sistemas de reacción eficaces ante emergencias, tal y como accidentes automovilísticos.

Aunque el IoT ha generado gran expectativa gracias a las importantes funcionalidades que prestaría a la sociedad en general, también ha despertado la preocupación de múltiples sectores que consideran que la privacidad de los ciudadanos así como la confidencialidad empresarial podrían ser fácilmente vulneradas por gobiernos o compañías privadas que puedan acceder al sin fin de información censada por los nuevos dispositivos interconectados a Internet. Frente a esto la regulación regional debe hacer fuerte hincapié en identificar los aspectos que deben ser protegidos en toda implementación que se pueda llevar a cabo en los años venideros.

La continuación de este paper esta estructurada de la siguiente manera. En la sección II se presenta una breve revisión del estado del arte, ciertas generalidades de las comunicaciones tipo *machine to machine* (M2M) y potenciales aplicaciones. Enseguida, en la sección III, se plantea la metodología a seguir. La sección IV está dedicada a analizar los principales riesgos en cuanto a seguridad y privacidad a los que se enfrentaran la sociedad en una posible universalización de IoT. En la sección V se construye un diagnóstico de las principales medidas regulatorias a nivel global referentes a las comunicaciones M2M en especial en torno a los servicios eCall eHealth. En la sección VI se entabla una discusión sobre las principales recomendaciones que el estado Colombiano debería seguir para afrontar los nuevos panoramas posibles. Finalmente en la sección VII se establecen las conclusiones y se enuncian ciertas direcciones en las que se podrían encaminar trabajos futuros.

## 2. ESTADO DEL ARTE

Las comunicaciones tipo M2M se han convertido progresi-

vamente en una realidad, principalmente por la evolución de tecnologías económicas emergentes como los módulos RFID (Radio Frequency Identity) ó los protocolos de comunicación inalámbricas Zigbee, Bluethooth que con el tiempo han logrado otorgar a los dispositivos la capacidad de censar, monitorear, procesar información e incluso interactuar con el ambiente o con otros dispositivos[5]. En la actualidad, existen en el mercado soluciones económicas y eficientes que serían el punto de partida para una masificación de dispositivos inteligentes y capaces de comunicarse con su entorno; sin embargo grandes retos técnicos aún deben ser afrontados si se pretende llegar a un IoT generalizado.

En primera instancia, las redes de comunicaciones móviles actuales están orientadas a comunicaciones tipo humano - humano, lo que representa el primer gran cambio de paradigma puesto que en el IoT el panorama sería muy distinto, con millones de dispositivos intentando acceder simultáneamente a recursos para compartir su información en la red llegando a unos niveles de congestión de acceso que con las tecnologías actuales no podrían afrontarse.

La naturaleza de la información también cambiaría puesto que una gran proporción consistiría en pequeños paquetes de datos producto de mediciones del entorno[6]. En este sentido, podría existir mucha información redundante, razón por la cual se requeriría de mecanismos para "'otorgar significado"' a la inmensidad de datos disponibles.[6]

Frente a esta inmensidad de dispositivos identificar exactamente "'a quién"' va dirigida la información implica un sistema unificado de identificación global que de capacidad para reconocer millones de objetos sin inconvenientes. Actualmente Internet se basa en la arquitectura TCP/IP que debido al crecimiento en el número de nodos a identificar debió evolucionar de IPv4 a IPv6 aumentando las direcciones disponibles. No obstante, TCP presenta un inconveniente debido a la cantidad de información requerida para la señalización de los segmentos intercambiados ya que, como previamente se mencionó, la cantidad de información en muchos casos serían segmentos simples de datos que no justificarían grandes cantidades de datos reservados para direccionar la información.

El siguiente gran reto hace referencia a la plataforma de comunicación que se requeriría para que dispositivos de todo tipo y de cualquier fabricante puedan intercambiar información sin inconveniente alguno[7]. En la actualidad existen aplicaciones funcionales que emplean plataformas de comunicación propias al sector específico en el que funcionan, lo que se traduce en una alta segmentación del mercado que requiere soluciones horizontales.

El mercado de aplicaciones que emplean comunicaciones M2M ha sido fuertemente influenciado por ciertas industrias que han identificado a esta tecnología como un mecanismo interesante para aumentar la eficiencia en los múltiples procesos que se llevan a cabo en cada uno de sus dominios. Las ventajas obtenidas han impulsado a que ciertos gobiernos encuentren en estas tecnologías soluciones eficientes para diversas problemáticas. Enseguida se mencionan brevemente los principales campos en los que se han identificado potenciales aplicaciones[8].

## 2.1 Aplicaciones industriales

### *2.1.1 Logística*

Una de las principales aplicaciones consiste en la optimización y el constante monitoreo de las cadenas de producción al interior de las fábricas y posteriormente la distribución de los lotes de producción. Actualmente ciertas industrias emplean RFID para etiquetar materiales al inicio de la producción y combinados con sistemas de control tipo SCADA ejercen un seguimiento y monitoreo constante durante todo el ciclo de producción, identificando las etapas más ineficientes [9]. Estos beneficios se reflejarían también en la agricultura aprovechando adicionalmente análisis medioambientales y de mercados para que el agricultor tome decisiones más inteligentes con sus cultivos.

### *2.1.2 Smart Grids*

Uno de los ejemplos más plausibles y objeto de gran inversión principalmente en USA y la Unión Europea son las denominadas "'Smart Grids"' o redes de distribución eléctrica inteligentes que aprovechan información aportada por diversos nodos pertenecientes a la red para determinar la manera más eficiente de producir, distribuir y consumir la energía eléctrica con el fin de hacer frente a problemáticas como el calentamiento global.

### *2.1.3 Building automation*

Un importante salto en la domótica tendría lugar gracias a la intervención de refrigeradores, sistemas de calefacción, hornos, sistemas de iluminación y cualquier objeto casero interconectado y con capacidad de decisión que mantenga constante comunicación con los habitantes de las viviendas y procure optimización del consumo energético y alerte sobre posibles requerimientos de mantenimiento o problemas de seguridad.

### *2.1.4 Entretenimiento*

La creciente demanda de servicios multimédia evidencia el gran potencial que tendría conectar objetos de la cotidianidad, principalmente vehículos, a servicios de entretenimiento en línea[8] Una posible aplicación conocida como "*Pay as you Drive*" permitiría a los conductores acceder en tiempo real a contenidos multimédia de su predilección a su vez que podrían pagar cuentas pendientes de servicios públicos ó renovar seguros vehiculares. Los pronósticos apuntan a que *wearables* tal y como el *smarthwatch* de Apple se convertirán en importantes medios de acceso a servicios de entretenimiento en línea.

## 2.2 Sector público

### *2.2.1 Smart cities*

La automatización de las ciudades especialmente para atacar los problemas de movilidad representan una oportunidad muy atractiva para los gobiernos locales que con medidas tradicionales no han logrado descongestionar las principales ciudades. En este ámbito existen propuestas como la instalación de señales de tránsito inteligentes que cambien de acuerdo a los contratiempos que ocurran en las vías y que combinados con semaforización dinámica enruten el tránsito de tal manera que se aprovechen más eficientemente las vías y la velocidad promedio aumente. Así mismo, existiría interoperatividad con los sistemas de transporte público dándole prioridad en las zonas de mayor congestión. Otras iniciativas hacen alusión a la instalación de sensores inteligentes que alerten a las autoridades en caso de detectar sustancias o potenciales peligros para la seguridad pública.

### 2.2.2 eCall

El servicio de *eCall* consiste básicamente en un tipo de "'caja negra"' instalada en los vehículos para que en caso de accidente se comuniquen automáticamente con el servicio de emergencia para suministrar información de ubicación y gravedad del incidente para así poder prestar eficientemente atención a los involucrados. El servicio de *eCall* es en realidad una iniciativa de ciertas casas automotrices que ya disponen del servicio para ciertos modelos, sin embargo dado el fuerte impacto que tendría sobre la seguridad civil múltiples gobiernos, como el caso de la Unión Europea, se encuentran trabajando en proyectos para universalizar este servicio en sus territorios asegurando además prioridad en los canales de comunicación de operadores móviles que emplearían para establecer las conexiones.

Sin embargo, los alcances de este servicio podrían ser mucho mayores si se adoptara como política gubernamental. En Colombia existen muchas zonas vulnerables a desastres naturales, con altos niveles de sismicidad, frecuentes inundaciones, deslizamientos, entre otros. Pese a que existen ciertos desarrollos que censan variables, tal como el nivel del agua en quebradas o riachuelos, son desarrollos aislados, cuya información no es difundida más allá de las comunidades locales.

Con *eCall*, redes de sensores inteligentes, intercomunicados con los sistemas de emergencia a nivel nacional junto con sistemas de difusión, podría representar un valioso ahorro de tiempo en el despliegue de recursos para atención a la calamidad y evacuaciones en zonas que podrían ser potencialmente afectadas.

### 2.2.3 eHealth

Los avances en telemetría combinados con dispositivos que empleen tecnologías alternativas de bajo consumo energético y alta fidelidad [10] permitirían el monitoreo remoto del estado de salud de pacientes evitando viajes innecesarios a centros hospitalarios otorgando, por ejemplo, mayor independencia a personas mayores. En esta categoría también se destacan sistemas orientados al seguimiento de deportistas con el fin de reprogramar rutinas de ejercicio.

En una escala mas global *eHealth* podría ser empleado para dar acceso a sistemas de salud a múltiples comunidades remotas en las que se carezca de especialistas. En Colombia se han hecho importantes avances para lograr interconectar, por medio de fibra óptica, cientos de corregimientos alejados de las grandes urbes, con lo cual ya se contaría con acceso a la red, primer elemento estructural requerido.

En una primera etapa la gran fortaleza de *eHealth* se centraría en el diagnostico y el seguimiento de pacientes con patologías específicas. En principio, existirían retos importantes en los sistemas de información que soporten el intercambio de información producto del monitoreo de los pacientes. En una etapa de mayor madurez tecnológica se podrían implementar centros especializados donde se ejecuten tratamientos o intervenciones de baja complejidad tele-dirigidos.

## 3. METODOLOGÍA

Este estudio esta estructurado según un método de análisis-síntesis. En primera instancia, se realiza una revisión y análisis de las potenciales vulnerabilidades a las que se enfrentarían los usuarios que cuenten con dispositivos inteligentes capaces de realizar comunicaciones tipo M2M. A continuación se construye un diagnóstico de las principales medidas regulatorias en el mundo entorno al IoT. Finalmente se efectúa un contraste entre los desarrollos existentes y las políticas implementadas poniendo en evidencia las principales discrepancias para luego centrar la discusión y sintetizar la principales recomendaciones que deberían ser tenidas en cuenta en Colombia a la hora de desarrollar políticas públicas relacionadas con el área.

## 4. RIESGOS EN SEGURIDAD Y PRIVACIDAD

En la literatura se acepta la seguridad de la información como la prevención del acceso no autorizado, el uso, la divulgación, la interrupción, la modificación, la inspección, el registro o la destrucción de información[11]. El concepto se fundamenta en seis pilares que dan sentido a los sistemas de información robustos[12]:

**Confidencialidad** asegura que solo las partes autorizadas sean capaces de entender la información; **Autenticación** habilidad para asegurar que una parte reciba la información de la fuente que solicita; **Integridad** asegura que un mensaje no es alterado durante la transmisión; **No repudiación** asegura que ni el transmisor ni el receptor nieguen el mensaje que ha sido enviado/recibido satisfactoriamente; **Disponibilidad** provee medios para asegurar que el sistema se encontrara disponible cuando sea necesario; **Autorización** habilidad para restringir y controlar acceso al sistema de información

En principio, debido a la naturaleza de las conexiones M2M altamente distribuidas, múltiples vulnerabilidades como la suplantación de identidad, clonación de autentificaciones, software adulterado, irregularidades en la configuración de los dispositivos así como ataques directos al core de la red [13] podrían ser objetivo inminente para que entes maliciosos accedan a información útil para fines privados.

En áreas públicas cientos de objetos interconectados podrían ser aprovechados para una vigilancia de masas constante así como el seguimiento y la trazabilidad del movimiento de los usuarios. Muchas entidades podrán colectar información de usuarios sin que estos se percaten para venderla a terceros y así hacer inferencia de comportamientos futuros.

En aplicaciones de *eHealth*, por ejemplo, sería posible identificar a pacientes con VIH lo cual podría ser blanco de empresas farmacéuticas para ofrecer tratamientos e incluso, en manos indebidas, esta información podría ser divulgada desencadenando discriminaciones sociales. La privacidad de usuarios podría ser seriamente afectada gracias a políticas débiles que no restrinjan la manera como se blindan las conexiones y a su vez la manera como es empleada la información colectada.

En la actualidad, existe una importante penetración en el mercado de dispositivos inteligentes diferentes a smarthphones tal y como lo reporta eMarketer (figura [1]). En este reporte cerca del 27% de usuarios que mencionaron no tener dispositivos inteligentes se refirieron al temor de que su privacidad fuera vulnerada o que cierta información personal fuera empleada por terceros, como su principal causa para

[1]Privacy: The Next Big Smart-Device Topic?. Disponible en: `http://www.emarketer.com/Article/Privacy-Next-Big-Smart-Device-Topic/1011822`

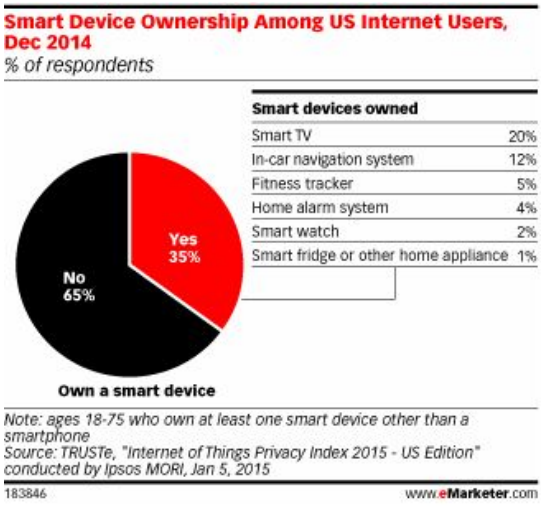


**Figure 1: Propiedad de dispositivos inteligentes entre internautas de Estados Unidos.**[1]

no adquirir estos productos.

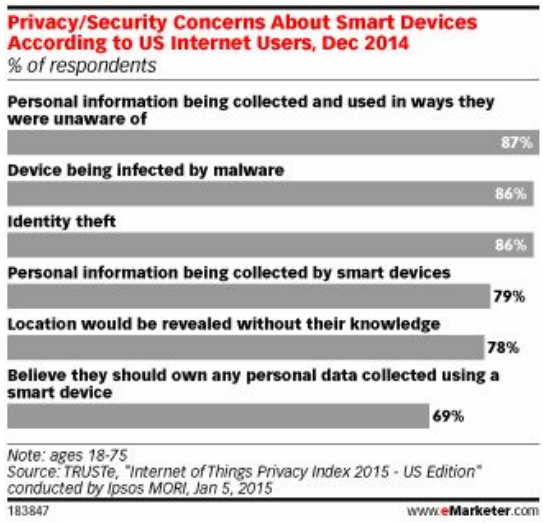


**Figure 2: Cuestiones de privacida entorno a los dispositivos inteligentes.**[2]

En la figura [2] se ilustra los principales temores referentes a privacidad y seguridad de aquellos usuarios que cuentan con dispositivos inteligentes. En este reporte es evidente que existe preocupación sobre las vulnerabilidades informáticas que tienen los nuevos dispositivos. La principal preocupación recae en el potencial uso y colección inadvertida de la información. En [14] se describen las categorías de ataques informáticos que pondrían en riesgo la privacidad de los usuarios:

- **Información de primera mano**: En esta categoría el atacante obtiene la información directamente del usuario. Aunque el usuario nunca desee revelar su información, problemas intrínsecos de seguridad en las aplicaciones o dispositivos que emplea pueden dar origen a "fugas de datos". Las *cookies* almacenadas en los exploradores pueden ser blanco de terceros para identificar los comportamientos de búsqueda e incluso contraseñas. Una tendencia cada vez más frecuente son las "trampas" en redes sociales ó sistemas de mensajería en los que los usuarios terminan develando datos claves.

- **Murmullos**: Ocurre cuando la información de un usuario almacenada en alguna entidad es trasmitida a otra sin la previa autorización. Esta modalidad ya ocurre en múltiples aplicaciones que venden la información relacionada con las tendencias de consumo de usuarios.

- **Observación**: Una de las grandes características del IoT es observar y censar el ambiente en tiempo real intercambiando información automáticamente sin la necesidad de intervención humana. Información concerniente a la ubicación geográfica, hábitos, gustos sería empleada por los dispositivos para los fines para los cuales fueron desarrollados; sin embargo, el mayor inconveniente ocurriría si los dispositivos almacenaran esta información ya que la comunicación entre los mismos dispositivos podría ser un blanco sensible para obtener información.

- **Interferencia**: En este mecanismo se desarrollan "mapas" que reflejan las actividades, comportamientos de consumo y otros patrones de movilidad a partir de cierta información colectada. Estudios como el presentado en [15] evidencian cómo es posible, a partir de modelos probabilistas que se alimentan de información relativa a patrones de movilidad, determinar la identidad de una persona en un grupo específico de usuarios que emplean un esquema de seudónimos en el sistema de localización interna de un laboratorio. En el IoT la ubicación sería un dato de fácil acceso, que complementado con todo tipo de información colectada por el resto de dispositivos interconectados que convivirían en la cotidianidad podría dar lugar a que los ataques por interferencia fueran muy comunes y sus resultados muy precisos.

## 5. POLÍTICAS PÚBLICAS PARA EL IOT

Las discusiones de privacidad deben ser sensitivas ante el impacto cultural, las normas y el ambiente antes de aplicar conceptos universales. En países con ingresos menores, la política de privacidad se ve como un lujo que es relegado a un segundo plano debido a la presión de sectores económicos particulares[16]. El desarrollo de políticas evidencia una madurez gubernamental para atender las demandas de la sociedad de la información.

Países donde los esfuerzos por la protección de la privacidad son muy pobres harán más vulnerable a la población con la introducción de servicios tipo M2M, puesto que se debería recurrir a tecnologías dedicadas a blindar las conexiones lo que se traduciría en sobrecostos. Sin embargo, al no ser exigidos por ley, en muchos casos estos sobrecostos serían obviados por los operadores del servicio convirtiéndose en blancos potenciales para piratas informáticos.

En países en vía de desarrollo es común adoptar políticas de potencias establecidas. Esta práctica puede considerarse

[2]Privacy: The Next Big Smart-Device Topic?. Disponible en: `http://www.emarketer.com/Article/Privacy-Next-Big-Smart-Device-Topic/1011822`

acertada si las condiciones de contexto son muy similares a las presentes en la región en la que se pretendan instaurar. A modo de ejemplo mucha de la regulación existente en privacidad informática se desarrolló cuando la computación era jerárquica y centralizada. Los cambios hacia una computación distribuida hacen que el manejo y el seguimiento de la información de los usuarios pueda significar un potencial riesgo que no esta considerado en los articulados difundidos y aceptados.

Existen gobiernos que han prestado fuerte interés en el desarrollo e implementación a gran escala de servicios tipo M2M (*eCall*, *eHealth*) por lo cual ya cuentan con importantes avances en temas regulatorios. El primer ejemplo se remonta a la comisión europea que ha liderado el macroproyecto *eCall* en toda la Unión Europea que aseguraría su implementación total para finales del 2017. El sistema está basado en mensajería tipo sms generada en "cajas negras" instaladas en todos los modelos recientes de automóviles que junto a un sistema de sensores realice llamadas a la línea de emergencia en caso de un accidente, permitiendo la transmisión efectiva de datos, tales como coordenadas y estado de los ocupantes o el automotor, hacia un sistema público de respuesta inmediata o agencias de emergencias locales mediante los canales de voz de las redes conmutadas públicas.

La comisión europea ya ha definido el primer borrador con los principales aspectos regulatorios para asegurar el despliegue de una infraestructura pública interoperable a lo largo de la EU[17][18]. Con respecto a temas de seguridad se especifica que el sistema sería un sistema durmiente en el que no existiría ningún intercambio de información a menos que ocurriera un evento que active los múltiples sensores en el vehículo o sea activado manualmente por el usuario con lo cual no existiría trazabilidad mientras no exista una emergencia. El sistema debe notificar al usuario con claridad los mecanismos empleados para difundir su información en caso de accidente además de mencionar que la referencia legal en la que trabajaría *eCall*.

La protección de datos estará acorde a las regulaciones previas en la EU[19] en las que se especifica que ni los operadores ni los prestadores de servicio podrán difundir o almacenar la información colectada por el sistema. Los centros que atiendan las llamadas de emergencia (PSAPS) solo almacenaran temporalmente los datos correspondientes durante un periodo finito de tiempo mientras la emergencia es atendida. La información que llegara a ser colectada no podría ser procesada si existe el riesgo de interferir en cualquier medida con las libertades de expresión, desarrollo personal, privacidad, conducta empresarial, propiedad intelectual o cualquier otra especificada en el articulado. En los casos que requieran procesar información personal (e.g seguridad nacional) debe existir una notificación a los entes reguladores.

La regulación existente en *eHealth* hace referencia a aspectos generales como la notificación clara al paciente de qué datos han sido colectados de su parte, el procesamiento de esta información con el consentimiento del paciente para que el mismo u otras personas con patologías similares puedan resultar beneficiadas, la confidencialidad en los datos puesto que son susceptibles a exclusión social y estigma si los diagnósticos son publicados. En aplicaciones de *eHealth* la principal ventaja es llegar a lugares remotos, en este contexto el roaming es un aspecto clave para la interoperabilidad en las redes y la cobertura nacional [16] [20].

En el más reciente reporte del programa eHSA de África [21] se identifican los marcos regulatorios mas avanzados en términos de buenas prácticas orientadas a la masificación de servicios eHealth en el que se destacan cinco puntos fundamentales:

**Identificación y autenticación**: Cada gobierno debe desarrollar un régimen unificado para la identificación de los entes pueden tener acceso a la información medica compilada.

**Protección y privacidad de la información**: Existencia de sistemas robustos y unificados que aseguren el acceso, la fiabilidad y la seguridad de la información medica antes potenciales riesgos de infiltración.

**Sistemas nacionales de estándares sobre eHealth**: Con esto los datos médicos pueden ser consistentemente almacenados e intercambiados para fines adecuados.

**Inversión en infraestructuras TIC**: Fuertes desarrollos en equipos electrónicos que aseguren la integridad del paciente en todos los procedimientos o monitoreos que se lleven a cabo, así como la precisión y confiabilidad en la transmisión de los datos médicos.

**Servicios nacionales de banda ancha**: Colaboración conjunta de entidades privadas y gubernamentales para alcanzar conectividad de calidad en los lugares más remotos de los territorios nacionales.

En Colombia la estructura regulatoria en telecomunicaciones presenta un atraso en términos de seguridad de la información y protección de la privacidad de los ciudadanos. Las medidas existentes velan por asegurar la competencia en los mercados existentes, ampliar la infraestructura, realizar un uso eficiente del espectro radioeléctrico y velar por la universalidad del servicio[22]. Existen medidas, como la aceptación de IPv6 como nuevo estándar para el direccionamiento en Internet ó la exigencia de Roaming Nacional a los operadores móviles que empiezan a asegurar un contexto para la viabilidad de servicios como *eHealth*, sin embargo para el gobierno nacional el IoT es todavía una ficción y por ende los potenciales riesgos aún no son tenidos en cuenta.

# 6. FORMULACIÓN DE RECOMENDACIONES

Es evidente que el nuevo nivel de interconectividad que se pretende alcanzar con el IoT cambiaría los paradigmas en cuanto a la manera como las ciudades operan, las industrias producen e incluso la manera como vive el ser humano. Los gobiernos, en su deber de velar por el beneficio de sus ciudadanos, tendrán que enfrentarse a diversas incógnitas como ¿Se debería garantizar acceso universal a servicios como *eCall* o *eHealth*? ¿Sería ético realizar vigilancia de masas con el fin de asegurar la protección de la misma ciudadanía y del patrimonio material? ¿Cómo asegurar la anonimidad de los usuarios y evitar fugas de información que puedan ser aprovechadas por entes maliciosos?[23]

El primer punto susceptible de regulación es el licenciamiento del espectro radioeléctrico. El desarrollo de nuevos servicios tipo M2M requerirá de condiciones aptas para su normal funcionamiento, como se espera que posean una larga vida útil se debe asegurar que exista espectro disponible para que los servicios puedan ejecutarse. Al masificarse este tipo de servicios en una banda no licenciada se incrementan la probabilidades de que terceros puedan interferir y acceder directamente a los canales transporte; no obstante, obligar a que los servicios se ejecuten en bandas licencias ocasionaría

un impacto negativo en el desarrollo de nuevas iniciativas en esta área en especial en pequeñas y medianas organizaciones que no cuenten con los recursos para acceder a las subastas correspondientes. Por lo tanto, *la ANE debería definir bandas dedicadas a servicios M2M y disponer los mecanismos necesarios para que pequeños competidores puedan acceder al licenciamiento de segmentos del espectro correspondiente.*

Un punto clave es la estandarización del direccionamiento que debería ser implementada para asegurar la diferenciación global de cada dispositivo que acceda a la red. Este direccionamiento único presenta potenciales inconvenientes para la privacidad del usuario final. *Los entes reguladores deberían exigir mecanismo robustos para el enrutamiento de información en la que se empleen esquemas de seudónimos entre ciertas etapas del transporte de la información para disminuir las probabilidades de identificación del cliente final.* Esta técnica es susceptible a métodos de computación persuasiva, sin embargo si se acompaña con estrictas medidas de protección de información de subscriptores en las bases de datos de los operadores de estos servicios se podría hacer frente a las métodos computacionales existentes.

El usuario final debe tener la capacidad para definir qué organizaciones pueden emplear su información por lo cual *Colombia debería disponer mecanismos para que los ciudadanos puedan regir la disponibilidad de su información clínica y debería existir el "derecho al olvido" con los cual el usuario podría definir si erradicar de manera definitiva su historial clínico en todas las bases de datos en las que sea almacenada.*

La discusión toma más matices si se argumenta que mediante un seguimiento masivo de la evolución de pacientes con determinada enfermedad se podrían obtener datos valiosos que conducirían a potenciales tratamientos. Según las recomendaciones de la OECD [3] "la clave reside en que los gobiernos identifiquen los ambientes en los cuales la información debería ser colectada para fomentar el beneficio colectivo y en esta medida dictaminar las regulaciones correspondientes". *La CRC debería determinar los casos y las entidades que pueden disponer de la información colectada masivamente por usuarios M2M con fines investigativos asegurándose que el usuario siempre sea notificado de que su información podría ser usada para estos fines.*

Bajo el marco de proyectos bandera como *Vive Digital*[24], la promoción del desarrollo de contenidos y aplicaciones podría estar orientado al desarrollo de plataformas y sistemas de información especializados en soportar sistemas de telemedicina y atención de emergencias distribuidas. *El gobierno colombiano debería promover campañas que incentiven la incursión en el desarrollo de plataformas y sistemas de información que soporten servicios M2M*

Con el fin de implementar eficazmente sistemas tipo eCall *el estado colombiano debería exigir a los operadores móviles la asignación de canales de conexión prioritarios, de tal manera que si un servicio requiere acceder a la red no posea problemas de acceso. Adicionalmente los operadores deberían proveer de información georeferencial que permita determinar con mayor exactitud la ubicación de los dispositivos que hagan uso del servicio.*

*En Colombia se debería implementar un articulado semejante al 95/46/EC presente en Europa, en el que se definan las características de la protección de los derechos individuales en torno al procesamiento de la información personal y el libre movimiento de dicha información entre los distintos entes involucrados, ajustándolo al nuevo contexto que implica desarrollos como cloud computing, ubicuidad computacional, procesamiento distribuido, identificación universal y seguimiento geográfico.*

# 7. CONCLUSIONES Y TRABAJO FUTURO

El IoT se esta posicionando como una tecnología que generara un gran impacto en las dinámicas sociales, al punto de poner en riesgo libertades individuales como la privacidad. En este sentido, las medidas regulatorias son un requerimiento fundamental para generar el contexto adecuado y proteger a los ciudadanos.

Servicios como *eCall* ó *eHealth* exponen las grandes prestaciones que los desarrollos basados en comunicaciones M2M ofrecerían a la sociedad. No obstante, ponen en evidencia la fragilidad y la obsolescencia de múltiples articulados desarrollados en torno a la seguridad de la información.

La implementación de un marco regulatorio consistente sobre la privacidad en aplicaciones tipo M2M a nivel global y sobre todo es países en vía de desarrollo se divisa como un cambio a largo término mientras los gobiernos se concientizan sobre los nuevos retos y cambios que poseerá una sociedad totalmente interconectada.

El establecimiento de regulación coherente y ajustada a las necesidades del país es el primer paso para que Colombia pueda incursionar en el mercado del desarrollo de servicios orientados al IoT. Futuros trabajos podrían estar encaminados a la discusión de aquellos segmentos de mercado que el gobierno colombiano debería promover para que el país crezca en desarrollo de contenidos y servicios que puedan ser, incluso, distribuibles en otras regiones.

# 8. REFERENCES


[1] D. Katusic, M. Weber, I. Bojic, G. Jezic, and M. Kusek, "Market, standardization, and regulation development in machine-to-machine communications," in *Software, Telecommunications and Computer Networks (SoftCOM), 2012 20th International Conference on*, Sept 2012, pp. 1–7.

[2] E. Fleisch, "What is the internet of things? an economic perspective," Auto-ID Lab ETH/HSG, Zürich, St. Gallen, Auto-ID Labs White Paper WP-BIZAPP-053, January 2010.

[3] OECD, "Machine-to-machine communications: Connecting billions od devices," *OECD Digital Economy Paper*, no. 192, 2012.

[4] Ericsson, "Ericsson mobility report: On the pulse of the networked society," ., p. 32, November 2014. [Online]. Available: http://www.ericsson.com/res/docs/2014/ericsson-mobility-report-november-2014.pdf

[5] J. Ma, "Internet-of-things: Technology evolution and challenges," in *Microwave Symposium, IEEE MTT-S International*, June 2014, pp. 1–4.

[6] D. Singh, G. Tripathi, and A. Jara, "A survey of internet-of-things: Future vision, architecture, challenges and services," in *Internet of Things, 2014 IEEE World Forum on*, March 2014, pp. 287–292.

[7] M. Castro, A. Jara, and A. Skarmeta, "An analysis of m2m platforms: Challenges and opportunities for the internet of things," in *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on*, July 2012, pp. 757–762.

[8] K. S. Yeo, M. C. Chian, T. C. Wee Ng, and D. A. Tuan, "Internet of things: Trends, challenges and applications," in *Integrated Circuits (ISIC), 2014 14th International Symposium on*, Dec 2014, pp. 568–571.

[9] M. Weyrich, J.-P. Schmidt, and C. Ebert, "Machine-to-machine communication," *Software, IEEE*, vol. 31, no. 4, pp. 19–23, July 2014.

[10] G. Roa, T. Le Pelleter, A. Bonvilain, A. Chagoya, and L. Fesquet, "Designing ultra-low power systems with non-uniform sampling and event-driven logic," in *Integrated Circuits and Systems Design (SBCCI), 2014 27th Symposium on*, Sept 2014, pp. 1–6.

[11] E. Amankwa, M. Loock, and E. Kritzinger, "A conceptual analysis of information security education, information security training and information security awareness definitions," in *Internet Technology and Secured Transactions (ICITST), 2014 9th International Conference for*, Dec 2014, pp. 248–252.

[12] M. Jantscher and P. H. Cole, "Security and authentication primer," *Auto-ID Labs, White Paper Series on Anti-Counterfeiting and Secure Supply Chain:*, p. 40, 2006.

[13] R. C. Soumya Rajan, "Secure schemes for m2m communication," *International Journal of Enfineering & Science Research*, vol. 5, no. 1, pp. 27–33, 01 2015.

[14] M. Elkhodr, S. Shahrestani, and H. Cheung, "The internet of things: Vision amp; challenges," in *TENCON Spring Conference, 2013 IEEE*, April 2013, pp. 218–222.

[15] A. Beresford and F. Stajano, "Location privacy in pervasive computing," *Pervasive Computing, IEEE*, vol. 2, no. 1, pp. 46–55, Jan 2003.

[16] W. H. Organization, "Legal frameworks for ehealt," *Global observatory for eHealth series*, p. 4, 2012. [Online]. Available: http://whqlibdoc.who.int/publications/2012/9789241503143_eng.pdf

[17] E. Commission, "Directive 2010/40/eu of the european parliament and of the council with regard to the harmonised provision for an interoperable eu-wide ecall," *Official Journal of the European Communities*, p. 4, November 2012.

[18] ——, "Proposal for a regulation of the european parliament and of the council concerning type-approval requirments for the deployment of the ecall in-vehicle system and amending directive 2007/46/ec," *Official Journal of the European Communities*, p. 14, June 2016.

[19] ——, "Directive 95/46/ec on the protection of individuals with regard to the processing of personal data and on the free movement of such data," *Official Journal of the European Communities*, p. 9, October 1995.

[20] S. Callens, "The eu legal framework on e-health," in *Health Systems Governance in Europe*, E. Mossialos, G. Permanand, R. Baeten, and T. K. Hervey, Eds. Cambridge University Press, 2010, pp. 561–588, cambridge Books Online.

[21] ESA, "Satellite-enhanced telemedicine and e health for sub-saharan africa (ehsa) programme study on regulatory aspects," *Global observatory for eHealth series*, p. 37, September 2013. [Online]. Available: http://www.greenfield.org.za/downloads/eHSA%20Reg%20Study%20Summary%20Report.pdf

[22] OECD, "Oecd review of telecommunication policy and regulation in colombia," December 2014.

[23] D. Katusic, A. Marcev, R. Vulas, and G. Jezic, "Machine-to-machine: Emerging market and consequences on existing regulatory framework," in *Telecommunications (ConTEL), 2013 12th International Conference on*, June 2013, pp. 317–324.

[24] MINTIC, "Vive digital, documento vivo del plan," *Ministerio de las tecnologías de la Información y las comunicaciones de Colombia*, no. I.0, 2011.