COMILLAS
UNIVERSIDAD PONTIFICIA

Facultad de Ciencias Económicas y Empresariales, ICADE

Análisis de los beneficios y riesgos del 'Internet of Things' para el envejecimiento de la población en la Unión Europea

Autora: Johanna Amy O'Sullivan
Director: Miguel Angel López Gómez

MADRID | Abril 2020

Resumen

Este documento analiza los beneficios y riesgos de los dispositivos conectados a el 'Internet of Things'. Los beneficios identificados incluyen una mejor atención médica, una vida independiente más fácil y mejores beneficios sociales. Mientras que los riesgos hacen referencia a la amenaza de violaciones de la seguridad, el aumento del aislamiento y el incremento de las cuestiones éticas. La demografía de la sociedad en la que se centrará este documento es la de los ciudadanos mayores de 65 años de la Unión Europea, que se consideran la población envejecida. La demografía en la Unión Europea está cambiando y mostrará un porcentaje mayor que nunca de personas mayores de 65 años. Por lo tanto, es necesario establecer soluciones tecnológicas para satisfacer las necesidades de esta población. Mediante el uso de dispositivos conectados al 'Internet of Things', este grupo demográfico podrá depender menos de los jóvenes de la sociedad, ya que en el futuro habrá menos de ellos en comparación con la población que envejece. La Unión Europea, a través de la Comisión Europea, aspira a convertirse en líder mundial en la implantación de un ecosistema del IoT y en los últimos años ha puesto en marcha una serie de iniciativas y planes que tienen efectos directos en los dispositivos y tecnologías del IoT utilizados por la población de edad avanzada de la Unión Europea. A pesar de los planes que la Comisión de la UE ya ha puesto en marcha, faltan sistemas de autenticación y políticas homogéneas que los fabricantes y productores de productos del IoT puedan seguir cuando diseñen productos del IoT, lo que puede causar graves violaciones de la seguridad y la protección de datos. Sin embargo, se deja muy claro que los beneficios de la tecnología y los dispositivos del IoT son muy elevados, especialmente para satisfacer las necesidades de la población que envejece.

The purpose of the document is to analyse the benefits and risks of 'Internet of Things' connected devices. The benefits identified include improved health care, easier independent living and improved social benefits. While the risks include the threat of security breaches, increased isolation and heightened ethical issues. The demographic of society that this document will focus on is citizens over the age of 65 in the European Union who are considered among the ageing population. The demographics in the European Union are shifting and will show a larger percentage of people over the age of 65 than ever before. It is therefore necessary to establish technological solutions to meet the needs of this population. Through the use of 'Internet of Things' connected devices this demographic will be able to rely less on younger demographics of society as there will be less of them compared to the ageing population into the future. The European Union, through the European Commission, aspires to become a world leader in the implementation of an IoT ecosystem and in recent years has launched a series of initiatives and plans that have direct effects on devices and technologies of IoT used by the elderly population of the EU. Despite the plans that the EU Commission has already put in place, there is a lack of homogeneous authentication systems and policies for IoT product manufacturers and producers to follow when designing IoT products, which can cause serious violations of the security and data protection. However, it is made very clear that the benefits of IoT technology and devices are very high, especially to meet the needs of the aging population.

Índice del trabajo

1. Índice de abreviaturas

IoT – Internet of Things (Internet de las cosas)
RFID - Radio-Frequency Identification (identificación por radiofrecuencia)
UE – Unión Europea
AIOTI - The Alliance for the Internet of Things Innovation (Alianza para el Internet de las Cosas)
DDoS - Distributed Denial-of-Service (Denegación de Servicio Distribuido)
GDPR - General Data Protection Regulation'

2. Índice de tablas y gráficos

3. Objetivos del TFG

El objetivo del presente documento es evaluar diversos beneficios y riesgos relacionados con el uso generalizado de los dispositivos de conexión a Internet de los objetos por parte de la población mayor de 65 años en la Unión Europea. Se trata de analizar las investigaciones existentes sobre las consecuencias de la adopción del uso de esos dispositivos en la vida cotidiana y cuáles serán los efectos en los ciudadanos de la Unión Europea. El objetivo es descubrir una variedad de ventajas y desventajas de estos dispositivos en relación con la vida cotidiana, los aspectos de socialización, los aspectos de salud. También se pretende descubrir los posibles riesgos que pueden surgir de la adopción generalizada de este tipo de dispositivos conectados y cómo se puede proteger a este grupo demográfico de la sociedad. El objetivo es explorar la variedad de métodos que la Unión Europea ha establecido o está estableciendo para regular estos dispositivos y hacerlos seguros para su uso por parte de sus ciudadanos.

4. Metodología de investigación

En esta labor se utilizará una combinación de datos cuantitativos y cualitativos que se obtendrán a través de fuentes secundarias. Los datos cuantitativos se utilizarán para determinar las pautas de los beneficios y riesgos de los objetos conectados al "Internet of Things" y para hacer generalizaciones sobre la población destinataria del estudio, los mayores de 65 años. Los métodos cualitativos se utilizarán para obtener una mejor visión en profundidad de cómo estos dispositivos afectan a la vida de estas personas. Los materiales se proporcionarán a través de la biblioteca de la universidad y su extenso archivo de revistas académicas, así como mediante el uso de estadísticas de datos de la Unión Europea para comprender la situación en la Unión Europea. En el caso de las revistas académicas, el contenido se clasificará en beneficios, riesgos y comprensión del efecto general sobre el envejecimiento de la población, mientras que los datos estadísticos se examinarán en Excel y se agruparán en los datos pertinentes que resulten apropiados para el sector de los mayores de 65 años.

5. Justificación por interés empresarial o académico del estudio

El crecimiento de la población de personas mayores de 65 años es un sector de la sociedad en rápido crecimiento y, a medida que las personas envejecen, se vuelven más alfabetizadas en informática y tecnología. Eventualmente llegaremos a un punto en la sociedad donde las personas mayores en la sociedad habrán crecido con Internet en sus vidas. A medida que crezca la eficiencia y las capacidades de la tecnología, especialmente en el "Internet of Things", habrá una gran confianza en esto como lo es hoy en día con Internet, los motores de búsqueda y las redes sociales. Creo que este es un área de gran oportunidad para las empresas dedicadas al desarrollo de tecnología que pueden ofrecer servicios o productos especializados en el envejecimiento de la población.

6. Marco Teórico

6.1. ¿Qué es el Internet de las cosas?

El Internet of Things (IoT) es un sistema de comunicación por el cual una variedad de objetos se conecta entre sí y con Internet. Semánticamente, IoT significa una "red mundial de objetos interconectados con dirección única, basada en protocolos de comunicación estándar" [1] El término fue usado por primera vez por Kevin Ashton del Instituto Tecnológico de Massachusetts en relación con la necesidad de un sistema estandarizado de computadoras para capturar información del mundo real y entenderla. El objetivo de estos dispositivos conectados es obtener datos generados por sensores, dispositivos y máquinas controladas a distancia, entornos monitorizados, coches y edificios. [2]

Los objetos del IoT tienen características como la existencia, el sentido de sí mismos, la conectividad, la interactividad, la dinamicidad y, en algunos casos, la conciencia ambiental. La existencia se refiere al hecho de que los dispositivos y objetos existen en un mundo físico pero su tecnología permite su existencia virtual. El sentido de sí mismo se refiere al hecho de que cada objeto IoT tiene una identidad única y puede comportarse de manera autónoma. La conectividad se refiere a la idea de que los dispositivos del IoT pueden comunicarse con otras entidades del IoT. La interactividad se refiere a la idea de que los dispositivos y objetos del IoT pueden funcionar y colaborar con la interacción ya sea con humanos o máquinas y pueden producir y consumir una amplia gama de servicios. La dinamicidad se refiere a la idea de que los objetos pueden interactuar con otros objetos en cualquier momento, en cualquier lugar y, de cualquier manera. La característica final de la conciencia ambiental sólo está presente en algunos objetos del IoT y describe la función de los sensores en la determinación de los datos físicos y virtuales de su entorno. Por ejemplo, un objeto provisto de etiquetas de identificación por radiofrecuencia (RFID) no tendría esta capacidad, pero tendría las otras cinco características. [3]

La oportunidad de conectar objetos cotidianos a Internet marcará una diferencia significativa en la vida de las personas de todo el mundo y abrirá oportunidades que nunca fueron posibles. A medida que las tecnologías de identificación automática, datos distribuidos y comunicaciones inalámbricas han mejorado en los últimos 15 años, la posibilidad de un mundo del IoT se ha hecho posible. La RFID está a la vanguardia de cómo se hace posible el IoT. Estas etiquetas de identificación se pueden adherir a los objetos y se identifican a través de su identidad virtual en Internet. Sus identidades pueden ser leídas de forma inalámbrica a través de un sistema de tres partes. El sistema de tres partes incluye una etiqueta transpondedora que se adhiere al objeto, un sistema lector que lee la etiqueta en el objeto y finalmente un sistema de back-end donde se almacenan y capturan todos los datos sobre el objeto. [4] Las tecnologías de sensores también pueden ser utilizadas en el seguimiento y monitoreo de los objetos IoT. Estos sensores permiten el monitoreo de la condición de los dispositivos conectados a el IoT y nos permiten ver la información sobre el estado de los objetos. [5] Está claro que para que los objetos IoT funcionen y se sumen a nuestra vida cotidiana, la RFID y la tecnología de los sensores deben funcionar en colaboración y deben estar integradas.

El diagrama proporciona una visión general de cómo funciona cada capa de un dispositivo conectado al IoT. Hay cinco capas.

- Capa uno (capa de borde): las redes de sensores, RFID, proporcionan identificación y almacenamiento de información.
- Capa de acceso: primera etapa del manejo de datos. Realiza la comunicación entre plataformas.
- Capa de Internet: medios comunes de comunicación
- Capa de middleware: gestión de dispositivos y gestión de la información
- Capa de aplicación: entrega de varias aplicaciones

La capa de borde del sistema es la capa de hardware que se utilizan como sensores de datos primarios que se utilizan en el campo. Muchas de estas piezas de hardware se utilizan para proporcionar identificación y almacenamiento de información, recopilación de información, procesamiento de información, comunicación y control.

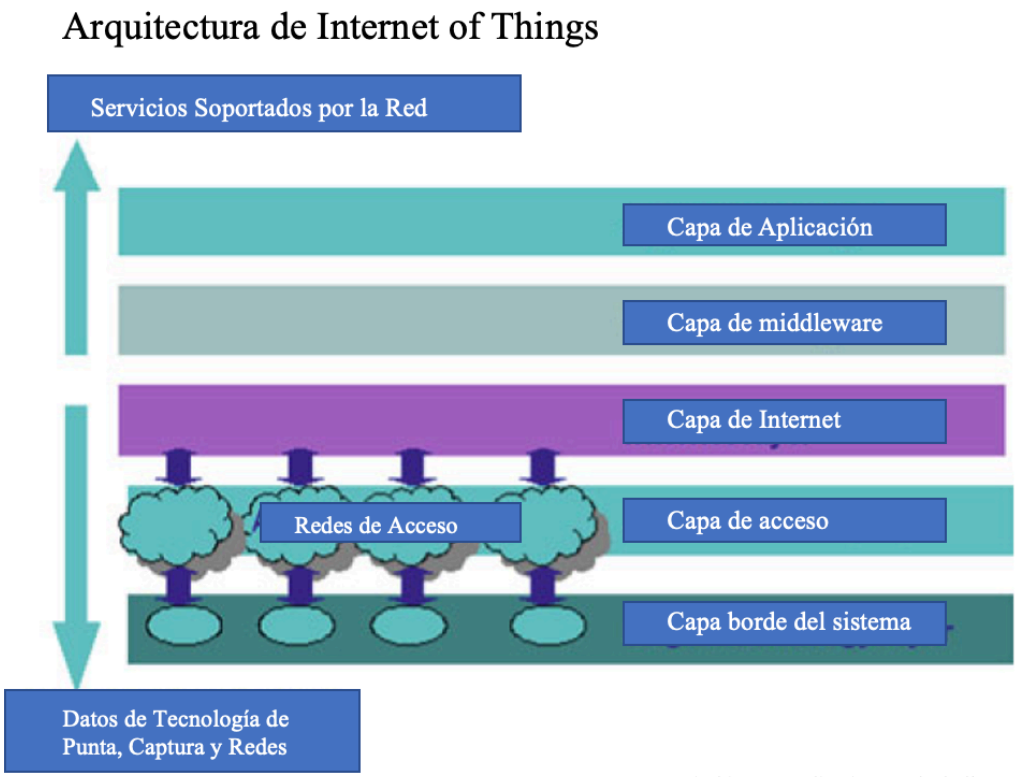
La capa de acceso es la tecnología que asegura la dirección del enrutamiento de los mensajes, la publicación de la información y también realiza la comunicación entre plataformas.

La capa de Internet se utiliza en el sistema para proporcionar los medios comunes para la comunicación por las otras capas y por otros dispositivos del IoT también conectados a través de la Internet.

La capa de middleware es una de las capas más importantes en la arquitectura del dispositivo del IoT y opera bidireccionalmente. Actúa como la interfaz entre la capa de hardware en la parte inferior y la capa de arquitectura en la parte superior. Esta capa responde a las funciones necesarias de gestión de dispositivos y gestión de la información. Esta capa también es importante para encargarse del filtrado de datos, la agregación de datos, el análisis semántico, el control de acceso y el descubrimiento de información.

La capa de aplicación de la parte superior es necesaria para entregar varias aplicaciones a diferentes usuarios del IoT. Las aplicaciones pueden incluir la fabricación, la logística, el comercio minorista, el medio ambiente, la seguridad pública, la atención sanitaria y la alimentación y la medicina. [6]

‘Arquitectura del IoT’ – Grafico 1



Fuente: Internet of Things: Applications and Challenges in Technology and Standardization
Debasis Bandyopadhyay · Jaydip Sen
(Abril 2011)

La estructura de estas capas en los dispositivos del "Internet of Things" indica que para el correcto funcionamiento de estos dispositivos todos deben seguir una estructura similar a esta. Esto da a todos estos dispositivos un rasgo común y ayudará a la Unión Europea a comprender cómo funcionan estos dispositivos y cómo pueden trabajar con los fabricantes para crear medidas de seguridad que puedan ayudar a proteger a los ciudadanos de la Unión Europea que dependerán de estos dispositivos en su vida cotidiana. La estructura puede ayudar a la Unión Europea a determinar qué elementos del dispositivo necesitan directrices más estrictas y posibles leyes contra posibles amenazas a la seguridad.

Se espera que el Internet of Things (IoT) actúe como un factor de enorme importancia en la innovación y la competitividad de la UE en el futuro. Con el creciente interés de la Unión Europea por convertirse en líder mundial en el despliegue de dispositivos y servicios del IoT, se están creando más puestos de trabajo y la necesidad de desarrollar ecosistemas del IoT confiables está en primer plano. Se prevé que para finales de 2020 habrá 4,5 millones de desarrolladores que contribuyan al IoT en la Unión Europea y que se espera un futuro crecimiento en la zona. [7]

En la UE, la cantidad de dispositivos conectados al IoT aumentó de 1,8 millones en 2013 a unos 6.000 millones en 2020, lo que ha dado lugar a que el mercado del IoT en la UE tenga un valor superior a un billón de euros. [8]

Con el fin de abordar el futuro del IoT en Europa, la Comisión Europea lanzó la "Alianza para el Internet de las Cosas" (AIOTI) en marzo de 2015. Se lanzó en asociación con los actores de la industria del IoT y tiene como objetivo poner a la UE a la cabeza en el campo del IoT mediante la creación de un ecosistema europeo del IoT.

Los mercados con las oportunidades de crecimiento más realistas según la Comisión Europea son la fabricación inteligente, los hogares inteligentes y la salud y el bienestar personal inteligentes.

La fabricación inteligente se refiere a los avances en la provisión de sensores, medición, control, gestión de la energía y comunicación en la automatización de fábricas para producir una mayor eficiencia, una mayor flexibilidad y menores costes operativos en el entorno de la fabricación en toda la UE.

Las casas inteligentes permitirán a los propietarios controlar la iluminación, la calefacción, la ventilación, los electrodomésticos y las cerraduras y puertas de seguridad. Esta es ya una esfera que se está desarrollando rápidamente tanto en la UE como en todo el mundo. Se ha identificado que la seguridad en el hogar es el aspecto más importante de los hogares inteligentes. Implica el uso de cámaras de vídeo y sensores para rastrear una serie de variables como la calidad del aire, la vibración, el sonido, el movimiento y la temperatura. La Comisión Europea reconoce que las funcionalidades de los hogares inteligentes son importantes para la población que envejece y explica que el IoT puede "aumentar la eficiencia en la atención, promover la independencia y mejorar la calidad de vida de las personas mayores y sus cuidadores". El uso de sensores de movimiento en el hogar de una persona puede ayudar a alertar a un cuidador, un vecino, un familiar, los servicios sociales o los servicios de emergencia. El IoT también puede ayudar a la detección temprana de riesgos y posibles enfermedades mediante la vigilancia de las pautas diarias de la persona mayor en su hogar. La Comisión reconoce que, a menos que haya más hogares inteligentes y servicios basados en el IoT disponibles en los hogares, más ciudadanos de edad avanzada dependerán de las instituciones sanitarias y de atención a largo plazo, lo cual es un costo que muchos Estados de la UE tendrán que afrontar con dificultad.

En el sector de la salud y el bienestar personal de los servicios del IoT que la Comisión destacó, habrá más barreras para su adopción en el futuro debido a cuestiones de acceso a los datos y propiedad de estos. El IoT ayudará a aliviar las futuras presiones del aumento de los gastos de atención sanitaria y del número de pacientes, lo que está especialmente relacionado con el envejecimiento de la población.

Ejemplos de cómo el IoT ha mejorado los retos sociales en la UE son las "Farolas Inteligentes de Ahorro de Energía" de Barcelona, en las que la ciudad disponía de farolas equipadas con sensores que permitían el control automático de la luminosidad mediante el análisis de la contaminación acústica y atmosférica, así como de la densidad de población, lo que se traducía en un ahorro de energía del 30% cada año. En los Países Bajos se estableció un sistema del IoT para apoyar el control de la salud en casa para las personas que viven con múltiples condiciones crónicas, que mostró un 20% de aumento en la eficiencia de los esfuerzos de atención. [9]

6.2. Estadísticas demográficas

A medida que más personas se conectan a Internet y utilizan objetos conectados, debemos considerar quiénes son estas personas en la sociedad. En esta sección, se explorarán las estadísticas demográficas cambiantes y, por lo tanto, las personas que realizarán la transición al uso de objetos conectados en sus vidas.

En este documento la "población envejecida" se referirá a los mayores de 65 años. Se trata de una porción de la población de todo el mundo que ha tenido un enorme crecimiento en los últimos años y que se espera que constituya una mayor parte de la población de la mayoría de los países del mundo. Esto se enfocará más adelante en esta sección. El envejecimiento de la población ha cambiado en los últimos decenios y hay más enfoques sobre la continuación del trabajo, la participación activa en el trabajo voluntario, la incorporación a grupos sociales, la vuelta a la educación, el desarrollo de nuevas aptitudes y los viajes. Hay una amplia gama de políticas que también están cambiando para este grupo demográfico. Hay un enfoque en los diferentes requisitos de salud y atención, los mercados laborales, la seguridad social, la seguridad económica y las finanzas gubernamentales. Dentro de la UE, el mayor número de personas de 65 años o más registrado en 2011 se encuentra en Madrid con 989 mil personas y en segundo lugar en Barcelona con 949 mil y en tercer lugar en Roma con 809 mil residentes. [10]

La población del mundo era de 7.710 millones de habitantes en 2019, lo que supone un enorme crecimiento con respecto a los 6.540 millones de 2005. Sin embargo, lo más interesante es que el porcentaje de adultos mayores de 60 años también ha aumentado del 10,3% en 2005 al 13,2% en 2019. Desglosando esto aún más, en África el porcentaje de adultos mayores de 60 años sólo ha aumentado del 5,1% en 2005 al 5,5% en 2019, en América del Norte esta cifra ha aumentado del 16,8% al 22,6%, en Asia ha aumentado del 9,1% al 12,7% y en Europa esta cifra ha pasado del 20,6% al 25,3%. [11] El porcentaje de personas mayores de 60 años aumentó en todas las regiones del mundo, excepto en el África occidental y el África central, y estas cifras sólo disminuyeron en un 0,1% y un 0,3% respectivamente. En la mayoría de las regiones también se produjo un cambio en el porcentaje de niños de entre 0 y 14 años. [12] En general, a nivel mundial esta cifra ha disminuido del 28,1% al 25,6% y, si se examina más detenidamente cada región, la única que registró un ligero aumento de esta demografía fue Europa oriental, que pasó del 15,4% en 2005 al 16,9% en 2019. %. [13] Este cambio demográfico se ha debido en gran medida a la disminución de las tasas de mortalidad de las personas de edad, a la evolución de la atención médica y a la mejora de las condiciones de vida y de trabajo.

En relación con los hábitos de vida del envejecimiento de la población, las estadísticas muestran que en 2016 el hogar más común en la UE estaba formado por una sola persona. Estos hogares representaron el 32.5% de la participación del total de hogares. Por lo general, estos hogares de una sola persona se han observado en regiones de la capital de la UE y con más mujeres (18,4%) que hombres (14,1%) viviendo solas. En la UE, en 2016, las personas solteras de 65 años o más constituían el 14,1% de todos los hogares. [14]

En relación con el turismo, muchos de los ancianos de la UE encuentran placer en viajar y utilizan el tiempo libre de su jubilación para viajar tanto a su país como a otros países. En 2013, el 47,1% de todos los ciudadanos de la UE mayores de 65 años participaron en el turismo, sin embargo, el futuro de estas estadísticas dependerá de factores financieros y de salud. [15]

Dado que la población de personas mayores de 65 años ha aumentado enormemente en Europa y es la segunda del mundo después de América del Norte, significa que se necesitan nuevas soluciones para los problemas que afronta esta población. Con la disminución a nivel mundial del porcentaje de niños, significará que habrá menos personas que dependan de la fuerza de trabajo para atender a la población que envejece a medida que envejecen y requieren ciertos tipos de atención. De aquí viene la oportunidad de los dispositivos conectados al IoT. Este grupo demográfico de la sociedad requiere cierta asistencia y ésta puede provenir de estos tipos de dispositivos. Además, las implicaciones de que más personas vivan solas en sus casas significan que pueden beneficiarse de los dispositivos del IoT en la vida cotidiana para el cuidado y también para la socialización y la conexión con los diferentes grupos sociales, ya que se ha demostrado que una mayor parte de la población que envejece sigue participando en el trabajo voluntario, viajando, desarrollando habilidades y uniéndose a grupos sociales. El uso de estos dispositivos en sus vidas puede ayudarles a conectarse con personas de ideas afines y aumentar la satisfacción de sus vidas. Con el potencial de un aumento en el uso de dispositivos del IoT por parte de este grupo demográfico, se presenta la necesidad de que el gobierno aumente su participación en la regulación de estos para proteger a sus ciudadanos.

6.3. Proyecciones de población

En la UE las proyecciones de población total son de 523.708.357 en 2050 y ahora en 2020 son de 514.292.912. En 2050 la proyección para la población de la UE mayor de 65 años es de 149.196.187 mientras que en 2020 es de 104.496.757. [16] Estas cifras pronosticadas son evidencia de que el envejecimiento de la población está creciendo a un ritmo rápido, en el que será necesario realizar cambios drásticos en la forma en que vive este grupo demográfico ahora. Será necesario que se tomen medidas para un mayor gasto del gobierno en atención médica, alojamiento apropiado y otros servicios específicamente para este grupo demográfico. Aquí es donde el uso de dispositivos IoT podrá ayudar en el cuidado y la gestión de la vida de este grupo demográfico.

6.4. Uso de la tecnología

El uso de Internet por parte de los estadounidenses mayores de 65 años ha aumentado del 14% en 2000 al 73% en 2019. En 2016, el 45% de los adultos mayores de 65 años usaron Internet al menos una vez a la semana en la UE contra el 82% de la población de la UE entre 25 y 64 años. La cantidad de adultos mayores de 65 años que usan internet se ha triplicado desde 2007, cuando sólo el 13% usaba internet semanalmente. Los países europeos que tienen el mayor uso de Internet entre sus poblaciones de edad avanzada en 2016 fueron Luxemburgo (88%), Dinamarca (81%) y Suecia (80%) y los más bajos fueron Bulgaria (12%), Rumania (13%) y Grecia (14%). En 2014, el 22% de los ciudadanos de la UE de entre 65 y 74 años utilizaron la banca por Internet, el 23% de ellos utilizaron Internet para hacer compras en línea, el 25% para leer las noticias y sólo el 10% para los medios de comunicación social. [17]

6.5. Necesidades de la población que envejece

A medida que las personas envejecen, la dependencia de los demás aumenta. Desde la infancia, la dependencia de un cuidador fue muy importante para el desarrollo y el cuidado de un niño, y luego en la edad adulta la necesidad de atención cambia. Otros ahora pueden necesitar su ayuda en la edad adulta para el cuidado y luego a medida que una persona envejece su dependencia de otros y la necesidad de cuidado aumenta de nuevo. Como ya hemos visto, el cambio demográfico ha demostrado que la población que envejece va a necesitar más cuidados que los bebés y los niños pequeños en las próximas décadas.

Las necesidades de los ancianos han permanecido iguales a lo largo de la historia, sin embargo, la entrega de estos es lo que va a cambiar en el futuro. Las necesidades de este grupo demográfico se dividen en necesidades físicas, intelectuales, emocionales y sociales.

Dentro de las necesidades físicas, dependiendo de su nivel de habilidad, pueden necesitar ayuda con la nutrición, dependiendo de su capacidad para cocinar por sí mismos debido a las restricciones en la movilidad. También pueden necesitar ayuda con la movilidad debido a una gama limitada de movimientos o a un cambio en la tolerancia y la capacidad para caminar. Este grupo demográfico también puede necesitar asistencia con la atención médica y la seguridad dentro de sus hogares y cuando están fuera en el mundo.

Dentro de las necesidades intelectuales, la población que envejece puede necesitar ayuda con la estimulación debido al hecho de que sufren de falta de coordinación, problemas de vista y oído. También pueden necesitar ayuda para aprender nuevas actividades porque a menudo han tenido que renunciar a trabajos o pasatiempos que antes disfrutaban. Es una oportunidad para que aprendan nuevas habilidades y pasatiempos, así como para estimular sus sentidos.

Dentro de las necesidades emocionales, la población de edad puede sufrir una pérdida de autonomía al haber perdido la capacidad de realizar las tareas cotidianas que solían realizar y puede necesitar la ayuda de la familia o de los cuidadores. También pueden sufrir un sentimiento de no pertenencia, ya que a menudo no han podido seguir trabajando o han perdido amigos y familiares en la vejez. Este grupo demográfico, entre todos los demás, necesita sentir que se le cuida.

Por último, dentro de las necesidades sociales, la población que envejece necesita comunicación en su vida cotidiana para evitar el aislamiento y la sensación de frustración. También necesitan interacción social fuera de su familia, que puede ser de sus compañeros o de otros en la sociedad. Esto ayudaría a prevenir problemas de salud mental.

Este tipo de necesidades pueden ser atendidas de muchas maneras diferentes y a través de diferentes personas. La población que envejece suele tener más contacto con los hospitales, los servicios sociales, los médicos generales, los centros de atención y los cuidadores en sus propios hogares. Las personas que trabajan en estas instituciones y servicios pueden ayudar a satisfacer estas necesidades. En un entorno más informal, la familia, los amigos, las parejas y los vecinos también pueden ayudar a satisfacer las necesidades de la población que envejece.

Sin embargo, en una sociedad en la que el uso de Internet entre la población de edad avanzada ha aumentado drásticamente en los últimos años y se espera que vuelva a aumentar en el futuro, existe la oportunidad de modificar la forma en que la sociedad se ocupa de la población de edad avanzada. A medida que una mayor parte de esta población utiliza la

tecnología e Internet, se presenta la oportunidad de recurrir a soluciones basadas en la tecnología en el sector de la atención de la salud, el sector de la vida independiente y el sector social para la población de edad avanzada. Todo lo cual satisfaría las necesidades de este grupo.

Se estima que entre el año 2000 y 2050 la proporción de ancianos dependientes que reciben atención informal aumentará de un crecimiento de entre el 64,8% en el Reino Unido y el 125% en España, por ejemplo. El cuidado informal suele ser llevado a cabo por familiares o vecinos que no reciben ningún tipo de compensación. El crecimiento del cuidado informal tiene aspectos tanto positivos como negativos. Los aspectos positivos incluyen que este cuidado es menos costoso que el cuidado profesional formal, como el cuidado en un hogar de ancianos, y también permite que la persona mayor permanezca en su hogar por más tiempo, lo que a menudo prefiere. Sin embargo, entre las dificultades figuran la falta de integración de los cuidadores informales en el sistema general de atención de la salud y la falta de coherencia en la prestación de esta atención debido a la falta de capacitación. [18]

7. Beneficios de la Internet de las cosas

7.1. Beneficios del cuidado de la salud

Ha habido un gran aumento en el uso de los teléfonos inteligentes por parte de los ‘baby boomers’, que son aquellos nacidos entre 1946 y 1964. El número de aplicaciones para el cuidado de la salud descargadas en iOS y Android se ha más que duplicado en menos de 3 años para llegar a más de 100.000, lo que demuestra que hay un aumento en la demanda de tecnología relacionada con el cuidado de la salud, especialmente entre la población de edad avanzada. La gente también está usando más la tecnología de vestir. Estos artículos de uso incluyen lentes de contacto que monitorean los niveles de glucosa, dispositivos auditivos que parecen aretes, muñequeras que monitorean la presión sanguínea del latido del corazón en calorías quemadas e instalan sensores que miden el peso, el equilibrio y la temperatura. [19]

En la atención sanitaria que afecta directamente al envejecimiento de la población, el IoT permitirá la interacción entre el paciente y el profesional de la salud. Objetos como "camas inteligentes" podrán detectar el movimiento del paciente y podrán ayudarlos con la necesidad de la ayuda de una enfermera. Mientras que los 'inodoros inteligentes' serán capaces de detectar automáticamente muestras de orina y enviar los datos a su médico, quien podrá determinar cualquier problema en una etapa temprana. [20] Un ejemplo de un sistema de gestión de la salud que se utiliza actualmente por la población de edad avanzada es 'Buddy'. Este sistema de gestión y control de la salud utiliza una aplicación que se puede llevar puesta para controlar la salud de la persona que envejece y utiliza la inteligencia artificial para predecir las caídas y hacer un seguimiento de los patrones de salud irregulares. Este sistema puede alertar a los cuidadores y a los servicios de emergencia de cualquier peligro para el usuario anciano.

El uso de la inteligencia artificial y de los mecanismos del IoT para ayudar a la población que envejece, especialmente para hacer frente al declive cognitivo a medida que envejecen, ha demostrado ser enormemente beneficioso. Ha demostrado que mejora la calidad de vida tanto de las personas mayores como de sus cuidadores. La tecnología de asistencia puede clasificarse en tres categorías: sistemas de garantía, sistemas de compensación y sistemas de evaluación. [21]

Un sistema de garantía tiene por objeto asegurar que los ancianos estén seguros y realicen las actividades cotidianas que normalmente llevarían a cabo. Un sistema de compensación ayudaría a los ancianos a realizar las actividades diarias. Un sistema de evaluación examinaría cómo le va al anciano sobre la base de la observación continua de las actividades frecuentes. Cada uno de estos diferentes sistemas utiliza la supervisión de las actividades para proporcionar información sobre el anciano. Esta información sería normalmente proporcionada por tecnología como las etiquetas de identificación por radiofrecuencia (RFID) adheridas a los objetos de la casa, incluyendo sensores de presión en las puertas de los refrigeradores o en las sillas. Los biosensores son otro tipo de tecnología utilizada que generalmente lleva la persona y miden los signos típicos del bienestar de la persona, como la frecuencia cardíaca y la temperatura corporal. Estos sistemas explicados a menudo utilizan redes bayesianas para evaluar el reconocimiento de la actividad.

Los sensores utilizados alrededor de la casa de un anciano en el sistema de aseguramiento rastrearían la interacción de la persona con su área y alertarían a un cuidador con informes regulares sobre la actividad de la persona, a los que se puede acceder por medio de una página web o para los que recibiría una notificación de emergencia si algo no le pareciera bien al anciano, lo que se basaría en las desviaciones de las tendencias normales. Un sistema de evaluación proporciona una evaluación continua del estado cognitivo de los ancianos.

Los sistemas de compensación supervisan la actividad de los ancianos y ayudan a la persona que utiliza las alarmas y los recordatorios a realizar las tareas necesarias sin intervenir realmente en su vida. Estos tipos de sistemas suelen ser adecuados para las personas que ya no pueden navegar por su entorno habitual debido a la disminución de su salud cognitiva. Estos tipos de sistemas podrían ajustarse a las desviaciones del horario de las personas, por ejemplo, si el anciano requiriera medicación a intervalos determinados, pero su horario se desviará un poco un día, el sistema de recordatorio lo tendría en cuenta y enviaría un recordatorio al anciano a una hora más adecuada en función de ese horario concreto de ese día. Para ello, el sistema tendría que estar al tanto de las actividades planificadas, evitar causar ineficiencia en la vida de los ancianos y evitar que éstos dependan excesivamente del sistema de recordatorio, ya que el propósito es hacerlos más independientes. [22]

Estos tipos de sistemas, por muy útiles que sean en la vida de los ancianos y sus cuidadores, no están concebidos para sustituir al cuidador humano y tienen por objeto habilitar a la persona de edad facilitándole la vida en sus hogares durante más tiempo y, por lo tanto, proporcionarle una calidad de vida más cómoda y mejor.

La tecnología que vigila y supervisa a las personas de edad puede ayudar a recordarles que deben llevar a cabo tareas y actividades cotidianas como comer, beber y tomar medicamentos. Pueden facilitar la supervisión de la persona a través de una enfermera o de los visitantes que aparecen en una pantalla de vídeo con la que la persona mayor puede interactuar. Los médicos pueden visitar a los pacientes virtualmente y su cara puede aparecer en el monitor del robot. [23]

Entre los ejemplos de sensores digitales que se utilizan actualmente en la atención de la salud figuran un sensor pegajoso a base de gel que vigila la actividad eléctrica en el órgano sin deslizarse, un sensor tipo parche que se mueve con la piel y registra y envía información sobre la salud a teléfonos inteligentes y computadoras sincronizadas, un sensor "Piel Electrónica" que se lleva en la muñeca y que vigila y trata los trastornos musculares en las

personas que sufren de Parkinson o epilepsia detectando los temblores y liberando la medicación incrustada en el parche que se absorbe a través de la piel, un sensor ingerible de Proteus Digital Health que monitoriza cuando un paciente ha tomado o no su medicación y proporciona datos biométricos como el ritmo cardíaco, los patrones de sueño, la actividad física y los niveles de estrés y el "HealthPatch", que es un sensor cutáneo biométrico que se ajusta al pecho del usuario y realiza un seguimiento del ritmo cardíaco, la variabilidad del ritmo cardíaco, el ritmo respiratorio, la temperatura de la piel, la postura corporal, los pasos y la detección de caídas o la gravedad de una caída y es capaz de captar continuamente mediciones biométricas de grado clínico. [24]

Otro ejemplo de una solución sanitaria del IoT es el de una empresa médica portuguesa llamada Sword Health, que ofrece un servicio digital que permite a los pacientes recibir fisioterapia en sus propios hogares. Los pacientes usan los rastreadores de movimiento de la compañía para digitalizar sus movimientos en detalle y comunicarse de forma inalámbrica con un terapeuta. El sistema del IoT proporciona una retroalimentación en tiempo real durante el tratamiento bajo la guía remota de los equipos clínicos.

Está claro que con el vasto despliegue de servicios y dispositivos alimentados por IoT, algunas personas se quedarán atrás y no se beneficiarán del IoT. Esto podría llevar a una falta de confianza en estas nuevas tecnologías. Por lo tanto, es de suma importancia que las empresas y los órganos rectores adopten estrategias e iniciativas que fomenten la confianza y la comprensión de los beneficios de estos sistemas del IoT, así como que tomen medidas para evitar y limitar los posibles riesgos que se examinarán más adelante. Con el aumento del uso de Internet y de los dispositivos por la población en general y entre la población de edad avanzada, la única manera de que estos sistemas tengan un verdadero éxito y se adopten ampliamente en el futuro es ganarse la confianza total de los usuarios. Una forma en que estas autoridades podrían generar confianza en estos nuevos sistemas que cambiarán abrumadoramente la vida de muchas personas en el envejecimiento de la población en el futuro es resaltar los beneficios de estilo de vida que tendrá esta tecnología. Esto se discutirá con más profundidad en el siguiente segmento.

7.2. Beneficios del estilo de vida independiente

El futuro de los objetos de la Internet de las cosas ofrecerá oportunidades completamente nuevas a la población de las que también se beneficiará en gran medida la población de edad avanzada. Los dispositivos del IoT serán útiles en el entorno del hogar de la persona mayor. Las personas prefieren la comodidad de sus propios hogares y con el aumento del número de personas de edad que se espera en el futuro el deseo de permanecer en casa sigue siendo el mismo, pero la necesidad de permanecer en casa en lugar de trasladarse a un centro de atención podría ser vital para la asignación de fondos de los gobiernos y el espacio en estos centros de atención. Por lo tanto, se han generado ideas para dar a la población que envejece un mejor nivel de vida viviendo de forma independiente. Un ejemplo es una nevera inteligente que se comunica con el contador de electricidad inteligente para consumir energía cuando sea más barata mejorará el estilo de vida de los usuarios ya que están usando energía más barata y consumiendo más eficientemente. Los consumidores se esfuerzan por obtener productos eficientes, que ahorren tiempo y dinero y, por lo tanto, este tipo de productos puede tener un gran éxito. Otra mejora del estilo de vida que se pudo observar en los dispositivos alimentados con IoT es el código de barras en los artículos del supermercado. El escaneo del código de barras permitiría al comprador acceder a información adicional en la que podría conocer las advertencias sobre alergias o la información nutricional adaptadas que

nunca sería posible incluir en el embalaje físico del artículo. [25] Este tipo de sistema de escaneo y personalización tiene un sinnúmero de otras aplicaciones especialmente relacionadas con el envejecimiento de la población, como el escaneo de medicamentos para ver cuánto y con qué frecuencia se debe tomar.

Se ha demostrado que el cuidado de una persona con demencia tiene un impacto en la salud mental del cuidador. Por consiguiente, se ha demostrado que la introducción de tecnología de asistencia en el cuidado de la persona con demencia reduce la ansiedad de los cuidadores con respecto a la persona. Una encuesta realizada muestra que el 87% de los parientes de una persona que sufre de demencia están a favor de las cámaras visibles. Mientras que, el 47% de los residentes están de acuerdo con ella y el 63% de los miembros del personal están de acuerdo con esta tecnología. La mayor preocupación expresada en la encuesta con el uso de esta tecnología fue la privacidad de los residentes, así como el acceso a las imágenes, cómo se almacenan y qué tan seguro es. Parecía que había más preocupación por la privacidad que por no causar daño a los ancianos. Una solución para colocar las cámaras en el hogar era colocarlas en el pasillo del residente, ya que esto permitiría vigilar la actividad en el hogar sin inmiscuirse en las rutinas y espacios privados de la casa. Otra solución propuesta fue que, al crear la tecnología, se desarrollara junto con los usuarios para asegurar que se hiciera de manera justa y ética. [26]

Un ejemplo de un sistema de automatización del hogar es una cerradura inteligente. Se trata de un sistema del IoT controlado a través de un teléfono móvil, mediante el cual el propietario de una casa podría bloquear y desbloquear las puertas de su casa utilizando su teléfono, así como identificar a la persona que toca el timbre a través de vídeos de seguridad y proporcionarle códigos de acceso temporales a la casa mientras vigila cuándo entra y sale de ella. Esto podría proporcionar a una persona mayor más independencia. [27]

Debido al número de personas y ancianos que utilizan dispositivos conectados a Internet, existe la posibilidad de utilizar todos los datos que se recogen para ayudar a los demás. Por ejemplo, si hay una persona mayor que ha comprado un nuevo dispositivo, pero no sabe cómo configurarlo con ciertos otros elementos en su casa, otra persona que ellos conocen ya tiene este dispositivo instalado en su casa y podría conectarse con el nuevo dispositivo de la persona para configurarlo en su red de dispositivos. Los dispositivos que se comunican entre sí ahorrarán tiempo a la persona mayor que tendrá que llamar a alguien para que le ayude o para buscar ayuda en línea. Esta es una forma en que la persona mayor puede recuperar su independencia a través del uso de tecnología socialmente conectada. [28]

La objetivación es un gran problema entre las personas mayores que son atendidas tanto por máquinas como por humanos. Se sienten como si ya no fueran tratados como humanos porque ya no pueden llevar a cabo tareas particulares por sí mismos. Sin embargo, la introducción de este tipo de robots podría en realidad potenciar a las personas mayores. Las personas mayores podrían ordenar el uso de un robot para ayudar con ciertas tareas cuando la instalación en la que están está muy ocupada y las enfermeras están ocupadas o incluso para tareas más íntimas como ducharse o usar el baño. El robot funcionaría como una extensión del cuerpo y la mente de la persona mayor. Esto les dará una mayor sensación de control y autonomía. [29]

Las compañías están reconociendo la necesidad de usar la tecnología para el bien. Un estudio realizado por Vodafone [30] demostró que la tecnología puede desempeñar un papel muy importante en el alivio de la soledad de las personas mayores y lanzó su campaña para

ofrecer talleres tecnológicos gratuitos a las personas mayores de todo el Reino Unido. Permitió que los participantes de edad avanzada aprendieran una variedad de nuevas habilidades para mantener las conexiones con la familia y los amigos, así como el acceso a los servicios comunitarios tradicionales. El objetivo general de la iniciativa de Vodafone era aumentar los conocimientos técnicos de los ancianos y aumentar su confianza mientras vivían independientemente de las personas con las que querían mantenerse en contacto.

7.3. Beneficios sociales

Las personas mayores, como todos los demás grupos demográficos de la sociedad, gustan de socializar y necesitan socializar como se esbozó en las necesidades de este grupo demográfico anteriormente. Es fundamental para la vida comunicarse e interactuar con otras personas fuera del hogar para mantener una buena salud y bienestar. Sin embargo, este grupo demográfico de la sociedad muestra más signos de soledad que cualquier otro, lo que está relacionado con la falta de participación social. La soledad se describe como un tipo de angustia que está asociada con "una percibida falta de conexiones y relaciones sociales". Entre el 10% y el 50% de la población que envejece sufre de una mayor soledad a medida que envejece. Las barreras a las que se enfrenta la población que envejece en la socialización incluyen la enfermedad, la discapacidad, la pérdida de amigos y familiares, la pérdida de una comunidad local y la percepción de una falta de oportunidades sociales. Dentro de la enfermedad y la discapacidad, los principales factores considerados por la población que envejece son cuestiones prácticas como la baja energía, la dificultad para utilizar el transporte público y los problemas de movilidad. Dentro de la pérdida de comunidad, gran parte de la población de edad siente que las personas que viven en su zona no se apoyan mutuamente como lo hacían en el pasado y se sienten abandonados por sus vecinos, lo que les hace querer participar menos en la comunidad. Dentro de la percepción de la falta de oportunidades sociales hubo una grave falta de conocimiento de las actividades, especialmente entre los hombres de la población de edad avanzada. La población que envejece también sufre de temores sociales que pueden incluir el temor al rechazo, el temor a perder su identidad "independiente", el temor a perder su identidad "juvenil". Uno de los principales temores que tienen los ancianos cuando desean participar en actividades sociales fuera del hogar es el temor al rechazo debido a que los miembros preexistentes de un grupo o club no están dispuestos a admitir nuevos miembros. La falta de autosuficiencia también es un factor que contribuye a la falta de socialización. La persona mayor puede sentir que el hecho de relacionarse con otros, que a menudo le exige depender de otros para ciertos servicios, le hace sentirse dependiente. A menudo sienten que las interacciones sociales deben ser recíprocas y a menudo no pueden proporcionar nada a cambio del servicio que reciben. El temor a perder su identidad "juvenil" proviene de socializar en un grupo de otras personas mayores y de sentir que las personas están enfermas, discapacitadas e incapaces y de no querer que se las asocie con eso. [31]

Es evidente la necesidad urgente de una solución para minimizar la soledad de este grupo demográfico. Los dispositivos IoT pueden ser la solución que se necesita. Las personas mayores a menudo dependen del teléfono para combatir la soledad y, por lo tanto, un sistema por el que puedan comunicarse a través de un dispositivo con vídeo o mantenerse al día con su familia y amigos a través de un dispositivo del IoT puede ser muy valorado por este grupo demográfico. [32]

Un ejemplo del uso de la tecnología IoT para que las personas mayores salgan de sus casas socializando y sintiéndose cómodas en su entorno sería la instalación de sensores en el lugar

que proporcionarían información sobre el entorno en el que se socializarán y controlarían la temperatura, el número de personas, las identidades de las personas y el clima. Esto puede ayudar a la persona mayor a prepararse para su salida social sabiendo qué esperar y qué ponerse dependiendo de la temperatura. Esto puede ayudar a aliviar la incertidumbre y proporcionarles confianza y un sentido de independencia. [33]

Los dispositivos del IoT que se centran en la compañía sugieren una mejora en los resultados de la soledad y una mejor calidad de vida para los ancianos que interactuaban regularmente con un perro robótico. Este tipo de compañía puede mejorar la interacción social de las personas, ya que el robot proporcionará un punto de conversación entre extraños. [34] Un ejemplo de este tipo de compañero del IoT robótico es la colección "Joy For All" de Hasbro. Ellos crearon perros y gatos robóticos con pelaje realista que hacen ruidos de mascotas y tienen sensores que responden a las caricias y abrazos con movimientos similares a los de los animales. El propósito de esto era permitir la felicidad entre la población envejecida y proporcionarles un compañero que pudiera acompañarlos a las salidas sociales.

Se han visto efectos positivos de la tecnología entre los adultos mayores en sus emociones y en la satisfacción de la vida. La tecnología proporciona una solución alternativa para aliviar la soledad y ayuda a combatir los efectos de la alienación entre los adultos mayores. El hecho de que estos adultos puedan formar nuevas relaciones sociales en línea conduce a una sensación de satisfacción vital. Se ha demostrado que el uso de Internet tiene un gran efecto en la satisfacción psicológica, económica y física de la vida. Se ha puesto de manifiesto que el apoyo social percibido, que es "una transacción interpersonal que contiene apoyo emocional, información o asesoramiento, ayuda instrumental o física y afirmación", ha ayudado a cosas como la adaptación, a hacer frente al estrés, a la salud física y material y a la sensación de aislamiento. Un estudio de 2.075 adultos estadounidenses mayores mostró que aquellos que usaban Internet tenían un 33% menos de posibilidades de sufrir depresión que los no usuarios, así como el hecho de que los adultos mayores ya con depresión podían reducir esos sentimientos de soledad y depresión a través del uso de Internet. [35]

Los adultos mayores han aumentado su uso de los medios sociales. Los estudios muestran que hubo un aumento del 70% en el uso de Internet por parte de las personas de 50 a 64 años y un aumento del 38% por parte de los mayores de 65 años desde 2000 a 2009 y su uso de los medios sociales aumentó un 88% y un 26% respectivamente. Reveló que los adultos mayores que utilizan este tipo de medios a menudo prefieren las funciones de mensajería instantánea más que cualquier otro. Estas funciones aliviaron el nivel de depresión y mejoraron la autoeficiencia y el apoyo social percibido. Además, las habilidades de Internet mejoraron la confianza en sí mismo, la autoeficiencia, la satisfacción de la vida y la calidad de vida. A pesar del riesgo de aislamiento social y de los riesgos para la privacidad asociados con el uso de los medios de comunicación social, se convino en general en que esos medios tenían una función positiva en lo que respecta a la formación de vínculos sociales y la integración social. [36]

Un estudio determinó que las personas mayores expuestas a la discriminación por motivos de edad, por ejemplo, a través del habla condescendiente, tenían un rendimiento mucho peor en las tareas cognitivas que las que no la experimentaban. Por lo tanto, la introducción de dispositivos del IoT permitiría a la persona mayor interactuar con un dispositivo que no los discrimine o los infantilice cuando se les habla. [37]

Un ejemplo de una solución creada para permitir a los ancianos socializar más y dejar sus hogares es el Busbot. Es un programa de vehículos sin conductor en Australia que sirvió como solución de transporte público para los ancianos durante 22 semanas. Debido al hecho de que más personas mayores están usando teléfonos móviles, el hecho de que este sistema fuera accesible a través de una aplicación telefónica lo hizo accesible a este grupo demográfico. La persona mayor abría la aplicación e introducía el destino deseado y era dirigida a una parada de autobús virtual cercana. El servicio operaba 30 viajes al día y era gratuito durante las 22 semanas de prueba. Este es un ejemplo de cómo la tecnología IoT podría ayudar a los ancianos de la sociedad a socializar con sus pares fuera de sus hogares y permitirles recuperar su confianza.

Otro ejemplo de un sistema del IoT para hacer frente a la soledad de los ancianos se llama ElliQ. Es un compañero robótico emocionalmente inteligente diseñado para hacer frente a la soledad de los ancianos. Utiliza la tecnología del IoT y la Inteligencia Artificial para determinar el comportamiento del usuario y sus preferencias para entregar notificaciones verbales que les recuerdan que deben tomar medicamentos y les permite hacer videollamadas. La comunicación verbal alivia la soledad y proporciona un método de socialización alternativo para la persona mayor.

'Resumen de Beneficios – Grafico 2

Beneficios del cuidado de la salud	Beneficios del estilo de vida independiente	Beneficios sociales
- Mejora de la interacción entre el profesional de la salud del paciente - Actualizando al cuidador con informes regulares del bienestar del usuario - Evaluación continua del estado cognitivo - Proporcionar recordatorios para realizar las tareas diarias	- Reduce la ansiedad del cuidador sobre la persona - Mejores sistemas de seguridad en el hogar - Mejora de la eficiencia energética - La instalación más rápida y fácil de nuevos dispositivos sin necesidad de asistencia externa - Independencia en las tareas íntimas	- Información sobre los entornos sociales externos - Los dispositivos permiten la comunicación física con extraños - Alivio de la depresión y aumento de la satisfacción de la vida

Fuente: elaboración propia

8. Riesgos de la Internet de las cosas

8.1. Riesgos de aislamiento

Se estima que el 90% de la población de más de 65 años quiere vivir en sus propios hogares el mayor tiempo posible. Sin embargo, vivir en casa hasta la vejez tiene una serie de inconvenientes, especialmente si la persona vive sola. Los factores que pueden resultar difíciles incluyen el miedo al aislamiento y la soledad, las caídas, el manejo de la medicación y el transporte. A menudo se debe a que los niños viven lejos, a la fragilidad, a que viven solos tras la muerte de su pareja o a las primeras etapas de la demencia, que obligan a las personas mayores a ingresar en centros de atención. [38]. Sin embargo, el uso de la tecnología del IoT en el hogar de las personas puede permitir que permanezcan más tiempo en el hogar. Esta tecnología podría incorporar un elemento de socialización para evitar los sentimientos de aislamiento social como se describió anteriormente. Este tipo de dispositivos alimentados por IoT podría crear un sentido de comunidad entre estos ancianos conectándolos a través de sus situaciones. Los dispositivos del IoT pueden tener diferentes tipos de conexión social, interna y externa. Interno se refiere a la conexión con otros objetos del IoT en el hogar, mientras que externo se refiere a la conexión de los dispositivos del IoT en el hogar con otros dispositivos del IoT en las casas de otras personas. Esto podría ser un elemento enormemente beneficioso del IoT y crearía un tipo de conexión social específicamente destinada a este grupo demográfico, ya que se ha observado anteriormente que es menos probable que este grupo demográfico utilice los medios sociales para conectarse con sus pares que las generaciones más jóvenes.

Los dispositivos del IoT diseñados para ayudar a vigilar a la persona mayor en su hogar podrían proporcionar una sensación de confianza y conexión, ya que tienen el conocimiento de que, si ocurre algo fuera de lo normal en su rutina diaria que pueda suscitar preocupación entre sus cuidadores, familiares o amigos, se les notificará cuando se detecte algo. El sistema se pondrá automáticamente en contacto con un cuidador, ya sea un profesional de la salud, un cuidador, un miembro de la familia o los servicios de emergencia, y puede disminuir los sentimientos de soledad y desconexión entre esta población que envejece. [39]

El aislamiento social es un factor que parece prevalecer más en este grupo demográfico que en cualquier otro y puede dar lugar a problemas de salud psicológicos y físicos para estas personas que sufren de aislamiento. El uso de dispositivos del IoT tiene la capacidad de reducir este tipo de aislamiento entre los ancianos, sin embargo, conlleva riesgos de un mayor aislamiento. Si se despliega el uso de robots de asistencia alimentados con IoT en el cuidado de los ancianos en centros de atención o incluso en sus propios hogares, las consecuencias del aislamiento podrían ser nefastas. Estos robots tienen la capacidad de ayudar con las tareas diarias como alimentar, lavar y ayudar a alguien desde una cama hasta una silla de ruedas. Estos robots pueden reconocer rostros y voces y a menudo pueden usar una combinación de comandos de voz y un puntero láser para llevar a cabo tareas específicas. Los riesgos que pueden surgir con este tipo de máquinas de asistencia pueden ser que la persona mayor tenga cada vez menos contacto humano que antes y una falta de control sobre su vida. Estas máquinas reducirán la valiosa interacción social entre los seres humanos y eliminarán la oportunidad de una comunicación humana cuidadosa. Ya hay muchas personas mayores que viven bastante aisladas y sufrirían aún más con la introducción de estos robots. Este aislamiento puede llevar a menudo a la demencia y a otras reducciones cognitivas. Se observa que las personas con mayor soledad suelen ser más propensas a desarrollar la enfermedad de Alzheimer. [40]

La tecnología que monitorea y supervisa a la persona mayor puede recordarle que debe realizar tareas y actividades diarias como comer, beber y tomar medicamentos. Puede facilitar la supervisión de la persona a través de una enfermera o de los visitantes que aparecen en una pantalla de vídeo con la que la persona mayor puede interactuar. Los médicos pueden visitar a los pacientes virtualmente y su cara puede aparecer en el monitor del robot. Sin embargo, las preocupaciones que surgen de este tipo de tecnología serían que nuevamente se reduciría el contacto y la compañía humana, así como la violación de su derecho a la privacidad. [41]

En la UE, en la actualidad, está claro que existe una gran preocupación de que el despliegue generalizado de dispositivos del IoT lleve a la alienación y el aislamiento porque los objetos alimentados con IoT son capaces de comunicarse con otros dispositivos alimentados con IoT, lo que significa que pierden el contacto con las preferencias humanas. La Comisión Europea quiere asegurarse de que los dispositivos y servicios del IoT mejoren la vida de los usuarios, dándoles poder mediante la aplicación de ciertas salvaguardias para proteger a los ciudadanos. El IoT, según la Comisión Europea, tiene la capacidad de establecer conexiones entre los seres humanos y el dispositivo alimentado por IoT que están utilizando. La tecnología del IoT tiene la capacidad de minimizar el aislamiento y proporcionar valiosos sistemas de movilidad y seguridad para mejorar la participación de las personas en la sociedad. Sin embargo, también identifica que cuanto más "inteligentes" sean los objetos, mayor será el potencial de uso indebido. [42]

8.2. Riesgos para la privacidad y la seguridad

El número de dispositivos conectados al IoT en todo el mundo aumentará de 20.350 millones en 2017 a 75.440 millones en 2025. Naturalmente, el aumento del número de este tipo de dispositivos aumentará el número de ataques a estos dispositivos. Muchos de estos ataques vendrán en forma de ataques DDoS, Denegación de Servicio Distribuido. Estos ataques ocurrirán debido al potencial de obtener grandes cantidades de datos de los usuarios y la posibilidad de obtener una ganancia financiera de esta información. En relación con el envejecimiento de la población, un ejemplo de este tipo de ataque sería comprometer un dispositivo médico implantado de un paciente y recuperar información personal de salud o detener el funcionamiento de este dispositivo, lo que podría tener graves consecuencias que pondrían en peligro la vida. [43]

En 2016, se produjo un ataque DDoS a gran escala que hizo que grandes sitios web como GitHub y Twitter fueran inaccesibles para los usuarios. Este ataque se llevó a cabo utilizando una red de robots y comprometió un gran número de dispositivos del IoT como cámaras IP, gateways y monitores de bebés. Este tipo de ataques continúa sucediendo ya que se ha observado que muchos estadounidenses son demasiado optimistas acerca de cómo se están utilizando sus datos y no consideran las amenazas. Por ejemplo, sólo el 26% de los estadounidenses no aceptan que su información de salud sea compartida con su médico.

A medida que los sistemas que alimentan los dispositivos del IoT se vuelven más complejos, la necesidad de interferencia humana entre los dispositivos es innecesaria. Los dispositivos alimentados con IoT pueden comunicarse entre sí. Por ejemplo, si un propietario de una casa tiene instalado un sistema de hogar inteligente alimentado por IoT, el termostato inteligente puede detectar cuando la temperatura dentro de la casa excede el límite y los enchufes inteligentes de la casa detectan que la unidad de aire acondicionado está en estado de

"apagado", entonces el sistema de hogar inteligente del IoT abrirá las ventanas de la casa. Este sistema no requiere de interferencia humana y puede operar de forma independiente. En términos de atacantes, puede que no sean capaces de comprometer directamente el sistema de hogar inteligente, pero pueden ser capaces de apuntar al ambiente circundante, lo que hace que el sistema de hogar inteligente se comunique. Por ejemplo, el atacante no atacaría directamente el termostato o la ventana automática, pero podría comprometer el enchufe inteligente, lo que activaría el aire acondicionado, lo que a su vez provocaría la necesidad de abrir automáticamente las ventanas y, por lo tanto, crearía una brecha de seguridad física. Los ataques a los sistemas del IoT en el hogar serían, por lo tanto, una combinación de mundos virtuales y físicos.

Cada vez hay más situaciones en las que se utilizan dispositivos del IoT y, por lo tanto, los dispositivos del IoT deben ser diseñados para una gran variedad de escenarios. Esto significa que cada hardware, software, sistema y requisitos de procesamiento son diferentes. Debido a los niveles de los nuevos dispositivos del IoT hay una falta de suficientes controles de seguridad antes de desplegar los dispositivos. Se encontró que más del 90% de los dispositivos del IoT tienen vulnerabilidades de seguridad que pueden ser fácilmente violadas por los atacantes. Además, debido a la cantidad de datos generados sobre los usuarios de estos dispositivos del IoT, se estimó que en 2016 más de 1 millón de dispositivos del IoT fueron atacados debido a la falta de defensas del sistema y de software antivirus. [44]

Los dispositivos del IoT que rastrean la información biológica de los usuarios, como el ritmo cardíaco, la presión arterial, las actividades diarias y la ubicación a través de medidores inteligentes y dispositivos que se pueden llevar puestos son motivo de preocupación cuando se trata de ataques al sistema del IoT. Los atacantes pueden utilizar esta información y con una precisión de más del 90% ver si la casa está ocupada o no a través del análisis de los datos de las alarmas de humo, los sensores de dióxido de carbono, así como el consumo de energía. La invasión de los dispositivos y la recolección de datos sin el conocimiento de los usuarios puede ser utilizada con fines de lucro. La información obtenida al atacar estos dispositivos puede ser vendida a agencias de publicidad y es una preocupación por las fugas de información de privacidad.

Es evidente que los fabricantes no prestan suficiente atención a la seguridad de sus dispositivos del IoT, ya que a menudo se considera una carga de costos adicionales al aplicar las medidas de seguridad. Actualmente, los fabricantes no prestan ni están obligados a prestar ningún servicio de seguridad a los clientes de los dispositivos del IoT. Por ejemplo, no se les exige que proporcionen ningún manual escrito para los clientes en relación con las sugerencias de seguridad o avisos sobre los productos. A menudo los clientes no saben qué información se está recopilando sobre ellos y, por lo tanto, no saben cómo pueden protegerse contra posibles amenazas de ataque. Con el uso generalizado de dispositivos del IoT y el aumento previsto de los mismos, los usuarios no tienen los conocimientos técnicos necesarios para saber cuándo un dispositivo ha sido comprometido y es probable que sigan utilizándolo sin saber que sus datos están siendo robados. [45]

El IoT permite que todo lo real se convierta en virtual, lo que significa que cada persona y cada cosa es localizable, direccionable y legible en Internet. Sin embargo, si no hay bases seguras en el despliegue de dispositivos y servicios del IoT, los riesgos superarán a los beneficios. Para implementar cambios en la seguridad de los dispositivos del IoT es esencial que los fabricantes y los gobiernos comprendan los riesgos actuales asociados con los escenarios del IoT.

Los problemas actuales relacionados con la naturaleza altamente distribuida del IoT, que significa que los componentes del sistema del IoT están ubicados en diferentes computadoras conectadas en red que tienen la capacidad de comunicarse entre sí mediante el paso de mensajes entre las computadoras. El uso de tecnologías frágiles en el IoT crea debilidades potenciales que pueden ser fácilmente atacadas por los piratas informáticos. A fin de evitar las amenazas a las debilidades de los actuales sistemas del IoT, el IoT debe desarrollarse con sólidos fundamentos de seguridad y debe incluir medidas de seguridad en todas las etapas de su utilización.

Al crear y fabricar dispositivos del IoT para el mundo de hoy, debe tenerse en cuenta la privacidad por diseño, la transparencia y la gestión de datos. La privacidad por diseño es un sistema por el cual los usuarios tendrían la capacidad de gestionar sus propios datos. Podrían decidir qué cantidad de sus datos quieren compartir con el propietario o el fabricante del dispositivo. Por ejemplo, si un usuario utiliza un dispositivo del IoT en un parque determinado de una ciudad y el dispositivo tiene la capacidad de compartir datos de localización, el usuario puede decidir compartir los datos de la ciudad en la que se encuentra, pero no del parque específico en el que se encuentra. La transparencia se refiere a la idea de que los usuarios deben saber quién está utilizando sus datos y para qué los están utilizando. La gestión de datos se refiere a la entidad que gestiona los datos personales de todos los usuarios del dispositivo del IoT. Esta es una tarea difícil, ya que algunas empresas pueden tener mejores o peores capacidades para gestionar estos datos debido a los recursos. Sin embargo, debe quedar claro que todas las políticas relacionadas con el almacenamiento y la gestión de datos cumplen la legislación sobre protección de datos, que es un elemento que tendrá una enorme importancia en el futuro de los dispositivos del IoT. [46]

Existen problemas de seguridad, privacidad y confianza en cuanto a posibles ataques DDoS y control de la información privada y personal, así como el control sobre la ubicación física y el movimiento de un usuario con el uso generalizado de dispositivos del IoT. Hay inconvenientes en el manejo de grandes cantidades de información como esta, sin embargo, parece que los beneficios potenciales de los dispositivos del IoT superan los inconvenientes. [47]

En 2012 la Comisión Europea introdujo su Reglamento de Protección de Datos a fin de abordar las cuestiones relativas a la protección de datos en la nueva tecnología. Garantiza la protección de los datos personales, que son todos los datos relacionados con el individuo. Esto es particularmente importante para los dispositivos del IoT, ya que estos dispositivos recogen grandes cantidades de información. Los riesgos para la privacidad se han vuelto muy predominantes con el uso de dispositivos del IoT que almacenan información en la nube, ya que los datos reunidos pueden utilizarse para identificar las pautas de comportamiento de los usuarios que pueden dar lugar a amenazas tanto en línea como fuera de línea. Por ejemplo, un ciberdelincuente puede utilizar la información reunida para obtener beneficios económicos utilizando la información bancaria en línea de la persona mayor, mientras que un delincuente fuera de línea puede utilizar la información sobre el comportamiento reunida para robar en la casa de una persona cuando no está en ella, ya que sabe que los sensores de la casa no han sido activados durante algún tiempo por la persona mayor. [48]

8.3. Riesgos éticos

Los problemas éticos surgen cuando hay una excesiva dependencia de los dispositivos o servicios del IoT por parte de la persona mayor. En lugar de ayudar en sus tareas diarias se vuelven demasiado dependientes y pierden su sentido de independencia. Cuando se diseñan tecnologías IoT para ser utilizadas por la sociedad, es importante que la tecnología beneficie realmente al usuario. La fase de diseño de la tecnología debe basarse en los derechos humanos. Los valores humanos que deben tenerse en cuenta en el desarrollo y la fabricación de tecnologías del IoT incluyen el bienestar humano, la propiedad y el patrimonio, la privacidad, la ausencia de prejuicios, la utilización universal, la confianza, la autonomía, el consentimiento informado, la responsabilidad, la identidad, la calma y la sostenibilidad ambiental. [49] Es evidente que cuando estos derechos humanos no son tenidos en cuenta por las empresas que producen dispositivos del IoT, específicamente en este caso que serán utilizados por la población de edad avanzada, surgen problemas éticos. El factor ético más importante es el bienestar humano y cuando no se tiene en cuenta puede haber consecuencias perjudiciales.

Por ejemplo, una tecnología impulsada por el IoT que ayuda a una persona de edad frágil que ha perdido gran parte de su movilidad es sumamente útil y puede ayudar a la persona de edad a adquirir un sentido renovado de independencia y confianza en su recién descubierta capacidad de moverse como lo hacía cuando era plenamente móvil. Esta tecnología de asistencia, cuando se fabrica teniendo en cuenta el bienestar humano, es ética. Esta tecnología que ayuda a los ancianos y les da un sentido de control y autonomía podría aumentar la capacidad de los ancianos para comunicarse con otros y satisfacer sus necesidades sociales y podría ayudarlos a desplazarse a los lugares de reunión social. Sin embargo, esta tecnología, si no se fabrica éticamente con gran preocupación por el estado mental de las personas mayores, podría tener consecuencias drásticas. Si la persona mayor puede controlar la tecnología para llevarla a los lugares a los que quiere ir, lo que impide que esta tecnología, mal fabricada éticamente, le arroje por un balcón si así lo solicita la persona mayor. La tecnología impulsada por IoT debe encontrar cuidadosamente el equilibrio entre la potenciación de la persona mayor y su movilidad, pero también la protección de situaciones potencialmente peligrosas. Las cuestiones éticas de la fabricación son complejas porque hay elementos de los estados cognitivos y físicos de las personas mayores que deben considerarse. También se plantean cuestiones éticas en relación con la seguridad de los demás que estarán rodeados por el anciano que comanda esta tecnología del IoT. Si la persona mayor solicitara el dispositivo del IoT para patear o lesionar a una enfermera a la que se culparía de ello, la persona mayor que tal vez no esté mentalmente en el estado mental adecuado para aceptar la culpa o la máquina que recibe órdenes de la persona mayor.

En relación con los robots alimentados con IoT que ayudan a los ancianos a vigilar su comportamiento y su salud, así como a ayudarlos físicamente y a proporcionarles compañía, hay que considerar si esta tecnología está beneficiando realmente a los propios ancianos y no está diseñada sólo para ayudar a la sociedad y a los cuidadores, y si los robots tuvieran un efecto negativo en el bienestar de la población que envejece, sería contra intuitivo diseñarlos y utilizarlos.

Las cuestiones éticas que pueden surgir con este tipo de máquinas de asistencia pueden ser que los ancianos tengan cada vez menos contacto humano que antes y una falta de control sobre sus vidas. Estas máquinas reducirán la valiosa interacción social entre los seres humanos y eliminarán la oportunidad de una comunicación humana cuidadosa. Ya hay

muchas personas mayores que viven bastante aisladas y sufrirían aún más con la introducción de estos robots. Este aislamiento puede llevar a menudo a la demencia y a otras reducciones cognitivas. Se ha demostrado que aquellos con mayores niveles de soledad son a menudo propensos a desarrollar la enfermedad de Alzheimer.

El diseño ético es un elemento enorme dentro de las cuestiones éticas relacionadas con los dispositivos IoT. Habría soluciones en esta área, como consultar a los usuarios, profesionales médicos y miembros de la familia mientras se crea la tecnología, pero esto es menos factible en un entorno comercial donde el productor de la tecnología busca sacar provecho del diseño de esta tecnología. Aunque si esto no es un problema en la producción la tecnología podría adaptarse a cada usuario específicamente. Podrían decidir junto con sus cuidadores o su familia con qué se sienten cómodos y con qué no.

Pueden surgir tensiones éticas cuando las empresas empiezan a querer utilizar las enormes cantidades de datos recogidos por los dispositivos del IoT para mejorar las oportunidades de negocio. Las oportunidades de monetizar los volúmenes de datos reunidos sobre el envejecimiento de la población están aumentando y será necesario establecer marcos para el uso ético de esos datos. Teniendo en cuenta la demografía prevista para el futuro del envejecimiento de la población, este sector de la sociedad será muy grande y será un objetivo que las empresas deberán explotar para obtener beneficios de la venta de bienes y servicios. Las empresas tendrán que ofrecer a los clientes y usuarios de sus productos y servicios la posibilidad de acogerse o no a las políticas de recopilación de datos de su empresa. La importancia de esto se ha hecho más evidente debido a la introducción de la 'General Data Protection Regulation' (GDPR) en la UE en 2016. Las personas mayores tienen menos probabilidades de sentirse cómodas con el uso de la tecnología y pueden ser más vulnerables cuando se les hace publicidad o cuando se trata de entender lo que se está haciendo con sus datos y, por lo tanto, deben establecerse políticas para proteger a este grupo demográfico [50].

Con las empresas cada vez más conscientes de los productos éticos en el mercado, el incentivo para crear productos y servicios del IoT éticos se ha hecho más frecuente. El diseño ético es un valor añadido a los bienes y servicios que los clientes están comprando y que son muy valorados y por los que los clientes están dispuestos a pagar. El diseño ético consiste en producir bienes y servicios impulsados por el IoT que respeten los derechos de los usuarios y no sólo se preocupen por obtener beneficios económicos. El diseño ético hace que las decisiones de diseño y diseño de algoritmos dependan del usuario y no simplemente del ingeniero y la empresa, como ocurre tradicionalmente. Los dispositivos del IoT que se diseñan éticamente quieren mantener el más alto nivel de libertad y elección individual y están diseñados para mitigar el riesgo de vulnerabilidades de seguridad.

Los dispositivos del IoT que se diseñan éticamente se basan en una variedad de características que incluyen el control de la recolección y distribución de datos, la aplicación de cambios en la reglamentación a lo largo del tiempo, el apoyo a diferentes contextos y las relaciones de apoyo. El control de los datos se relaciona con el productor del dispositivo del IoT que proporciona transparencia sobre la forma en que se reúnen y distribuyen los datos para su uso. La aplicación de las reglamentaciones a lo largo del tiempo se relaciona con la posibilidad de ampliar ciertas reglamentaciones nuevas sobre los dispositivos del IoT en las diferentes regiones en que funcionan. Apoyar los diferentes contextos se refiere a que la empresa productora diferencie entre los dispositivos que se utilizarán en el hogar y los que se utilizarán en el lugar de trabajo y adapte la forma en que están diseñados en relación con

estos casos de uso específicos. Mientras que las relaciones de apoyo se relacionan con la forma en que el usuario interactúa con el dispositivo y con quién se le permite acceder a los datos recopilados. Las empresas deben garantizar éticamente que haya confianza mutua entre los usuarios del IoT y el servicio de las empresas. El establecimiento de una autenticación por parte de las empresas para demostrar a los usuarios que son una entidad certificada que se ocupa de la información personal del usuario. De esta manera, la empresa puede crear confianza con el usuario y demostrar que la empresa puede ser considerada responsable por la forma en que utiliza los datos personales de los usuarios y recopila y distribuye los datos. El diseño ético reducirá el riesgo empresarial desde una perspectiva jurídica, fomentará una relación de confianza entre la empresa y el cliente y creará una sociedad en la que las personas se sientan bien utilizando productos y dispositivos del IoT en sus hogares. [51]

'Resumen de Riesgos' – Grafico 3

Riesgos de aislamiento	Riesgos para la privacidad y la seguridad	Riesgos éticos
- Posibles problemas psicológicos y físicos - Reducción de la interacción humana - Riesgo de demencia y otras reducciones cognitivas - Reducción de la compañía humana	- Dispositivos de asistencia sanitaria comprometidos - Ciberataques que resultan en violaciones de la seguridad física - Los atacantes podrían ser capaces de monitorear su presencia en el hogar - Robo de datos personales para obtener ganancias financieras	- Los sistemas pueden ser fabricados no teniendo en cuenta los derechos humanos - Peligro para los cuidadores si no se considera el estado mental del usuario - La tecnología podría dañar a las personas mayores en lugar de beneficiarlas - Riesgo de que los datos se almacenen incorrectamente

Fuente: elaboración propia

9. Legislación vigente en la Unión Europea

En la UE se están haciendo esfuerzos para poner a la UE a la cabeza del despliegue del IoT y ponerla por delante de regiones competidoras como Estados Unidos o Japón. El bloque introdujo su Estrategia de Mercado Único Digital, en la que se destaca la necesidad de evitar la fragmentación y fomentar la interoperabilidad para que el IoT alcance su máximo potencial en la región. La Comunicación de Digitalización y la Comunicación de Estandarización en la UE consideran necesario que la estrategia funcione siguiendo tres pilares, un mercado único para el IoT, un próspero ecosistema del IoT y un IoT centrada en el ser humano. La creación de un mercado único para el IoT significa que los dispositivos y servicios que utilizan el IoT podrán conectarse sin esfuerzo en cualquier lugar de la Unión Europea y escalar a través de las fronteras. El próspero pilar del ecosistema se basa en la creación de plataformas abiertas para ayudar a los desarrolladores a innovar. El pilar del IoT centrada en el ser humano está relacionado con el hecho de que todos los sistemas del IoT que funcionen en la UE respetarán los valores europeos y darán poder a las personas que utilizan estos dispositivos y servicios, y se mantendrán altos niveles de protección de los datos personales y la seguridad.

Actualmente, los desafíos que se plantean para la implantación de dispositivos y servicios del IoT en Europa están relacionados con la falta de normas comunes en el despliegue de dispositivos y servicios del IoT, y hay una falta de consenso en la coordinación de políticas de la UE. Esta falta de consenso podría causar otros riesgos, como el riesgo de un colapso del sistema entre los Estados miembros de la UE, el riesgo de un colapso del sistema entre las industrias y el riesgo de que los usuarios se vean obligados a compartir datos y cumplir con las malas prácticas actuales en lugar de desplegar un nuevo sistema del IoT centrado en el ser humano en el que los usuarios puedan confiar en el sistema porque se basa en principios que garantizan la integridad, la privacidad y la seguridad.

Es evidente que para que la UE despliegue un mercado único para el IoT debe facilitarse un flujo de datos mediante medidas que incluyan la generación de datos, la transferencia de datos, el almacenamiento de datos, el procesamiento de datos y la prestación de servicios de datos. Para que esto suceda, la UE ha establecido la estrategia del mercado único digital para adoptar la iniciativa de la libre circulación de datos. Esta iniciativa garantiza que los datos puedan fluir entre los Estados miembros sin barreras. Sin embargo, se han planteado preocupaciones sobre la propiedad de los datos en relación con esta iniciativa. Los problemas parecen surgir cuando los datos son generados por un dispositivo del IoT, como los datos de los sensores, y no están directamente relacionados con los datos personales del propietario. Los problemas con la identificación del propietario de los datos conducen a problemas de accesibilidad a los datos.

Debido a la creciente complejidad de los ecosistemas del IoT que contienen cada vez más pasos y actores como los fabricantes de productos, productores de software, empresas de análisis de datos y fabricantes de sensores, existe una mayor preocupación sobre la responsabilidad por los problemas que puedan ocurrir. Asignar la responsabilidad a cualquier actor o parte del ecosistema es una tarea difícil, ya que pueden surgir cuestiones como "quién es responsable de garantizar la seguridad del producto", "quién es responsable de garantizar la seguridad de manera permanente", y "cómo deberían asignarse las responsabilidades en caso de que la tecnología se comporte de manera insegura, causando daños".

Actualmente en la UE, en virtud de sus leyes, los productos y servicios son tratados de manera diferente cuando se trata de determinar la causa del fallo. El suministro de datos en el marco de un sistema del IoT se considera un servicio en la Unión Europea y, por lo tanto, identificar dónde se han producido daños o perjuicios por el suministro de datos falsos o por la falta de suministro de datos es más complicado que los protocolos de responsabilidad por productos en la UE en la actualidad.

En este momento la Unión Europea está especialmente centrada en desarrollar y fortalecer la confianza en el IoT entre sus ciudadanos. Está desarrollando la confianza, garantizando la seguridad y la protección de los datos personales y la privacidad, al tiempo que se centra en las necesidades de sus ciudadanos en la era digital. Se centra más en la creación de un sistema del IoT centrado en el ser humano, en el que el IoT potencie a las personas y no las transforme en rehenes de la tecnología. Esto se está haciendo, asegurando que los usuarios comprendan plenamente el papel, el funcionamiento y el impacto que la tecnología del IoT tiene en sus vidas, sus elecciones y su entorno. También se están estableciendo precauciones para garantizar que las personas adecuadas puedan acceder electrónicamente a todos los datos médicos del usuario y también para que los usuarios puedan mantener el control de sus propios datos y comprendan las repercusiones de compartir sus datos personales. La Comisión quiere asegurarse de que los sistemas del IoT sean confiables, aceptados, deseados,

accesibles y utilizables, y está tomando medidas para garantizar que la manera en que se diseñan los sistemas del IoT impida que los usuarios no utilicen los servicios, que sólo utilicen estos servicios y que ya no los utilicen cara a cara, que no entiendan la tecnología y, por último, que desconfíen de los sistemas basados en la tecnología.

Ya, mediante el despliegue del IoT en Europa se han tomado medidas para proteger los datos de los usuarios. Las empresas están innovando y desarrollando nuevas ideas y métodos para la protección de los datos personales de los usuarios con el fin de cumplir con esta legislación. Los conceptos de anonimización, por el que se elimina la información que puede identificar a una persona, de seudonimización, por el que se sustituye la información de identificación personal por identificadores artificiales, y de encriptación, por el que se codifican los mensajes para que sólo las personas autorizadas puedan leer la información, están siendo ampliamente utilizados en la UE debido a esta legislación.

En la Unión Europea, la directiva sobre la seguridad de la información en las redes, establecida en diciembre de 2015, pedía que los proveedores de tecnología ejecutaran más soluciones de seguridad cibernética. Esto implica que los operadores de ciertos sectores críticos identificados por los Estados miembros de la UE tomen medidas para gestionar los riesgos de sus operaciones que afectan directamente a la seguridad de las redes y los sistemas de información. Estos proveedores de tecnología también tienen que informar de cualquier incidente que tenga repercusiones importantes en la estabilidad de los servicios que prestan a los usuarios y estarían sujetos a auditorías por parte de las autoridades nacionales. Estos sistemas garantizan la transparencia y el cumplimiento por parte de las empresas que prestan servicios del IoT a los ciudadanos de la UE. [52]

10. Soluciones

Las soluciones que han sido propuestas por una variedad de fuentes implican considerar la creación e implementación de dispositivos y sistemas del IoT de diferentes maneras.

Como se ha mencionado, los valores humanos deben tenerse en cuenta al diseñar un robot y el principal es el bienestar humano. Los problemas surgen cuando a la persona mayor, que puede no estar en el estado mental adecuado, se le da el control de un dispositivo que está diseñado para escuchar lo que le indican que haga. Tiene que haber un equilibrio entre darles poder y mantenerlos a salvo. Se podría utilizar una forma de prueba de conducción para comprobar si la persona es capaz de operar estos robots. Permitir la personalización de la tecnología podría ser una solución útil para adaptarse a las necesidades específicas y al estado mental de cada usuario, porque un sistema que no es adecuado para una persona en particular podría hacerles sentir que están retenidos y que se sienten prisioneros dentro de su propio hogar. [53] Un sistema personalizado para un dispositivo del IoT utilizado por una persona de edad podría hacerse en colaboración con el usuario de edad avanzada, su cuidador o su familiar y un profesional de la salud que podría ayudar a proporcionar un diagnóstico sobre su estado mental y qué tipos de características debería tener el dispositivo del IoT para esta persona específica.

Entre las soluciones a los obstáculos que impiden la aplicación generalizada del IoT figuran el fomento de la confianza mediante la elaboración de disposiciones firmes de privacidad y seguridad, la redacción de principios de minimización de datos, la protección de datos por diseño y la protección de activos por defecto una vez que se adopte la reglamentación de protección de datos prevista y la concesión a los pacientes del control de sus propios datos.

Otra táctica propuesta sería consultar al personal, como médicos y enfermeras, que utilizarían la tecnología durante la fase de diseño del desarrollo de la aplicación, por ejemplo. Es evidente que las personas que viven en zonas rurales de todo el mundo podrían beneficiarse de este tipo de consulta a distancia con los profesionales médicos muestra que el 75% de la población del Reino Unido se conecta ahora a Internet para obtener información sobre la salud Y el personal médico del Reino Unido ya ha realizado visitas electrónicas, redactando recetas electrónicas y realizando un seguimiento digital a distancia en el sector de la salud, lo que sugiere que existe una voluntad de cambiar el sistema actual. [54]

Puede ser útil ofrecer programas de bienestar y cultura a través de una comunidad social en línea. Esto podría proporcionar beneficios directos accesibles a los adultos mayores. La aplicación de políticas y enfoques educativos centrados en el uso correcto de los medios sociales muestra mejoras en la calidad de vida de los adultos mayores y reforzaría sus necesidades de apoyo social. Debido al hecho de que cada vez más personas mayores están conectadas a Internet y a la predicción del crecimiento de los dispositivos y servicios del IoT, está claro que es necesario educar sobre estos dispositivos. Por ejemplo, el caso de uso de Vodafone explicado anteriormente es una forma en que una empresa que proporciona tecnología que sabe que será utilizada por la población de edad avanzada proporciona información y educación útiles a este grupo demográfico. Si más empresas pusieran en marcha este tipo de iniciativas, más personas mayores se sentirían cómodas con este tipo de tecnología del IoT y sabrían cómo están utilizando sus datos las empresas y cómo protegerse mejor de los posibles riesgos virtuales y físicos.

Para fomentar el uso generalizado de ciertas tecnologías podrían vincularse con la industria de los seguros. En el sector de los seguros, la aceptación de grabadores electrónicos en ciertas cosas como los automóviles puede vigilar la seguridad de la conducción de una persona y es probable que permita al usuario disponer de un seguro más barato basado en la seguridad del conductor. [55] La aplicación de estrategias a través de la industria de los seguros es una posible forma de confiar en el uso generalizado de los dispositivos del IoT. Si los ciudadanos de edad avanzada implementan la tecnología del IoT en sus hogares mediante el uso de casas inteligentes o ciertos aparatos conectados, se sentirán seguros al estar protegidos por un seguro, así como se beneficiarán de posibles pólizas de seguro de hogar más bajas, que a menudo son más altas para las personas de edad avanzada.

Un enfoque que podría adoptarse en el futuro del IoT y la protección de los datos de los usuarios es un sistema de autenticación mediante el cual podría utilizarse la bioidentificación, por ejemplo, utilizando una identificación mediante huellas dactilares en la apertura de una puerta de un determinado edificio seguro o un objeto personal como un pasaporte, una tarjeta de identificación o un teléfono inteligente. Los objetos del IoT también podrían diseñarse para defenderse de los fallos y ataques de la red. Deberían aplicarse mecanismos para que los objetos reaccionen a situaciones anormales y notifiquen a otros objetos esta amenaza y también para identificar a los operadores humanos de cualquier daño. Una vez que se ha producido un ataque, el dispositivo debería programarse para recuperarse rápidamente de los daños e identificar la ubicación de las zonas seguras e inseguras de la infraestructura para evitar nuevos ataques y promover el aprendizaje continuo en el área de los dispositivos del IoT, ya que va a ser un fenómeno tan omnipresente en el futuro. [56]

11. Conclusiones

Creo que, desde los puntos que he investigado en este trabajo, los beneficios de IoT para el envejecimiento de la población superan en gran medida los riesgos, además, algunos de los riesgos pueden ser eliminados en un futuro próximo con nuevas innovaciones tecnológicas. Con las mejoras en la tecnología vienen mayores habilidades y oportunidades para los humanos. Como hemos visto en la historia reciente, el mundo no puede vivir sin conexión a Internet y un número cada vez mayor de dispositivos domésticos conectados. En mi opinión, según las diferentes fuentes investigadas para este trabajo, el envejecimiento de la población será uno de los segmentos de población más afectados positivamente por estos dispositivos, ya que su atención médica y su vida social dependerán de ellos. Ha habido un gran aumento en el número de dispositivos de uso, así como en las aplicaciones sanitarias que se descargan. Los dispositivos 'IoT' que se están usando muestran mejores interacciones entre los pacientes y los profesionales de la salud, así como un mejor control de la persona mayor para ayudar a sus cuidadores y a los miembros de la familia. Estos dispositivos y sistemas están ayudando a la persona mayor con las tareas diarias como tomar medicamentos o realizar otras tareas necesarias. Los dispositivos están ayudando a detectar cualquier síntoma subyacente de la enfermedad que el usuario pueda estar mostrando para prevenir consecuencias graves. Los sistemas también han hecho que la vida en solitario sea más cómoda y agradable, ya que hay menos preocupaciones. Estos dispositivos están permitiendo que la persona se sienta mucho más independiente ya que ayudan a la seguridad del hogar, ahorrando energía y mejorando sus habilidades. Estos dispositivos del 'IoT' también están ayudando a la persona mayor a ser más social y a superar cualquier ansiedad social, dándole información sobre el lugar al que va a ir, permitiéndole conectar con su familia y amigos de nuevas maneras y también ganando confianza en sus habilidades de tecnología de la información.

Los usuarios de este tipo de tecnología se enfrentan a desafíos ya que son más vulnerables a las estafas y los ciberataques. El volumen de información sobre estos usuarios que se está generando está aumentando enormemente y, por lo tanto, es probable que sea un objetivo de los ciberdelincuentes. Los usuarios pueden experimentar el robo de su información, la piratería de sus dispositivos y posiblemente el fallo de estos dispositivos debido a esta piratería. También existe la amenaza de que se produzcan violaciones de la seguridad física y es posible que los delincuentes puedan piratear el sistema en línea para acceder al hogar de los usuarios. Además de estos riesgos de seguridad, existen riesgos de aislamiento para la población de edad avanzada. Pueden experimentar aislamiento social porque no tienen contacto con los cuidadores físicos. Esta falta de contacto humano esencial y de comunicación podría llevar a problemas de salud psicológicos o físicos.

Dado que este segmento de la población se utilizará y, dependiendo de estos objetos, serán los más atacados por los ataques cibernéticos y las invasiones de la privacidad, ya que a menudo son el segmento más vulnerable de la sociedad. Creo que los gobiernos deberán intervenir y trabajar con las compañías multinacionales que son las que en la mayoría de los casos desarrollan estos dispositivos conectados para crear marcos legales para diferentes niveles de seguridad en los artículos y una nueva legislación sobre ciberdelincuentes que violan la privacidad y seguridad de otros. También es fundamental que los gobiernos establezcan programas de educación para que la población que envejece se familiarice con las nuevas tecnologías que estarán disponibles para comprar en sus hogares y que se utilizarán en hospitales y centros de atención. También es importante que se mejore la tecnología para protegerse de los ciberataques.

12. Líneas de investigación futuras

Me hubiera gustado la oportunidad de explorar más profundamente las implicaciones para los ciberdelincuentes por parte de los gobiernos si hubiera encajado dentro de los parámetros de este trabajo. Hubiera sido interesante entender más profundamente qué tipo de planes necesitarán implementar los gobiernos para los dispositivos conectados y cómo los implementarán, por ejemplo, a nivel local, nacional o con otros gobiernos a nivel internacional.

Creo que sería interesante explorar cómo se están creando los dispositivos. Por ejemplo, hay alguna consulta con los cuidadores, los médicos o incluso los familiares de los usuarios de estos dispositivos. Este tipo de consulta puede dar lugar a mejores dispositivos que se ajusten a las necesidades exactas de este grupo demográfico y serviría para comprender mejor para quiénes están diseñando los fabricantes y cuáles son sus necesidades.

También me hubiera gustado investigar qué tipo de campañas, si las hubiera, realizan los gobiernos de Europa o incluso del resto del mundo en países más desarrollados tecnológicamente como los Estados Unidos de América o los países de Asia para educar a la población de edad avanzada sobre el uso generalizado de estos dispositivos y cómo pueden desarrollar sus conocimientos de tecnología de la información para poder utilizar cómodamente estos dispositivos en su vida cotidiana.

13. Bibliografía

[1] Bandyopadhyay, D. and Sen, J., 2011. Internet of Things: Applications and Challenges in Technology and Standardization. *Wireless Personal Communications*, 58(1).

[2] F. Meneghello, M. Calore, D. Zucchetto, M. Polese and A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8182-8201, Oct. 2019.

[3] R. Roman, P. Najera and J. Lopez, "Securing the Internet of Things," in Computer, vol. 44, no. 9, pp. 51-58, Sept. 2011.

[4] Sánchez López, T., Ranasinghe, D.C., Harrison, M. *et al.* Adding sense to the Internet of Things. *Pers Ubiquit Comput* 16**,** 291–308 (2012).

[5] S. Tozlu, M. Senel, W. Mao and A. Keshavarzian, "Wi-Fi enabled sensors for internet of things: A practical approach," in IEEE Communications Magazine, vol. 50, no. 6, pp. 134-143, June 2012.

[6] Bandyopadhyay, D. and Sen, J., 2011. Internet of Things: Applications and Challenges in Technology and Standardization. *Wireless Personal Communications*, 58(1).

[7] European Commission, 2016. *Advancing The Internet Of Things In Europe*. Brussels: European Commission.

[8] European Commission, 2016. *Advancing The Internet Of Things In Europe*. Brussels: European Commission.

[9] European Commission, 2016. *Advancing The Internet Of Things In Europe*. Brussels: European Commission.

[10] European Union, 2015. *People In The EU: Who Are We And How Do We Live?*. Luxembourg: Publications Office of the European Union.

[11] Ec.europa.eu. 2020. *Database - Eurostat*. [online] Available at: <https://ec.europa.eu/eurostat/data/database> [Accessed 23 February 2020].

[12] Ec.europa.eu. 2020. *Database - Eurostat*. [online] Available at: <https://ec.europa.eu/eurostat/data/database> [Accessed 23 February 2020].

[13] Ec.europa.eu. 2020. *Database - Eurostat*. [online] Available at: <https://ec.europa.eu/eurostat/data/database> [Accessed 23 February 2020].

[14] Ec.europa.eu. 2020. People In The EU - Statistics On Household And Family Structures - Statistics Explained. [online] Available at: <https://ec.europa.eu/eurostat/statistics-explained/index.php/People_in_the_EU_-_statistics_on_household_and_family_structures#Single-person_households> [Accessed 3 March 2020].

[15] European Union, 2015. *People In The EU: Who Are We And How Do We Live?*. Luxembourg: Publications Office of the European Union.

[16] Ec.europa.eu. 2020. *Database - Eurostat*. [online] Available at: <https://ec.europa.eu/eurostat/data/database> [Accessed 23 February 2020].

[17] European Union, 2015. *People In The EU: Who Are We And How Do We Live?*. Luxembourg: Publications Office of the European Union.

[18] Saltman, R., Dubois, H. and Chawla, M., 2006. THE IMPACT OF AGING ON LONG-TERM CARE IN EUROPE AND SOME POTENTIAL POLICY RESPONSES. *International Journal of Health Services*, 36(4), pp.719–746.

[19] Taylor, K., 2015. *Connected Health How Digital Technology Is Transforming Health And Social Care*. London: Deloitte LLP.

[20] *Studies in Big Data*, 2018. Internet of Things and Big Data Analytics Toward Next-Generation Intelligence.

[21] Pollack, M.E. 2005, "Intelligent Technology for an Aging Population: The Use of AI to Assist Elders with Cognitive Impairment", *AI Magazine,* vol. 26, no. 2, pp. 9-24.

[22] Pollack, M.E. 2005, "Intelligent Technology for an Aging Population: The Use of AI to Assist Elders with Cognitive Impairment", *AI Magazine,* vol. 26, no. 2, pp. 9-24.

[23] Sharkey, A. and Sharkey, N., 2010. Granny and the robots: ethical issues in robot care for the elderly. *Ethics and Information Technology*, 14(1), pp.27-40.

[24] Taylor, K., 2015. *Connected Health How Digital Technology Is Transforming Health And Social Care*. London: Deloitte LLP.

[25] Mattern, F. and Floerkemeier, C., n.d. From the Internet of Computers to the Internet of Things.

[26] Mulvenna, M., Hutton, A., Coates, V., Martin, S., Todd, S., Bond, R. and Moorhead, A., 2017. Views of Caregivers on the Ethics of Assistive Technology Used for Home Surveillance of People Living with Dementia. *Neuroethics*, 10(2), pp.255-266.

[27] *Studies in Big Data*, 2018. Internet of Things and Big Data Analytics Toward Next-Generation Intelligence.

[28] Atzori, L., Iera, A., Morabito, G. and Nitti, M., 2012. The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization. *Computer Networks*, 56(16), pp.3594-3608.

[29] Sharkey, A. and Sharkey, N., 2010. Granny and the robots: ethical issues in robot care for the elderly. *Ethics and Information Technology*, 14(1), pp.27-40.

[30] Oakley, M. and Bovill Rose, C., 2018. *Harnessing Technology To Tackle Loneliness*. [ebook] WPI Economics. Available at: <https://public-vodafone-a.s3-eu-west-

1.amazonaws.com/wp-content/uploads/sites/2/2019/03/Harnessing-technology-to-tackle-loneliness.pdf> [Accessed 16 February 2020].

[31] Goll, J., Charlesworth, G., Scior, K. and Stott, J., 2015. Barriers to Social Participation among Lonely Older Adults: The Influence of Social Fears and Identity. *PLOS ONE*, 10(2), p.e0116664.

[32] Goll, J., Charlesworth, G., Scior, K. and Stott, J., 2015. Barriers to Social Participation among Lonely Older Adults: The Influence of Social Fears and Identity. *PLOS ONE*, 10(2), p.e0116664.

[33] Atzori, L., Iera, A., Morabito, G. and Nitti, M., 2012. The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization. *Computer Networks*, 56(16), pp.3594-3608.

[34] Sharkey, A. and Sharkey, N., 2010. Granny and the robots: ethical issues in robot care for the elderly. *Ethics and Information Technology*, 14(1), pp.27-40.

[35] Nam, S., 2019. Mediating effect of social support on the relationship between older adults' use of social media and their quality-of-life. *Current Psychology*,.

[36] Nam, S., 2019. Mediating effect of social support on the relationship between older adults' use of social media and their quality-of-life. *Current Psychology*,.

[37] Levy, B., Slade, M., Chang, E., Kannoth, S. and Wang, S., 2018. Ageism Amplifies Cost and Prevalence of Health Conditions. *The Gerontologist*,.

[38] Forkan, A., Branch, P., Jayaraman, P. and Ferretto, A., 2020. An Internet-of-Things Solution to Assist Independent Living and Social Connectedness in Elderly. *ACM Transactions on Social Computing*, 2(4), pp.1-24.

[39] Forkan, A., Branch, P., Jayaraman, P. and Ferretto, A., 2020. An Internet-of-Things Solution to Assist Independent Living and Social Connectedness in Elderly. *ACM Transactions on Social Computing*, 2(4), pp.1-24.

[40] Sharkey, A. and Sharkey, N., 2010. Granny and the robots: ethical issues in robot care for the elderly. *Ethics and Information Technology*, 14(1), pp.27-40.

[41] Sharkey, A. and Sharkey, N., 2010. Granny and the robots: ethical issues in robot care for the elderly. *Ethics and Information Technology*, 14(1), pp.27-40.

[42] European Commission, 2016. *Advancing The Internet Of Things In Europe*. Brussels: European Commission.

[43] Zhou, W., Jia, Y., Peng, A., Zhang, Y. and Liu, P., 2019. The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. *IEEE Internet of Things Journal*, 6(2), pp.1606-1616.

[44] Zhou, W., Jia, Y., Peng, A., Zhang, Y. and Liu, P., 2019. The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. *IEEE Internet of Things Journal*, 6(2), pp.1606-1616.

[45] Zhou, W., Jia, Y., Peng, A., Zhang, Y. and Liu, P., 2019. The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. *IEEE Internet of Things Journal*, 6(2), pp.1606-1616.

[46] R. Roman, P. Najera and J. Lopez, "Securing the Internet of Things," in Computer, vol. 44, no. 9, pp. 51-58, Sept. 2011.

[47] Bandyopadhyay, D. and Sen, J., 2011. Internet of Things: Applications and Challenges in Technology and Standardization. *Wireless Personal Communications*, 58(1).

[48] Baldini, G., Botterman, M., Neisse, R. and Tallacchini, M., 2016. Ethical Design in the Internet of Things. *Science and Engineering Ethics*, 24(3), pp.905-925.

[49] Sharkey, A. and Sharkey, N., 2010. Granny and the robots: ethical issues in robot care for the elderly. *Ethics and Information Technology*, 14(1), pp.27-40.

[50] Baldini, G., Botterman, M., Neisse, R. and Tallacchini, M., 2016. Ethical Design in the Internet of Things. *Science and Engineering Ethics*, 24(3), pp.905-925.

[51] Baldini, G., Botterman, M., Neisse, R. and Tallacchini, M., 2016. Ethical Design in the Internet of Things. *Science and Engineering Ethics*, 24(3), pp.905-925.

[52] European Commission, 2016. *Advancing The Internet Of Things In Europe*. Brussels: European Commission.

[53] Sharkey, A. and Sharkey, N., 2010. Granny and the robots: ethical issues in robot care for the elderly. *Ethics and Information Technology*, 14(1), pp.27-40.

[54] Taylor, K., 2015. *Connected Health How Digital Technology Is Transforming Health And Social Care*. London: Deloitte LLP.

[55] Bandyopadhyay, D. and Sen, J., 2011. Internet of Things: Applications and Challenges in Technology and Standardization. *Wireless Personal Communications*, 58(1).

[56] R. Roman, P. Najera and J. Lopez, "Securing the Internet of Things," in Computer, vol. 44, no. 9, pp. 51-58, Sept. 2011.