¿Qué seguridad? Riesgos y Amenazas de Internet en la Seguridad Humana

What is a security? Risks and Threats in the Internet to Human Security

Rafael Rodríguez Prieto[1]
Universidad Pablo de Olavide (España)

Recibido: 15-01-16
Aprobado: 23-03-16

Resumen

El auge de Internet ha puesto en cuestión muchas normas y aproximaciones sociopolíticas, incluyendo la forma de pensar la privacidad, la seguridad o los riesgos. Estos temas están muy presentes en nuestra sociedad. Este artículo aborda la ciberseguridad sin perder de vista los grandes temas de Internet. Todo ello implica que haya modos distintos de pensar la guerra, la privacidad, los riesgos, los conflictos o las libertades civiles y cómo podemos ajustarlas para garantizar los derechos civiles y la paz en la arena internacional. Son cuestiones serias e importantes pero es precisamente porque importan a todos, es necesario evaluar el impacto de Internet en los mismos. Lo que se pretende en este trabajo es evaluar el papel de la ciberseguridad en la sociedad internacional. Cuando lo que está en juego es el futuro de la paz o nuestras libertades digitales, no se pueden dejar las soluciones solo en manos de gobiernos o expertos. Precisamos comprender qué sucede y calibrar su importancia. Los ciudadanos debemos ser parte de la solución.

Palabras-clave: internet, seguridad, sociedad internacional, ciberguerra, riesgos.

[1] (rrodpri@upo.es) Profesor Titular de Filosofía del Derecho, Universidad Pablo de Olavide. El presente estudio se enmarca dentro del proyecto de investigación: "Las Respuestas del Derecho Internacional y Europeo a los Nuevos Riesgos y Amenazas Contra la Seguridad Humana" (RASEGUR), Plan Nacional de I+D+I (Ref.: DER2015-65906-P) y de la Red de Excelencia sobre "Los actuales desafios del Derecho Internacional", del Plan Estatal de Investigación Científica y Técnica y de Innovación 2013-2016 (DER15-69273-RED).

Abstract

The rise of the Internet has unsettled many norms and socio-political approaches, including how we think about privacy, security or risks. These issues are everywhere throughout our society. This is a paper about cyber security and about big ideas in the Internet. There are different ways of thinking about war, privacy, risks, conflicts or civil liberties and how we can them fit together to guarantee civil rights and peace in the international arena. These are serious important and topics but it is precisely because they matter that it is necessary to evaluate the impact of the Internet on them. The point I want to make it is to evaluate the role of cybersecurity in the framework of international society. When it comes to the future of peace or our digital civil liberties, we can´t leave just the solutions to governments or experts. We all need to understand what is at stake and why it matters. Citizens need to be part of the solution.

Key-words: internet, security, international society, cyberwar, risks.

1. Introducción

Singer y Friedman relatan un hecho de gran interés que tuvo lugar en Londres en 2006. Mientras un alto cargo del gobierno sirio paseaba por la ciudad, un equipo israelí entró en su habitación e instaló un troyano en su computadora portátil. Gracias a ello, los israelíes pudieron acceder a una foto que, de no reconocer a los dos personajes que estaban en la misma, hubiera sido inocua: un líder del programa nuclear de Corea del Norte y el jefe de la Comisión Siria de Energía Atómica. Así, esta computadora se transformó en una verdadera alarma atómica (Singer & Friedman, 2015, 126). La ciberseguridad se ha convertido en un elemento central tanto para instituciones como personas. Es además un sector con un crecimiento vertiginoso. Se estima que las necesidades de expertos en esta área serán cada vez mayores, por lo que se trata de una de las profesiones y negocios con mayor futuro.

El efecto de la ciberseguridad en el ámbito de las relaciones y el derecho internacional y los derechos individuales está sujeto a una notable controversia. No existen respuestas fáciles y las preguntas que se formulan son difíciles de calibrar. ¿Hasta qué punto podemos entender la ciberguerra como una amenaza a la paz y la seguridad internacional? ¿Qué diferencias o qué aportan a este concepto otros anejos como ciberarma, ciberesponaje o ciberoperación? ¿Cómo separar el mito y la mera retórica de lo que es realmente relevante?

Internet se ha conformado como un elemento central de nuestras vidas. Nos relacionamos con él durante toda la jornada; desde su inicio hasta el final. Para algunos, encender su teléfono móvil y consultar los mensajes, que les han llegado por cualquiera de las redes sociales que existen, es la primera acción del

día. Posteriormente, nos sentamos delante de una computadora con acceso a la Red o almorzamos mientras revisamos nuestras páginas favoritas en la tableta o nuestra cuenta bancaria. En la tarde-noche vemos la televisión a través de cualquiera de los canales que transmiten películas o eventos deportivos a través de Internet. Estas actividades han sido naturalizadas de tal manera, en unos pocos años, que se han hecho tan indispensables como la higiene diaria o el sueño. Esta conectividad extrema implica, como cualquier parte de la actividad humana, consecuencias.

Como han señalado multitud de expertos la tecnología es política y con ella se obtienen y se pierden capacidades (Bowers, 2014). La sublimación neomitológica que envuelve la idea de lo digital no puede obstaculizar un análisis riguroso de los procesos sociopolíticos y económicos sobre los que influye. Un ejemplo reciente lo constituye el cibermédico. Hace unos meses aparecía en un periódico de Australia la noticia de que en el futuro no será necesario consultar a un médico como hasta ahora. Los pacientes desde su casa podrán obtener un diagnóstico en poco tiempo e incluso fabricarse sus propias píldoras en su impresora 3D.

No cabe duda de que la propuesta contiene elementos beneficiosos. En circunstancias especiales puede ayudar a una persona que se encuentra aislada, por ejemplo, a conocer la gravedad de la dolencia que le aqueja y planificar una evacuación. Puede ser un vehículo que permita la atención médica de comunidades o núcleos de población alejados o incomunicados. No obstante, también puede ser una información usada por compañías de seguros para denegar pólizas o una vía para prestar una atención sanitaria de segunda categoría a aquéllos que no puedan pagar un equipo médico humano. También podría ser una forma de prescindir de miles de médicos y enfermeras en un contexto de mercantilización de la atención sanitaria. De aislarnos más y generar más enfermedades mentales. Muchas personas van al médico esperando una palabra de alivio o el contacto con otro ser humano. La automatización del proceso liquidaría esta parte de la atención médica.

Este caso es un ejemplo más del posible impacto de Internet en las vidas de las personas. Tampoco se puede constreñir la experiencia cibernética a una relación entre el ser humano y la Red. Con el Internet de las cosas, serán los propios aparatos los que en los próximos años se comunicarán entre sí, intercambiando datos y tomando decisiones. Por citar el más obvio, la nevera realizará un inventario de los productos que alberga y enviara al supermercado una comunicación en la que requerirá las mercancías que faltan o están a punto de acabarse. Como anteriormente se afirmó, existen beneficios, pero también perjuicios. Habrá compañías que conozcan las características de nuestra dieta y podrán tener un perfil muy definido de nuestros gustos y de los productos que solemos consumir. Sabrán también si profesamos algún tipo de religión o

si abusamos de las grasas monosaturadas, lo que podría constituir un problema si estos datos llegan a nuestra compañía de seguros. Como señala Lucas, tomar precauciones elementales y tratar internet como otros servicios que requieren cautela, como el transporte y la salud, debiera conducir a una toma de conciencia en relación a que los servicios que se publicitan como gratis; éstos, en realidad, aprovechan nuestros datos y los de nuestros contactos o relaciones sociales (Lucas2015:264).

Entre las consecuencias más evidentes de la transformación tecnológica de Internet se encuentra, sin duda, la seguridad. Casi todo el mundo tiene un antivirus que cree inexpugnable. Empero, cuando se invoca la idea de seguridad debe también hacerse con cuidado. ¿A qué nos referimos? En el diccionario de la RAE seguridad es definida como la cualidad de lo seguro. Lo seguro sería aquello exento de riesgos. Una definición más cercana y, tal vez, de mayor concreción sería la que se encuentra en tercer lugar y en desuso, como "fianza u obligación de indemnidad a favor de alguien". Lo primero que se debe señalar es que en el mundo de Internet, más que nunca antes en la historia de la humanidad, la seguridad en su sentido más radical –eliminación de riesgos o indemnidad– es algo ucrónico, es decir imposible. Se pueden limitar o reducir las inseguridades que afectan a los seres humanos pero no eliminarla por completo.

La cuestión que se pretende responder en este trabajo es si Internet como tal puede constituir un riesgo relevante para la seguridad de las personas y los Estados. Para poder responder a dicha cuestión es necesario plantear hasta qué punto Internet puede garantizar y ampliar seguridad o reducirla e incluso suponer un riegos grave para la misma. Partiendo de la premisa de que ninguna acción o creación humana está exenta de riesgo, se debe dirimir si la tecnología que nos ocupa incrementa o reduce nuestra seguridad. Éste será el propósito fundamental de este trabajo. Esta investigación se ocupará de ello y de analizar estos matices que marcan tanto los diferentes tipos de seguridad que se estudiarán a propósito de la Red, como los procesos que determinan sus sentidos y tipos. Se finalizará con unas breves conclusiones que incidirán en la importancia de introducir la deliberación pública en un debate global sobre el futuro de Internet.

2. ¿Existe un riesgo real en Internet? Una aproximación a la ciberseguridad

La ciberguerra y el ciberterrorismo son dos aspectos centrales de la seguridad humana en la Red. ¿Hasta qué punto estas preocupaciones tienen o carecen de fundamento? Parecería que por las recientes pruebas nucleares de Corea del Norte, los atentados y la crueldad de Daesh o las eternas guerras

que se suceden en el corazón de la África subsahariana, el peso de Internet como amenaza a la seguridad internacional sería mínimo y que las factores tradicionales de desestabilización, propiciados por armamento convencional o nuclear, continúan siendo decisivos.

No obstante, organizaciones como la OTAN han elaborado planes e incluido los ciberataques entre los retos para la seguridad internacional. Así, la OTAN aprobó en 2008 su primera política de ciberdefensa después de los ataques contra Estonia. Este el primer acto documentado y probado de ataque a los sistemas informáticos de un estado (anteriormente tuvo lugar uno en Siberia que no ha sido reconocido ni documentado) vino motivado por la represión que hizo el gobierno estonio de la protesta de la minoría rusa por el cambio de ubicación de una estatua al soldado desconocido el día en que se conmemoraba la victoria de las tropas soviéticas en la II Guerra Mundial. En 2010, la OTAN adoptó en una conferencia en Lisboa el concepto de ciberdefensa y la idea de desarrollar un plan para su ejecución. Esta línea estratégica se desarrolló a lo largo de reuniones y compromisos en 2010, 2011, 2012 y 2014 hasta la actualidad.

De acuerdo a estudios como los de Arkin (2015) o Harris (2014) los ciberataques entre estados se han convertido en un hecho habitual. Para el primero, el efecto de la tecnología dron supone toda una revolución en sí (Arkin 2015: 6). Pero también deben ser tenidas en cuenta las amenazas que para la paz y seguridad internacionales constituyen las bandas de delincuentes o terroristas. Sin ir más lejos, no es descabellado pensar en posibilidades tales como la instalación de malware en centros donde se almacenan millones de datos o toma de control de reactores nucleares para hacerlos estallar. El avance de la tecnología ha tenido entre otras consecuencias, que las bandas organizadas para delinquir encuentren todo un arsenal de nuevas posibilidades. Los drones son usados por gobiernos con diferentes finalidades; de hecho, su uso militar ha generado enorme controversia. ¿Qué impide a grupos terroristas utilizar drones o troyanos para atentar dónde y cuándo lo deseen si cuentan con la tecnología que lo hace posible? El acceso a infraestructuras críticas de un estado, como servidores o satélites de comunicación muestra un nuevo tipo de vulnerabilidad, la cibernética, que podría causar un daño muy serio a la propia legitimidad del estado como garante de la seguridad. Si el estado no puede, en términos hobbesianos, garantizarla en tiempos de Internet, se podría cuestionar hasta su propia existencia. A este tipo de seguridad la denominaremos como interestatal y paraestatal.

A pesar de todo, existen enormes dudas en relación a la idea de ciberguerra y esta perspectiva puede cuestionarse de dos maneras. La primera es que aunque se reconozcan ciberataques entre estados, éstos no suponen riesgos evidentes a la seguridad internacional o por lo menos no al mismo nivel que

los tradicionales. Quizá se podría catalogar de conflictos de "baja intensidad" que se dan en el plano cibernético, pero que no se trasladan a la realidad ni ocasionan heridos o muertos. Por otra parte, también se podría añadir que estas tensiones se encuentran más vinculadas a la propaganda –o al espionaje– y que realmente no constituyen una amenaza relevante, más allá de ser un hecho que se ha dado por otros medios más rudimentarios en otros momentos de la historia humana.

Situar los efectos de Internet sobre la seguridad en estos términos implicaría que valorar aspectos como la seguridad en las comunicaciones no está directamente vinculada con un acto de guerra. Para la postura que entiende que Internet se constituye en una amenaza cierta y muy relevante a la seguridad internacional no se puede minusvalorar la seguridad en las comunicaciones. De hecho, otro de los aspectos centrales de la seguridad puede denominarse como cívico-política. La seguridad de las comunicaciones de individuos y estados está más en entredicho que nunca antes. Uno de los derechos fundamentales conquistados a lo largo de procesos históricos que tuvieron un alto coste en vidas humanas, puede estar en entredicho a causa del control que se ejerce sobre la intimidad de las personas. Ya no es solo que el teléfono móvil que usamos suministre datos sobre nuestra vida o permita nuestra localización: el propio material genético secuenciado puede ser una de las mayores herramientas de control de la historia. Las grandes empresas almacenan y procesan nuestros datos. A la vez, estos entes, de acuerdo con entidades gubernamentales, facilitan información personal sobre las personas, con lo que logran ventajas competitivas que engordan la cuenta de resultados de la misma. Los gobiernos usan software espía contra los ciudadanos. Internet depende de una infraestructura, de un cuerpo físico que tiene sus dueños, lo que permite el control sobre el flujo de información (Savat2013). Esta información sensible es almacenada y puede ser tratada de forma ilícita. Pero también puede ser robada por una potencia extranjera o por una banda organizada para delinquir. Los daños que este tipo de situaciones pueden ocasionar a la vida de las personas o a un gobierno, podrían ser de enorme gravedad y afectar, no solo a elementos políticos o cívicos, sino también económicos.

El uso de la Red como una herramienta para desestabilizar estados mediante flujos de entrada y salida de capital, que en unos pocos minutos son capaces de arruinar la economía de países, no debería pasarse por alto. Las crisis económicas son factores de enorme desestabilidad que pueden conducir a conflictos sociales graves que amenacen la paz y la seguridad mundiales. La seguridad socioeconómica de personas y Estados depende de nuevos actores que en la sociedad global se han configurado como muy relevantes. Organizaciones multilaterales, de integración regional, grandes empresas con PIB superior al de estados son entes que un análisis riguroso no puede

ignorar. Internet, como en los casos anteriores, abre posibilidades de mejora en áreas como la educación. Pero también intensifica los efectos perversos de un modelo de relaciones productivas que pretende reducir la influencia de la variable humana a la mínima expresión. La seguridad laboral y social de los seres humanos puede quedar seriamente comprometida a causa de la creciente automatización y externalización. Nos encontramos con un movimiento doble. Por un lado, gracias a la Red, se pueden obtener trabajadores a precios muy bajos. Se puede contratar a alguien a miles de kilómetros por un salario inferior al que se pagaría a un trabajador local, ya se trate de una labor poco especializada o incluso que requiera un alto grado de formación. Pero por otro lado, y gracias a los procesos de creciente automatización que tiene a los robots como elementos centrales del mismo, se puede prescindir de los trabajadores humanos. Se les puede expulsar del mundo del trabajo.

Este proceso también tiene consecuencias que afectan a las propias relaciones sociales de los individuos. Hay autores que estudian familias postfamiliares, donde sus miembros conviven bajo el mismo techo, pero todos están conectados a dispositivos electrónicos (jugando en línea, consultando una web pornográfica o hablando con "amigos" cibernéticos) en diferentes áreas de la casa (Turkle2011). Todo ello genera nuevo modos de sociabilidad que deben ser tenidos en cuenta en una reflexión seria sobre la seguridad humana en Internet.Para una correcta valoración de la entidad del riesgo de Internet a la seguridad se han de analizar estos tres tipos de ciberseguridad que implican la relevancia de Internet como amenaza a la paz y la seguridad internacionales.

De cualquier manera, al usar este tipo de conceptos nos movemos en un terreno resbaladizo, tal y como han puesto de manifiesto expertos como Thomas Rid. El uso de analogías para referirnos a actividades que desarrollamos en la Red es un factor que no debiera ser tomado a la ligera. Hablamos de "almacenar" en un disco duro o en una "nube" y de usar antivirus. Se utilizan constantemente metáforas para acciones que son nuevas y que carecen de conceptos que las expliquen con una claridad semántica mayor. El propio concepto de ciberseguridad exige un conocimiento amplio y multidisciplinar (Rid2013:164-165).

Este análisis no es inmune a una serie de reduccionismos e irresolubles paradojas contenidas en la colisión entre cuestiones como los derechos civiles y la seguridad nacional, el progreso económico y la seguridad social o el desarrollo de la Red y el humano. Realmente, estas paradojas responden en realidad a una comprensión reduccionista de la Red y a un interesado intento de conducir la reflexión al terreno de la dialéctica, donde uno de los polos termina siendo privilegiado en perjuicio del otro. Aislar la seguridad del resto de los procesos vinculados a Internet termina sesgando el propio objeto de análisis. Estas paradojas responden en realidad a una comprensión reduccionista de la

Red y a un interesado intento de conducir la reflexión al terreno de la dialéctica, donde uno de los polos termina siendo privilegiado en perjuicio del otro.

Cuando se plantea la paradoja entre seguridad nacional y la protección de los derechos civiles se da en términos que hacen imposible el mantenimiento y protección de estos últimos, que son excluidos en beneficio de una particular comprensión de la seguridad que se entiende ha de primar sobre cualquier otro elemento en discusión. La contradicción se plantea en términos abstractos y se la aleja conscientemente de las condiciones materiales y sociales de los individuos. Las consecuencias de este planteamiento no pueden ser obviadas. Privacidad e intimidad de los ciudadanos han quedado reducidas a términos inaceptables. Como se aborda en este texto, se ha incrementado de manera extrema el control de los ciudadanos por parte de entes gubernamentales y empresas. Simplemente hemos llegado a un punto en que cualquiera de nuestras actividades puede ser perfectamente seguida, documentada y analizada. El hecho de que no interfiera en la mayoría de los casos en la vida diaria de las personas, no significa que no exista. Tampoco los gobiernos dictatoriales suelen interferir en la vida de la mayoría de los ciudadanos –por ejemplo en China–, sin embargo tienen noticia de ellos y pueden activar la maquinaria del estado en cuanto lo consideraran oportuno. Hoy esa maquinaria es tanto estatal como paraestatal y las empresas privadas colaboran activamente en la misma para obtener ventajas.

Progreso económico y seguridad social es también otro tipo de dialéctica que se ha trasladado a Internet de la sociedad no cibernética. Se establece la idea de que existe una incompatibilidad manifiesta entre el crecimiento y la seguridad laboral y social de los ciudadanos. Simplemente se contraponen ambos polos con la intención de privilegiar uno de ellos. Lo mismo sucede con el desarrollo de la Red y el desarrollo humano.

Todas estas paradojas parten de una concepción reduccionista e ideologizada del problema que privilegia uno de los polos respecto a otros. El usuario de Internet o internauta es reducido a un mero consumidor, lo que además implica la limitación de la innovación. Las amenazas sobre la democracia y la libertad se limita a un asunto sobre comunicaciones o seguridad que es tratado de forma parcial y que solo trasciende a la deliberación pública de manera fragmentaria. Todo ello repercute en una concepción de la Red vinculada a un tecnodarwinismo social que impone una lógica que sitúa la democracia y los derechos humanos como elementos marginales de la misma.

Para analizar estos desafíos y problemas se han de estudiar las tensiones, tendencias y procesos que se producen dentro de Internet, permitiéndonos acceder a cómo se distribuye, se produce y se accede al poder en un contexto socio-histórico determinado. La proposición se basa en el establecimiento de un modelo de análisis para contemplar la disposición del poder en la Red, pudiendo establecerse tendencias e inclinaciones, por lo tanto también podríamos encuadrar nuestro enfoque dentro de los análisis procesuales.

3. Tipos y relevancia de las ciberamenazas a la seguridad humana

Un análisis de los procesos y alcance de las amenazas a la seguridad humana del uso de Internet precisa tanto del estudio de su tipología como de su intensidad. El objetivo es evaluar la relevancia de las mismas y su impacto en la seguridad internacional. Así, se pueden distinguir tres tipos de ciberamenazas: los interestatales y paraestatales, los cívicos-políticos y las que afectan a la seguridad socioeconómica-personal. Las tres se encuentran interconectadas en procesos que trascienden el espacio cibernético y se encuentran determinadas por las relaciones de producción, la hegemonía en la arena global y el establecimiento de relaciones de poder y dominación. Tal y como sucede con el concepto de seguridad, las amenazas a la misma deben ser analizadas en su complejidad y en el marco de los procesos que tienen lugar. De nada servirían enfoques unidimensionales que nos sitúan ante dialécticas manidas y reduccionistas anteriormente aludidas, que siempre privilegian uno de los polos de discusión y, por supuesto, son irresolubles. Buen ejemplo de ello es la manida dialéctica entre seguridad y libertad, tan privilegiada estos días en los medios de comunicación y, desgraciadamente, tan presente en estudios académicos.

La cuestión de la seguridad frente a los derechos es quizá de las que más celebridad y difusión ha alcanzado para al final primar las restricciones en los derechos civiles y justificarlas de acuerdo a una concepción de la seguridad ideologizada y particular. El planteamiento que se hace en este trabajo va más allá de esa visión limitada que no conduce más que a la solución que previamente se tenía en mente. Para ello se presentará el problema en toda su complejidad, trascendiendo enfoques unidimensionales y simplistas. Se cuestionará tanto el sentido de la propia seguridad, como de las amenazas y la concepción que se tiene de la Red como producción de significados y relaciones sociales, políticas y económicas. Una vez analizados los tipos se estudiará la relevancia de las amenazas y su significación global.

Se pueden distinguir diversas posiciones que reflejantanto la falta de un criterio común, como la necesidad que existe de desarrollar y profundizar en este campo del conocimiento. Todo el mundo parece estar de acuerdo en que la ciberseguridad es un hecho trascendental tanto a nivel institucional como personal; no obstante, a partir de ahí comienzan los desacuerdos, especialmente en el grado de importancia de la misma y sus efectos.

En este sentido, se pueden distinguir dos grandes posiciones que se han desarrollado en dos obras muy recientes y que, con las salvedades propias de un tema donde también existen otros enfoques, ejemplifican muy bien esta separación. Por un lado, tenemos a Thomas Rid, con su libro *Cyber war will not take place*, y por otro, la célebre obra de Richard A. Clarke y Knake *Cyber*

War. The Next Threat to National Security. Mientras que el primero critica el alarmismo de Clarke y discute el uso del concepto de ciberguerra, el segundo la sitúa como uno de los escenarios más peligrosos para la paz y la seguridad mundiales en la historia y critica que las autoridades de su país no hagan todo lo que debieran para proteger su infraestructura en caso de ciberguerra (Clarke y Knake 2010: 144).

Con el fin de evaluar los riesgos, Clarke y Knake diseñaron un esquema donde se puntúan tres factores decisivos en un escenario de ciberguerra: capacidad ofensiva, defensiva y dependencia de los sistemas informáticos. Así, en su estudio toma los principales estados del mundo y establece, de acuerdo a estos criterios, unos porcentajes que tratan de definir la mayor o menos vulnerabilidad. Así, sitúan a China como un país con una alta capacidad de defenderse, ya que puede desconectar su red del resto del planeta; sin embargo EE.UU. carece de ella porque su red está operada por compañías privadas que son además propietarias de la misma. Existe, a su juicio, una brecha en la ciberguerra que puede animar a estados a atacar a EE.UU. Esta brecha no se reduciría simplemente aumentando el poder de ataque: ha de urgentemente mejorarse la capacidad defensiva (Clarke& Knake 2010: 148-149).

No cabe duda, de que los ataques entre estados se han multiplicado en los últimos años. Este tipo de agresión sutil puede generar enormes problemas que repercuten en la seguridad de sus ciudadanos. De acuerdo a Bobby Akart, existe una diversidad de conceptos (ciberguerra, ciberterrorismo, ciberespionaje, cibervandalismo) que a veces se confunden entre sí por su escasa claridad; es por ello que debido a la falta de una definición ampliamente aceptada y cristalizada en un tratado internacional que la aclare, la norma no escrita es limitar la definición de ciberguerra (Akart 2015: 17-18). Thomas Rid redefine el concepto en términos que desafían las clásicas ideas de guerra y confrontación, en la medida de que Internet podría suplir de forma sorprendente la violencia por acciones no violentas con tres vectores (espionaje, sabotaje y subversión). Un acto de guerra ha de ser instrumental, político y violento; de acuerdo a estas premisas Rid estima que no existen en la historia ejemplos de ciberguerra que reúna los tres criterios; incluso es complicado encontrar alguno que cumpla con uno (Rid 2013:4). Rid también señala que la propia acuñación de ciberguerra para un conflicto en el ciberespacio procede de la Fuerza Aérea de EE.UU. y su propósito de extender su influencia y obtener un mayor presupuesto (Rid2013: 165). A juicio de esta perspectiva, el concepto de ciberguerra genera más problemas que soluciones y no estaría justificado.

Rid toma de Clausewitz las tres condiciones que han delimitado lo que es un acto de guerra de forma clásica y convencional. Sin embargo, para Clarke y Knake, ciberguerra es un hecho cierto y que además incrementa las posibilidades de la guerra convencional (Clarke& Knake 2010: xiii). Desde estas posturas se

debieran trascender las características tradicionales de la guerra y el conflicto para acomodarlas a los procesos tecnológicos en curso. Quizá esta polémica admita enfoques complementarios y no tan tajantes. Como señalan Singer y Friedman, definir ciberguerra no es tan complicado; en realidad los elementos clave de la guerra en el ciberespacio tienen sus paralelos con la guerra en otros espacios (Singer & Friedman, 2014, 121). Desde esta óptica, aunque no se pueda atribuir directamente a un caso de ciberguerra documentado las características tradicionales de un acto de guerra, sí se podría hacer a las consecuencias que se derivan de los mismos. Pero tampoco se pueden descartar actos de guerra que en un futuro cercano se ajusten a la definiciones más clásicas, como por ejemplo el uso de malware para convertir en una bomba una refinería de petróleo, donde los procesos de automatización son cada vez mayores y la dependencia de los sistemas informáticos es una realidad innegable. Una bala o bomba en sí son inofensivas. Son las consecuencias de su uso lo que genera un acto de guerra. Por consiguiente, aunque directamente el craqueo de un sistema pueda resultar inofensivo en sentido de causar heridos o muerte, a medio plazo pueden ser tan o más demoledoras que un acto de guerra con armamento convencional. La inmediatez o no de las consecuencias no debiera impedir asumir la relevancia de una tecnología que no solo incluye el control de redes de comunicación entre sus posibilidades.

Una definición mínima de ciberguerra usada por buena parte de los expertos es relacionar dicho concepto con acciones realizadas por un estado nación con el fin de penetrar en los ordenadores o redes de otro con el fin de causar daños o desórdenes. Estas ciberoperaciones se pueden graduar en diferentes tipos que van desde el vandalismo, la intrusión, infiltración, la denegación del servicio o la combinación de éstas y en cinco grados de importancia, que van desde un daño mínimo –tipo 1– hasta los efectos catastróficos sobre el país –tipo 5– (Valeriano& Maness2015:85).

Sin embargo, aunque los ciberataques entre estados se hayan convertido en hechos comunes, no suelen trascender. Los manuales de la OTAN sobre aplicabilidad del derecho internacional a la ciberguerra no definen el término de manera específica aunque lo distingue de ciberoperaciones. Lo que se hace es definir ciberarmas, como aquellas que pueden destruir objetos y herir o asesinar a personas (Akart2015:26). Parece como si el desconocimiento de la opinión pública se complementara con una escasez de claridad en el tratamiento de estas amenazas en las instituciones que debieran velar por la seguridad.

Por otra parte, también existen dentro de esta tipología las amenazas que son desarrolladas por organizaciones terroristas o grupos de distinto signo que tratan de lograr sus objetivos mediante vías similares a las usadas por los estados y mediante el uso de estas ciberarmas. Dentro de esta categoría se podrían distinguir las acciones realizadas por bandas delictivas organizadas

con diferentes objetivos, que van desde el lucro a las acciones terroristas. Tal y como insiste Marc Goodman en su libro *Future Crimes*, algunos expertos en contraterrorismo han calificado a Internet como "universidad terrorista" un lugar donde se pueden aprender nuevas técnicas y donde las posibilidades son cada vez mayores (Goodman2015). Las bandas de delincuencia organizada usan los mecanismos tecnológicos más desarrollados para el logro de sus objetivos.

El terrorismo ha encontrado en Internet una interesante veta a explorar. La Red facilita que estas organizaciones puedan dar un paso de gigante en sus acciones. La automatización hace posible que se pueda prescindir del factor más sensible en cualquier tipo de acción terrorista: el humano. No resulta fácil encontrar a personas que se decidan a suicidarse en un avión. Pero puede ser factible encontrar vías que desde tierra permitan el control de un avión para estrellarlo contra un área urbana muy poblada. Tampoco resulta fácil sortear las medidas de seguridad de una central nuclear, pero se puede prescindir de ello, si se logra acceder al sistema que controla el funcionamiento de la misma. ¿Son estas afirmaciones demasiado alarmistas?

Puede que sea altamente improbable un Pearl Harbor o un Hiroshima cibernético, pero tampoco debiera tomarse a la ligera los riesgos que puede entrañar el uso de malware en caso de estados y empresas (Rid, 2013, 174). Los ciberataques a estados y otras entidades, como empresas son hechos preocupantes y que han motivado la apertura de una línea de colaboración entre grandes corporaciones privadas y el gobierno de EE.UU. que matizan las observaciones de Clarke. Fue precisamente la compañía Google, la que después de recibir un ciberataque por el gobierno chino, estableció una colaboración que hoy continúa con la NSA, que es la agencia estadounidense que se ocupa de la ciberseguridad. Ha sido el propio presidente Obama el que ha comparado a la NSA con aquellos primeros patriotas estadounidenses que vigilaban a los británicos, para luego comparar su papel con el de aquellos que interceptaron los mensajes del eje durante la II Guerra Mundial o controlaron los movimientos de los confederados (Harris2014:216).

Como señalan Powers y Jablonsky, el mundo de Internet no está exento de la lucha por la hegemonía y el uso masivo de propaganda en beneficio propio. LaAdministración Obama usa la retórica de la "conectividad" para impulsar la hegemonía de EE.UU. frente a rivales como China. El control de la infraestructura que hace posible Internet invalida el mensaje de políticos como Hillary Clinton. De acuerdo al mismo, Internet puede ser tratado como un espacio público. Sin embargo, el conjunto de redes de ordenadores apropiados y operados de forma privada y de los servidores accesibles a los usuarios alrededor del mundo hacen de la Red algo muy distinto. La verdadera ciberguerra no se centraría solo en la ciberseguridad sino en la lucha por

legitimar las instituciones y normas existentes que gobiernan Internet para asegurar el dominio mercantil y un modelo de desregulación que beneficie a las grandes empresas privadas aliadas y a flujos de información controlados por entidades como la NSA (Powers y Jablonsky 2015: 182 y 100).

Los ciudadanos merecen que se debata sobre ciberseguridad y el alcance real de las amenazas más allá de alarmismos o de mitos que no se compadecen con la realidad de la entidad de las cibermanezas sin estridencias ventajistas o alarmismos. EE.UU. protege sus intereses, como a su vez hace China o cualquier otro gobierno. La sociedad internacional ha de establecer los cauces jurídicos para que el producto de una deliberación pública pueda servir a la ciudadanía y a la paz y seguridad internacionales. En esta necesaria deliberación pública debieran incluirse aquellas amenazas que implican una sistemática erosión de los derechos civiles y políticos. La responsabilidad de los estados y de corporaciones privadas debiera ser asumida.

Los actos de ciberguerra perpetrados por estados u organizaciones terroristas pueden tener efectos devastadores en la seguridad en una doble vertiente: internacional y personal. Pero no solo eso: su propia naturaleza implica además poner en serio riesgo derechos individuales que parecían inamovibles en las democracias occidentales. Derechos civiles y políticos que quedarían en entredicho tanto como consecuencia de la perniciosa y errónea dialéctica entre libertad y seguridad, por un lado. Por otro, el uso que se puede hacer de los datos personales y del control sobre los ciudadanos que las nuevas tecnologías ofrecen. La conexión a Internet es un producto de nuestra época. Se ha convertido en un lugar común subrayar la importancia de la misma en la transformación de las sociedades y el desarrollo económico. Ya hemos visto que hay que tomar con cuidado esta retórica de la conectividad. También hay también voces que denuncian que un exceso de ella puede volverse en contra de los usuarios. Es el caso de David Davidow que en su libro con el muy significativo título *Overconnected: The Promise and Threat of the Internet* refiere esta realidad, especialmente vinculada a la inestabilidad que ciertos rumores hábilmente difundidos en la Red, junto al *feed back* que generan, tienen en el mundo económico (Davidow 2011: 200).

Más allá de esta preocupación, este tipo de amenazas constituye el sector más evidente de los peligros que a la seguridad genera Internet. Cabe distinguir entre varios subtipos: aquéllas que implican el espionaje de gobiernos hacia los ciudadanos; las que se desarrollan mediante la recopilación, explotación y procesamiento de datos de usuarios por empresas privadas; las que protagonizan la propias empresas privadas en relación a usuarios, cuando se arrogan el derecho de censurarlos o reducir cualquier tipo de derechos o libertades, sin las debidas garantías procesales. Todo ello conforma un *ciberleviatán* que pone en grave riesgo la seguridad jurídica y política de los ciudadanos. Derechos que

han tenido como fin garantizar una esfera de privacidad para los ciudadanos pueden verse en entredicho. También todos aquellos que los salvaguardan de controles no realizados en el marco del Estado de Derecho. Estos controles pudieran ser desarrollados tanto desde instancias gubernamentales como desde corporaciones privadas.

Esta grave erosión de derechos civiles y políticos configura una muy preocupante amenaza a la seguridad de las personas. Los gobiernos tienen herramientas de control nunca antes vistas. La concentración empresarial en Internet supone *per se* una amenaza muy relevante a la seguridad, puesto que estos entes se rigen por objetivos que imponen su cuenta de resultados y sus accionistas. Sus objetivos pueden ser muy legítimos siempre que no desborden el marco jurídico al que están obligados y el cumplimiento de los derechos fundamentales. Las revelaciones de Snowden ponen de manifiesto hechos tan preocupantes como que el gobierno de EE.UU. ordenara a Verizon que le suministrara acceso a los metadatos de las comunicaciones realizadas a través de su servicio, lo que contravenía el mandato de la NSA y posiblemente la Constitución de los EE.UU. Así mismo, Microsoft ayudó a la NSA y al FBI a compilar datos de sus usuarios. Mediante el programa PRISM la NSA requirió a Google, Microsoft, Yahoo, Facebook, Apple, entre otras, a suministrarle datos personales de sus clientes. LA NSA sugiere sistemáticamente a las empresas de alta tecnología el uso de "puertas traseras" que reduzcan el nivel de encriptación de los mensajes (Deibert2013:xi-xii).

Los acuerdos y alianzas, que se mencionaron en el punto anterior, pueden ser una herramienta para la ciberdefensa entre estados y la lucha contra organizaciones terroristas y bandas criminales organizadas, pero tampoco se puede ignorar el elevado riesgo que supone para las libertades públicas el hecho de que la censura se esté estableciendo como la regla general en la Red y que las grandes empresas sean depositarias de una información que los ciudadanos pueden confiarles, pero que transferida a instancias gubernamentales puede tener usos que conculquen derechos fundamentales de los mismos. Autores como Neil Richards han insistido en la relevancia de proteger la privacidad intelectual en nuestros días, es decir, los datos sobre lo que leemos, el contenido de nuestros correos o las llamadas telefónicas (Richards2015:160). A nivel europeo, existen proyectos de espionaje masivos como el MUSCULE, capaz de acceder a la información de los usuarios antes de que sea encriptada o los mecanismos de vigilancia masiva en Internet de las inteligencias francesa, española, alemana y sueca en cooperación con el británico GCHQ (Powers y Jablonski 2015: 190).

Derivado de ello, y de la posición de poder e influencia que la concentración de propiedad otorga a las grandes empresas, se encuentra no solo la alianza gubernamentales sino también la amenaza a la neutralidad de la Red. Se trata

de un desafío igualmente decisivo. La seguridad de las comunicaciones y la posibilidad de que éstas se den en un contexto equilibrado. Uno de los factores que más preocupa a los usuarios, la censura, se encuentra también vinculada a varios factores: la neutralidad; la titularidad privada de sitios que son usados como espacios públicos; los límites al ejercicio de la tutela judicial efectiva.

Se reclama una ciberteoría para responder a estos extraordinarios desafíos que están transformando el mundo de forma radical: la propia concepción de los derechos o las relaciones sociales. Pero tal vez, como afirma Ronald Deibert, podría ser suficiente con la aplicación de los grandes principios que han regido las sociedades más justas, libres y prósperas (Deibert2013:236). En concreto, la ciberseguridad vinculada a la ciberguerra, el ciberterrorismo o el control de los ciudadanos, genera muchos y comprensibles recelos. Se entiende no solo como una manera de fortalecer el aparato militar gubernamental, sino como una forma de control ilimitado. ¿Qué es la democracia sin privacidad? Pero a la vez, no se pueden ignorar las vulnerabilidades que encierra esta sobreconexión generalizada a la Red y las oportunidades en un sentido y otro de la misma. Es imprescindible entender Internet como una plataforma de encuentro común que garantice derecho y establezca deberes a los usuarios. Entre estos deberes se encuentra la última de las tipologías que se ha referido, la socioeconómica y personal.

Este conjunto de desafíos a la seguridad humanas son, tal vez, los que suelen ser más negligentemente desatendidos, pero su relevancia es proporcional a su influencia en aspectos que conforman las condiciones materiales en las que las personas desarrollan sus vidas. Y no solo eso. Este tipo de amenazas también pudieran condicionar la forma en que tanto nosotros como las generaciones futuras se relacionarán entre sí. En un sentido nada ha cambiado porque continuamos viviendo en comunidad, pero en otro, todo ha cambiado porque la percepción de la interdependencia entre las personas y su conexión es mayor que en ninguna época anterior (Waite 2015: 118). Todo ello genera consecuencias. El sentimiento de aislamiento, la presión social, la incapacidad para desarrollar habilidades sociales básicas, si no es mediante el uso de una pantalla, han de ser tomados en consideración en un trabajo sobre desafíos de Internet a la seguridad humana.

Periódicamente salen a la luz investigaciones que advierten sobre efectos indeseados de las redes sociales sobre grupos sociales determinados, como el caso de adolescentes. Ningún colectivo es invulnerable a los problemas que se derivan de su uso. El abuso de las redes sociales implica que pudiéramos estar enviando más emoticonos y mensajes que abrazos y besos reales. Hay personas que se sienten más cómodas con sus robots; dicen que ellos no les fallan. La cuestión es que es la sociedad la que está fallando a personas que dicen algo así (Turkle 2015: 358).

No obstante, aún no existe un debate serio sobre las consecuencias sociales de Internet, ni tampoco una educación específica dirigida no solo a prevenir desórdenes en la conducta, sino a permitir a los usuarios un aprovechamiento mayor de un recurso que, en demasiados casos, queda restringido a la utilización de en muy limitado elenco de aplicaciones.

Volviendo a elementos de orden socioeconómico, no puede dejar de llamar la atención el creciente uso de procedimientos que reducen puestos de trabajo en diversos sectores a cambio de que sea el consumidor el que realice el trabajo por sí mismo. No cabe duda de que una aculturación de los ciudadanos más jóvenes en el "hágalo usted mismo", derivado del uso de Internet y de las nuevas tecnologías, favorece tales pretensiones. De esta forma, bancos, supermercados o compañías aéreas pueden engordar su cuenta de resultados y prescindir de miles de trabajadores porque los consumidores han "aceptado" realizar un trabajo que, en principio, no les corresponde. Así, en un buen número de supermercados de las grandes cadenas australianas como Woolworth o Coles, son los propios consumidores los que hace de cajeros y se cobran los productos. En España está creciendo el número de actividades en las que el banco obliga al cliente a usar cajeros. De lo contrario cobran comisiones abusivas para prestar un servicio que antes era normal. En EE.UU. lo que empezó siendo una forma cómoda de viajar, si se llevaba poco equipaje y no era necesario facturar maletas, se está convirtiendo en la regla general. Los propios usuarios obtienen en las máquinas su tarjeta de embarque y realizan todos los demás trámites para facturar el equipaje. La aculturación realizada gracias a Internet ha sido un factor decisivo para que este tipo de estrategias tengan los resultados que las grandes empresas esperaban.

Estos ejemplos no son nimios. Internet tiene efectos positivos en el desarrollo económico, pero si se atiende a la cuestión que se plantea en este trabajo, la amenazas a la seguridad humana, Internet plantea un panorama inquietante. Puede intensificar y agudizar los procesos socioeconómicos que se vienen desarrollando en las últimas décadas de la mano del neoliberalismo y que comprometen gravemente los derechos laborales y sociales, hasta el punto de que en el ideario neocontractualista estos derechos no son reconocidos como tales. Como señala en un muy reciente estudio Nick Dyer, sobre el impacto de Internet en el mundo del trabajo, el desarrollo del capitalismo contemporáneo genera creciente niveles de automatización, que tiene un doble efecto: por un lado se crea un gran número de población excedente; por otro el trabajo se precariza aún más no solo a niveles básicos, sino incluso especializados (Dyer 2015: 196).

El *outsourcing*, la precarización laboral y la automatización son elementos que no pueden pasar desapercibidos. La espacialización es una de las características fundamentales de la economía política de la comunicación.

Ésta actúa en el caso que nos ocupa, ampliando las posibilidades de las grandes empresas de contratación de mano de obra en regiones deprimidas del planeta. Pero no solo se trata de trabajadores escasamente cualificados, los denominados *turks,* sino también de especialistas altamente cualificados a los que se les retribuye muy por debajo de sus colegas europeos o estadounidenses. Esta dinámica cuenta con una doble vuelta. Los procesos de automatización erosionan la posición de los trabajadores y pueden ser decisivos para que el capitalismo prescinda de ellos. Si el pensamiento postfordista había entendido que Internet y las nuevas tecnologías eran una oportunidad para que el trabajo prescindiera del capital y se apropiara de los medios de producción sobre la base de una estrategia cooperativa que usara la innovación como factor de emancipación sociolaboral, hoy nos percatamos que el capitalismo puede ser el que prescinda del trabajo. Incluso aquellos trabajos más especializados están en peligro como antes se señalaba. Con la revolución de la acumulación y procesamiento de datos, lo que se ha venido en denominar *big data*, se automatizan muchos procesos de toma de decisiones gracias a algoritmos. Sin ir más lejos, en noviembre de 2013 Google solicitó una patente que permite crear mensajes de correo electrónico de respuesta y mensajes en redes sociales personalizados basados en todos los datos acumulados sobre la persona (Ford 2015: 93)

De acuerdo a las últimas estimaciones, en los EEUU sobrará en los próximos años alrededor del 60% de los trabajadores (Kaplan 2015). Estamos probablemente ante una de las amenazas más reales a la seguridad humana y la estabilidad de las sociedades. ¿Qué consecuencias puede tener esta masiva expulsión del mundo del trabajo? ¿Qué significará este hecho para el desarrollo personal de millones de personas?

Ya se puede apreciar en barrios de California la desigualdad entre las élites de las grandes empresas tecnológicas y los trabajadores o personas en paro y las tensiones que se están generando. Reacciones como el consumo colaborativo están precarizando trabajos como el de los taxistas, con cuantiosos beneficios para grandes empresas que están detrás de empresas como Uber. Las consecuencias para la seguridad humana de esta erosión de los derechos sociales pueden hacerse evidente a medio y largo plazo. Internet podría condenarnos a conflictos sociales que generarían periodos de enorme inestabilidad.

Una vez estudiadas los tipos de ciberamenazas y analizado su relevancia se puede llegar a la conclusión de que Internet supone un riesgo cierto para la seguridad internacional y para las personas. El siguiente epígrafe se centrará en el análisis de las consecuencias de estos riesgos y en presentar, brevemente, algunas propuestas para una reevaluación de la ciberseguridad vinculada a los procesos que tienen lugar en la Red. El concepto que se usará será el de censura digital (Rodríguez Prieto 2012). Como se ha mencionado anteriormente, es

imprescindible que se establezca un debate y una reflexión colectiva sobre Internet, los derechos y los deberes. No ha existido hasta el momento, lo que no solo ha lastrado la cuestión regulatoria, sino también aspiraciones tan relevantes como la garantía de la paz y seguridad internacional o la protección de los derechos humanos. De hecho, ambos elementos, nada novedosos, deberían ser principios rectores en la conformación de un Internet más seguro, pero también más respetuoso con derechos que tanto esfuerzo demandaron.

4. Consecuencias para la seguridad humana y propuestas

Entender los procesos en Internet es imprescindible para una evaluación de las consecuencias que éstas tienen en la seguridad humana.

Se pueden identificar dos procesos que se agrupan en dos haces de tendencias para el análisis de Internet y, en consecuencia, para los riesgos o amenazas a la seguridad humana en el mismo. Por un lado, tenemos aquellas que se corresponden con un conjunto de "síntomas" que constituyen la censura digital. Este tipo de censura está constituida por una serie de restricciones de contenidos que suponen una grave amenaza a la seguridad y a los derechos y libertades. Las restricciones podrían resumirse en el siguiente cuadro:

R1: Restricción a la libertad de acceso.

R2: Restricción a libertad de intercambio y comunicación.

R3: Restricción a la tutela judicial efectiva.

R4: Restricción a la creatividad político, social y económica.

R5: Restricción a la seguridad.

Estas restricciones de contenidos contienen dos tendencias fundamentales que conformarían el marco de análisis que se propone:

T1: Tendencia al control sobre el acceso a la información y sobre los contenidos.

Esta tendencia englobaría el conjunto de las restricciones a las que hemos hecho referencia.

T2: Tendencia a la construcción de un universo simbólico monocultural.

Esta tendencia se ocuparía de la construcción del imaginario simbólico centrado en la privatización y en la mercantilización de contenidos y acciones y generador de graves riesgos.

Este conjunto de tendencias interaccionadas, ya sea de forma concertada o no, limitan, reducen o liquidan las posibilidades de Internet como generador de vías para la comunicación de los ciudadanos en el marco de las garantías expresadas en los convenios internacionales sobre Derechos Humanos.

La interacción entre estas tendencias implica un proceso, cuyo fundamento filosófico se sustenta en un proceso de control, cosificación y mercantilización

de Internet. Este enfoque filosófico implica una serie de valores que actúan de tal forma que reproducen en Internet la hegemonía vigente en el resto de áreas de la realidad no cibernéticas.

En lo referido a la seguridad, las tendencias que se vinculan para su análisis con procesos que ponen en grave riesgo la seguridad han crecido exponencialmente en los últimos lustros. Los ataques mediante procedimientos cibernéticos que comprometen la misma en las personas y estados son una realidad tangible, aunque escasamente divulgada en la opinión pública. De hecho, no existe una percepción clara de esta amenaza por el común de los ciudadanos. Los terribles atentados de París en que los terroristas iban armados con AK 47 y cinturones de explosivos cabe ser identificados con maneras propias del siglo XX. En el siglo XXI los procedimientos podrían ser aún más mortíferos de mayor impacto si estados o grupos terroristas logran el control de infraestructuras sensibles entre las que estarían medios de transportes, redes eléctricas, centrales térmicas o centrales nucleares con el uso de malware. Thomas A. Johnson identifica tres infraestructuras que por su importancia y su debilidad ante ciberataques son críticas: transporte, energía, sistema eléctrico, y telecomunicaciones (Johnson:2015:46-53). Tampoco es descartable el uso de drones a modo de los que ya emplean los estados para llevar a cabo ataques terroristas masivos y bien planificados en áreas urbanas. La dependencia de la tecnología y las insuficiencias en la seguridad nos hacen, paradójicamente, más vulnerable que nunca a posibles ataques masivos y de extrema gravedad. Antes era necesario hacerse con los mandos de un avión con el concurso de pilotos suicidas; hoy es posible derribar ese mismo avión desde tierra, prescindiendo del factor humano. Las fugas de información que se producen a diario y que incrementa el negocio de los seguros de internet son factores que amenazan también la seguridad.

No obstante, estas amenazas ciertas a la seguridad humana a través de Internet son seguidas de medidas que amenazan la seguridad jurídico-política de las personas, así como la social. Los recortes en derechos y en la privacidad de normas vinculadas con la amenaza terrorista como la *Patriot Act*, en EE.UU. o la reforma constitucional en Francia después de los atentados de París de 13 de noviembre de 2015, establecen límites a libertades públicas muy cuestionables en virtud de la seguridad. Pero ciertamente, estas medidas son solo un aspecto superficial, aunque muy relevante, de la grave erosión de los derechos individuales en los gobiernos representativos occidentales. No se desea disminuir la gravedad de medidas jurídicas como las mencionadas. No obstante, se debe señalar que la recogida y explotación de los datos personales es una de las más poderosas amenazas a la seguridad jurídico política de los ciudadanos. Los mecanismos para rastrear cualquier movimiento o actividad de los ciudadanos comprometen gravemente nuestra seguridad. La ingente

cantidad de información –*big data*– recolectada por las grandes empresas y gobiernos –o ambos en cooperación– no solo liquida la privacidad. También puede suponer una doble amenaza. Por un lado, esa información pudiera caer en manos de organizaciones terroristas o bandas dedicadas al crimen organizado. No es descabellado pensar que la vulnerabilidad de los centros donde se almacena dicha información puede ser aprovechada por organizaciones o personas interesadas en realizar un uso criminal de los datos. Por otra parte, no podemos confiar ciegamente en que los gobiernos y, mucho menos las grandes corporaciones privadas, no hagan un uso de los mismos que contravengan cualquier derecho fundamental.

Nuestra seguridad socioeconómica se puede ver seriamente comprometida con el uso de Internet. El proceso de extrema y radical mercantilización puede tener en la Red un extraordinario aliado. En primer lugar, los trabajos de millones de personas se pueden ver afectados por el *outsourcing*. Esto significa que Internet se utiliza para el reclutamiento de mano de obra que carece de unos estándares de seguridad y derechos laborales mínimos. Este hecho ha permitido que trabajo cualificado haya seguido un camino similar al de la maquila u otras industrias que se han deslocalizados en busca de trabajadores con condiciones laborales más precarias y legislaciones medioambientales y de todo tipo más permisivas o inexistentes. En el caso del trabajo más cualificado, se usa mano de obra que se encuentra en estados donde los salarios son bajos y existe personal con la formación suficiente para realizar un tipo de trabajo que requiere una especialización o formación media-alta o alta.

Pero internet y el cambio tecnológico, no solo permite prescindir de trabajadores cualificados de un determinado área geográfica para buscarlos en el otro extremo del mundo. También posibilita directamente el prescindir de cualquier trabajador humano. El aumento de los procesos de automatización y el uso de robots con capacidad de tomar decisiones puede permitir a medio plazo la sustitución de una cantidad muy significativa de trabajadores humanos por máquinas. Si la inteligencia artificial continúa su avance, nos podemos dar de bruces con una realidad que sobrepase las peores pesadillas que comprometen la seguridad humana. Seres humanos que no tienen ningún objeto en la vida; que carecen de trabajo, de manera de ganarse la vida, de desarrollarse como personas o simplemente de ocupar su tiempo. Este hecho puede generar una crisis sin precedentes a nivel mundial que comprometa la seguridad a todos los niveles y desde todos los puntos de vista.

Ante este escenario, no caben propuestas simples ni trampas o dialécticas estériles que siempre privilegian una interpretación particular de uno de los dos polos en detrimento del otro (seguridad y libertad). Una vez que es evidente el problema de ciberseguridad queda el aspecto de la propuesta.

Lo primero que se debe señalar es que la ciberseguridad no es un aspecto que podamos separar del resto de problemas y desafíos que afectan a Internet. Tratar de resolver las evidentes amenazas que afectan a la paz y la seguridad internacionales sin, en un primer estadio, no entender la seguridad desde una perspectiva amplia y compleja que implica tanto a derechos civiles y políticos como sociales, es un error grave. En un segundo estadio, tampoco se puede conocer y mucho menos comenzar a solucionar este problema sin entenderlo en relación con otros desafíos que plantea la Red, como la neutralidad o los procesos de extremistas de mercantilización de la misma, por poner dos de las preocupaciones fundamentales. Las grandes compañías tienen como uno de sus objetivos principales la erosión de la privacidad, ya que ésta ayuda a obtener mayores beneficios.

Para ello es necesario conocer y estudiar las tendencias que desafían los procesos descritos anteriormente; síntomas de una apertura digital opuesta a la censura digital. Internet está en construcción y ello implica que se den posibilidades de control, pero también posibilidades de desarrollo y fortalecimiento de los derechos fundamentales. Este tipo de apertura está integrada por una serie de desarrollos de contenidos que a su vez generan una serie de tendencias. Los desarrollos podrían resumirse en el siguiente cuadro:

R1: Desarrollo de la libertad de acceso.
R2: Desarrollo de la libertad de intercambio y comunicación.
R3: Desarrollo de la tutela judicial efectiva.
R4: Desarrollo de la creatividad político, social y económica.
R5: Desarrollo de una ciberseguridad amplia y democrática.

Tales desarrollos de contenidos se materializarían en dos tendencias fundamentales que conforman el marco de análisis:

T1: Tendencia la apertura en el acceso común a la información y sobre los contenidos.
T2: Tendencia a la construcción de un universo simbólico diverso y cooperativo.

Ambas tendencias se encuentran interconectadas entre sí y son el producto de los desarrollos de contenidos aludidos. Los procesos de desarrollo de la Red colisionan o complementan; desafían o aceptan, relaciones de dominio sociopolíticas, económicas y culturales del mundo no cibernético y nutre la lucha de fuerzas críticas con el orden geopolítico y socioeconómico hegemónico. No se puede entender Internet, la ciberseguridad o cualquier otro aspecto sin aludir a las relaciones de poder y dominio.

Los procesos actuales de definición y desarrollo de la Red no son espacios fijos, ni realidades concretas y definitivas, son tendencias, posiciones, prácticas, que agrupadas en diferentes conjuntos nos dan pie para la construcción de cada uno de los términos. Es más, en un mismo campo aparecen rasgos de una y otra tendencia, de hecho, yendo más lejos, es posible observar que en un mismo actor pueden concurrir acciones que estén ubicadas en uno o en otro lado. Al plantearnos un abordaje así, la construcción de conceptos que emergen del propio contexto analizado es una necesidad epistémica.

La ciberseguridad debe ser contextualizada en los procesos de diverso signo que actúan sobre Internet y le dan forma. Ésta ha de comprenderse vinculada a la manera en que afectan a las relaciones de poder y dominio. Una reflexión y deliberación sobre qué Internet queremos, implica preguntarnos por los propios procesos sociales que se dan en los espacios no cibernéticos y sobre la dominación o la libertad. Aspectos como la regulación precisan de la conciencia de que hay una serie de derechos, a los que se han denominado como humanos, que deben quedar garantizados en todos los ámbitos de la realidad humana. Que la propia ciberseguridad precisa de ellos, tanto en un sentido que la garantice, como en una medida que no los asfixie.

Ciberseguridad puede sonar a algo novedoso y rompedor, pero al fin y al cabo, se continúa hablando de lo mismo: de la necesidad de poner límites a la dominación, sea del tipo que sea, y a las agresiones que se producen en el curso de su despliegue.

5. Conclusiones

La seguridad es un concepto complejo, que debe ser contextualizado y situado en los procesos sociales. Como se ha apreciado en este trabajo, existe una semántica hegemónica de la seguridad que encierra al mismo en una dialéctica que compromete seriamente las libertades públicas. Después de los atentados de Nueva York, Madrid, Londres y París, se está abriendo paso una doctrina que la afirma sin ningún tipo de complejos que si se desea seguridad, se deben aceptar un recorte radical de los derechos civiles que tanto costó lograr. Desgraciadamente, ninguna ley, ni ningún servicio de policía o de inteligencia puede garantizar que no habrá un grupo de personas dispuestas a matar y a morir ya sea con un cinturón bomba, ametrallando en plena calle o derribando un avión de pasajeros. La sensación de seguridad es muy diferente de una seguridad real. Es dicha sensación, con la que las autoridades pueden comerciar. El problema es que puede salir demasiado cara en términos de derechos y libertades públicas.

Encerrar la seguridad en los estrechos márgenes anteriormente descritos falsifica y mutila la idea. Un enfoque ampliado y complejo de la seguridad, como el que se ha sostenido y justificado en este artículo implica no caer en dialécticas estériles y desarrollar un mayor rigor metodológico en el análisis del núcleo central de esta investigación vinculado al efecto de Internet sobre la seguridad. La primera conclusión que cabe extraer es que las amenazas estudiadas agudizan las tradicionales. Con Internet los riesgos a los que los ciudadanos están sometidos se incrementan de manera exponencial. Lo que antes precisaba de un elaborado plan de vigilancia de una persona, hoy puede ser desarrollado prácticamente desde cualquier computador personal con acceso a Internet; las agresiones a un estado –ya fuera de otro estado o de una organización terrorista– precisaban tradicionalmente de movimientos de tropas, de elaboradas estrategias que aprovecharan el factor sorpresa y de suministros, entre otras infraestructuras. Con el desarrollo de Internet y todo tipo de software malicioso, se puede prescindir de todo ello. Es más: se esperan en los próximos años notables mejoras en la automatización, la robótica, inteligencia artificial o, incluso, biología, que pueden incrementar aún más las amenazas. Secuenciar el ADN terminará siendo barato y una forma de control que superará la ejercida hoy a través de los teléfonos móviles.

Una segunda idea es que la seguridad está sometida a un proceso extremo de mercantilización semejante al que tiene lugar en la Red en sí. Prueba de ello es el relevante nicho de negocio de los seguros informáticos. También el auge de las empresas dedicadas a la seguridad y al control de estas amenazas. Esta mercantilización incide en los acuerdos que se producen entre grandes empresas de la Red con instituciones gubernamentales. Así, se ceden datos personales de usuarios sin control judicial, conformándose una realidad cada vez más beligerantes con los derechos y libertades básicas.

Una tercera conclusión es el efecto político y económico de estas amenazas. Las amenazas terroristas o de bandas organizadas apuntalan liderazgos débiles entre los políticos occidentales. El miedo provoca no solo que los ciudadanos puedan ser más susceptibles de abandonar derechos individuales básicos; también de buscar una cierta proyección en gobiernos deslegitimados por sus políticas impopulares hacia el estado del bienestar y su falta de liderazgo para resolver los problemas reales o enfrentarse a los grandes poderes económicos. Este hecho es uno de los más preocupantes ya que supone una falsificación de la democracia.

Una última conclusión es que la seguridad en Internet depende de los procesos de la propia Red. No se pueden divorciar de ellos, ni de los que tienen lugar en el mundo no cibernético. No existen soluciones mágicas, pero hemos llegado a comienzos del siglo XXI con una serie de derechos garantizados muy importante fruto de luchas sociales de gran significación histórica. La pregunta

sería si estamos dispuestos a tirar todo por la borda en beneficio de un enfoque sesgado y reduccionista de la seguridad. Como se ha estudiado en este trabajo la seguridad es evitar un ciberataque sobre la infraestructura crítica de un estado, pero también es evitar el control de sus ciudadanos sin las garantías procesales que garantiza el Estado de Derecho. Y, por supuesto, es evitar una inseguridad económica y social que amenaza la estabilidad de las sociedades y, por tanto, la paz y la seguridad internacional. El reto es magnífico y el trabajo por delante, tanto a nivel jurídico como político, también. La transformación social es comparable en su calado a la revolución industrial. Por tanto, proporcional para los derechos y libertades y la democracia.

Referencias bibliográficas:

Akart, B., *Cyber Warfare: Prepping for Tomorrow: Volume 1*, Freedom Preppers, 2015.

Arkin, W. M., *Unmanned: Drones, Data, and the Illusion of Perfect Warfare*, New York, Little, Brown and Company, 2015.

Bowers, C. A.,*The false promises of the digital revolution: how computers transform education, work, and international development in ways that are ecologically unsustainable*, New York, Peter Lang Publishing, 2014.

Clarke, R. A. & Knake, R. K, *Cyber War: The Next Threat to National Security and What to Do About It*, New York, Harper Collins, 2010.

Davidow, W. H., *Overconnected: the promise and threat of the Internet*, New York, Delphinium Books, 2011.

Deibert, R. J., *Black Code*, Toronto, Mcclelland & Stewart, 2013.

Harris, S., *@War. The Rise of Cyber Warfare*, London, Headline, 2014.

Johnson, T. A., *Critical Infrastructure, Key Assets: A Targey Key Environment* in, Johnson, T. A. (ed.), *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*, Boca Raton, CRC, 2015.

Kaplan, J., Human *Need Not Apply. A Guide to Wealth and Work in the Age of Artificial Intelligence*, New Haven, Yale University Press, 2015.

Lucas, E., *Cyberphobia: Identity, Trust, Security and the Internet*, New York, Bloomsbury, 2015.

Powers, S. M., Jablonski, M., *The Real Cyber War: The Political Economy of Internet Freedom*, Chicago, University of Illinois Press, 2015.

Richards, N., *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*, New York, Oxford University Press, 2015.

Rid, T., *Cyber War Will Not Take Place*, London, Hurst & CO, 2013.

Rodríguez Prieto, R., "Contra la mitificación de Internet. Una aproximación a la tensión entre un imaginario mercantil y un imaginario compartido en Internet", Revista Internacional de Pensamiento Político, 7, 2012.

Savat, D., *The Uncoding the Digital: Technology, Subjectivity and Action in the Control Society*, New York, Palgrave Macmillan, 2013.

Singer, P. W., Friedman, A.,*Cybersecurity and Cyberwar: What Everyone Needs To Know®*, New York, Oxford University Press, 2014.

Turkle, S., *Alone Together. Why We Expect More from Technology and Less from Each Other*, New York, Basic Books, 2011.

Turkle, S., *Reclaiming Conversation. The Power of Talk in the Digital Era*, New York, Penguin Press, 2015.

Valeriano, B., Maness, R. C., *Cyber War versus Cyber Realities: Cyber Conflict in the International System*, New York, Oxford University Press, 2015.

Waite, C., *The digital evolution of an American identity*, New York, Routledge, 2012.