TECNOLOGÍA Y SEGURIDAD JURÍDICA EN EL CIBERESPACIO: UN NUEVO TERRITORIO, "CYBERIA" DEL RIESGO GLOBAL A LA CONFIANZA DIGITAL

ÁNGEL SATUÉ DE CÓRDOVA MINGUET

ASESOR JURÍDICO SECTOR PÚBLICO EMPRESARIAL. ANALISTA INTERNACIONAL

Fecha de recepción: 24/11/2021. Fecha de aceptación: 14/03/2022

RESUMEN

El mundo es global y complejo. Lleno de riesgos globales. El advenimiento de nuevas tecnologías ha hecho del mundo un lugar más pequeño al estar hiperconectado. La globalización es, en parte, resultado de la tecnología digital. También habitamos un tiempo más rápido. Surgen nuevos retos. Muchas de las disrupciones generadas por la tecnología digital son percibidas como riesgos globales, como el fracaso de la gobernanza tecnológica, pues no sabemos cuándo ocurrirán o su impacto o cómo gestionarlas. El cambio tecnológico, que es digital, nos introduce en la era "tecnolítica" y emerge "Cyberia", como territorio nuevo de algoritmos, creado inicialmente por el hombre y que debe ser debidamente regulado y protegido. En el ciberespacio se hace más necesaria que nunca una regulación, o "Lex Informática", que habrá de ser híbrida, en la que sea posible la convivencia de órdenes jurídicos diversos. Estudiar este contexto es necesario para aproximarnos al estudio de la relación entre tecnología y seguridad, en particular, entre tecnología y autoridades de policía y de justicia penal. La rápida evolución tecnológica y la globalización han planteado nuevos retos en el ámbito de la protección de los datos personales, y del uso de la tecnología. La regulación adecuada que se propone, que es el marco de juego para la actuación de las autoridades policiales, coadyuva a la seguridad de "Cyberia" y, por tanto, a la ciberseguridad en un sentido amplio. Además, aportar seguridad jurídica y delimitar la actuación de las autoridades policiales, a través de la consolidación de un marco normativo adecuado, y partir del previo conocimiento de la relación existente entre tecnología digital y autoridades policiales y de justicia penal, también coadyuva a la ciberseguridad.

Palabras clave: tecnología, digital, globalización, tecnología digital, autoridades policiales, ciberseguridad, era tecnológica, seguridad, ciberseguridad, riesgo global, hard law, soft law, derecho global, lex informatica, geopolítica.

ABSTRACT

The world is global and complex. Full of global risks. The advent of new technologies has made the world a smaller place by being hyperconnected. Globalization is, in part, a result of digital technology. We also inhabit a faster time. New challenges arise. Many of the disruptions generated by digital technology are perceived as global risks, such as the failure of technological governance, because we do not know when they will occur or their impact or how to manage them. Technological change, which is digital, introduces us

into the “technopolitical” era and then “Cyberia” emerges as a new territory of algorithms, initially created by man and which must be duly regulated and protected. In cyberspace, a regulation, or “Lex Informática”, is more necessary than ever, which will have to be hybrid, in which the coexistence of different legal orders is possible. It is necessary to study this context in order to approach the study of the relationship between technology and security, in particular, between technology and police and criminal justice authorities. Rapid technological evolution and globalization have posed new challenges in the field of personal data protection and the use of technology. The proposed appropriate regulation hereinafter, -which is the framework for the actions of law enforcement authorities-, contributes to the security of “Cyberia” and thus to cybersecurity in a broad sense. Also, contributes to cybersecurity, providing legal certainty and delimiting the actions of law enforcement authorities, through the consolidation of an appropriate regulatory framework, and starting from the prior knowledge of the existing relationship between digital technology and law enforcement and criminal justice authorities.

Keywords: technology, digital, globalization, digital technology, law enforcement authorities, Cyberia, technological age, security, cibersecurity, global risk, hard law, soft law, global law, lex informatica, geopolitics.

1. EL MUNDO GLOBAL ES V.U.C.A[1]

El secretario general de las Naciones Unidas, Antonio Guterres, dijo que vivimos “en una época de anarquía en el ciberespacio, de erosión de los acuerdos de control de armas, de aumento de las desigualdades, de retroceso de los derechos humanos y de un régimen comercial mundial inclinado en contra de los pobres” (Guterres, 2021: 85). También que hay que evitar una nueva guerra fría entre EE.UU. y China, que divida el mundo, lo que se llama la “Gran Fractura”, o el desacople entre ambas economías, con el riesgo evidente de que surjan a su vez divisiones geoestratégicas y militares.

Se trata de un entorno V.U.C.A.: volátil (de rápidos cambios, que requiere visión); incierto (es decir, impredecible, que requiere compresión); complejo (es decir, que le afectan muchas causas interrelacionadas, que requiere claridad); ambiguo (es decir, que caben múltiples interpretaciones, que requiere agilidad para conocer). Es un mundo altamente vulnerable y la pandemia ha acelerado ciertas corrientes de fondo[2]. El equilibrio y la estabilidad, bien vendrán de la mano de la cooperación, bien de la peligrosa disuasión (Panda, A. 2021)[3].

1 El concepto V.U.C.A. se acuñó a finales de los años 80 https://usawc.libanswers.com/faq/84869 . En la actualidad hay novedosos acrónimos que tratan de superar, para unos, o de concretar, para otros, el concepto V.U.C.A.. Jamais Cascio acuñó en 2020 el concepto B.A.N.I. (Brittle (Frágil), Anxious (Ansioso), Non-linear (No lineal) e Incomprehensible (Incomprensible)). Disponible en: https://medium.com/@cascio/facing-the-age-of-chaos-b00687b1f51d Más información en: https://ideas.llorenteycuenca.com/2021/03/tras-el-vuca-las-transformaciones-del-mundo-bani/

2 Consultar la serie de vídeos del Centro Frederick S. Pardee, de la Universidad de Boston para el estudio del Futuro a Largo Plazo. Por ejemplo, el experto en política comercial Dani Rodrik cree que la pandemia está acelerando la “retirada de la hiperglobalización” que ya estaba en marcha antes de la pandemia, o el decano fundador de la escuela Kennedy de Harvard, Graham Allison, denomina que vivimos una “rivalidad subyacente, fundamental, estructural y tucydideana”, en la que China amenaza con desplazar a la potencia establecida, EE.UU.

3 Disponible en: https://www.defensenews.com/land/2021/10/20/chinese-hypersonic-missile-test-unlikely-to-trigger-arms-race-experts-say/

El Foro Económico Mundial divide precisamente los riesgos globales en seis categorías: económicos, medioambientales, geopolíticos, sociales y tecnológicos. En su terminología, riesgo global es "aquel evento o condición incierta que, si llega a ocurrir, puede causar un impacto significativo negativo a varios países o industrias en el lapso temporal de 10 años" (Foro Económico Mundial, 2021:87).

En este artículo nos centramos en el riesgo tecnológico, en uno de los seis subriesgos asociados[4]: el fallo en el gobierno de la tecnología, concebido como:

"la falta de marcos, instituciones o normas aceptados mundialmente para el uso de redes y tecnologías digitales críticas, como resultado de que diferentes estados o grupos de estados adopten infraestructuras, protocolos y/o normas digitales incompatibles" (Foro Económico Mundial, 2021:89).

En el medio plazo, esta falla, de producirse, sí tendrá alto impacto y, dado el entorno geopolítico, es cada vez más probable. No obstante, en 2021 no está entre los riesgos globales que son altamente probables y de alto impacto[5]. Igualmente en Foro Económico Mundial, el "Global Future Council On Frontier Risks", lista otra serie de riesgos globales[6], que llama fronterizos, con el objetivo de estar preparados ante una eventual crisis. En ellos la tecnología tiene gran impacto.

Sobre riesgos globales y su probabilidad de ocurrencia, la literatura ha elaborado las teorías famosas de los cisnes negros, de Nassin Taleb, y de los rinocerontes grises, de Michele Wucker[7]. Pero si ponemos el acento más bien en su regulación y su gestión una vez que se concretan tales riesgos, en lugar de en su probabilidad de impacto o de aparición, los riesgos globales serían más parecidos a un toro ante un torero.

Y es que los riesgos globales son como toros, bóvidos de fuerza descomunal y gestos imprevisibles, que tanto han deslumbrado al mundo mediterráneo. Bóvidos que se torean, es decir, se pueden gestionar con muchas garantías de éxito, siempre que, como en el arte del toreo, pongamos en marcha procesos para una buena faena. Estos procesos, necesariamente globales, de escala planetaria y holísticos, para la atenuación de los riesgos, son como en el arte del toreo una mezcla de torero, casta, raza y capote, o de instituciones, métodos y procesos de decisión y gestión y de tecnología digital.

2. ¿QUÉ ENTENDEMOS POR GLOBALIZACIÓN?

Antes de continuar, conviene aproximarse a la noción de globalización, que es el contexto en el que inevitablemente vivimos. En 1999, la Open University publicó la

4 Son estos: Externalidades adversas asociadas con avances tecnológicos, caída de infraestructuras de información críticas, desigualdad digital, concentración de poder digital, fallos en medidas de ciberseguridad y fallos en el gobierno de la tecnología.

5 Disponible en: https://www.weforum.org/reports/the-global-risks-report-2021

6 Estos expertos del Foro Económico Mundial, por ejemplo, hablan de colapso de las democracias, ingeniería genética aplicada a humanos, el control neurológico, la disrupción geomagnética, la aparición de interfaces cerebro-máquina, el caos social y anarquía, guerra, China, India, el Internet de las Cosas, la proliferación de armas nucleares de menor escala, el derretimiento del permafrost en el Ártico, etc. Disponible en: https://www.weforum.org/reports/the-global-risks-report-2021.

7 Disponible en: https://crisisyriesgos.llorenteycuenca.com/2021/03/12/de-cisnes-negros-y-rinocerontes-grises-como-anticipar-riesgos-de-reputacion/

obra “Transformaciones Globales”. Definía la globalización como:

“una transformación en la organización espacial de las relaciones sociales, un aumento en su extensión, intensidad, velocidad e impacto. Este proceso -o conjunto de procesos- genera flujos y redes transcontinentales o interregionales de actividad, interacción y ejercicio de poder” (HELD, 1999: 32-86).

Se trata, por tanto, del proceso resultante de la capacidad de ciertas actividades de funcionar como unidad en tiempo real a escala planetaria[8].

La globalización es posible no tanto por una conciencia de pertenencia a la humanidad[9], sino más bien consecuencia de la tecnología digital (sistemas de información, de telecomunicaciones) y del transporte, capaces de dar forma a toda una red de flujos e intercambios planetarios.

Hace décadas el profesor Kenichi Ohmae, uno de los mayores expertos de la globalización económica, decía que “el próximo escenario global presenta tantos desafíos como oportunidades simplemente porque el mundo no tiene ya fronteras” (Ohmae, 2008: 52 a 58). Caracterizaba la economía global por estas notas:

A. No tiene fronteras. Aunque el final del estado-nación es muy discutible, desde luego, el final de este como único actor en el escenario global es patente. Las fronteras de los estados-nación se han replegado ante las Cuatro “C” (Comunicaciones –sin cables-, Consumidores –globales-, Capital –sin fronteras- y Corporaciones –casi estados-globales-), si bien vivimos signos de reversión.

B. Es invisible. En el sentido de que es electrónica, basada en los novedosos sistemas tecnológicos que se caracterizan por la inmediatez y la gran cantidad de información que pueden albergar. Por ejemplo, la proliferación de la tarjeta de pago (o el teléfono móvil) como medio de pago sería un caso paradigmático.

C. Cibernéticamente conectada gracias a una tecnología cada vez más barata (Internet y “el móvil, objeto de devoción de lo digital” (Byung-Chul, 2016:26)), en la que se produce la transferencia instantánea de gran cantidad de información.

D. Se mide en múltiplos, para las empresas globales, que tienen en cuenta oportunidades de negocio a medio y largo plazo.

Sin embargo, actualmente se percibe un cierto retroceso en la globalización en algunos aspectos como, por ejemplo, la confianza global, si bien vivimos aún en una inercia de la globalización de procesos, por ejemplo, logísticos e interdependencias.

Estamos observando cómo las relaciones de poder, basadas en el conflicto y la colisión directa, prevalecen sobre aquellas basadas en la persuasión. Emerge el conflicto en las cadenas de valor de todo tipo de sectores económicos, por lo general fuerte y globalmente integradas. Cualquier desacoplamiento, por envidias, miedos, recelos, conveniencia, ideología, en sí mismo es un grave riesgo global. La revolución tecnológica, si bien propicia la redistribución de las relaciones globales de poder, y esos procesos globales, favorece al tiempo, unas nuevas relaciones de desconfianza globales en términos de competición geopolítica, hasta el punto de la emergencia de bloques

8 Para conocer el nivel de globalización que existe actualmente en el globo, se acepta el índice compuesto del Instituto Económico Suizo de Zúrich (en alemán, KOF).

9 Disponible en: http://www.sociedadglobal.es/patriotismo-global-o-patriotism-for-humanity-richard-falk/

comerciales de países, que se agrupan no tanto ya por ideología, sino por tecnologías dominantes. La tecnología se convierte en un oxímoron, pues se concibe como una ideología, y por definición la ideología (ideas) no es tecnología (técnica), ni viceversa.

¿Estamos en un "gridlock" (Hale, Held et Young 2013:14-48), un embotellamiento de la globalización como consecuencia de las interdependencias globales? ¿Es la globalización la que propicia el nacimiento de un sistema normativo de gobernanza global, o es este resultado de las interdependencias de la globalización, o ambas cosas como sostiene la teoría de las instituciones, propugnada por el profesor Keohane (Hale, Held et Young 2013:15)? ¿Qué lo provoca? ¿La tecnología vivida como ideología? ¿Es esta la razón de que haya nacionalismos y populismos, de identidad, de ideología, de tecnología, pues tal es la magnitud de los cambios? ¿Es el origen de la crisis de representación en que viven las democracias liberales (Müller, J-W 2018)[10]? ¿Existe una crisis energética y/o del empleo evitable, o es inevitable? ¿Solo pueden mejorar dos de estos tres factores: Globalización, Soberanía Nacional y Democracia (Ortega, 2018)[11]? ¿Es la globalización el final de la geografía (Dickem)[12] y es verdad que la tierra no es plana, pues hay gran cantidad de procesos globales económicos superpuestos en múltiples niveles? ¿La ciberseguridad exigirá una aproximación entre sector público y privado, para converger en una regulación capaz de mitigar el riesgo, por ejemplo, de que se produzca un catastrófico ciberataque (Hale, Held et al (2017):227?

Todas estas preguntas nos llevan a preguntarnos el papel de la tecnología, en concreto la digital, en una globalización que es distinta a todas las anteriores, por la magnitud, alcance, profundidad y velocidad de las interacciones mundiales de personas, bienes, servicios, capital, ideas y datos que la conforman, totalmente condicionadas por la "omnipresencia de las tecnologías integradoras" (organización Mundial de Comercio 2021:14)[13] que hacen posible e impulsan tales interacciones.

3. TECNOLOGIA DIGITAL Y GLOBALIZACIÓN

El advenimiento de nuevas tecnologías ha hecho del mundo más pequeño al estar hiperconectado. Esta globalización a la que asistimos en el siglo XXI lo es en parte por el proceso de digitalización, dado que ciberespacio y globalización van unidos, pues:

"la globalización entendida en su forma moderna, necesita del ciberespacio porque se basa en su estructura y capacidades para su propia existencia. La descentralización que caracteriza desde su inicio al diseño cibernético influye y condiciona la vida en el mundo real (…) De este modo, las instituciones que surgieron den las postrimerías de la segunda guerra Mundial (…) se muestran poco eficientes en estos días en la gestión del mundo global" (Gómez de Ágreda 2012:179).

Se caracteriza por la cantidad descomunal de datos e información circulando por infraestructuras, tratándose, almacenándose, accesible a escala planetaria.

10 Disponible en: https://www.bbvaopenmind.com/wp-content/uploads/2018/03/BBVA-OpenMind-Jan-Werner-Muller-The-Rise-and-Rise-of-Populism-1.pdf

11 Disponible en: https://blog.realinstitutoelcano.org/la-voladura-del-trilema-de-rodrik/ ; entrevista a Dani Rodrick, LetrasLibres, de 16 de junio de 2020. Disponible: https://letraslibres.com/economia/la-globalizacion-en-tiempos-de-rodrik

12 Disponible en: https://www.bbvaopenmind.com/articulos/el-mundo-no-es-plano-la-profunda-desigualdad-geografica-de-la-globalizacion/

13 Organización Mundial del Comercio. (2021) "Economic Resilience and Trade".

La tecnología digital ha sido clave para el éxito de la globalización. Sin embargo, o por esto, la globalización, compuesta por instituciones, actores, procesos y normas, está al borde del colapso. Puede deberse a una fatiga sistémica y unos desfasados engranajes de la globalización, incapaces de acomodar la generalización de las relaciones y los intercambios de toda índole. Pero la falla de la regulación de la tecnología es más posible que antes. Y es un riesgo, eminentemente trasversal y global.

La tecnología digital que poseemos -¿o nos posee? (Byung-Chul, 2016:26)- ha sido capaz de ensanchar el mundo conocido, creando una realidad virtual, que configura un nuevo espacio, el ciberespacio –solo espacio global común ("global common") en apariencia-.

Los rasgos globales de la nueva sociedad cibernética emergente, y los rasgos cibernéticos de una nueva sociedad global emergente, precisan de una reformulación del papel de los estados nacionales, de los actuales organismos internacionales, de los propios procesos productivos industriales, de logísticos y de consumo, y toda su cadena de valor asociada. También, los derechos y libertades de las personas, el papel de las fuerzas de seguridad, la propia concepción de la persona e identidad humana, de la antropología (Han 2018:72), van a requerir de una reinterpretación.

La actual tecnología institucional, en la que incardinamos los derechos y libertades, va muy por detrás de la tecnología y de la evolución ética del ser humano. Así, es difícil que la tecnología sirva al ser humano y sea un mero instrumento. Pasa a ser un fin.

A esta globalización digital se la llama Cuarta Revolución Industrial (López 2019). La transformación tecnológica de la inteligencia artificial[14] –desde una más estrecha a una más general, que supera la capacidad de entendimiento y aprendizaje humanos (National Intelligence Council 2021:58)-, el "Machine Learning", el 5G, el Internet de las Cosas -¿habrá un Internet de las personas interconectadas o ciborgs?-, la biotecnología, la robótica, los nuevos materiales, etc., ocasionan disrupciones, con alto impacto en las relaciones sociales, en el ánimo de las personas, en la ecología humana y en las relaciones entre los actores del globo (Foro Económico Mundial 2019:15). En concreto, la tecnología de lo digital. En este artículo, el concepto digital lo integran "los tres pilares clave de la revolución cibernética, como la computación en la nube, Big Data, Internet de las cosas" (Ministerio de Defensa 2020:33), así como la tecnología de cadenas de bloques o "blockchain" o las tecnologías del aprendizaje profundo o incluso la computación cuántica.

En esta etapa de la globalización, la tecnología posibilita la globalización virtual. Sobre la base de lo digital surge un mundo hiperconectado (National Intelligence Council 2021:55), donde los productos y servicios del mundo físico se van a entrelazar en una compleja cadena global de bienes y servicios[15], que serán también virtuales de mundos virtuales. Lo físico y lo inmaterial se relacionan sin duda pues muchos servicios en la actualidad van a requerir de bienes y materias primas de la nueva economía, como cables, semiconductores, placas fotovoltaicas, coltan del Congo, litio chileno…

14 En el nuevo libro de Henry Kissinger, "The Age of AI", junto con Eric Schmidt (ex executive chairman of Google), y Daniel Huttenlocher (decano de MIT Schwarzman College of Computing), se advierte del riesgo de la IA y su impacto en los asuntos humanos, por su poderío e impredicibilidad.

15 Revolución del transporte, de la logística, de la cadena de frío, de los sistemas de pago, de los asuntos militares, etc.

liberándose enormes sinergias e interrelaciones, pero posibilitando la aparición y concreción de nuevos riesgos globales.

4. TECNOLOGÍA DIGITAL Y RIESGO GLOBAL

Muchas de las disrupciones de la tecnología digital son percibidas como riesgos globales, pues no sabemos cuándo ocurren, ni su impacto y/o cómo gestionarlas. Precisamente esta percepción del riesgo tan diversa entre personas, entre culturas y países (Wucker 2021:95), hace que una comprensión total del propio contexto global en el que emerge la tecnología, y que esta ayuda a configurar también, sea tan importante.

Vivimos en un mundo en que los países están adaptando sus desfasadas estructuras e instituciones, su propio sistema operativo, para afrontar una serie de riesgos globales, entre los que están desde luego, a parte de las tradicionales rivalidades de tipo comercial, la asociada con el liderazgo tecnológico.

Entonces, ¿se trata en sí misma de un riesgo global la tecnología o como dice el actual representante de España ante la UNESCO[16], cuando habla de inteligencia artificial como un cuchillo de Albacete, que dependerá del buen o mal uso que se haga? ¿Será posible aprovechar la tecnología, quedando la técnica al servicio de la ciudadanía y la democracia (Lasalle, J.M. 2019:15)?

Es tal el cambio de paradigma y de época[17] que parecería natural ver a priori la tecnología como un riesgo, pero ¿lo fueron en otras épocas de la humanidad el fuego, la madera o una piedra? Por definición, la tecnología[18] es un riesgo y una oportunidad[19], no es ni buena, ni mala ni neutral, simplemente es, lo que implica que ha de evaluarse en cada momento las circunstancias de su uso[20]. Las nuevas tecnologías aumentarán el riesgo de que los delincuentes aprovechen las ventajas de la innovación con fines malintencionados[21], pero también de perseguirlos.

Partiendo de la definición de riesgos globales del Foro Económico Mundial, estos serían los derivados del mal uso de la tecnología, como la concentración de poder, las brechas de seguridad en sistemas de comunicaciones, la ausencia de medidas desde el diseño y por defecto en materia de privacidad durante la fabricación de dispositivos o la elaboración de procesos, etc.

16 Andrés Perelló, 2021, "Discurso de Clausura conmemoración 75 aniversario de UNESCO", Caixaforum.

17 Discurso de Año Nuevo, 2020, papa Francisco. "La que estamos viviendo no es una época de cambios, sino un cambio de época".

18 Definición de tecnología según la Real Academia Española de la Lengua: "1. Conjunto de teorías y de técnicas que permiten el aprovechamiento práctico del conocimiento científico"; o "4. Conjunto de los instrumentos y procedimientos industriales de un determinado sector o producto".

19 P9_TA(2021)0405. Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)): "A. whereas digital technologies in general and the proliferation of data processing and analytics enabled by artificial intelligence (AI) in particular, bring with them extraordinary promises and risks;"

20 Primera Ley de Kranzberg. Disponible en: https://es.wikipedia.org/wiki/Neutralidad_tecnológica

21 Bruselas, 24.7.2020, COM (2020) 605 final, COMUNICACIÓN DE LA COMISIÓN sobre la Estrategia de la UE para una Unión de la Seguridad. Pág. 5 https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0605&from=EN

También es relevante la velocidad de los cambios tecnológicos, que afectan a una mayor probabilidad de ocurrencia e impacto (ataques a sistemas en sistemas de salud[22], mal uso de programas de vigilancia como el caso Pegasus, desacople en el mercado de trabajo (Garicano (2019: 50, 51).

Pero hay un riesgo probablemente superior asociado con la tecnología digital. Esta es totalizante de todos los aspectos de la vida de las personas, poseyendo la facultad de provocar cambios sistémicos, con más frecuencia que en otras épocas. Es necesario conocer este contexto para reinterpretar el papel del estado y los cuerpos de seguridad interior.

En esta línea, la tecnología digital debe ser gestionada y regulada adecuadamente, pues tanto una mala o excesiva regulación o la ausencia de la misma, tiene efectos imposibles de prever. Esta regulación es parte de una noción amplia de la ciberseguridad. Sería como un toro. Un riesgo que cuando embiste es una oportunidad para realizar una buena faena.

5. Y LLEGÓ CYBERIA: LA CIBER GLOBALIZACIÓN REGULADA

El cambio tecnológico, que es digital, nos introduce en la era "tecnolítica" y emerge "Cyberia", como territorio nuevo de algoritmos, creado inicialmente por el hombre y que debe ser debidamente regulado y protegido, que describe bien el mundo de lo digital e Internet. La etimología del prefijo "ciber", lo encontramos en el griego antiguo, "kybernetes", que era el timonel o persona al gobierno de la nave. Fue Norbert Wiener cuando en 1948 publicó una obra sobre el control de las máquinas y de sus procesos. Emergió la ciencia cibernética. A finales de los años 80 se acuñó el término "cyberspace", en inglés, en la novela Neuromante[23].

Nace gracias a la tecnología, en el marco de la globalización, con externalidades en el mundo físico y virtual y provoca una revolución ontológica (Lasalle 2019:71) y, de identidad de la persona, del propio capitalismo y de la gobernanza global, y en múltiples aspectos de la vida de los estados y de las propias personas, como la seguridad.

Cyberia es un mundo superpuesto y generador a los procesos de la globalización, donde el ser humano y las cosas interactúan, siendo la primera vez que estas últimas lo pueden hacer entre ellas, y que los seres humanos pueden interactuar con todos los seres humanos y cosas del planeta, también en mundos virtuales.

Cyberia es el ciberespacio regulado, y es clave para la seguridad jurídica y para la propia seguridad de Cyberia, la ciberseguridad.

En la era "tecnolítica" actual, Cyberia supone la manifestación de la globalización digital y del cambio tecnológico, donde la noción de soberanía, históricamente vinculada a un territorio y delimitada por unas fronteras, como la geopolítica, se difumina como tantos otros conceptos.

22 Disponible en: https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/

23 Disponible en: http://jamillan.com/v_ciber.htm

Para el Departamento de Defensa de EE.UU., el ciberespacio se trata de:

"un dominio global dentro del entorno de la información, compuesto por una infraestructura de redes de tecnologías de la información interdependientes, que incluye internet, las redes de telecomunicaciones, los sistemas de información y los controladores y procesadores integrados junto con sus usuarios y procesadores" (Gómez de Ágreda, 2012: 170, 171).

A diferencia del ciberespacio Cyberia emerge cuando está aquel debidamente regulado a escala global, ayudando a conformar el sistema legal de la globalización. Toda otra regulación parcial y cerrada, o estatal y cerrada, sin puntos de conexión con otras áreas de Cyberia o jurisdicciones, no conformaría Cyberia, sino que sería simplemente una reducción de la misma.

Esto nos plantea una interesante cuestión sobre el sistema jurídico de la sociedad global y digital pues no existe hoy un Derecho Global concebido como sistema jurídico completo y cerrado al modo kelseniano.

El profesor de la Universidad de Harvard, Dani Rodrik, apostó en plena pandemia Covid-19 por las "reglas globales para la convivencia"[24], desde el campo del comercio y las inversiones, pero también de la salud pública o el cambio climático. Para el académico:

"las normas globales tienen la ventaja de que pueden, potencialmente, aumentar la eficiencia, reducir los costos de transacción y multiplicar las economías de escala. Pero tienen la desventaja de que reducen la autonomía -de los estados-, lo que puede impedir la democracia -pues son los estados nacionales donde el estado de derecho es plenamente eficaz-, y también pueden inhibir la diversidad y la experimentación de políticas a nivel nacional".

Entonces, para Rodrik, estas reglas globales deberían actuar sobre todo para limitar las políticas del tipo "beggar-thy-neighbour" -la lucha contra los paraísos fiscales- y asegurar aquellas otras enfocadas en preservar los denominados "global public goods" o bienes globales de dominio público- la regulación del clima y aspectos relativos a la salud pública.

En nuestra opinión, estas reglas globales son constituyentes de la noción misma de Cyberia, como ciberespacio ciberseguro, donde impera la seguridad jurídica. En la sociedad global y digital, diversos actores globales estarían involucrados en la elaboración y aplicación de normas comunes globales ("global rules"), aunque parciales, en un campo que debería ser de "reserva de globalidad", como la tecnología digital[25], que "ya no (es) un sector específico sino el fundamento de todos los sistemas económicos innovadores modernos" (García y Villarino 2021:46)[26]. La tecnología, como elemento transversal a la sociedad entera (Aznar 2016:44).

El emergente sistema multipolar del concierto mundial, que se proyecta totalmente en Cyberia, debe aún ir encontrando un nuevo equilibrio (Ruperez 2009:133), como si fuera una corrida de toros, o una sinfonía, que significa acuerdo, en griego, de donde nace la armonía.

24 Disponible en: https://www.prospectmagazine.co.uk/magazine/dani-rodrik-globalisation-trade-coronavirus-who-imf-world-bank , 4 de mayo de 2020.

25 Otras áreas son las pandemias, las migraciones, las catástrofes, el cambio climático, la privacidad, la propiedad intelectual, la competencia…

26 Disponible en: https://www.fundacionalternativas.org/public/storage/publicaciones_archivos/4a9e89b4185b6c4ef37bfe31580394c0.pdf

Este sistema multipolar, caracterizado por la noción de fragmentación, tiene ante sí el reto de la protección y promoción de los derechos y libertades y del papel del estado y el gobierno de la esfera digital, en un contexto de pugna geopolítica.

Se suscitan preguntas, como si en Cyberia el "tecnopoder", controlador de los fenómenos algorítmicos de la transformación digital y de la estructura lógico-matemática del capitalismo cognitivo (Lasalle 2019:93), podrá ser democráticamente controlado[27], de modo que se produzca una distribución de poder entre los actores globales implicados, o si Cyberia se convertirá en el campo de juego donde fenezca el orden liberal (privacidad, habeas corpus, presunción de inocencia, imperio de la ley, separación de poderes) tras la pugna entre las potencias y nuevos actores entre sí (De la Rasilla 2008:28), resultando un nuevo orden en esta neo era "tecnolítica". No en vano, en las próximas décadas se va a dar un incremento de la competición planetaria por los elementos esenciales para la obtención de la supremacía tecnológica (Baños 2019:265), como el talento, el conocimiento y los mercados (National Intelligence Council 2021:54).

Pero una pregunta destaca sobre todas las demás: ¿qué sistema normativo se requiere en Cyberia para que se considere debidamente regulada y, por tanto, se pueda hablar de plena seguridad en Cyberia, ampliando la noción de ciberseguridad tratando de evitar precisamente la ocurrencia de una falla de regulación de la tecnología?

6. SISTEMA NORMATIVO DE CYBERIA

"Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial"[28]. Se comprueba que la escala de la regulación debe ser global, pero la realidad es que no existe en la mayoría de las materias una regulación global, y el ámbito digital no es la excepción, pese a los esfuerzos, por ejemplo, de la Unión Europea.

En el futuro, Cyberia podría ser una hiper-tecno-poliarquía (Dahl 1989: 18), o bien, transformarse en un tecno-totalitarismo (Aznar 2016:44), y su sistema legal, que configura en última instancia el de la globalización, estaría llamado a evitarlo, por medio de la adecuada regulación. Por ejemplo, regulando el multilateralismo (a su vez, asentado en la descentralización de las relaciones internacionales), y la propia tecnología, a fin de conjurar los riesgos crónicos de la globalización. Sin una adecuada regulación, este sistema podría ser en sí mismo, otro riesgo global de la tecnología digital, al menos desde la perspectiva de las democracias liberales.

En todo caso, el sistema normativo de Cyberia habría de propiciar la participación; la transparencia; el ejercicio legítimo de competencias por los distintos niveles de decisión; la eficiencia y el control independiente de las decisiones; el compartir riesgos ("risk pooling") y la cooperación y coordinación, en materia objeto de reserva de globalidad.

27 P9_TA (2021)0405 "Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters", European Parliament resolution of 6 October 2021, on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)): "6. Underlines that any technology can be repurposed and therefore calls for strict democratic control and independent oversight of any AI-enabled technology in use by law enforcement and judicial authorities, especially those that can be repurposed for mass surveillance or mass profiling;"

28 Reglamento General de Protección de Datos Personales. Considerando Sexto.

La globalización exige un "sistema jurídico global", que podría ser completo y cerrado, a modo del sistema kelseniano, con una constitución formal global, o bien un sistema más abierto, con una suerte de constitución material no escrita ("Common law"), o un sistema hartiano (Turégano 2017:247), basado en la "regla de reconocimiento" (Nunez 2018:134) , en el que existe una diversidad de regímenes jurídicos que se organizan de modos diversos, sin tener que presuponer necesariamente, como supuso Kelsen, la existencia de una regla superior a la que estarían subordinados los sistemas (Turégano 2017:247). Cyberia, también.

Estos principios y reglas globales se pueden ir esbozando parcialmente, por zonas del saber, como, por ejemplo, respecto del comercio internacional ("Lex Mercatoria"), o para regular la tecnología digital. Pueden esbozarse desde grupos de naciones, como el G-20 o el G-7, en clara colaboración con empresas, o por actores de la incipiente sociedad civil global. La inexistencia de un poder ejecutivo, legislativo o judicial global, unido a la celeridad, interrelación e interdependencia de los intercambios comerciales, humanos y culturales, y a la dificultad de alcanzar plenos acuerdos donde confluyan todos los estados del planeta, provoca una etapa de transición, donde formas tradicionales de Derecho, como las leyes y tratados internacionales ("Hard Law"), conviven con normas de terceros actores no estatales, o de escasa o nula fuerza vinculante ("Soft Law"), como leyes modelo, reglas de derecho, principios, reglas, estándares o directrices en base a usos y costumbres del comercio internacional[29].

Desde la lógica del cosmopolitismo jurídico, sería deseable que quedase supeditada tanto la tecnología generadora de la infraestructura, como las relaciones y transacciones que se produjeran en ella, a unas normas de Derecho Global –fuesen de "Hard Law" (entre estados y/o organismos internacionales) o de "Soft Law". Podría surgir una "Lex Informática"[30] o Ciberderecho (García 2018), con elementos de "Hard Law" y "Soft Law", que favoreciese y protegiese la seguridad, el libre acceso y por igual de todos los agentes con intereses en la infraestructura o el principio de neutralidad, así como el principio de participación -involucrando a estados y otros actores privados, como ICANN, y otras fundaciones privadas y grandes empresas como las GAFA, TUNA y BATX.

29 El pensador y experto en la globalización, Arunabha Ghosh, sostiene que, por ejemplo, los acuerdos multilaterales medioambientales gozan de escasa eficacia, en tanto sus estructuras de gobierno se encuentran fragmentadas por la concurrencia de múltiples estados y son difusas, al no presentar una relación jerárquica clara entre sí, ni con otros instrumentos jurídicos internacionales clave, lo que ahonda en ocasiones en su falta de coherencia, con el añadido de las dificultades de interpretación, así como en falta de transparencia y una adjudicación precisas de responsabilidades. Las normas de "Hard Law" como las de "Soft law" pueden adolecer de estos mismos problemas.

30 En el presente documento no se utiliza el término de "Lex Informática" en el sentido acuñado por el profesor Reidenberg, para referirse al conjunto de normas, reglas e instrucciones –electrónicas, propias del hardware y de software- para regular los flujos de información en el entorno digital, impuestas por las redes tecnológicas y de comunicación, en lugar del derecho tradicional. La tecnología "blockchain" sería un claro exponente. Por el contrario, "Lex Informática" será más bien el "Ciberderecho" o "la rama jurídica propia de Internet y del entorno digital". Para profundizar en la "Lex Informática", consultar: REIDENBERG, Joel R. "Lex Informatica: the formulation of Information Policy Rules through technology", Fordham Law School, p. 556 y 585, 1997. Disponible en: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1041&context=faculty_scholarship. LAMBERS, Rik, "Code is NOT law", IViR Amsterdam, 2004. Disponible en: www.indicare.org CITA A: LESSIG, Lawrence. "Code and Other Laws of Cyberspace", 1999. Para profundizar en la diferencia, y en la noción de "Blockchain" como Derecho, o criptoderecho o código tecnológico, consultar: VV.AA. Coord. GARCÍA MEXÍA, Pablo. "Criptoderecho. La regulación de Blockchain", Cap. II "Del ciberderecho al criptoderecho. La criptoregulación", GARCÍA MEXÍA, Pablo. Ed. Wolters Kluwer, 2018.

Comprobamos el reto que supone para el Derecho Global abordar la regulación de una materia sujeta a tantas constricciones. La cuestión jurídica se agrava, pues el ciberespacio se trataría de una especie nueva del genio humano dentro del territorio de un país, de varios y/o en alguno o algunos de los bienes globales.

En todo caso, en el ciberespacio se hace más necesario que nunca una regulación, que habrá de ser híbrida, en la que sea posible la convivencia de ordenes jurídicos diversos no sustentada, necesariamente, en relaciones jerárquicas de supra o subordinación, sino en criterios de compartición, coordinación y subsidiariedad, ni siquiera sobre la base del territorio. Esta regulación será compleja, por las características propias de la realidad virtual, la ausencia de fronteras, la inmediatez, la celeridad del cambio tecnológico, el vínculo con lo físico, el gran alcance de toda acción en el ciberespacio, y la dificultad de, en su caso, trazar el origen de toda conducta en el ciberespacio. Pero este orden jurídico, que aportará seguridad jurídica, ayudará a conformar la propia seguridad de Cyberia, esto es, la ciberseguridad ensanchando la noción del concepto.

Para profundizar en la noción de regulación adecuada de Cyberia, interesa la definición del Gobierno de EE.UU. de ciber-normas y de regulación del ciberespacio de la era Trump[31]. Aquellas son tanto el derecho internacional –"Hard Law"-, como las normas voluntarias y normas no vinculantes –"Soft Law"-, en el ámbito del ciberespacio. Son normas estabilizadoras y de mejora de la seguridad que definen un comportamiento aceptable para todos los estados. Además, promueven una mayor previsibilidad y estabilidad. Habría que añadir, que no solo para todos los estados sino para el conjunto de actores de la nueva sociedad global. Con anterioridad, EE.UU. asentó los principios básicos de tal regulación del ciberespacio[32] que, aunque superados en la era Trump, bien podrían orientar la regulación en Cyberia. Son estos:

- *Promover las normas y construir la seguridad internacional: Construir un consenso global con respecto al comportamiento responsable de los estados en el ciberespacio, incluyendo la aplicación del derecho internacional existente para mejorar la estabilidad, fundamentar las políticas de seguridad nacional, fortalecer las asociaciones y evitar interpretaciones erróneas que puedan conducir a conflictos.*

- *Combatir la ciberdelincuencia: Mejorar la capacidad de los estados para luchar contra la ciberdelincuencia, incluyendo la promoción de la cooperación internacional y el intercambio de información, y la formación de las fuerzas de seguridad, especialistas forenses, juristas y legisladores.*

- *Reforzar las políticas públicas y la gobernanza de Internet: Desarrollar políticas que promuevan las normas internacionales y la innovación; mejorar la seguridad, la fiabilidad y la resistencia; ampliar la colaboración y el estado de derecho; y promover estructuras e instituciones inclusivas de gobernanza de Internet que incluyan a las partes interesadas del gobierno, la sociedad civil y el sector privado y que sirvan efectivamente a las necesidades de todos los usuarios de Internet.*

- *Apoyar la libertad de Internet: Preservar y ampliar Internet como un espacio abierto y global para la libertad de expresión y para la organización e interacción de toda la gama de intereses y esfuerzos humanos; promover el consenso internacional sobre la aplicación de los derechos humanos en el ciberespacio; proporcionar apoyo político y técnico a las personas que se enfrentan a la represión en Internet; y animar a las empresas a adoptar prácticas y políticas que respeten los derechos humanos en línea.*

31 "National Cyber Strategy of the United States of America", September 2018, Disponible en: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

32 "Estrategia Internacional para el Ciberespacio", 2011. Disponible en: https://2009-2017.state.gov/s/cyberissues/strategy/index.htm

- *Realizar la debida diligencia en materia de ciberseguridad: Desarrollar y reforzar las relaciones con otros países para mejorar la ciberseguridad mundial, mejorando la defensa de las redes nacionales y las capacidades de gestión y recuperación de incidentes; aumentar la participación en las estructuras de ciberseguridad regionales y mundiales existentes; y cooperar en los esfuerzos para hacer frente a las amenazas de interés mutuo.*

- *Desarrollar Internet y las tecnologías de la información y la comunicación (TIC) para el crecimiento económico: Ampliar la infraestructura de las TIC, aumentar el acceso a Internet y fomentar la producción de contenidos en línea atractivos y contextualmente relevantes para los usuarios locales como medio para catalizar el desarrollo económico y social.*

En este sentido, el Consejo de Seguridad Nacional español, en su reunión del día 12 de abril de 2019, dijo que aún falta definir "un marco internacional, para la prevención de conflictos, la cooperación y la estabilidad en el ciberespacio, en el que se apliquen los principios de La Carta de Naciones Unidas en su totalidad, el Derecho Internacional, los Derechos Humanos y el Derecho Humanitario Bélico, así como las normas no vinculantes sobre el comportamiento responsable de los Estados". Es la denominada pesadilla jurídica (Reguera 2015).

Dicho esto, el propio padre de la web, Tim Berners Lee[33], menciona la idea de una Norma Fundamental, capaz de regular la web entera, sus problemas monopolísticos derivados de que el primer ganador se lleva todo el mercado mundial, el acceso a los datos personales, los sesgos de participación entre mujeres y hombres, entre el Norte y el Sur Global…

Igualmente, tenemos la infructuosa iniciativa NetMundial, para la gobernanza de los retos que trae Internet[34]. Es, como sabemos ya, un guiño kelseniano que parece que vuelva una y otra vez, al mismo nivel de la propuesta idealista del profesor Luigi Ferrajoli (Ferrajoli 2020), de una Constitución de la Tierra que incluirá el ciberespacio como un nuevo mundo o la del jurista Ingolf Pernice, director del Instituto Humboldt para Internet y la Sociedad, favorable a un tipo de gobernanza del ciberespacio repartida entre los niveles nacional, supranacional y global (Gómez de Ágreda 2020:340).

7. PROSPECTIVA GEOPOLÍTICA –DIFUSA- PARA CYBERIA

Cabe tratar de indagar en el futuro, desde el dintel de su puerta. El futuro ineludiblemente pasa por la nueva frontera de lo digital. Este mundo digital es además el nuevo campo de batalla. Un primer escenario de combate, donde se da antes el conflicto, donde los intereses geopolíticos y geoeconómicos de las naciones y los otros actores trasnacionales se baten y se retan, para lo cual necesitan de la tecnología digital.

Este nuevo mundo digital podría ser ya poswestfaliano, sin estados, pero los estados siguen teniendo mucho que decir. Aunque el ciberespacio no es más que "una serie de centros gigantescos de computación distribuidos por todo el mundo e interconectados que dan servicio a todos los usuarios de tecnología de la información en el mundo" (Calero 2015:227), o una especie de neo-red de electricidad, una "utility" (Lasalle 2019:34) en términos económicos, alimentada por datos, que pasan a ser "commodity", el nuevo ecosistema digital rompe con el mundo anterior, hasta con el

33 Disponible en: https://www.ted.com/talks/tim_berners_lee_a_magna_carta_for_the_web?language=es

34 Disponible en: https://netmundial.org/

Derecho anterior pues es un nuevo ecosistema disruptivo, donde la interdependencia, la interconexión, las transacciones electrónicas, la pluralidad, la proliferación de redes, dan vida a una nueva globalización. Es un nuevo territorio-no-territorio, una tierra ignota que no estaba ahí, acaso un "no lugar" (Augé 2014:67) cibernético que se va creando por el propio ser humano (¿y las máquinas?), donde por lo general los estados westfalianos se mueven mal, pues no hay fronteras o, al menos, surge un nuevo tipo de fronteras (Lasalle 2019:206)[35] y de relaciones e interacciones, lícitas e ilícitas, morales e inmorales, en todo caso, cibernéticas.

Por tanto, importa y mucho regular el ciberespacio, para que sea Cyberia. Decían los clásicos que el Derecho nace dentro de la sociedad para regularla (ubi societas, ibi ius). Pues bien, la regulación de la tecnología digital, que impacta en la misma ordenación del ciberespacio, es clave que se haga desde el propio cuerpo social y político humano. Es normal que surja una versión lógica, digital, del estado y de la sociedad global, como evolución natural del "Estado-Red" o "Estado en Red" (Castells 2000:12), transformado por efecto de la globalización.

En este nuevo ecosistema humano, global y de alta complejidad se requiere de una estrategia internacional para su utilización y desarrollo que armonice los distintos componentes que entran en juego (Molina 2014:12).

El Derecho ha de ser parte de esta estrategia, y tenderá a interaccionar con esta parcela del saber en el ciberespacio –el ciberderecho-, aunque sea para dirimir asuntos de territorialidad o jurisdicción, o delimitando estándares legales para las arquitecturas tecnológicas enfrentadas en una era de competición geopolítica.

En el ciberespacio, se reformula constantemente la noción de soberanía sobre un territorio y sobre unos ciudadanos, pero acontece la pugna geopolítica.

Podría ser considerado un nuevo bien común o "global common" como los océanos, el espacio o los cuerpos celestes, pero el ciberespacio es "una infraestructura con elementos físicos y lógicos, a parte de su impronta virtual, eminentemente privada por lo que resultaría complicado atribuir titularidad pública y derecho universal de uso al ciberespacio" (Gómez de Ágreda 2020:340), lo que complicaría su reconducción a ser considerado un bien común ("global common").

Se podría decir del ciberespacio que va más allá de ser un espacio común global, aunque llama poderosamente la atención que el resumen ejecutivo de la Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional, que aprueba la Estrategia Nacional de ciberseguridad 2019, se refiera al primer capítulo, como "El ciberespacio, más allá de un espacio común global", cuando el propio capítulo se titula en realidad "El ciberespacio como espacio común global". En cualquier caso, no resta esta opinión que, a pesar de ser una infraestructura privada, regida en parte, tanto por normas privadas como por normas de estados u organismos internacionales, que su utilización y explotación deban, en todo caso, ponerse al servicio del bien común.

35 El autor explica, sobre la frontera, una nueva definición: "El concepto de frontera tradicional geográfica se sustituye por el concepto de lejanía o cercanía asociada a un nuevo concepto de distancia basado en múltiples factores o dimensiones no geográficas".

En esa sociedad digital anticipada por la tecnología, Han habla de una nueva definición de "Smart Power" (Han 2016:27) que se hace más "smart" o inteligente y más "power" o poder, a medida que se hace más digital. El reto está en si esta nueva sociedad está pensada para las personas, si es humano-céntrica la digitalización o no[36].

El Derecho regulará este nuevo mundo, y las relaciones de poder y geopolíticas influirán en él, nuevamente, como sujeto actor y como sujeto paciente, en espera de ese ideal kantiano y kelseniano de un Derecho Universal, con una Justicia Universal y una Norma Universal.

Como apunta la experta Raquel Jorge-Ricard, "la tecnología y sus impactos en los derechos humanos se han convertido en una nueva herramienta geopolítica, de política interna y de multilateralismo" (Jorge-Ricard 2020). Igualmente, el experto futurista Abishur Prakash[37] advierte de una era de globalización vertical, con nuevas barreras, esta vez digitales ("tecno-nacionalismo"), y de una bifurcación de los estándares tecnológicos y regulatorios en torno a grupos de países que buscan la hegemonía tecnológica. El efecto indeseado es compartimentar Cyberia como utopía digital. Un ejemplo es la Resolución 74/247[38] de Naciones Unidas, sobre "Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos", promovida por la Federación Rusa y apoyada por China, Corea del Norte, Cuba, Nicaragua, Siria o Venezuela[39], "a fin de elaborar una convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos". Existe un riesgo real de división del mundo en bloques, diferenciados en la manera de combatir el cibercrimen, concebir lo que es utilizar tecnologías de la información, etc. pudiendo llegar a hacer la cooperación impracticable.

La regulación de Cyberia y su regulación de, por y para humanos, y de la tecnología digital, pasa a ser esencial como factor de mitigación del riesgo de sus externalidades. El código informático no puede arrogarse nunca funciones para-legislativas o para-judiciales, cuestionando la propia idea de Justicia, la propia idea de Derecho y, por lo que respecta al sistema de producción normativa, la propia idea de Democracia.

En Cyberia el Derecho se emancipa del territorio, pero, esto solo sucede en abstracto, pues en realidad hay múltiples puntos de conexión con la soberanía. Además, no es soportable un sistema legal donde no queda el dolo, la imprudencia, la interpretación de la norma, su aplicación proporcionada, la empatía del juzgador, del aplicador, del legislador, de los operadores jurídicos, de las fuerzas y cuerpos de seguridad, sufrientes de sus mismas decisiones, como parte de un único cuerpo social.

36 P9_TA (2021) 0405 "Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters", European Parliament resolution of 6 October 2021, on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)): "E. whereas AI technology should be developed in such a way as to put people at its centre, be worthy of public trust and always work in the service of humans; whereas AI systems should have the ultimate guarantee of being designed so that they can always be shut down by a human operator;"

37 Disponible en: https://www.trtworld.com/magazine/how-technology-is-shaping-a-new-era-of-vertical-globalisation-51151

38 Disponible en: https://undocs.org/es/A/RES/74/247

39 Disponible en: https://www.ashurst.com/es-es/news-and-insights/legal-updates/spanish-digital-newsflash-january-2020/

Solo el tiempo, dado que el espacio no cuenta ya, tiene algo que decir para conocer hacia dónde vamos. En Cyberia el estado, y la provisión de su seguridad, puede transformase, pero no desaparecer, haciendo más necesario que nunca, posiblemente, la coordinación jurídica y colaboración política, más que en la concentración de poder en un nivel supranacional o estado mundial. Asimismo, la cooperación entre lo público y lo privado, y el maridaje regulatorio, entre técnicas de "Hard Law" y "Soft Law". En otro plano, no habría seguridad, además, de existir una regulación exógena al ser humano, proveniente de una inteligencia artificial autónoma, independiente y consciente.

En Cyberia, el ciudadano accede a una plataforma global (Saran 2020) donde el estado o sus sub-entidades regionales, o las supranacionales, aparecen en el mismo mundo digital, en el mismo plano casi horizontal. En el mundo digital, como espacio de la Humanidad, no parece que tenga sentido la soberanía y sí una regulación legal global. Lo cual anticipa muchas preguntas, pero una vuelta al orden westfaliano no parece tampoco fácil ni probable, "pues han surgido instituciones comunes y desafíos globales" (López-Aranda 2020:113 y 117), y por el empuje del sector privado.

8. EL FUTURO DE LA RELACIÓN ENTRE LA TECNOLOGIA DIGITAL Y LAS AUTORIDADES POLICIALES Y DE JUSTICIA PENAL EN CYBERIA

La Unión Europea es el ente político más próximo a la noción de Cyberia que encontramos en el mundo, debido a la completa ordenación de la tecnología digital en sus múltiples variantes. Es la institución que ha realizado el mayor esfuerzo normativo[40] hasta la fecha, tratando de conjurar aquel riesgo que apuntaba el Foro Económico Mundial, sobre el fallo del gobierno de la tecnología.

De hecho, la soberanía digital de la Unión Europea va a depender de su capacidad de almacenar, extraer y tratar datos, mientras cumple con los derechos fundamentales, con la seguridad y la confianza digital (Comisión europea 2021:21), en áreas como la protección de datos personales, consumidores, competencia y responsabilidad (Ministerio de Defensa 2018:36) y de la colaboración con actores privados.

No obstante la enorme influencia y efecto magnético de la normativa europea, y su capacidad de influir en diferentes grupos de países, interesados en comerciar con el mayor mercado del planeta, el entorno geopolítico V.U.C.A. actual ha convertido la tecnología digital en uno de sus campos de batalla principales, sobre todo entre EE.UU. y China.

Esto nos remite constantemente a la pregunta de qué tipo de ordenamiento global gobernará o influirá en los asuntos relativos a la tecnología global y la gestión de los riesgos internacionales asociados a ella. Y si participará o no, o cómo el sector privado. Asimismo, nos debe llevar a estudiar la relación entre tecnología y seguridad (Mölling 2021:2) y, más en particular, entre tecnología y autoridades de policía y de justicia penal.

40 En breve serán de aplicación los Reglamentos del Parlamento Europeo y del Consejo, relativos a: (1) un mercado único de servicios digitales (Ley de servicios digitales); (2) a la gobernanza europea de datos (Ley de Gobernanza de Datos); (3) por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial). Asimismo, encontramos el RGPD, el Reglamento ePrivacy, el Reglamento eIDAS2, el Reglamento DORA (Ley Resiliencia Operativa Digital) y las Directivas NIS2.

En este sentido, la regulación de la Unión Europea en áreas como la competencia en los mercados digitales (tipo "techlash"[41]), a través de la Directiva de mercados digitales, asume como necesaria la intervención y el control estatal sobre las grandes empresas tecnológicas. Intervención, por otro lado, no exenta de riesgo para el equilibrio entre derechos digitales, innovación y rentabilidad (Foro Económico Mundial 2021: 34). Pero esto es tan solo una parte de la regulación necesaria. De hecho, a medio plazo, como se ve en la "Encuesta de Percepción de Riesgo Global", los europeos clasifican el "Fracaso de la gobernanza tecnológica" como un riesgo crítico, y esto es, como sabemos, un asunto importante y urgente para la Unión Europea, donde los países poseen sus propias estrategias en materia de IA, la cuántica o el hidrógeno, faltando cooperación y cohesión (Loeskrug-Pietri 2021:12).

Siguiendo a los juristas y políticos López Garrido y Nicolás Sartorius, que prologan la obra de García y Villarino, en su edición de Wolters Kluver, Europa "ha de afrontar una regulación extensa e intensa de los fenómenos digitales" y son plenamente conscientes de que "acertar en la normatividad de la sociedad digital es esencial" (García y Villarino 2021).

Llevado al campo de la seguridad pública interior, en concreto a la actividad de las Fuerzas y Cuerpos de Seguridad del Estado[42], asemejando la Unión Europea a Cyberia, "la rápida evolución tecnológica y la globalización han planteado nuevos retos en el ámbito de la protección de los datos personales", y del uso de la tecnología, habiéndose "incrementado de manera significativa la magnitud de la recogida y del intercambio de datos personales. La tecnología permite el tratamiento de los datos personales en una escala sin precedentes para la realización de actividades como la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales".

Pues bien, llegados a este punto, pensamos que el concepto de regulación adecuada del ciberespacio es parte de la noción de ciberseguridad. Y en este concepto es clave repensar el papel del binomio tecnología-autoridad policial y judicial penal y, en el futuro, el papel del sector privado y su propia participación elaborando normas de tipo "Soft Law".

Obviamente, la noción más técnica y tradicional de ciberseguridad ha de seguir vigente, pero en su sentido más lato, ha de incluir una adecuada regulación de la

41 El "TechLash" es un término acuñado por The Economist en 2018 para denominar las reacciones críticas contra los gigantes tecnológicos de Silicon Valley como Facebook, Google y Amazon derivadas de sus malas praxis y actuaciones.

42 Ley Orgánica 7/2021, de 26 de mayo, (BOE núm.126, de 27/05/2021), de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, objeto de transposición de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo: Artículo 4. De acuerdo con este artículo, se entienden por Fuerzas y Cuerpos de Seguridad del Estado: las autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal; las Administraciones Penitenciarias; la Dirección Adjunta de Vigilancia Aduanera; el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias; la Comisión de Vigilancia de Actividades de financiación del Terrorismo.

tecnología digital, a fin de que no se actualice el riesgo global de un fallo de regulación de la misma, lo cuál sería crítico y existencial, en Cyberia, pero desde luego, para el mundo tal y como lo conocemos.

La tecnología digital y sus cambios afectan desde luego a las Fuerzas y Cuerpos de Seguridad del Estado, al igual que moldean a la propia sociedad, que aquellas deben proteger, para el cumplimiento, en las democracias liberales, de los derechos fundamentales de los ciudadanos libres e iguales.

Las actividades realizadas por la policía u otras fuerzas y cuerpos de seguridad y sistema judicial se centran principalmente en las siguientes actuaciones, que también se dan en Cyberia: a) prevención, investigación, detección, persecución, enjuiciamiento y castigo (o rehabilitación) de infracciones penales, incluidas, las actuaciones policiales en las que no queda constancia de si un incidente es o no constitutivo de infracción penal; b) aquellos otros casos de aplicación de medidas coercitivas (en manifestaciones, grandes acontecimientos deportivos y disturbios); c) de mantenimiento del orden público, con fines de protección y prevención frente a las amenazas para la seguridad pública y para los intereses públicos fundamentales jurídicamente protegidos que puedan ser constitutivas de infracciones penales[43].

En consecuencia, en Cyberia la tecnología, en su relación con las Fuerzas y Cuerpos de Seguridad del Estado, debe concebirse en un doble plano: por una parte, para ayudar; por otra parte, para sustituir.

Ayudar, en el sentido de complementar la acción humana en la toma de decisiones, que deberá descansar siempre en el nivel humano. Sustituir, en el sentido de dejar libre el elemento humano para realizar funciones de mayor valor añadido y variabilidad, por tanto, dejando a la tecnología para tareas mecánicas, burocráticas, de precisión en el análisis de datos, de elaboración de patrones de conducta o elaboración de perfiles. En todo caso, la regulación en Cyberia está llamada a permitir a humanos y máquinas digitales trabajar juntos. O como dice Wucker, hacer que la tecnología trabaje para el humano y no al revés (Wucker 2018).

En todo caso, nuevas formas criminales, nuevas tecnologías y cambios en las comunidades y en la propia sociedad, remueven las bases del trabajo policial y de su misión.

Toda actuación policial basada en información de inteligencia específica y en métodos predictivos, con tecnología digital que permita la elaboración de perfiles, debe respetar unas garantías concretas, en particular en materia de privacidad, incluida una justificación objetiva y razonable, como recomienda la Agencia Europea de Derechos Fundamentales, en unas indicaciones que bien podrían llegar a ser Derecho de tipo “Soft Law”, en su versión más “Soft”[44]. Asimismo, la tecnología brindará nuevas herramientas, tales como el procesamiento digital de pruebas, el análisis

43 Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo: Considerando 12.

44 Guía para prevenir la elaboración ilícita de perfiles en la actualidad y en el futuro, FRA - European Union Agency for Fundamental Rights, 2018, pág. 19. Disponible en: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_es.pdf

geoespacial, analítica de imagen, análisis digital forense, cribado de datos… que permitirán a las autoridades policiales encontrar más rápidamente la información pertinente, dado el uso que los criminales, a su vez, hacen de la tecnología digital (Deloitte 2019)[45], exigiendo la constitución de observatorios tecnológicos avanzados y el acceso a ingentes recursos presupuestarios, la cooperación con la industria de la seguridad y la protección civil, así como de talento, que habrá que atraer (y retener) a través de políticas de recursos humanos. Prueba de ello, podría ser la reciente regulación del "Protocolo adicional segundo al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas"[46], que ratificarán los Estados de la Unión Europea, en interés de esta.

Pero, además, resulta importante añadir a las funciones tradicionales de policía en Cyberia, la de la presencia de las Fuerzas y Cuerpos de Seguridad en la propia red, de modo que sea capaz de construir lazos con la comunidad que debe proteger, para defenderla del crimen y, como anticipábamos, atraer el tipo de talento necesario para interactuar en un entorno digital y con herramientas digitales (Deloitte 2019)[47]. La tecnología también debe contribuir a construir esta presencia en Cyberia.

Por todo ello, ha de existir un marco normativo, un orden legal, adecuado, que asiente los principios de actuación de cómo interactuar en el medio cibernético por parte de las autoridades policiales, también con la comunidad, mitigando los riesgos potenciales (Soulava, Cameron y Ying, 2021), construyendo un sistema normativo basado en la seguridad jurídica y la confianza legítima, que permita en último término ese ayudar y ese sustituir arriba referidos. Como sucede en la Unión Europea, el sector público ha de ser el impulsor. En el ínterin, será preciso construir una cultura de la seguridad que se asiente en el principio del respecto a los derechos fundamentales, la cultura de la innovación, el principio de una comunidad tan segura en el mundo real como en el cibernético, el principio de la colaboración humano-máquina, y sector público-sector privado, y el de unas autoridades capaces de atraer y retener talento digital.

Así, la necesidad de mitigar el riesgo global de la ausencia de una regulación, por su inaplicación, o por el fracaso de su gobernanza de la tecnología digital, se traduce en la necesidad de favorecer la confianza digital, a través de un sistema normativo adecuado, y contando con unas autoridades policiales y una justicia penal a la altura de los retos y desafíos digitales. Los propios de la cambiante tecnología digital, y los exógenos, como el muy camaleónico crimen digital.

La regulación de la tecnología digital, su gobernanza, la "Lex Informática", la ciberregulación adecuada, Cyberia en definitiva, es clave para la construcción de la confianza digital, como factor ampliado de la ciberseguridad.

Una ciberseguridad, que como sucede con la seguridad, no es producto final sino proceso (Ecija 2017: Capítulo 9). Además, esta confianza, que se ve influenciada por múltiples factores (sociales, tecnológicos, económicos, medioambientales, políticos y

45 https://www2.deloitte.com/content/dam/Deloitte/xe/Documents/public-sector/DI_Future-of-law-enforcement.pdf

46 Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=COM:2021:718:FIN y en https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

47 Disponible en: https://www2.deloitte.com/content/dam/Deloitte/xe/Documents/public-sector/DI_Future-of-law-enforcement.pdf

legales (Deloitte 2021)[48]), sirve como principio inspirador a toda actuación policial, de manera que, delimitando y entendiendo el marco legal y el contexto digital, también se coadyuva a la consecución de la ciberseguridad, desde la dimensión de la relación de las autoridades con el hecho digital.

9. CONCLUSIÓN

En conclusión, se ha de aspirar a una regulación adecuada de la tecnología digital, con impulso por parte del sector público –de estados y organismos internacionales-, sin posiblemente excluir ciertas autorregulaciones tasadas del sector privado. En particular, en materia de seguridad, la regulación adecuada es condición "sine qua non" para la ciberseguridad concebida en sentido amplio, y el papel público será si cabe mayor, y en cooperación con otros estados o niveles públicos de gobernanza, incluida la instancia supranacional. Idealmente, pues, es deseable transitar por fórmulas convencionales (tratados) multilaterales bajo los auspicios de Naciones Unidas (Remiro 2010:691).

Si de la tecnología depende nuestro bienestar, de su adecuada regulación, centrada en la persona y sus derechos fundamentales, depende nuestro estilo de vida libre, en un régimen de opinión pública, en una economía abierta, y en un Estado democrático, Social y de Derecho. La tecnología digital, el pensamiento técnico, pide creyentes, pero necesita personas formadas, ciudadanos que la humanicen (Mounier 2014:472), en definitiva, confianza.

BIBLIOGRAFÍA

Augé, Marc. (2014). "El antropólogo y el mundo global". Ed. siglo veintiuno.

Aznar Fernández-Montesinos, F. (2016). "Cuadernos de Estrategia 197. La posverdad. Seguridad y defensa". Cap. Primero: El mundo de la posverdad". Instituto Español de Estudios Estratégicos.

Baños, P. "El dominio mundial. Elementos del poder y claves geopolíticas". Ed. Ariel.

Calero, A. (2015) "El ciberespacio y el control de las redes", en la Monografía 147, "Geopolítica líquida del siglo XXI", Escuela Superior de las FF.AA., Ministerio de Defensa.

Castells, M. (2000). "Globalización, Estado y sociedad civil: el nuevo contexto histórico de los derechos humanos", ISEGORÍA/22.

Comisión europea (2021) "2021 Strategic Foresight Report the EU´s capacity and freedom to act". European Commision.

Dahl, R. A. (1989). "La poliarquía. Participación y oposición", Ed. Tecnos.

De La Rasilla, I. (2008) "Re-equilibrio multipolar y paz democrática universal", en la obra de Kegley, C. y Raymond, G. "El desafío multipolar. La política de las grandes potencias en el siglo XXI", Almuzara.

48 Disponible en: https://www2.deloitte.com/us/en/insights/topics/digital-transformation/digital-trust-for-future.html

Deloitte. Gelles, M.; Mirkow, A.; Mariani, J (2019) "The future of law enforcement. Policing strategies to meet the challenges of evolving technology and a changing world".

Deloitte. Lux A., Lobbes, M., Buchholz S., Dankworth E., Pfeil K., Kaiser M., Göbel A., Biberacher F., Wenner M., Oerter T. (2021) "Future of digital trust. Driving forces, trends and their implications on our digital tomorrow". Issue 8/2021. March.

Dickem, P. (2020). "El mundo «no» es plano: la profunda desigualdad geográfica de la globalización". BBVAOPENMIND.

Ecija, A. (2017). "El ciberespacio un mundo sin ley", Wolters Kluver.

Ferrajoli, L (2020). "Una Costituzione della Terra", Il Manifesto, Quotidiano comunista, 21.02.2020.

Foro Económico Mundial. (2021). "Appendix A: Description of Global Risks".

Foro Económico Mundial. (2021). "Description of Global Risks 2021".

Foro Económico Mundial. VV.AA. (2019). "Globalization 4.0 Shaping a New Global Architecture in the Age of the Fourth Industrial Revolution", White Paper, April.

García, P. (2018). "Criptoderecho. La regulación de blockchain". Cap. II "Del ciberderecho al criptoderecho. La criptoregulación", Edición nº 1, LA LEY 13759/2018.

García, P. y Villarino, J. (2021). "¿Qué sociedad digital queremos? Alternativas regulatorias para una Europa digitalmente soberana". Wolters Kluwer Legal & Regulatory & Fundación Alternativas. Online.

Garicano, L. (2019). El contrataque liberal. Ed. Península.

Goldin & Mariathasan. (2014). "The Butterfly Defect: How Globalization Creates Systemic Risks, and What to do About It", Princeton University Press.

Gómez de Ágreda, Á. (2012). "El ciberespacio como escenario de conflictos. Identificación de las amenazas", en la Monografía: "El ciberespacio: muevo escenario de confrontación", CESEDEN, Ministerio de Defensa, Nº 126.

Gómez de Ágreda, Á. (2020)."Mundo Orwell", Ed. Planeta.

Guterres, A. (2021). "It´s time to pull together", The World in 2021, The Economist.

Hale, T., Held, D. et al (2017) "Beyond Gridlock", Ed. Polity.

Hale, T.; Held, D. & Young, K. (2013). "Gridlock. Why global cooperation is failing when we need it most". Ed. Polity.

Han, Byung-Chul. (2016). "Psicopolítica", Ed. Herder.

Han, Byung-Chul. (2018). "En el enjambre", Ed. Herder.

Held, D. y VV.AA. (1999). "Global Transformations: Politics, Economics and Culture", Stanford: Stanford University Press.

Jorge-Ricard, R. (2020). "Derechos digitales: un marco necesario, pero (todavía) insuficiente". Real Instituto Elcano. Disponible en: https://blog.realinstitutoelcano.org/derechos-digitales-un-marco-necesario-pero-todavia-insuficiente/

Lasalle, J.M. (2019) “Ciberleviatán. El colapso de la democracia liberal frente a la revolución digital”. Ed. Arpa.

Loeskrug-Pietri A. (2021). “Strategic Compass, Promoting Technological Sovereignty and Innovation: Emerging and Disruptive Technologies. A Workshop Report”. German Council on Foreign Relations No. 21. November.

López, C. (2019). “Wotan, la sociedad abierta y sus nuevos enemigos”, LetrasLibres.

López-Aranda, R. (2020). “El futuro de Occidente en el orden global”. “Panorama Estratégico 2020”. Instituto Español de Estudios Estratégicos.

Ministerio de Defensa. (2018). “Panorama de tendencias geopolíticas. Horizonte 2040”.

Molina, J. M. (2014) “Globalización, Ciberespacio y Estrategia Especial Consideración a la Estrategia de la Información”, Instituto Español de Estudios Estratégicos.

Mölling, C. (2021). German Council on Foreign Relations No. 21 November, “Strategic Compass, Promoting Technological Sovereignty and Innovation: Emerging and Disruptive Technologies, A Workshop Report”

Mounier, E. (2014). “El personalismo. Antología esencial”.

Müller, J-W. (2018). “The rise and rise of populism?”, BBVAOPENMIND.

National Intelligence Council. (2021). “GLOBAL TRENDS 2040”. March.

Nuñez, C. (2018) “El constitucionalismo cosmopolita en debate”. Trabajo Fin de Máster. Tutor: ANSUATEGUI, Francisco Javier. Universidad Carlos III, de Madrid.

Ohmae, K. (2008). “El próximo desafío global. Desafíos y oportunidades en un mundo sin fronteras”. Verticales de bolsillo. Wharton School Publishing.

Organización Mundial del Comercio. (2021) “Economic Resilience and Trade”.

Ortega, A. (2018). “La voladura del trilema de Rodrik”. Blog Real Instituto Elcano.

Panda, A. (2021). Carnegie Endowment for International Peace.

Reguera, J. (2015) “Aspectos legales en el ciberespacio”. GESI.

Remiro, A. (2010). “Derecho Internacional. Curso General”, Ed. Tirant lo Blanch.

Rupérez, J. (2009) “El espejismo multilateral. La geopolítica entre el idealismo y la realidad”. Almuzara.

Saran, S. (2020) “Navigating the Digization of Geopolitics”, “Shaping a Multiconceptual World”. WEF.

Soulava, B; Cameron, H.; Ying, V (2021) “Data rules for machine learning: How Europe can unlock the potential while mitigating the risks”. Atlantic Council´s Cyber Statecraft Initiative. Scowcroft Center for Strategy and Security.

Turégano, I. (2017) “Derecho transnacional o la necesidad de superar el monismo y el dualismo en la teoría jurídica, Derecho PUCP, Universidad Castilla- La Mancha, Nº 79.

Wucker, M. (2018). “How to have a good Fourth Industrial Revolution”, World Economic Forum.

Wucker, M. (2021) “You are what you risk”. Ed. Pegasus Books, NY-London.