
Sociedades tecnológicas

La tecnología como catalizadora del cambio social

Enrique Ávila Gómez

La sociedad occidental se ha desarrollado, a partir de la Revolución Francesa, sobre firmes cimientos que nos adscribían, como individuos, a un territorio, a un determinado modelo cultural. Nos envolvían en un conjunto de seguridades y certezas que nos permitían transitar por la vida, en general, pudiendo calcular, con cierta exactitud, una aspiración de futuro, siempre mejor que el pasado que dejábamos atrás. Frecuentemente, estas certezas se transformaban en papel mojado en virtud de la aparición de lo que podríamos denominar, situaciones de crisis o, tal y como refiere Taleb Nassim, los denominados «cisnes negros» que, en forma de conflictos, procesos revolucionarios, dinámicas sociales sobrevenidas o, directamente, guerras, alteraban ese supuesto futuro previsto.

Tras un proceso de adaptación, inherente al propio ser humano y que, por otra parte, es lo que le permite su altísima resiliencia como especie, frente a un entorno muchas veces agresivo con ésta

(aunque, en realidad, es nuestro comportamiento vírico el que constituye la mayor de las amenazas contra el resto del ecosistema global que nos contiene), se producía un proceso evolutivo que se desarrollaba a través de los años hasta la eclosión de la siguiente situación de crisis, realimentando un ciclo de destrucción-reconstrucción-evolución que ha configurado el propio proceso evolutivo de la humanidad hasta el momento actual.

El modelo de democracia-liberal parecía haberse impuesto a nivel global cuando eclosiona, apoyado en este modelo globalizador, la tecnología como elemento catalizador de cambios que impactan sobre los individuos, los grupos, las sociedades, culturas al completo, haciendo de este momento histórico en el que desarrollamos nuestras actividades uno de los momentos más complejos, frenéticos y apasionantes de la historia de la especie. Varios son los elementos que, a mi juicio, caracterizan este apasionante momento de la historia que nos ha tocado vivir y que suponen un punto de disrupción en los modelos de evolución seguidos hasta el momento:

- Procesos de globalización económicos, sociales y culturales.
- Evolución de los modelos productivos fuertemente concentrados hacia otros en los que la desintermediación y la desconcentración van adquiriendo un papel relevante.
- Alta esperanza de vida que provoca enormes cambios en las estructuras sociales al hacer convivir hasta cinco generaciones en un mismo momento histórico. A medio plazo, incluso, se atisban aspiraciones de inmortalidad, al menos conceptualmente, con las consecuencias que ello tendría en la ética, la moral, la filosofía y la teología.
- Despoblación de amplios territorios al tiempo que diversos factores (ecológicos, conflictos, inseguridad...) provocan migraciones masivas hacia zonas más ricas.

- Doble bomba demográfica, una directa y otra inversa, que se desarrolla sobre zonas de conflicto.
- Conflictos con *proxies* de intermediación, entre los aspirantes a liderar las diferentes regiones estratégicas en las que parece descomponerse un mundo claramente convertido en unipolar tras la caída de la URSS.
- Posible transición hacia la desaparición de las estructuras sociales clásicas eliminando ciertos roles prefijados, con los cambios disruptivos que ello conlleva en todo lo referente a los «asideros» emocionales y sentimientos de pertenencia a estas mismas estructuras sociales.

Todos estos elementos, y muchos más que podrían glosarse, se apoyan, sin duda, en la tecnología como facilitadora e inductora del cambio social emergente. La tecnología se posiciona como el elemento transversal en el que se apoyan muchos de estos cambios, siendo indiciario de lo antedicho el sector al que pertenecen las principales empresas a nivel global, todas ellas tecnológicas frente a la progresiva pérdida de relevancia de las corporaciones que lideraron la Segunda Revolución Industrial.

La inmediatez de las comunicaciones globales, el acceso al conocimiento generado por millones de personas de toda condición, modelo social y cultural, género o edad, la posibilidad de superar los objetivos productivos de la Segunda Revolución Industrial, basados en planes de intermediación muy rígidos, la evolución de los tratamientos de salud y la posibilidad de participación por parte de todo ciudadano en los procesos de toma de decisión política que, anteriormente, les estaban vedados, configuran la mayor de las revoluciones a las que se ha enfrentado el ser humano como especie. Y es la tecnología la que cataliza esta revolución. Podríamos decir que, en cierto modo, hemos iniciado un juego hasta hace poco reservado al ámbito de la teología y ello induce lo que podría-

mos considerar como un punto de singularidad tecnológica alimentada por el progresivo acercamiento a la consecución del concepto de Inteligencia Artificial fuerte o la propia percepción, aún difusa, de que el ser humano adquiere, en cierto modo, el «poder de Dios», el poder de crear a nuevos seres, el poder de aspirar a la propia inmortalidad.

La incorporación masiva de la tecnología a nuestras sociedades avanzadas induce un conjunto de efectos, de dinámicas sociales que, no por conocidas, dejan de ser peligrosas. Enunciemos por ejemplo el concepto de olocracia que, según Polibio, es una forma degenerada de la democracia, lo mismo que la monarquía degenera en tiranía o la aristocracia lo hace en oligarquía... La olocracia o «gobierno de la muchedumbre», parece ser una definición casi exacta de lo que conocemos como «legislar en caliente» ¿Qué son las denominadas en el mundo anglosajón como *fake news* o desinformaciones sino la clásica acción de inteligencia realizada con el fin de imponer una supuesta verdad a un determinado grupo social con un fin político? Toda esa desinformación, posiblemente orientada hacia un fin (aunque no siempre), impacta sobre la población que, a su vez, ve su juicio mediatizado por la acción de unos algoritmos creados para la obtención de un beneficio económico y no, desde luego, para la aspiración al «bien común». El «gobierno de la muchedumbre», esa olocracia, no es sino una manifestación del impacto que tiene la tecnología, por su inmediatez y globalidad, para desplegar un elemento clásico de inteligencia para la consecución de un determinado fin, ya sea éste militar, económico, político o social, predeterminado.

El acceso a la información no nos libra de sufrir problemas (y éstos son muy graves), de infoxicación. Y van a más. ¿Por qué? Porque, además del impacto de la actividad humana en la Red, nos encontramos con que estamos introduciendo trillones de dispositivos que tienen tres características que hemos de conocer para

evaluar correctamente los riesgos inherentes a nuestra decisión de hacerlo: tienen capacidad de cómputo, capacidad de almacenamiento y, sobre todo, capacidad de interconexión. Configuran enormes redes de sensores que vuelcan a la Red miríadas de datos que poderosos algoritmos transforman en información, conocimiento e inteligencia y que, en muchas ocasiones, permiten obtener conocimiento de la mera actividad de los seres humanos que se aprovechan de sus ventajas, sin necesidad de personificar al ser humano concreto. La individualización se produce por la mera actividad, sin importar de quién se trate, sino, por ejemplo, sus patrones de gasto, a la hora de orientar el acceso a una determinada información. El modelo descrito induce peligrosos sesgos que impactan, de manera directa, sobre capas completas de la población, en una acción que supone un torpedo en la línea de flotación de conceptos fundamentales en una democracia como son los de igualdad de oportunidades. El algoritmo no ofrece determinada información a quien no tiene, supuestamente, necesidad de conocerla.

Además de lo antedicho, y con consecuencias aún por evaluar, desde hace años, muchos de los procesos de toma de decisión que gobiernan nuestras vidas no son tomados por seres humanos sino por algoritmos, algunos de ellos con capacidad de aprendizaje. Nuestras capacidades, como seres humanos, no sirven para gobernar sociedades tan complejas como las nuestras. La enorme complejidad de la logística necesaria para que nuestras sociedades se desarrollen sin grandes sobresaltos, impide que nuestras pobres capacidades como seres humanos, que nos permitían sobrevivir en la sabana, sean suficientes para poder dar respuesta a los problemas a los que se enfrenta una sociedad tan compleja como la que hemos generado. Pensemos, por ejemplo, en el tiempo adecuado que requiere la toma de decisión de nuestros procesos logísticos de suministro de agua, energía, alimento o asistencia sanitaria, que se

encuentran fuera del alcance, completamente, de las capacidades de los seres humanos para la toma de decisión en los procesos que gobiernan el suministro de esos servicios básicos.

Ciberseguridad en la Red

Internet... La Red... La génesis de la estructura sobre la que se apoyan nuestras sociedades es militar. Su diseño se orienta hacia la resiliencia y no hacia la seguridad. El objetivo de los protocolos de comunicación y de la propia infraestructura de comunicación se orientaba hacia que algún nodo de la red ARPANET sobreviviese a un ataque nuclear de la extinta URSS para lanzar un contraataque. Ese modelo desborda rápidamente su objetivo inicial cuando se intuye la posibilidad de generar valor económico sobre su infraestructura y rápidamente se convierte en una red de propósito general en el que se empiezan a desarrollar actividades comerciales con la provisión de servicios cada vez más complejos y veloces. La eficiencia conseguida es tan alta que, en un momento difuso, las denominadas infraestructuras críticas, las que proveen de servicios esenciales a la sociedad, se integran en esta red de propósito general. Este proceso de integración mejora, sin duda, la eficiencia de los sectores estratégicos e impulsa la generación de nueva tecnología que, a su vez, genera nuevas áreas de negocio y más riqueza, en un proceso que no parece terminar y que continúa actualmente pero, del mismo modo, con la integración de estas redes industriales y, sobre todo, con la producción masiva de dispositivos de control en modelos productivos descentralizados y con poco o nulo control sobre la fabricación de estos dispositivos a integrar en grandes redes industriales, se inducen peligrosos riesgos que es necesario valorar adecuadamente y mitigar en lo posible.

El diseño inicial de Internet, orientado a la resiliencia, tiene consecuencias estructurales que determinan muchos de los problemas que sufrimos en la actualidad en materia de ciberseguridad: prácticamente es imposible saber quién hace qué cosa en la Red. Sin poder atribuir la autoría, es imposible determinar consecuencias legales sobre la responsabilidad. Se desarrolla, debido a esta carencia estructural, todo un ecosistema de empresas que, por un lado, ofrecen servicios «gratuitos» a los pseudónimos (que no anónimos) usuarios de la Red. Por otro lado, y de forma paralela, se desarrolla un ecosistema de empresas que intentan abastecer de ciberseguridad a los actores de la Red, ya sean proveedores de servicios o usuarios de los mismos. Una consecuencia lógica del modelo y, desde luego, describirlo no significa criticarlo. Siendo cierto todo lo antedicho, no lo es menos que, como ha ocurrido, a lo largo de la historia de la especie humana, parte de las actividades de determinados individuos y grupos en la Red han generado un ecosistema de aprovechamiento del incauto, del no preparado o del enemigo. Aparecen, en este escenario, y se desarrollan con posterioridad, las estructuras que ofrecen al mejor postor sus especiales conocimientos en materia de Seguridad TIC, conculcando las diferentes leyes nacionales e internacionales que, trabajosa y lentamente, se han ido promulgando por todo el planeta. Se trata de los grupos que ofrecen servicios CaaS de «Crime as a Service» y que, con recursos asimétricos y bajo riesgo (tanto el suyo como el percibido por la propia sociedad agredida), ofrecen la comisión de actividades delictivas en la Red a cambio de un precio.

La Red, sin duda, es un campo de batalla. Y un campo de juego. De un juego complejo, multidimensional, en el que las piezas del juego no se mueven sujetas a ninguna regla conocida, en el que los tiempos de respuesta son cada vez más bajos y, en definitiva, en el que tampoco están demasiado claros los objetivos del juego. Reiteramos que, este juego, además, aunque intuitivo como

importante tanto por los decisores estratégicos de los Estados y las corporaciones, como por las sociedades que son sujeto de la acción de este modelo tecnológico, aún no es percibido con toda la profundidad que el fenómeno merece, provocándose una cierta asimetría entre el riesgo efectivamente percibido y los recursos dedicados a mitigarlo.

La ciberseguridad aún es tratada, en muchos ámbitos, como un gasto y no como una inversión. Parece increíble que se acepte que este modelo tecnológico es la infraestructura en la que se apoya, no ya sólo el desarrollo continuado de nuestro modelo social, con sus claros oscuros pero, sin duda, en una clara dirección de avance, con la generación de actividades económicas de alto valor añadido pero que, de forma paralela, no se acepte que, tal y como está concebido el modelo, se hace preciso asegurar el que es el activo más importante de cualquier estructura productiva o gubernamental en la actualidad: la información. Pero no sólo ésta sino también los procesos de tratamiento de la misma para convertirla en conocimiento y, en el caso más trabajado y óptimo, en inteligencia que permitirá adoptar decisiones informadas por parte de los propios decisores estratégicos. La protección adecuada de estos activos se configura, junto con la detección temprana del talento, su reclutamiento y la preservación del mejor dentro de la organización, como el elemento estratégico de cualquier corporación que pretenda aspirar a sobrevivir en este intricado mundo del siglo XXI.

La defensa de los perímetros tecnológicos de hace sólo diez años, a partir de un modelo y de una estructura de ciberseguridad estática ha quedado definitivamente obsoleto. Lo mismo que cuando se inventó la artillería como fuerza ofensiva, dejaron de tener interés las fortificaciones como estructuras defensivas, los perímetros clásicos de ciberseguridad, basados en infraestructuras estáticas, han dejado de ser los más relevantes en el nuevo modelo. Precisamente son los seres humanos, con sus sesgos cognitivos y

sus vulnerabilidades intelectuales los que, portadores y/o usuarios de soportes tecnológicos cada vez más numerosos y automatizados, los que se están manifestando como los elementos más vulnerables del modelo. Educar (que no concienciar), es un proceso a muy largo plazo que puede superar nuestras capacidades en el corto plazo y todos somos conscientes de las consecuencias. La eclosión de los modelos de fractura social, que personalmente denomino «de binarización», ya sea por intereses espurios de grupos, organizaciones, estructuras políticas e, incluso individuos, se han transformado, en este modelo de circulación de información sin filtro, sin control, haciendo uso de personalidades pseudónimas que impiden la determinación de las responsabilidades en la Red, en un grave problema en materia de Ciberinteligencia y este problema induce dificultades que se antojan complicadas de resolver en el modelo de desarrollo tecnológico actual.

La ateritorialidad del dominio del Ciberespacio, otra de sus características estructurales de importancia fundamental, en el que no hemos entrado en este artículo, induce riesgos determinantes y adicionales al modelo. Si tenemos dificultades a la hora de determinar la autoría y, además, dependemos de las estructuras de cooperación policial y judicial a la hora de perseguir las actividades ilícitas en la Red, creo que podemos imaginar la magnitud del problema al que nos enfrentamos. Además de lo antedicho, pensemos en que las infraestructuras de telecomunicaciones ya no son propiedad de los Estados sino de Corporaciones Transnacionales cuyos objetivos pueden encontrarse claramente desalineados con lo que consideraríamos como «interés general» de la sociedad global. Una vez descrito el escenario, aunque sea con un trazo grueso, hemos de trabajar en encontrar soluciones a los problemas enunciados.

No quiero terminar este artículo sin ofrecer esperanza. También se ha desarrollado tecnología que permite pensar que sería

plausible mejorar nuestra posición actual, si es que aceptamos que queremos mantener conceptos y estructuras de poder provenientes de nuestro modelo analógico (lo cual puede ser o no ser deseable pero, afortunadamente, no he de ser yo quien tome decisiones a ese respecto). Las antedichas capacidades tecnológicas relacionadas con la transposición del concepto de Estado de Derecho y de Separación de Poderes, que son las bases de nuestros Estados Democráticos, han sido desarrolladas tecnológicamente. La Identidad Soberana, reconocida a nivel internacional (a pesar de ser un problema jurídico de enorme complejidad), podría devenir en la posibilidad de atribución de la responsabilidad a los actores de la Red entre los que se encontrarían, sí, las personas físicas y jurídicas pero, incluso más importante aún en el medio y largo plazo, los dispositivos y, sobre todo, los algoritmos y las Inteligencias Artificiales que impactan en los procesos de toma de decisión. El concepto de separación de poderes, la trazabilidad de las actividades y la transparencia de las mismas, estarían apoyadas, al menos conceptualmente, por estructuras de tipo *blockchain*, poniendo especial énfasis tanto en los algoritmos criptográficos utilizados como en el modelo de «mineros» que daría soporte a los apuntes en el bloque. La tecnología existe. No ha sido diseñada específicamente para el fin propuesto, pero podría asegurar la transposición de nuestras estructuras analógicas de protección de los Derechos Fundamentales al modelo tecnológico que asegura, al menos de momento, la resiliencia social. A medio plazo, la introducción de nuevas tecnologías relacionadas con la biotecnología, el cambio de modelo de producción de energía, los procesos de reutilización de los cada vez más escasos recursos disponibles a través del rediseño de los procesos productivos en modelos de la denominada «economía circular», la propia progresiva hibridación de la especie con dispositivos avanzados que permiten mejorar la salud y ampliar la esperanza de vida, entre otras posibilidades, dibujan un horizonte a la

vez prometedor y de riesgo sobre el que tendremos que trabajar para mitigar, en la medida de lo posible, estos últimos y avanzar en los primeros. Una era asombrosamente extraña y apasionante la que estamos viviendo. Tendremos que reflexionar mucho. Alentar el pensamiento profundo, desarrollar nuevas ontologías y esperar, posiblemente, el advenimiento de un nuevo Rousseau o de un nuevo Montesquieu que ayude a rediseñar el concepto de separación de poderes y de salvaguarda de los derechos fundamentales. Pero eso, probablemente, lo habrán de hacer las generaciones que denominamos como «nativos digitales». Su visión es diferente, a veces, muy creativa y muy lateral a nuestro propio modelo de pensamiento. Habremos de confiar en su buen juicio.

E. A. G.

