Antonio A. Martino
(compilador)

De Luis XIV
Al Estado inteligente

Las transformaciones de la Administración del Estado por las nuevas tecnologías

Martino, Antonio A.

De Luis XIV al Estado inteligente: la transformación de la Administración del Estado por las nuevas tecnologías / Antonio A. Martino compilación

1ª ed. - Ciudad Autónoma de Buenos Aires: Astrea, 2023.
Libro digital, PDF

Archivo Digital: descarga y online
ISBN 978-987-706-468-1

1. Administración Pública. 2. Tecnología Informática. I. Martino, Antonio Anselmo , comp. II. Título.
CDD 351

EDITORIAL ASTREA

ÍNDICE GENERAL

INTRODUCCIÓN

Los artículos que aquí se presentan son de autores que han presentado conferencias en el ciclo de 2021 De Luis XIV al Estado inteligente, promovido por el SAI (Sistemas Administrativos Inteligentes) de la Academia Nacional de Ciencias de Buenos Aires durante el año 2021.

El ciclo trato de las transformaciones que acaecieron en las Administraciones (entendiendo la de los tres poderes: Ejecutivo, Legislativo y Judicial) por la introducción de nuevas tecnologías.

El título quería llamar la atención sobre las transformaciones que fue sufriendo la Administración desde la concepción unitaria y vertical que el rey francés impusiera entre fines de 1600 y los albores de 1700.

Con la muerte de su padre a los 5 años debió someterse a la regencia de su madre, Ana de Austria y las enseñanzas de dos cardenales: el italiano Mazzarino y el francés Richelieu, gobernó sobre un país de 19 millones de habitantes que era aventajado en el comercio y que debía todavía encontrar una identidad.

Hasta que edificó Versalles la monarquía francesa era itinerante. A partir de entonces toda la vida política y administrativa se concentró allí. Luis XIV convirtió a los consejos en verdaderos ministerios administrativos. El Conseil d'en Haut o Consejo Supremo fue el principal órgano de gobierno. De él quedaron excluidos los príncipes de sangre e incluso la propia reina madre. Creó organismos nuevos para una monarquía que cada vez más era una máquina burocrática: el Conseil de Dépêches para las relaciones con las provincias, el Conseil des Finances, el Conseil de Justice o la inspección general de hacienda. Para garantizar el orden interno y el cumplimiento de la voluntad regia, Luis XIV fortaleció un eficacísimo cuerpo de intendentes, verdadero instrumento de represión de la monarquía. Conseguir la obediencia a la autoridad monárquica en el interior y asegurar la hegemonía y reputación francesas en el exterior fueron las reglas esenciales de la política del Rey Sol.

Jean-Baptiste Colbert, antiguo intendente de Mazarino y hombre de gran inteligencia política, fue su principal consejero durante buena parte del reinado. Nombrado controlador general de finanzas, se encargó de la reorganización del Consejo de Hacienda y recibió las secretarías de Estado de la Marina y de la Casa del Rey. De él dependían los intendentes de provincias, el comercio, la navegación, las aguas y bosques y las colonias ultramarinas. Para evitar la concentración de poder en manos de Colbert, Luis XIV entregó los ministerios del ejército de tierra y de política exterior a otros consejeros.

Desde entonces pasaron muchas cosas, empezando por la Revolución de 1789 pero la Administracion centralizada y manejada por ministerios se mantuvo apenas cambiada por los nuevos tiempos, después de la Segunda Guerra Mundial. La Administracion comenzó a ser también horizontal y a extender sus rayos de acción incorporando cada vez más la necesidad del administrado que había vivido en sombras.

La revolución que produce Internet en 1992 ha invadido toda la vida y no podía dejar de acometer a la Administración.

Las nociones de gobierno abierto, la lenta transformación de una burocracia de papel en una burocracia digital fue modelando lo que hoy tratamos de describir como un camino al Estado inteligente. Falta camino a recorrer, falta cultura en la sociedad para adecuarse al nuevo mundo y falta todavía cultura en la propia administración para adecuarse a los medios modernos.

De ello, de las ventajas de una administración transparente y también los peligros. De ambos se trata en el libro.

Hay autores argentinos, uruguayos, italianos, brasileños, españoles y esto permite ver el fenómeno de la administración digital en el contexto de diferentes culturas políticas, jurídicas, sociales y económicas.

La riqueza del libro consiste en el tratamiento teórico del tema del gobierno digital y práctico con ejemplos concretos en países concretos en dos continentes.

Buena lectura.

SAI - Sistemas Administrativos Inteligentes

"*Después del Sistema Público de Identidad Digital - SPID: perfiles virtuosos y criticidades de la ciudadanía digital*"

Por Valentina Grazia Sapuppo

1. Los conceptos de /qué entendemos por/ identidad digital y ciudadanía digital

El concepto de Identidad Digital incluiría, por un lado, la proyección de la identidad personal de un individuo en la web, y por otro, todas aquellas técnicas de identificación de la persona que le permiten actuar en realidad virtual, utilizando herramientas informáticas. La Identidad Digital es reconocida para todos, ciudadanos y extranjeros, así como para los representantes legales de las personas jurídicas[1].

El concepto de Ciudadanía Digital, en cambio, podría entenderse como una extensión de la ciudadanía tradicional, es decir, como el conjunto de derechos y deberes que, gracias al apoyo de determinadas herramientas y servicios informáticos, contribuyen a simplificar la relación entre los ciudadanos, empresas y administraciones públicas, realizando la participación en la sociedad de la red. En este sentido, a partir de 2017 el CAD - Código de Administración Digital, disciplina italiana clave de la que hablaré en breve, define la naturaleza de las llamadas Tarjeta de Ciudadanía Digital[2], y prevé el derecho, reconocido a los ciudadanos y empresas, a una identidad y domicilio digital, así como el derecho a utilizar los servicios públicos online de forma sencilla y mobile-oriented, así como el derecho a participar efectivamente al procedimiento administrativo por vía electrónica y para realizar los pagos digitalizados.

2. Evolución histórica

Este tema tiene su origen en el proyecto más amplio de una Europa digitalizada, cuyo objetivo es maximizar el uso de herramientas digitales, para completar el proyecto de un mercado único digital europeo, a partir de la Directiva 2006/123/CE del

---

[1] La identidad digital para uso profesional transmite, además de los datos de la persona física, también los datos de la persona jurídica (por ejemplo, el número de IVA, el tipo de empresa, etc.) y puede ser necesaria para acceder a servicios dedicados a fines profesionales: • para uso profesional de la persona física, que transmite únicamente los datos de la persona física; • para uso profesional de la persona jurídica, que proporciona los datos de la persona física y dé la organización a la que pertenece. El responsable legal de una organización (empresa, entidad, negocio, etc.) puede solicitar y utilizar su identidad digital para acceder a los servicios en línea. Para ello también es posible dotar a sus empleados de identidades digitales para el uso profesional de la persona jurídica.

[2] Al respecto, leemos: "el derecho de los ciudadanos y empresas, 'también mediante el uso de las tecnologías de la información y la comunicación ...a acceder a todos los datos, documentos y servicios de su interés en modo digital... con el fin de garantizar la simplificación en el acceso a los servicios personales 'y' reducir la necesidad de acceso físico a las oficinas públicas'".

Parlamento Europeo y del Consejo sobre servicios en el mercado interior.

Por lo tanto, es fundamental el mutuo reconocimiento transfronterizo de las funciones administrativas esenciales, incluida la identificación electrónica, los documentos electrónicos, las firmas electrónicas y los servicios de entrega electrónica, así como la interoperabilidad de los servicios de administración electrónica en toda la Unión Europea.

Desde 2013, en Italia, se establece el marco regulatorio del SPID, en línea con las hipótesis adelantantes en los principales Estados miembros de la Unión Europea, hipótesis imaginadas para superar las limitaciones de la preexistente Carta Nacional de Servicios - CNS - y la Cédula de Identidad Electrónica[3] - CIE. Todo esto, también, con el fin de evitar que el delicado tema de acceso a los servicios públicos para los ciudadanos, cada vez más problemático de gestionar a nivel de administraciones individuales por los costos y crecientes problemas de seguridad - podría convertirse en prerrogativa de individuos privados sin ningún control por parte del Estado. Il Governo Italiano cominciò a realizzare l'idea di un sistema di identità federate private, in modo tale da poter avviare tale progetto pluriennale a costo zero.

El 9 de diciembre de 2014 se publicó en el Boletín Oficial la primera medida normativa de implementación del SPID, que prevista luego por el Código de Administración Digital[4] - CAD para la gestión de la identidad digital de ciudadanos y empresas y, con un posterior decreto col que se atribuyó a Agencia para Italia Digital - AgID la tarea de adoptar las regulaciones adecuadas para permitir la aplicación del sistema SPID.

De esta forma AGID, en 2015, emitió la normativa con la que se identificaron:

- las reglas y métodos técnicos para implementar el sistema SPID;

- los métodos para acreditar a los sujetos que pueden emitir la identidad digital;

- los procedimientos adecuados para permitir a los administradores emitir identidades digitales mediante el uso de sistemas de identificación computarizada para los solicitantes.

3. La situación en Italia

Para aquellos que no tienen claro cómo opera la jerarquía de las fuentes europeas con respecto a los estados miembros individuales, simplemente me gustaría aclarar que cada intervención reguladora italiana en el campo de la digitalización de servicios no es más que un ejercicio de transposición de opciones supranacionales,

[3] Para más información sobre este punto, vid. https://temi.camera.it/leg18/post/la-carta-di-identit-elettronica.html?tema=temi/tl18_informatizzazione_delle_pubbliche_amministrazioni.

[4] Actualmente está vigente la sexta versión, la cual se puede consultar en el enlace: www.agid.gov.it/it/agenzia/strategia-quadro-normativo/codice-amministrazione-digitale.

de la Agenda Digital Europea[5]. La primera referencia orgánica para las tecnologías de la información en la administración pública fue el decreto legislativo 39/1993, cuyo objetivo era regular el diseño, desarrollo y gestión de los sistemas automatizados de información de las administraciones estatales. Con la subsiguiente ley 59/1997, con el objetivo de reducir la burocracia y simplificar las relaciones entre la administración pública y el ciudadano, se contempla la sustitución del documento de identidad en papel por el documento electrónico. La ley 127/1997 introdujo la Cédula de Identidad Electrónica - CIE y con el decreto presidencial 513/1997 la firma digital, mientras que el protocolo informático - y en consecuencia la gestión de los flujos de documentos han sido regulados por la D.P.R. 428/1998. La disposición fundamental de esta primera fase de normalización, que apunta a una reorganización orgánica de todo el sector, es el decreto presidencial 445/2000, que disponen, en un solo texto, todas las disposiciones legislativas y reglamentarias sobre documentación administrativa, informática y de papel, introduciendo la sustitución de la misma.

El siguiente paso se da en 2005 cuando se recogen todas las disposiciones relativas a la actividad digital de las administraciones públicas y se reordenan en un solo texto normativo, el Código de Administración Digital - CAD, establecido con decreto legislativo 7 de marzo de 2005, n. 82, posteriormente modificado e integrado primero con el decreto legislativo 22 de agosto de 2016 n. 179, con el decreto legislativo 179/2016 que transpone el Reglamento eIDAS, del que hablaré en breve.

Con el decreto legislativo 13 de diciembre de 2017 n. 217, Italia ha tomado medidas para promover e implementar los derechos de ciudadanía digital, hasta los últimos cambios dictados por el decreto legislativo 16 de julio de 2020, no. 76 convertidos, con modificaciones, por ley 11 de septiembre de 2020, n. 120.

4. La situación en Europa

El 19 de febrero de 2020, la Comisión Europea presentó un paquete de propuestas para promover y apoyar el proceso de transición digital, que incluye:

- la comunicación sobre “Dar forma al futuro digital de Europa” COM (2020) 67[6];

---

[5] Agenda Digital Europea, Bruselas, 19.5.2010 COM (2010) 245 - Comisión Europea - Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones.

[6] La Comunicación “Dar forma al futuro digital de Europa” COM (2020) 67 demuestra como este proceso de digitalización, destinado a la aproximación entre los ciudadanos y las administraciones públicas, aún tiene un largo camino por recorrer.

Entre los objetivos declarados: - mejorar la vida de los ciudadanos, también mediante el uso de tecnologías para interactuar con las administraciones y los proveedores de servicios públicos; - contribuir a una sociedad abierta, democrática y sostenible; - garantizar la seguridad de los usuarios en línea; - permitir el desarrollo de empresas digitales innovadoras; - garantizar el control por parte de los ciudadanos de sus datos y de su identidad digital - fiables también en el sector privado a través del Reglamento eIDAS [Reglamento de identificación electrónica y servicios de confianza, Reglamento de la UE 910/2014] que introdujo un marco estandarizado para la aceptación de firmas e identidades electrónicas.

- Comunicación sobre la estrategia europea de datos COM (2020) 66;

- el Libro Blanco sobre inteligencia artificial COM (2020) 65.

En la reunión extraordinaria del Consejo Europeo, celebrada en octubre de 2020, los líderes de la UE pidieron a la Comisión de presentar una “brújula digital” que defina el horizonte digital europeo 2030 y redactar un plan para la identificación electrónica [e-ID] pública y segura y que, también, tuvo en cuenta las firmas digitales interoperables para garantir a las personas el control de sus datos e identidad en la red mediante el acceso a servicios digitales públicos, privados y transfronterizos.

Sin querer sobrecargar demasiado mi presentación, completo el análisis del marco regulatorio haciendo algunas referencias al reglamento UE no. 910/2014 Reglamento de Identificación Electrónica y Servicios de Confianza - eIDAS, base reguladora comunitaria sobre identidad digital, implementada en Italia con el decreto legislativo 179/2016 que modificó e integró el Código de Administración Digital - CAD.

De hecho, con respecto a los sistemas de identificación electrónica identificados por la Directiva 1999/93/CE dedicada a las firmas electrónicas, el Reglamento eIDAS, con el objetivo de facilitar el uso transfronterizo de los medios de identificación electrónica de los distintos Estados miembros, establece las condiciones en qué Estados miembros reconocen los medios de identificación electrónica de las personas físicas y jurídicas de otro Estado miembro, gracias al principio de mutuo reconocimiento y mutua aceptación de los sistemas de identificación electrónica interoperables “e-ID”. Para acelerar todo este proceso, a través de los denominada Trust Service Providers - TSP, eIDAS:

- simplifica las condiciones de competencia para los Trust Service Providers que actualmente operan como entidades acreditadas para el desarrollo de dichos sistemas;

- reconocen a ciudadanos y empresas los derechos a la identidad y el domicilio digital, a utilizar servicios públicos en línea y orientados a dispositivos móviles, a participar de manera efectiva en el procedimiento administrativo por vía electrónica y a realizar pagos digitalizados;

- promueve la elevación del nivel de calidad de los servicios públicos y de confianza en digital, tanto mediante el establecimiento de la Oficina del Defensor del Pueblo Digital en el AgID, como aumentando el alcance de las sanciones que se pueden imponer si Trust Service Providers violan las normas;

- establece la figura del Comisario de Agenda Digital, que podrá hacer uso de los entes públicos y tomar el lugar de las administraciones competentes para tomar las medidas necesarias para la implementación de los objetivos marcados.

5. ¿Qué es SPID y para qué servicios se aplica?

En Italia, a partir del 10 de septiembre de 2019, los ciudadanos pueden utilizar su identidad digital SPID para acceder a los servicios digitalizados de las administraciones públicas europeas, superando los antiguos procedimientos que requerían la

visualización de documentos de identificación o código de acceso[7].

El decreto del presidente del Consejo de Ministros de 24 de octubre de 2014, también conocido como decreto SPID, define en el art. 1, lett. *o*, la identidad digital como la "representación informática de la correspondencia uno a uno entre un usuario y sus atributos de identificación, verificada a través de todos los datos recogidos y registrados en formato digital". Básicamente, se trata de una identidad digital pública formada por un par de credenciales estrictamente personales (username y password), que habilita los usuarios para realizar determinadas actividades en la red y con las que se puede acceder a los servicios online de la administración pública. El sistema público de identidad digital SPID, está conformado por un conjunto abierto de entidades públicas y privadas que, previa acreditación por parte de AgID, gestionan los servicios de registro y la provisión de credenciales y herramientas de acceso a la red para ciudadanos y empresas. Para obtener las credenciales SPID, simplemente haga una solicitud a unos de los Identity Providers acreditados por AgID, que en Italia son: Aruba, Infocert, Intesa, Namirial, Poste, Register, Sielte, Tim o Lepida, etc. Además de estos administradores privados, en Italia está previsto el RAO - Oficial de autoridad de registro. Es una Administración pública, o una oficina autorizada por ella, que puede activar el SPID a solicitud de los interesados.

Identity Providers ofrecen diferentes tipos de activación y tres niveles diferentes de seguridad:

- nivel 1, con las credenciales SPID del usuario (nombre de usuario y contraseña);

- nivel 2, con credenciales SPID y la generación de un código de acceso de contraseña temporal de un solo uso (OTP) o el uso de una aplicación accesible a través de un dispositivo, como uno smarthphone;

- el nivel 3, que prevé el uso de soluciones de seguridad adicionales y cualquier dispositivo físico (por ejemplo, smart cards) que son proporcionados por Identity Providers.

6. ¿Cuáles son los perfiles virtuosos y las criticidades de SPID?

Gratis, sencillo y seguro. IA pesar del fuerte aumento en el uso de SPID y el número de Tarjetas de Identidad Electrónicas - CIE - activadas por los ciudadanos, las empresas continúan ignorando las dos herramientas o tienen dificultades para implementarlas por diversas razones. Básicamente, el gobierno italiano presionó a SPID de manera inadecuada y apoyó pochito a los proveedores privados, solo para

[7] Art. 64 CAD, Sistema público de gestión de identidades digitales y modalidades de acceso a los servicios prestados en línea por las administraciones públicas, "Promover la difusión de los servicios en línea y facilitar el acceso a los mismos por parte de ciudadanos y empresas, incluso en el movimiento, el sistema público para la gestión de la identidad digital de los ciudadanos y las empresas, SPID", ha sido creado por la Agencia para la Italia digital, que se puede ver en el enlace: https://docs.italia.it/italia/piano-triennale-ict/codice-amministrazione-digitale-docs/it/v2017-12-13/_rst/capo5_sezione3_art64.html.

sobrecargar el sistema con el click day[8]. Frente a la utilidad del SPID para facilitar el acceso autenticado a diversos servicios (para acceder a los avisos del concurso, los sitios previdénciales, el sitio web de la Agencia Tributaria, acceder a fascículo electrónico, cashback, bonificación de movilidad, bonificación de vacaciones), existen varias cuestiones críticas. Entre estos, más del 75% de las activaciones se realizan con un procedimiento físico en la oficina de Poste Italiane, ya que el reconocimiento remoto casi siempre se paga. Otro aspecto crítico es que, según el aviso AGID n° 31 del 5 de octubre de 2020, no es posible tener varias identidades digitales conectadas al mismo número de teléfono. Sin embargo, para mejorar la accesibilidad a los servicios públicos digitales por parte de los ciudadanos más frágiles, sí podrán delegar a quienes ya cuenten con las credenciales, superando así la anterior prohibición. El problema es que todavía falta el decreto de actuación previsto por el Decreto de Simplificación - D.L. 77 de 2021, que establecerá los procedimientos operativos de este Sistema de Gestión de Delegaciones SPID. Otra criticidad es que quien estas en posesión del SPID corre el riesgo de ver su desactivación automática por inactividad o, incluso, por la expiración del plazo de validez.

7. Comparación de legislación italiana y argentina y europea

El decreto ley 34/2019, denominado Decreto de Crecimiento, había introducido otras medidas para asegurar el desarrollo del proceso de digitalización en el interés general, permitiendo el acceso a los servicios de la Administración Pública de forma simplificada, optimizando su uso y logrando una mayor eficiencia, oportunidad y uniformidad de distribución en todo el territorio nacional.

También se ha reformado el Código de Administración Digital - CAD (decreto legislativo 179/2016 que modifica el decreto legislativo 82/2005) con el objetivo de crear una carta de ciudadanía digital que permiten el acceso digital de ciudadanos y empresas a los datos y servicios de las administraciones públicas.

Con el decreto-ley del 16 de julio de 2020, n° 76, que contiene medidas urgentes de simplificación e innovación digital, se propuso una intervención orgánica urgente que forma parte de la agenda de simplificación administrativa para el período 2020-2023 y que prevé:

- el acceso a todos los servicios digitales de la Administración Pública a través de SPID, cédula de identidad digital (CIE) y a través de AppIO;

- el domicilio digital para profesionales, incluidos los no inscritos en los registros;

- la simplificación y el fortalecimiento del domicilio digital para los ciudadanos;

- la presentación de auto certificaciones, solicitudes y declaraciones directamente a través de AppIO;

- simplificaciones para la emisión de las cédulas de identidad digital - CIE;

[8] Para obtener más información sobre la fragilidad de esta infraestructura, consulte: /www.agendadigitale.eu/cittadinanza-digitale/identita-digitale/salviamo-spid-dal-prossimo-grande-crash-ecco-cosa-fare/.

- una plataforma única para la notificación digital de todos los actos de la Administración Pública y vía PEC de los actos judiciales;

- la simplificación de la firma electrónica avanzada;

- apoyo para el acceso de personas con discapacidad a herramientas informáticas;

- reglas homogéneas para todas las Administraciones Públicas para compras digitales, formación digital de empleados públicos y diseño de servicios digitales para la ciudadanía;

- la simplificación y el fortalecimiento de la interoperabilidad entre las bases de datos públicas y las medidas para garantizar la plena accesibilidad y el intercambio de datos entre las Administraciones Públicas;

- la simplificación y el fortalecimiento de la plataforma nacional de datos digitales, orientada a fomentar el uso de activos de información pública.

8. La situación en Argentina

En Argentina, en virtud de lo dispuesto en el art. 99, inc. 1, de la Const. nacional, con el decreto 434 de 2016[9], con la aprobación del Plan de Modernización del Estado, el gobierno pretendía llevar a cabo un proyecto estructurado en un marco de plena transparencia administrativa, orientada a mejorar las capacidades del Estado como condición necesaria para el desarrollo económico, productivo y social del país y para mejorar la calidad de vida de los ciudadanos, mediante el uso de recursos y el desarrollo de tecnologías aplicadas a la administración pública central y descentralizada.

Todo ello ha llevado a la implementación de proyectos que han permitido asistir a las administraciones provinciales y municipales y al gobierno de la Ciudad Autónoma de Buenos Aires, sobre la base del principio de mutua confianza. Además, para la ejecución del Plan de Modernización del Estado se han atribuido al Ministerio de Modernización diversas competencias de actuación.

En la presentación al Plan de Modernización del Estado se afirma, en concreto, que “es necesario incrementar la calidad de los servicios que presta el Estado integrando las Tecnologías de la Información y las Comunicaciones, simplificando los trámites, favoreciendo la reingeniería de procesos y ofreciendo a los ciudadanos la posibilidad de mejorar el acceso a la información personalizada a través de medios telemáticos coherentes y completos ...fomentando la participación activa de la ciudadanía en los procesos de toma de decisiones, así como en el diseño, implementación, seguimiento y evaluación de las políticas públicas”.

El Plan está estructurado en 5 ejes:

• Plan de Tecnología y Gobierno Digital: Se propone fortalecer e incorporar

[9] Ministerio de Modernización, decreto 434/2016, Plan de Modernización del Estado. aprobación. Bs. As., 3/1/16, visible en el enlace: http://servicios.infoleg.gob.ar/infolegInternet/anexos/255000-259999/259082/norma.htm.

infraestructura tecnológica y redes con el fin de facilitar la interacción entre el ciudadano y los diferentes organismos públicos. Asimismo, se busca avanzar hacia una administración sin papeles, donde los sistemas de diferentes organismos interactúen autónomamente;

• Gestión Integral de los Recursos Humanos: Es fundamental que la gestión de las personas se acompañe de un proceso de cambio organizacional que permita avanzar en su jerarquía, facilitando el aprendizaje y la incorporación de las nuevas tecnologías y procesos para lograr la profesionalización de los trabajadores de la administración pública;

• Gestión por Resultados y Compromisos Públicos: La institucionalización de procesos que permitan tanto la definición clara de prioridades para la toma de decisiones, como la evaluación de los procesos mediante los cuales se plasmarán e implementarán dichas decisiones y la correspondiente reasignación de recursos, son aspectos fundamentales en la búsqueda de un Estado socialmente eficiente y completo. Asimismo, es necesario promover la cultura de la eficiencia pública, a través de un modelo de gestión que haga énfasis en los resultados y en la calidad de los servicios, con flexibilidad en la utilización de los medios; pero estricto en la prosecución de sus fines, basados en sistemas de rendición de cuentas que aumenten la transparencia de la gestión;

• Gobierno Abierto e Innovación Pública: Junto a la eficiencia de los servicios prestados por el Estado debe promoverse la más amplia participación posible de la comunidad en la evaluación y el control de los programas del Estado y de las instituciones públicas, de manera que se renueve la confianza en el vínculo entre los intereses del Estado y los intereses de la ciudadanía;

• Estrategia País Digital: Se trata de un eje transversal a los cuatro anteriores, orientado a crear alianzas con las administraciones públicas provinciales, municipales y de la Ciudad Autónoma de Buenos Aires, con el objetivo de fortalecer los lazos existentes para avanzar dentro de un marco de intercambio y colaboración mutua, poniendo al servicio del desarrollo conjunto de las administraciones, las experiencias y prácticas exitosas existentes en todo el territorio nacional.

Para la realización de un Gobierno Tecnológico, el proyecto normativo argentino prevé la gestión documental y la creación de un archivo electrónico con el fin de facilitar la gestión de documentos, acceso y duración de la información, así como la implementación de una plataforma de información digital de procesamiento remoto de las relaciones con el ciudadano, basada en sistemas de gestión documental y de registro de nacimiento. Este último, en particular, estaba previsto para implementar iniciativas encaminadas a consolidar los sistemas de identificación electrónica de personas que permitan la firma remota - estructurada desde 2017 en una Plataforma de Firma Digital Remota - que conecta, a través de un Legajo Único Personal Informatizado, cualquier persona que mantenga una relación con la Publica Administración en el suministro de bienes y servicios y en la validación de documentos.

Por lo tanto, con el fin de establecer las condiciones tecnológicas, legales y administrativas necesarias y suficientes para que la Administración abandone el papel y se convierta en una oficina digital remota con servicios de acceso permanente y global, completo y sencillo a sus procedimientos de forma digital, con el decreto 733

de 2018[10], que contiene las disposiciones para Tramitación digital completa, remota, simple, automática e instantánea se concebí el documento informático como "el elemento mínimo que compone la gestión administrativa digital, y al trámite como medio principal de organización de la acción administrativa estatal y de acceso de los ciudadanos a los bienes y servicios que brindan los organismos públicos y, en muchos casos masivos también, a los servicios que brindan empresas y organizaciones de la sociedad a particulares".

Con el trabajo sobre el Ecosistema de Gestión de Documentos Electrónicos (GDE), plataforma horizontal que permite la creación, registro y archivo de documentos electrónicos para llevar a cabo todos los trámites de registro, control y resolución, acompañado de una sólida arquitectura legal que garantiza la plena vigencia jurídica de documentos electrónicos y su procesamiento en este sistema, implementado por la plataforma de Trámites a distancia (TAD), se fortalece la estrategia de modernización administrativa orientada a facilitar el acceso del ciudadano a los trámites de la Administración a través de:

- la autenticación del usuario de TAD con el Código Tributario de la Administración Federal de Ingresos Públicos (AFIP);

- la Clave de la Seguridad y de la Seguridad Social (ANSES);

- la Plataforma Central de Autenticación Electrónica (PAEC);

- el servicio Autenticar.

Además, para facilitar la comunicación y transmisión entre las Administraciones Públicas y para automatizar el mayor número de decisiones posibles y eliminar por completo el uso de papel, se ha dispuesto la creación del Módulo de Interoperabilidad del Sistema de Gestión de Documentos Electrónicos (INTEROPER.AR), que es administrado por un organismo central, dotado de registros distribuidos y autónomos, así como la creación e implementación del Registro Legajo Multipropósito (RLM).

9. Legislación europea

En el marco regulatorio europeo, con el Reglamento eIDAS y el Reglamento General de Protección de Datos - RGPD, los Estados miembros han tenido que armarse de buenas intenciones porque la transformación digital de la administración, la Privacy (por Diseño y por Defecto) y la Protección de Datos son los objetivos clave de la Agenda Digital Europea y, en consecuencia, de la estrategia nacional italiana, para su pleno cumplimiento.

Uno de los objetivos del Reglamento eIDAS, por ejemplo, es hacer que el sistema de identificación electrónica esté sujeto al mutuo reconocimiento, lo que significa que, si un Estado miembro permite el uso de una herramienta de identificación electrónica para el acceso a los servicios digitales online de un organismo del sector

[10] Ministerio de Modernización, decreto 733/2018, DECTO-2018-733-APN-PTE - Tramitación digital completa, remota, simple, automática e instantánea, Bs. As., 8/8/18, visible en el enlace: http://servicios.infoleg.gob.ar/infolegInternet/anexos/310000-314999/313243/norma.htm.

público, esto acceso también debe concederse a través de la herramienta de identificación expedida en otros Estados miembros.

Por último, con la Comunicación COM (2021) 118 final titulada “Brújula digital 2030: el camino europeo para la década digital” del 9 de marzo de 2021, la Comisión Europea presentó su visión sobre las perspectivas de la transformación digital de Europa para 2030.

La Comunicación se desarrolla en cuatro sectores que constituyen la brújula digital de Europa:

- habilidades digitales;

- infraestructuras digitales seguras y sostenibles;

- transformación digital de las empresas;

- digitalización de los servicios públicos.

Con respecto a la digitalización de los servicios públicos, el objetivo de la Unión Europea es garantizar que la vida democrática y los servicios públicos online sean totalmente accesibles para todos, incluidas las personas con discapacidad. Se trata de crear un ambiente digital que proporcione herramientas fáciles de usar, eficientes y personalizadas con altos estándares de seguridad y privacidad. Además, garantizar el voto electrónico alentaría una mayor participación de los ciudadanos en la vida democrática.

En resumen, los objetivos a alcanzar para 2030:

- Servicios públicos básicos: 100% online;

- Salud en línea: registros médicos 100% disponibles;

- Identidad digital: 80% ciudadanos que utilizan la identificación digital.

10. La protección legal de la identidad digital

Entre los perfiles orientados a la protección legal de la Identidad Digital encontramos:

- la protección de la privacidad, que tiene como objetivo proteger la identidad digital del usuario;

- la protección de datos personales;

- la seguridad de las infraestructuras digitales, para proteger la identidad del usuario en términos de autenticación / identificación e vietar la clusterizacion.

En el contexto italiano existen garantías y principios que se encuentran principalmente en el Reglamento General de Protección de Datos y el Código de Privacidad e el CAD. Por ejemplo, se prevé que los datos personales –comunicados a los Identity Provider– no puedan ser utilizados con fines comerciales, ni ser cedidos a terceros sin la autorización del usuario y, de conformidad con el art. 5 del Reglamento General de Protección de Datos, deben ser tratados de manera lícita, correcta y transparente. Por ejemplo, también, los datos personales (datos obtenidos automáticamente durante la

navegación por el sitio: dirección IP adquirida a través del registro de acceso al sitio; datos proporcionados por los usuarios a través del servicio HelpDesk: nombre, dirección de correo electrónico) son tratados por AGID en la ejecución de tareas institucionales de interés público y/o en todo caso vinculado al ejercicio de sus poderes públicos y deberes institucionales, con especial referencia al art. 64 del CAD. Los usuarios tienen derecho a obtener acceso a sus datos personales, la corrección o cancelación de los mismos, la limitación de su procesamiento, el derecho a oponerse al procesamiento y el derecho a la portabilidad de los datos de conformidad con los arts. 15 y siguientes del Reglamento General de Protección de Datos. El cumplimiento de las normas de procesamiento de datos es supervisado por AgID y el Garante para la protección de datos personales.

11. El garante para la protección de datos personales

En la larga historia de SPID, el garante ha sido llamado repetidamente porque solicitado desde AgID[11]. A través de un diálogo constante entre AgID y el garante, están tratando de dar un salto adelante, eliminando la identificación en presencia con el propósito de emitir el SPID. AgID, de hecho, ha considerado necesario introducir nuevos procedimientos que permitan de emitir de forma remota la identidad digital de una forma más sencilla, para que, a través de esta simplificación, pueda ampliar la audiencia de personas que solicitan y obtienen la identidad digital. A través de los informes semanales elaborados por los responsables de SPID, la autoridad puede, de hecho, realizar los controles necesarios e identificar nuevas medidas técnico-organizativas para fortalecer estos procedimientos, en relación con los perfiles críticos vinculados al tratamiento de datos personales por parte de los Identity Provider.

Por último, cabe señalar aquí que se están examinando alla Camera un proyecto de ley destinado a potenciar el uso del DNI electrónico (CIE) como medio para conocer la identidad del ciudadano y el acceso del propio ciudadano a los servicios online. De hecho, entre los primeros actos del nuevo Gobierno de Draghi, encaminados a la realización de la digitalización de la Administración Pública[12] y en el PNRR - Plan Nacional de Recuperación y Resiliencia, observamos la adopción del decreto-ley 1 de marzo de 2021, n° 22 que, además de reorganizar las competencias de algunos ministerios, también interviene sobre las funciones del Gobierno en el ámbito de la innovación tecnológica y la transición digital, coordinados para el Primer Ministro. Al

[11] Ver la Opinión a la AgID sobre el proyecto de resolución que modifica el reglamento que contiene los métodos de implementación para la creación del SPID y sobre el proyecto de determinación destinado a regular un nuevo método de verificación de identidad a distancia con la ayuda de una transferencia bancaria, 17/9/20, enlace: www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9461061.

[12] La digitalización, la innovación y la seguridad en las AP es uno de los tres componentes de la Misión n° 1 del Plan denominado Digitalización, innovación, competitividad y cultura. Ya con la ley de presupuesto 2020 y el decreto-ley 162 de 2019, que contiene la prórroga de plazos y otras disposiciones, se han previsto diversas medidas para promover y potenciar la informatización de la administración pública. La difusión de la administración digital continuó con el decreto-ley 76/2020 de medidas urgentes de simplificación e innovación digital.

respecto, el garante ha emitido una opinión favorable[13], de conformidad con el art. 36, párr. 4 y 57, párr. 1, lett. *c*, del Reglamento, sobre el proyecto de decreto del presidente del Consejo de Ministros.

12. La protección de datos personales en Argentina

Hemos visto cómo Argentina desde 35 años lleva a cabo un proceso innovador que le permite combinar las nuevas fronteras de protección de los derechos fundamentales con mecanismos concretos de protección de los ciudadanos digitales individuales.

De hecho, desde 1994, leamos en el art. 43 de la Constitución Argentina, que "Toda persona puede interponer acción expedita y rápida de amparo, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un tratado o una ley. En el caso, el juez podrá declarar la inconstitucionalidad de la norma en que se funde el acto u omisión lesiva".

Con la disposición 11 de fecha 22 de septiembre 2006, la Dirección Nacional de Protección de Datos Personales se aprobó el documento "Medidas de Seguridad para el Tratamiento y Conservación de los Datos Personales Contenidos en Archivos, Registros, Bancos y Bases de Datos Públicos no estatales y Privados".

Con la Ley de Protección de los Datos Personales[14] - ley federal argentina, actualizada en 2016, que se aplica a la protección de datos personales dentro del país y en los casos en que los datos sean transferidos para su procesamiento a través de fronteras nacionales, el hábeas data sigue siendo considerado como un derecho autónomo[15] que se identifica con la palabra Amparo[16]. Esta ley ha señalado a la Agencia de Acceso a la Información Pública como el organismo responsable del control de los datos personales, que tiene la tarea de identificar medidas de seguridad adicionales.

Además, se consagra en el art. 9 de esta ley que "el responsable o usuario del

---

[13] Opinión sobre el proyecto de decreto de la PCM, a propuesta de la Ministra de Innovación Tecnológica y Digitalización y de la Ministra de Administraciones Públicas, en acuerdo con el MEF, por el que se modifica el decreto de la PCM de 24 de octubre de 2014, a adoptarse de conformidad con art. 64, párrafo 2-sexies del decreto legislativo 7 de marzo de 2005, n. 82, 15/4/21, disponible en el enlace: www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9590366.

[14] Protección de los Datos Personales, Ley 25.326. Disposiciones Generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales. Sancionada: 4/10/00. Promulgada Parcialmente: 30/10/00. Visible en el enlace: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm.

[15] Guadamuz, Andrés, *Habeas Data: The Latin-American Response to Data Protection*, "The Journal of Information, Law and Technology (JILT)", 2000.

[16] Con la palabra Amparo queremos decir "Protección". Para un análisis más profundo, ver Guadamuz, *Habeas Data vs the European Data Protection Directive*, "The Journal of Information, Law and Technology (JILT)".

archivo de datos debe adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad y confidencialidad de los datos personales, a fin de evitar su adulteración, pérdida, consulta o tratamiento no autorizado y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado".

Con la resolución 47 de 2018[17] se establecieron nuevas medidas de seguridad, en línea con las Buenas Prácticas en Materia de Simplificación del decreto 891 de 1 de noviembre de 2017[18], destinadas a proteger la confidencialidad e integridad de los datos personales durante el tratamiento, desde la recolección hasta la eliminación. Se ha actualizado la lista de medidas de seguridad, datos sensibles y no sensibles, y controles recomendados para administrar, planificar, controlar y mejorar la seguridad durante el procesamiento de datos personales, identificando en la recolección de datos, en el control de acceso y de cambios, backup y recuperación, la gestión de vulnerabilidades, la eliminación de datos, los incidentes de seguridad y los entornos de desarrollo son los lugares donde puede ocurrir una lesión.

La protección de datos, por tanto, es fundamental porque este proceso de digitalización es fundamental para Argentina.

13. Conclusiones

De este análisis podemos concluir que, efectivamente, aún queda mucho por hacer. El largo y laborioso proceso de digitalización, nos lleva a tener, nuevamente en 2021, sitios de legislación abiertos, a pesar de la experiencia con la pandemia Covid-19. Está claro que los objetivos perseguidos son más que virtuosos, pero ¿conseguiremos realmente, primero en Europa y luego en Italia, cruzar la meta marcada por la Agenda Digital?

También está claro que aún queda mucho trabajo por hacer, como había dicho, tanto en Argentina como en Italia, para fomentar una cultura digital generalizada. No basta con dotar las herramientas a los ciudadanos para acceder a la Administración Pública digital.

Necesitamos trabajar para formar, instruir y educar los ciudadanos digitales, alcanzando un empoderamiento concreto tanto de los ciudadanos como de los empleados públicos, pero, sobre todo, debemos trabajar seriamente para superar la brecha digital. ¿Cómo podemos hablar del Estado Inteligente cuando todavía estamos estancados en el siglo XIV?

---

[17] Medidas de Seguridad, Tratamiento y Conservación de los Datos Personales en Medios Informatizados, sancionada 23/7/18, publicada en el Boletín Nacional del 25/7/18. Visible en el enlace: www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-47-2018-312662/texto.

[18] Buenas Prácticas en Materia de Simplificación del decreto 891 de fecha 1/11/17, visible en el enlace: http://servicios.infoleg.gob.ar/infolegInternet/anexos/285000-289999/285796/norma.htm.

Del gobierno electrónico al Estado inteligente

"Si comparamos el valor índice de desarrollo del gobierno digital de Naciones Unidas (EGDI) por región geográfica, observamos que el valor promedio de América Latina y el Caribe se encuentra por encima de regiones como Oceanía y África, pero detrás de Europa y cerca de Asia. Por otra parte, si analizamos el índice en sus últimas ediciones, podemos identificar que el componente de servicios en línea es aquel que tiene un mayor avance. Por otra parte, los valores en materia de capital humano e infraestructura parecen no mejorar de manera significativa".
Informe Cepal Séptima Conferencia Ministerial sobre la Sociedad de la Información de América Latina y el Caribe E-lac 2022

Por Antonio A. Martino

1. El tema

En lo que va del siglo el Estado ha tenido varias transformaciones y la más importante es debida a la introducción de nuevas tecnologías en la praxis administrativa. El Estado que se fue consolidando desde la lejana visión central y vertical de Luis XIV fue abriéndose a prácticas más democráticas, es decir horizontales y transparentes. Y más eficientes.

Desde Montesquieu el Estado cuenta con tres poderes: Ejecutivo, Legislativo y Judicial y cada uno de ellos tiene una Administración.

Las formas de esas administraciones dependen de la forma política del Estado. Puede ser federal o unitario. La manera en la que se estructura el poder político para ejercer su autoridad en el Estado, coordinando todas las instituciones que lo forman, hace que cada forma de gobierno precise de unos mecanismos de regulación que le son característicos.

Cuando se piensa en Administración se evoca la palabra "expediente" y ella conlleva la idea de retrasos, pasos engorrosos, maraña y de allí "burocracia", pero esta palabra no es descriptiva, como debería serlo, sino peyorativa, evocadora de sin fin de inútiles vueltas.

En las sociedades occidentales la participación política está en decadencia desde décadas. Los canales tradicionales de comunicación unidireccional vinculados a la televisión o a la radio no fueron capaces de superar la crisis de la democracia participativa, considerando que la política democrática es comunicación y que la transparencia, la rendición de cuentas, se sostienen en la comunicación bidireccional; de contacto directo político-ciudadano.

Los comportamientos electorales pueden cambiar en función de la comunicación y en los comicios municipales el conocimiento y comunicación tiene tanto peso como la ideología en la decisión del voto; sin embargo, en las elecciones generales los medios de comunicación tienen mayor influencia en el voto del ciudadano. En la sociedad industrial los políticos tenían que dominar el lenguaje de la TV pues interesaba más la intensidad de la reacción que la duración del mensaje; debían emplear frases contundentes.

En la Sociedad de la Información, con la Internet, esto cambia considerablemente pues la sociedad gana pluralismo y hay más voces que se hacen oír. Aparecen los Blogs como una forma de emitir opinión e información, que podemos considerar como una forma de periodismo alternativo (aportan visiones diferentes de las noticias, ignoradas por los grandes medios).

En la Sociedad de la Información los Blogs políticos se multiplican enormemente y desborda el debate tradicional unidireccional. Los activistas encuentran en la Web, en el Blog o en el Wiki un instrumento para insistir y crear opinión. Particularmente las herramientas de comunicación electrónica son positivas pues rompen el monopolio informativo y permiten cuestionar la información libremente. Permiten aportar ideas y restituir el pensamiento político.

"Sí, ya no es necesario recurrir, ni tampoco esconderse, detrás de los tomos sobre leyes y fallos, casi intimidatorios y capaces de albergar al conocimiento jurídico y controlar el ingreso a ese mundo críptico. Ni siquiera es necesario ir a una biblioteca jurídica, sino solo usar el celular o cualquier otro dispositivo electrónico.

Por tanto, el desafío actual no es obviamente conocer el material jurídico, y particularmente la ley, sino aprender a leerlo e interpretarlo; y el primer paso en este sentido es conocer las fuentes y cómo resolver los eventuales conflictos entre éstas. Pensemos que las fuentes se multiplicaron en las últimas décadas y presentan desafíos difíciles de resolver (por ejemplo, los fallos de la Corte IDH; el derecho débil; y los precedentes, entre tantos otros).

El segundo paso consiste en saber leer ese material (interpretarlo), y razonar sobre hechos y derecho (argumentar y justificar). Este razonamiento exige, asimismo, incorporar conocimientos no jurídicos, pues no es posible interpretar el derecho solo desde el estrecho corredor del mundo jurídico. Así, por ejemplo, el abogado no puede desconocer las herramientas económicas básicas o las miradas filosóficas y sociológicas sobre el derecho.

Entonces, no solo es necesario cambiar el método de aprendizaje, sino básicamente el modo de pensar, razonar y argumentar en derecho"[19].

Cuando se habla de Administración se piensa en "expediente" y "trámite" y las dos palabras están cargadas de pesimismo y de añosa parsimonia. Cuando en verdad son palabra que deberían atraer definiciones descriptivas. Burocracia es también un término lleno de tardanzas.

Luis XIV logró crear un Estado moderno ágil, abierto y manejado desde un solo lugar con tanto éxito que los demás países trataron de imitarlo. Después de la Revolución el Estado francés siguió siendo modelo. En el siglo XX se fue delineando un Estado más universal. Va consolidándose el local y comienza la descentralización. En el siglo XXI se pide mayor horizontalidad y automación.

Si pensamos en nuestro país del 2004 a hoy el tamaño del Estado se duplicó

[19] Balbín, Carlos, *Crisis del derecho administrativo*, Bs. As., Astrea, 2020.

en relación al PBI"[20].

2. El Estado como sistema

El Estado es un sistema con sus elementos (composición) una organización (estructura), un entorno, un intercambio de inputs y outputs, con el mismo y una mecánica que consiste en los cambios que va produciendo.

La composición de un sistema es la colección de sus partes (protones, neutrones y electrones en el sistema atómico; personas, empresas, clubes y círculo de amigos en el sistema social) y se las llama componentes.

El entorno es la colección de cosas que modifican a los componentes del sistema o que resultan modificados por ellos, pero que no pertenecen a la composición.

La estructura es la colección de relaciones o vínculos que establecen los componentes. Los vínculos que se dan entre los componentes de un sistema constituyen la endoestructura, mientras que los establecidos entre los componentes y elementos del entorno conforman la exoestructura del sistema.

El mecanismo es la colección de procesos que se dan dentro de un sistema y que lo hacen cambiar en algún aspecto (el mecanismo de radiación electromagnética de un átomo es un proceso en el que un electrón cambia de estado de energía, el comercio es un mecanismo económico de los sistemas sociales humanos).

Una colección puede tener una composición constante o no, solo si la tiene es un conjunto. Dado que los sistemas concretos están siempre en flujo, su composición puede cambiar con el tiempo, como un lenguaje natural. Con excepción del universo todo tiene un entorno con el cual interactúa. Vínculo simboliza la relación que transforma los miembros relacionados. La exoestructura de un sistema incluye dos particularmente importantes: el inputs y outputs. El primero es la colección de acciones de los elementos del entorno sobre el sistema, el segundo es la acción del sistema sobre el entorno. El subconjunto de la exoestructura que contiene solo los miembros del sistema que mantienen relaciones directas con el entorno puede denominarse contorno del sistema.

El modelo de sistema expresado debería ser complementado con un modelo de emergencia y extinción, o sea de generación y descomposición de sistemas.

Las totalidades poseen propiedades de las cuales sus partes carecen. De esas propiedades globales decimos que son emergentes. Las propiedades emergentes no son distributivas sino globales.

Puede denominarse extinción la pérdida de propiedades de niveles superiores. Habida cuenta que las propiedades son poseídas por las cosas, la extinción de una característica de la descomposición de un sistema de cualquier clase.

La descomposición la produce el debilitamiento de los vínculos internos que

---

[20] Cabot, Diego, *El gasto público, un problema crónico en el medio de todos los males argentinos*, "La Nación", 14/5/22.

mantienen unido el sistema. Puede ocurrir de varias maneras la más común es la intrusión de un agente externo.

Si bien el conocimiento de un sistema concreto radica en la descripción de los cuatro aspectos mencionados, la explicación científica del comportamiento del mismo la brinda la descripción de su(s) mecanismo(s), es decir de los procesos de los cuales resultan la emergencia, la estabilidad, el cambio y la desintegración de un sistema.

Según Bertalanffy[21], el sistema es un conjunto de unidades recíprocamente relacionadas; se deducen dos conceptos: el propósito (u objetivo) y el de globalización (o totalidad). Esos dos conceptos reflejan dos características básicas en un sistema.

Para François[22], el mundo real es una complejidad organizada que demanda una visión sistémica. ¿Cuál es la organización interna del sistema? ¿Cuáles son sus estructuras y subestructuras? ¿Cuáles son sus funciones principales y subordinadas? ¿A qué función corresponde cada estructura?

Un sistema es un objeto complejo estructurado, cuyas partes están relacionadas entre sí por medio de vínculos (estructura) pertenecientes a un nivel determinado. Además, los sistemas se caracterizan por poseer propiedades globales (emergentes o sistémicas) que sus partes componentes no poseen.

Una sociedad humana es un sistema compuesto por personas y diversos subsistemas sociales unidos entre sí por vínculos de varios tipos: biológicos, políticos, económicos, etcétera. Estudiarlo requiere la construcción de un modelo que consiste en la descripción de la composición (C), el entorno (E), la estructura (S) y el mecanismo (M) del sistema.

El mecanismo es la colección de procesos que se dan dentro de un sistema y que lo hacen cambiar en algún aspecto. Más precisamente, si bien el conocimiento de un sistema concreto radica en la descripción de los cuatro aspectos mencionados, la explicación científica de su comportamiento la brinda la descripción de sus mecanismos, es decir, de los procesos de los cuales resultan la emergencia, la estabilidad, el cambio y la desintegración de un sistema.

El Estado puede ser visto como un sistema o subsistema de un sistema mayor que es el país y del cual forma parte. Es un conjunto de individuos que está unido por lazos parentales, un sistema jurídico, normas sociales de convivencia, unidades productivas, costumbres, una o más lenguas comunes y en general valores compartidos respecto de muchas cosas, comenzando por la noción de sucesión en el poder.

El Estado debe tener, como dijimos antes, la descripción de la composición (C), el entorno (E), la estructura (S) y el mecanismo (M) del sistema.

Además, la adaptación, que se configura por la relación del sistema con el medio exterior, dentro del cual se encuentra y con el que, a su vez, interactúa. Y también la persecución de objetivos, que consiste en la movilización de las energías del

---

[21] Von Bertalanffy fue un biólogo y filósofo austríaco, reconocido fundamentalmente por su teoría general de sistemas, General system theory: foundations, development, applications.

[22] François (ed.), *International Encyclopedia of Systems and Cybernetics*.

sistema hacia las metas que se han propuesto.

La de integración, que se define por las acciones que permiten mantener la coherencia del sistema.

Con respecto a la composición, debe tener: *a*) un sistema de normas para aplicar (derecho vigente); *b*) actores (funcionarios, jueces, empleados administrativos); c) ciudadanos y habitantes del territorio nacional; *c*) una cultura estatal, y *d*) una sociedad civil.

El entorno se refiere a: *a*) el derecho como praxis social; *b*) la sociedad como organización; *c*) el sistema político; *d*) los países con los cuales se tienen relaciones jurídicas, y *e*) el contexto internacional.

La estructura depende de cada país, pero en general hay Ministerios Nacionales que dependen si el Estado es Federal o Unitario, Organizaciones políticas provinciales y municipales, tres poderes divididos en Ejecutivo, Legislativo y Judicial. Hay una endo estructura que representa la manera de organizarse de los sistemas nacionales y una exoestructura más ligada a la organización política general del país, provincia o municipio[23].

El mecanismo del sistema es el más difícil de describir, pero da las pautas más claras sobre las leyes sistémicas que caracterizan un determinado sistema de Estado nacional (o regional o local) y como va modificándose con el paso del tiempo y las nuevas costumbres y tecnologías.

Un sistema es adaptativo si, cuando hay un cambio en su entorno o estado interno que reduce su eficiencia en la prosecución de uno o más de los propósitos que definen sus funciones, reacciona en respuesta cambiando su propio estado o el de su entorno de manera tal que aumente su eficacia respecto de este propósito o propósitos. Desarrollan sus acciones y existencia en un entorno que interactúa con ellas, que, en la mayoría de los casos, se constituye en un sistema cultural que hasta posee su propio lenguaje. En su proceso evolutivo se dan los fenómenos de autoorganización y, según una corriente de opinión, autopoiesis; aparecen y desaparecen atractores, se producen catástrofes, etcétera.

3. El EDI

En los años 80 y 90 del siglo pasado las empresas importantes (y los Estados inteligentes) comenzaron a ocuparse de un tema disruptivo: la transmisión electrónica de datos EDI[24].

Así como los romanos lograron tener un imperio por medio de sus carreteras (le vie: la via Appia, la Clodia, la Aurelia… alrededor de cien mil kilómetros de

[23] Martino, Antonio A., *Fundamental requirement from the organizational and normative point of view for a digital government and development*, presentado en E-Government Proceedings of the Fifth Congress of the European Association of Legislation (EAL), Atenas, 2015.

[24] El EDI es un formato estándar para intercambiar información entre dos organizaciones de forma electrónica en lugar de utilizar documentos en papel.

carreteras surcaban el imperio en todas direcciones y permitían que un ejército se trasladara en forma velocísima, o que llegaran las mercaderías o mejor aún los mensajes y las órdenes. Las vías romanas convertían al Imperio en instantáneo. Dos mil años después el mejoramiento de los medios de comunicación y de transporte permitieron tejer una red mundial de comercio que abarcaba todo el planeta pero que estaba basada en los documentos comerciales de papel[25]. Cada vez que se vendía un objeto debía acompañarse toda la documentación que exigían las burocracias nacionales y las aduanas y debían expedirse por los correos de la época. Muchas veces llegaba antes la mercadería que la documentación y al capitán del barco se le ponía un problema serio: si esperaba la documentación debía esperar para desembarcar la mercadería, pero cada día parado el barco en un puerto devengaba costos muchas veces salados, entonces los capitanes inventaron un documento que no estaba en ningún registro nacional o internacional: la declaración del capitán. Declaraban, firmaban y descargaban.

La situación era insostenible y ya existían programas de computación que permitían redactar documentos sumamente precisos y despacharlos por redes que las propias empresas y las propias organizaciones estatales habían ido creando: había transmisión de paquetes de datos nacionales Franpac, Itapac, etc., y redes comerciales como Odette para los automóviles. Surgió entonces la idea de crear un documento único y eso es EDI.

El EDI, más que un nuevo sistema de comunicación, se está transformando en una nueva manera de hacer negocios. Operatividad continua con supresión de las barreras del huso horario, superación de todas las limitaciones de las barreras lingüísticas, porque todo es confiado a los estándares de los mensajes.

Importante también el hecho de la integración de otros servicios telemáticos a valor agregado que se integran en los servicios EDI. La reducción de los tiempos es extraordinariamente grande y sobre todo la drástica (esto ha sido el origen del EDI) reducción de los contenidos de los depósitos en cada empresa, puesto que la información y la documentación, instantáneas, hacen que las reservas puedan limitarse al mínimo.

Obviamente, para afrontar una comercialización global como es la que se está perfilando en este momento en el mundo, es necesario tener la información y la preparación para ser competitivo prácticamente en todo el planeta. Esto hace que el EDI sea una vía obligada, sobre todo en presencia del mercado único del 1992.

La instantaneidad lograda por los romanos con los caminos se la quería lograr en el comercio con el EDI. Todo funcionó bien mientras se trató de burocracias nacionales y redes de negocios como Odette o Swift para los bancos. Nació entonces la necesidad de extender el EDI a las pequeñas y medianas empresas pues las grandes ya lo hacían.

Se crearon entonces los EDI nacionales. En Europa ya creada la Comunidad

[25] Un día imprimimos toda la documentación que debía acompañar a un automóvil para viajar de Chicago a Génova. La imprimimos en una hoja continua de computación de entones, 1986, y tenía 15 metros de largo.

económica europea, en Bruselas se reunía el EDiforum Europa compuesto por los representantes de los diferentes países europeos, doce si mal no recuerdo y se comenzó a trazar la forma electrónica de los documentos[26]. En esta parte nos fue muy bien y logramos reglamentar 273 documentos, empezando por la factura.

Nos fue muy mal en lograr que las pequeñas y medianas empresas usaran el EDI. Fracasamos. Pero íbamos por el buen camino: en 1982 nace Internet y con su difusión, el comercio electrónico. Ahí si el mundo se volvió instantáneo y quien adoptó el comercio electrónico vendió en el mundo, quien no, vende en su pueblo. Hasta el día de hoy[27].

4. El impacto tecnológico

Novedades: - vehículos autónomos, que tienden a reducir drásticamente los costos de transporte y logística, pero requieren una seguridad cibernética sólida, una revisión de responsabilidad civil y un reciclaje rápido de los actores involucrados. - el procesamiento de imágenes alteradas, con una amenaza alarmante de propagación viral de falsedades. - la introducción de modelos robóticos que apuntan a detectar posibles fraudes, sobreprecios y corrupciones, aunque con la inagotable posibilidad de falsos positivos. - asistencia digital para la toma de decisiones públicas, basada en evidencia, manejando volúmenes gigantes de datos (a menudo de baja calidad), con el doble objetivo de proteger datos confidenciales y elegir estándares sostenibles, en lugar de adoptar la ecuación reduccionista de costo-beneficio monetario.

En este paso, vale la pena mencionar la inaceptabilidad manifiesta de, mediante el uso de software secreto, para estimar el riesgo de recurrencia del acusado, con el consiguiente aumento de la pena - El diagnóstico computarizado de enfermedades genéticas, basado en la identificación facial, con la precaución recomendada, en este y otros casos similares, para no debilitar la relación terapéutica cara a cara y la responsabilidad correspondiente. - aprendizaje profundo y la red neuronal artificial, inspirado en la biología, con contribuciones conspicuas, por ejemplo, a la biometría, pero que corre el riesgo de contaminaciones algorítmicas perturbadoras de anidación mal reguladas. - el uso de análisis predictivo, en relación con los procedimientos legales, con la nota de la observancia de los principios éticos no disponibles (como la transparencia, la no discriminación y el “usuario bajo control”).

También es necesario salvaguardar el derecho a una explicación clara de las razones subyacentes a las decisiones algorítmicas. De hecho, el derecho a la

---

[26] Por representar a un ente estatal de investigaciones, fui nombrado presidente del Ediforum Italai e iba a Bruselas cada 15 días a negociar con los otros partners europeos la forma de los documentos. ¿Porque digo negociar? Porque antes de partir preguntaba a las empresas italianas qué sistema querían obtener y obviamente me pedían que fueran aquello más cercanos a los modelos italianos, pero tenía que negociar con otros 11 representantes.

[27] “El comercio, que era ya ocupación de gente de baja condición, lo fue también de pícaros y se tuvo por bribones a todos los comerciantes. Cuando se prohíbe una cosa natural o necesaria o lícita, solo se consigue degradar y pervertir a los que la hacen, y alguien ha de hacerla”; Montesquieu, *Del espíritu de las leyes*, libro XXI cap. XX.

explicación, consagrado en el art. 20 de la Ley Brasileña de Protección de Datos Personales, garantiza el acceso a la privacidad de los pasos lógicos que conforman la decisión artificial inteligente. En vista de esto, en el campo administrativo, es necesario expandir el espectro efectivo de publicidad y motivación. Es decir, el incumplimiento de la obligación de revelar los pasos lógicos que guían la decisión artificial provoca la inversión de la carga de la prueba del vínculo causal, a favor de la persona afectada. En las relaciones administrativas, el Poder Público es responsable de probar que los algoritmos elegidos no tienen efectos legalmente perjudiciales, hostiles a los fundamentos congruentes de hecho y de derecho. Y es apropiado hacerlo explícitamente, según lo determine la Ley de Procedimiento Administrativo.

5. Gobierno abierto

La definición de Gobierno Abierto que aparece en "Open Government: Gobierno Abierto": Aquel que entabla una constante conversación con los ciudadanos con el fin de oír lo que ellos dicen y solicitan, que toma decisiones basadas en sus necesidades y preferencias, que facilita la colaboración de los ciudadanos y funcionarios en el desarrollo de los servicios que presta y que comunica todo lo que decide y hace de forma abierta y transparente.

En esta definición se pone de manifiesto el reto que supone la existencia de un Gobierno Abierto para las autoridades políticas y las administraciones públicas.

El Gobierno Abierto sacude los cimientos propios del sistema democrático actual, sustentado en el mero ejercicio de elecciones periódicas, profundizando cambios estructurales fundamentados en la existencia de herramientas de Transparencia para la acción gubernamental y en el que deben existir lugares de colaboración y participación ciudadana

Quedan de esta manera señalados 3 elementos sobre los que descansa el Gobierno Abierto: la Transparencia, la Participación y la Colaboración, y que constituyen la visión seminal del concepto propuesta por Barack Obama.

• "Transparencia (Saber). Un gobierno transparente proporciona información sobre lo que está haciendo, sobre sus planes de acción, sus fuentes de datos, y de sobre lo que puede ser considerado responsable[28].

• Participación (Tomar parte). Un gobierno participativo promueve el derecho de la ciudadanía a participar activamente en la formulación de políticas públicas y facilitar el camino para que las administraciones públicas se beneficien del conocimiento, ideas y experiencia de los ciudadanos. Promueve la creación de nuevos espacios de encuentro que favorezcan el protagonismo e implicación de los ciudadanos en los asuntos públicos.

• Colaboración (Contribuir). Un gobierno colaborativo compromete e implica a los ciudadanos y demás agentes sociales en el esfuerzo por trabajar conjuntamente

[28] Fuente: Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), Ministerio de Industria, Energía y Turismo, www.ontsi.red.es/ontsi/sites/default/files/objetivos_estrategias_y_actuaciones_gobierno_abierto.pdf.

para resolver los problemas nacionales. Ello supone la cooperación y el trabajo coordinado no solo con la ciudadanía, sino con las empresas, asociaciones y demás agentes, y permite el esfuerzo conjunto dentro de las propias administraciones, entre ellas y sus funcionarios transversalmente".

No obstante, para la Alianza para el Gobierno Abierto (OGP), son cuatro los elementos sobre los que descansa el concepto de Gobierno Abierto:

• "Rendición de Cuentas: Existen reglas, normas y mecanismos para que los actores gubernamentales justifiquen sus acciones, respondan a críticas o requerimientos y acepten responsabilidad por omisiones en lo referente a leyes y compromisos.

• Tecnología e Innovación: Los gobiernos reconocen la importancia de: proveer a los ciudadanos acceso abierto a la tecnología; las nuevas tecnologías como impulsoras de la innovación; y la importancia de aumentar la capacidad de los ciudadanos para utilizar tecnologías. Según su propia web "La OGP busca que, de manera sostenida, los gobiernos sean más transparentes, rindan cuentas y mejoren la capacidad de respuesta hacia sus ciudadanos, con el objetivo final de mejorar la calidad del gobierno, así como la calidad de los servicios que reciben los ciudadanos. Esto requiere un cambio de normas y cultura para garantizar un diálogo y colaboración genuinos entre gobierno y sociedad civil"[29].

• Participación Ciudadana: Los gobiernos procuran que sus ciudadanos se involucren en debates públicos, provean insumos y contribuyan a un régimen más innovador, efectivo y receptivo.

• Transparencia: La información sobre las actividades y decisiones gubernamentales está abierta y actualizada, además es exhaustiva y se encuentra disponible al público en cumplimiento con estándares de datos abiertos (p.ej., datos legibles, sin procesar)[30].

Una visión más práctica es la que "en el que se analizan los diferentes contenidos de los planes de acción de los países miembros de la Alianza para el Gobierno Abierto (OGP), estableciendo una agrupación por categorías de las acciones que se incluyen en los mismos. En concreto, se podrían englobar en:

• Categoría 1. Ampliar la información pública disponible para la ciudadanía. En la que se incluirían acciones para: • Promover la transparencia activa (Proactive Disclosure); • Desarrollar repositorios institucionales abiertos; • Desarrollar portales de datos abiertos.

Todo esto se va multiplicando día tras días pues aparecen nuevas formas de usar las tecnologías en la Administracion, hasta la recaudación de impuestos o tasas se ve afectada, como por ejemplo en Italia el sistema de pagos.

PagoPa es un proyecto que promete simplificar la vida de los ciudadanos y las empresas eliminando el papeleo, las colas en los mostradores y los formularios que

[29] Open Government Partnership www.opengovpartnership.org/es.

[30] Ver Oszlak, Oscar - Kaufman, Ester, *Teoría y práctica del gobierno abierto: Lecciones de la experiencia internacional*, 2014.

hay que rellenar con la misma información una y otra vez. El cajón digital de PagoPa se ha puesto en marcha en 2022 y será la herramienta en la que se podrán almacenar documentos y certificados, incluidos los de valor legal, realizar pagos digitales a las administraciones públicas y compartir datos. Hasta ahora se han sumado la Agencia Tributaria, el Inps y el Registro Nacional de Población Residente (Anpr).

6. Partidos políticos y movimientos sociales

El partido como parte total[31] se ha visto favorecida en su asentamiento institucional por la conversión de la tarea de coordinación en la labor fundamental de los sistemas políticos de finales del siglo XX y principios del siglo XXI; este fenómeno supone una de las transformaciones políticas y constitucionales más importantes de los últimos cien años.

No obstante, una vez culminado este proceso de consolidación institucional y constitucional de los partidos, y quizá también por ello, ese "príncipe moderno" se ha visto afectado de manera cada vez más intensa por la creciente desafección social hacia una vida política que se percibe, por una parte importante de la sociedad, como un espacio poco transparente, donde la preocupación esencial es el puro ejercicio del poder y casi cualquier cosa vale para conservarlo, pues prima el partidismo y el cálculo sectario y, por si fuera poco, se está viendo afectado de manera cada vez más frecuente por casos de corrupción.

Paralelamente se advierte un resurgimiento de los movimientos ciudadanos como entidades de protesta frente a esos excesos pero, y aquí radica un matiz muy importante, también de propuesta de otras políticas y modos distintos del ejercicio del poder. Cuál es el destino histórico de los partidos en este momento histórico, si miramos desde dos libros de gran éxito: Ulrich Beck y Pierre Rosanvallon, por el riesgo y la desconfianza[32] con el objetivo de, en palabras también de Rosanvallon, no de "despolitizar la democracia" sino, por el contrario de "repolitizarla", de darle más centralidad a lo político y eso implica que progresen, al mismo tiempo, la calidad de la regulación democrática y la atención a la construcción democrática.

En la teoría política la transformación de los partidos se ha calificado de diferentes maneras, pero hay coincidencia, en lo esencial, de que se ha pasado primero de un sistema de partidos como organización de afiliados, o partido de masas, a un partido catch-all (en la terminología de Otto Kirchheimer)[33], que ha desembocado, finalmente, en un entramado de partidos basados en los cargos públicos o en las

---

[31] La expresión "parte total" constituye un oxímoron, pero es utilizada a partir de la idea del constitucionalista italiano Mortati, Costantino en *Istituzioni di diritto pubblico*, Cedam, Padova, 1991, t. II, p. 796.

[32] Ulrich, Beck, *Risikogesellschaft. Auf dem Weg in eine andere Moderne*, Frankfurt, Suhrkamp, 1986; edición española: La sociedad del riesgo. Hacia una nueva modernidad, Paidós, 2006; Pierre Rosanvallon, *La contra-démocratie. La politique à l`âge de la défiance*, Paris, Éditions du Seuil, 2006; hay versión española: *La contrademocracia. La política en la era de la desconfianza*, Manantial, 2007.

[33] *The Transformation of Western European Party Systems*, en La Palombara, Joseph - Weiner, Myron (eds.), "Political Parties and Political Development", Princeton University Press, 1966.

instituciones públicas[34].

Diversos factores, como la ampliación progresiva del sufragio en los Estados democráticos en la primera mitad del siglo XX, la consolidación de procesos electorales competitivos, y las innovaciones tecnológicas y organizativas provocaron que los tradicionales partidos defensores de intereses particulares, profesionales, de clase o de creencias, se fueran transformando en partidos de integración de masas con la consiguiente burocratización y especialización técnica, y la consolidación del liderazgo, en la línea bien descrita hace un siglo por Robert Michels en las páginas de su libro *Los partidos políticos*[35], que no en vano subtituló *Un estudio sociológico de las tendencias oligárquicas de la democracia moderna*. Una vez que los partidos de masas vislumbraron la oportunidad real de participar e influir en las políticas gubernamentales y de formar parte de los gobiernos, tanto sus líderes como sus estructuras organizativas empezaron a centrarse de manera predominante en los procesos de captación de la voluntad de los electores. Es bien conocida y está documentada la influencia de las tesis expuestas por Michels en el análisis que sobre los partidos hicieron autores clásicos como Max Weber, James Bryce o Duverger[36].

Los sucesivos cambios sociales y políticos (la movilidad social, laboral y geográfica, la consolidación de los medios de comunicación de masas, la mejora educativa…) influyeron también en las formaciones políticas, que, cada vez en mayor medida, pudieron ir incorporándose al ejercicio de funciones de gobierno, dejando de ser así, con notorias excepciones, meros partidos de oposición.

Merced a estas transformaciones, en la actualidad la importancia política e institucional de los partidos no resulta tanto de su mera existencia o del tamaño de la organización, sino de la función concreta que tienen en un determinado sistema para la formación del gobierno; en suma, de los patrones institucionales en los que se muevan, de su capacidad de maniobra y de su influencia real en los procesos de toma de decisiones.

Así llegamos, en los Estados democráticos avanzados, a una situación del

---

[34] Ver Gunther, Richard - Montero, José R. - Linz, Juan J., tanto en su versión en lengua inglesa *Political Parties: Old Concepts and New Challenges*, Oxford, Oxford University Press, 2002, como en la más reciente edición castellana: *Partidos Políticos. Viejos conceptos y nuevos retos*.

[35] En palabras de Michels, "la especialización técnica que resulta inevitablemente de toda organización extensa hace necesario lo que se ha dado en llamar la conducción experta. En consecuencia, el poder de determinación llega a ser considerado como uno de los atributos específicos del liderazgo, y las masas lo pierden gradualmente mientras se concentra en las manos de los líderes. De este modo, los líderes que al principio no eran más que órganos ejecutivos de la voluntad colectiva, se emancipan pronto de la masa y se hacen independientes de su control… Es innegable que la tendencia oligárquica y burocrática de la organización partidaria es una necesidad técnica y práctica, producto inevitable del propio principio de organización… Por razones técnicas y administrativas, no menos que por razones tácticas, una organización fuerte necesita un liderazgo igualmente fuerte… A medida que la profesión de políticos se hace más complicada… se necesita que quien deba comprender la política posea una experiencia más amplia y un conocimiento más extenso. Esto hace aún más grande la diferencia entre los líderes y el resto del partido… esta competencia especial, este conocimiento de expertos, que el líder adquiere en cuestiones inaccesibles, o casi inaccesibles, para la masa, le da seguridad en su posición" (Bs. As., Amorrortu, 1979, vol. 1, p. 77, 80 y 122).

[36] Duverger, Maurice, *Les partis politiques*, Paris, Armand Colin, 1951.

sistema de partidos que, ya entrado el siglo XXI, puede calificarse de primacía de "partidos en las instituciones públicas". Esta preeminencia del liderazgo institucional no se proyecta en exclusiva sobre la propia organización interna de la formación política –"los líderes se han convertido en el partido, el partido se ha convertido en los líderes"–, marginando la importancia política, electoral y económica de los afiliados en las decisiones y orientación del partido, sino que ha transformado también el funcionamiento de las propias instituciones estatales y sus relaciones recíprocas, y este cambio lo han provocado, en buena medida, los propios partidos desde dentro de las instituciones[37].

Dentro de los partidos ha contribuido a que esos mismos principios de funcionamiento se trasladaran a las instituciones en las que aquéllos se han asentado y ha propiciado, junto a otros factores, el ascenso del Gobierno dentro de las relaciones entre poderes, justamente el órgano que a los promotores en su momento de la teoría de la separación de poderes les parecía una instancia bastante inofensiva.

Ahora bien, en este triunfo institucional del sistema de partidos y en la conversión del partido gobernante en "Príncipe moderno", en la afortunada expresión de Gramsci, va implícito su cuestionamiento cuando empiece a evidenciarse su limitada capacidad para dar respuesta a los problemas de la nueva modernidad.

Sin embargo, no parece que los partidos sean del todo conscientes de esta realidad ni de la emergencia de una nueva cultura política descentralizada que ha generado, también en palabras de Beck, unas redes de cooperación o de rechazo, de negociación, de reinterpretación y de posible resistencia de manera transversal a toda la estructura vertical y horizontal de capacidades y competencias.

Dos tendencias triunfan: los que dicen no ocuparse de política (y por eso no se llaman partidos, sino movimientos) y los que manifiestan rabia social como los indignados, cinque stelle, en Italia). También es cierto que las nuevas tecnologías permiten una mayor participación, casi democracias directas como en el Presupuesto participativo o en los partidos piratas[38].

Sobre las nuevas tecnologías vale la pena reflexionar sobre la participación del presidente de Ucrania, Zelenski, a todos los foros internacionales (Davos comprendido) mientras está bloqueado territorialmente por fuerzas armadas rusas.

En las sociedades occidentales la participación política está en decadencia desde décadas. Los canales tradicionales de comunicación unidireccional vinculados a la televisión o a la radio no fueron capaces de superar la crisis de la democracia participativa. considera que la política democrática es comunicación y que la transparencia, la rendición de cuentas, se sostienen en la comunicación bidireccional; de contacto directo político-ciudadano. Los comportamientos electorales pueden cambiar en función de la comunicación y en los comicios municipales el conocimiento y

---

[37] López Pina, Antonio (ed.), *Democracia representativa y parlamentarismo. Alemania, España, Gran Bretaña e Italia*, Madrid, Secretaría General del Senado, 1994, p. 213 y 214.

[38] Ver Martino, Antonio A., *Crisis de la democracia participativa: alternativas participativas o democracia directa con medios electrónicos*, "Revista Eumonia" n° 14, abril - septiembre 2018, p. 9 a 32, DOI: https://doi.org/10.20318/eunomia.2018.4153.

comunicación tiene tanto peso como la ideología en la decisión del voto; sin embargo, en las elecciones generales los medios de comunicación tienen mayor influencia en el voto del ciudadano.

En la sociedad industrial los políticos tenían que dominar el lenguaje de la TV pues interesaba más la intensidad de la reacción que la duración del mensaje; debían emplear frases contundentes. En la Sociedad de la Información, con la Internet, esto cambia considerablemente pues la sociedad gana pluralismo y hay más voces que se hacen oír. Aparecen los Blogs como una forma de emitir opinión e información, que podemos considerar como una forma de periodismo alternativo (aportan visiones diferentes de las noticias, ignoradas por los grandes medios).

En la Sociedad de la Información los Blogs políticos se multiplican enormemente y desborda el debate tradicional unidireccional. Los activistas encuentran en la Web, en el Blog o en el Wiki un instrumento para insistir y crear opinión. Particularmente las herramientas de comunicación electrónica son positivas pues rompen el monopolio informativo y permiten cuestionar la información libremente. Permiten aportar ideas y restituir el pensamiento político.

Las actuales democracias se enfrentan a una situación paradójica. Tenemos las generaciones más preparadas que ha habido, todos con la suficiente formación y conocimiento para realizar un ejercicio crítico sobre el gobierno de nuestra sociedad, y tenemos en nuestras manos una herramienta formidable para poder intervenir directa y automáticamente en tiempo real expresando nuestras opiniones, nuestros argumentos y nuestra voluntad sobre las decisiones que debemos tomar como sociedad. Tenemos en nuestras manos hacer realidad ese sueño que nos acompaña desde que nuestros antepasados los revolucionarios del siglo XVIII proclamaron la como principio articulador de los nuevos regímenes representativos en los que desembocó la modernidad. Es el sueño que empuja a movimientos ciudadanos como Democracia Real Ya, como los partidos piratas, como Change.org,y tantos otros. Y paradojas de la vida, ese sueño parece que se nos escape entre los dedos.

Y eso es debido a que las nuevas tecnologías exigen una preparación y una exactitud que muchas veces no se cumple y al hecho que olvidamos que toda esta novedad debe ser aceptada y actuada por seres humanos que están más bien acostumbrados (aun) a una lógica gutenberiana. También olvidamos la dificultad de las personas mayores a adaptarse al uso de nuevas tecnologías[39].

Es que como decía Stefano Rodotà[40] estas tecnologías procuran instrumentos capaces de estimular los comportamientos racionales, que van más allá de los solos procesos de decisión y cubren el entero período entre una elección y otra. Por ejemplo:

---

[39] Un caso relevante era el de Norberto Bobbio, quien siempre sigo mis investigaciones con científica curiosidad, pero que me decía que lo dispensara de usar las tecnologías que lo distraían de lo que quería hacer. Y era Bobbio.

[40] Rodotà, Stefano, *Il diritto di avere diritti*, Laterza, 2013. Tuve el privilegio que Rodotà fuese consejero del Instituto di Documentazione Giuridica del Consejo Nacional de Investigaciones italiano que dirigí entre 1982 y 1993.

a) Internet puede permitir el acceso directo de los ciudadanos a las informaciones en manos públicas y a determinadas categorías de informaciones en manos privadas.

b) Los ciudadanos pueden en todo momento, de forma instantánea y con facilidad dirigirse a las instancias políticas, decisorias o no, sugiriendo, proponiendo o, simplemente, facilitando información.

c) Internet permite fórmulas como el o la encuesta de opinión deliberativa, que conjugan las técnicas del muestreo con el trabajo deliberativo en grupo, esto es, sobre respuestas no fundadas sobre la técnica alternativa sí/no o del cuestionario.

d) Al combinar elementos de conocimiento y de intervención puede contribuir a establecer nuevos Conocimiento. Intervención no formalizada Valoración crítica mecanismos de control de las instancias decisorias (por ejemplo, la publicación de las baremaciones de concursos abiertos en la red).

e) Se podría regular el carácter vinculante para la toma en consideración por parte de sujetos públicos de tales propuestas ciudadanas cuando se canalizaran a través de estos medios (por ejemplo, iniciativa legislativa popular vía firma digital).

f) Las posibilidades aquí son infinitas, aunque no exentas de riesgo (se pueden utilizar, por ejemplo, técnicas como las del muestreo olas de rotación entre los ciudadanos consultados).

g) Los ciudadanos pueden asumir la gestión, por ejemplo, de determinadas categorías de servicios con efectos de descentralización y desestatalización.

h) Las alternativas deben diseñarse de tal forma que innovaran las tradicionales formas del referéndum. Estos instrumentos, para ser eficaces, requieren, según su opinión, la preventiva definición de un adecuado cuadro institucional.

7. La fragilidad de la democracia

La democracia siempre ha sido un sistema excepcional de gobierno. Si revisamos la historia humana, hay poca democracia y mucha autocracia. Las democracias se consolidaron después de la segunda guerra mundial y por un periodo que comenzó a declinar a fines del siglo pasado.

¿Porque la democracia es frágil? Porque debe luchar con armas claras y honestas a quienes por perpetuarse en el poder consideran que cualquier medio es útil desde la mentira, el robo y el engaño. Dicho así parece muy fácil y en verdad es muy difícil gestionar el poder democráticamente cuando los autócratas mienten, engañan y hasta usan la inversión del significado de las palabras para enrostrar a los demócratas sus propios vicios. La última alternativa es nivelar a todos hacia abajo con el slogan “todos roban” o “todos mienten”.

Recientemente se han puesto de moda las tres “P”: populismo (divide y vencerás, promete y gana), la polarización (el uso y abuso de la discordia) y la posverdad (¿a quién creer?) y frente a esto tres alternativas: la primera es tratar de aplicar su ambicioso programa de cambio a través de acuerdos oportunistas con determinados dirigentes, partidos de la oposición y grupos sociales hostiles a él, lo que

inevitablemente le obligará a hacer concesiones. La segunda alternativa es proponer al país un acuerdo nacional amplio e incluyente: una alianza amplia que permita tomar decisiones importantes y que sea sincera y creíble podría darle el apoyo que necesita, pero aun así tendría que hacer concesiones que podrían ser difíciles de digerir para el presidente y quienes lo apoyaron en la campaña que lo llevó al máximo cargo. La tercera opción restante es comportarse como los presidentes de las tres P han hecho en otras partes del mundo: debilitar subrepticiamente las instituciones, las normas, los controles y los equilibrios que definen la democracia. En Latinoamérica, se tiende a esta tercera desastrosa estrategia.

En su obra 1984, Orwell[41] pone como lemas del partido dominante, el Insog (que sería el acrónimo de socialismo ingles): La Guerra es Paz, La Libertad es Esclavitud y la Ignorancia es fuerza. Y es curioso que en una carta de octubre de 1949 que Aldous Huxley envió a George Orwell para agradecerle que le mandara su libro 1984; dice que, su propia visión del autoritarismo del futuro, la contenida en Un mundo feliz, era mucho más acertada. Ambos autores son dubitativos del futuro de la democracia y conciben dos formas de la tiranía que nos espera: la que vendrá a través de la represión, "instigando y empujando a la obediencia" (el modelo Orwell); o la que se impondrá mediante la sugestión y la seducción, haciendo que seamos inducidos a "amar nuestro sometimiento" (el modelo Huxley).

Actualmente en ciencia política se limita a describir prolijamente cada avance de los partidos populistas, identificamos a sus votantes, hacemos llamadas de alerta ante la aparición de los "hombres fuertes" y sus sibilinas y torticeras estrategias de comunicación con las masas, u observamos cómo aumenta en las encuestas el número de personas que no ven imprescindible el vivir bajo un sistema democrático.

8. Conclusiones

Con la llegada de Internet, 1992, se produce una transformación total de nuestras vidas tal que desaparece una era caracterizada por la difusión de la escritura, Gutenberg (1452). La transformación es tan radical que, si un abogado hubiese dormido un decenio, al despertar no reconocería lo que están haciendo sus pares como "ejercicio profesional". A diferencia de lo que hubiese sucedido entre 1500 y el 2000.

El derecho se ocupa de regular la vida en sociedad, cambiando el contexto material de la misma, necesariamente debe cambiar el derecho. Aparecen nuevas circunstancias (los viejos límites temporales o espaciales se borran) hay nuevos sujetos (el gestor de red) nuevos derechos (habeas data, ciudadanía digital) y es menester dictar nuevas normas, nuevos reglamentos.

Los cambios por nuevas invenciones fueron generalmente plurigeneracionales: pasar del mundo agrícola al industrial, la introducción del automóvil, la radio o la televisión, pero los cambios de la nueva era son mucho más veloces. La velocidad ha entrado en nuestras vidas tan raudamente porque ahora las actualizaciones no son generacionales, sino decenal, a veces quinquenales y en muchos casos anuales.

---

[41] Orwell, George, *Nineteen Eighty-Four*, 1949.

Es decir, el derecho puede tomar algún respiro para actualizarse, pero como se dice en música del allegro “non troppo”. De hecho, algunas constituciones van tomando acto de los nuevos derechos, pero son sobre todo los Tribunales constitucionales, que son empujados por actores desesperados por la aparición de automóviles autónomos o armas autónomas, reconocimientos faciales, monedas cripto, fake news, quienes deben anticipar el contenido constitucional, siguiendo una tradición que permite el juego de los tres poderes. Y de allí se pasa a las leyes y reglamentos tanto supranacionales, como los de la U.E. cuanto nacionales y aun locales, como los municipales.

Stefano Rodotà, diputado en el Parlamento italiano y europeo desde 1979, titular de en la Autoridad italiana para la protección de datos personales, fue además, Consejero del Istituto per la Documentacione Giuridica, del Consejo Nacional de Investigaciones italiano que dirigí entre 1983 y 1992, escribió un texto “La vida y las reglas” analiza los límites del Derecho en relación a contenidos que atañen a la dignidad humana, la libertad y los derechos fundamentales en general. En una original división estructural visita el cuerpo, la soledad, el don, la casualidad, el gen, el clon, el dolor, el cuidado, el final y el poder. Son planteamientos muy emotivos cuya poética es íntegramente conforme con un alto grado de profundización jurídica en la materia.

De las tantas cosas que aprendimos de él, valga esta reflexión sobre el cuidado que el derecho tiene que tener de los cambios en la vida humana, la tutela de las libertades y los sutiles límites entre el derecho y el no derecho.

Vale la pena desterrar dos vicios de nuestro tiempo: el primero confundir digital con inmaterial. Lo digital es material pues los programas y los datos se desarrollan en máquinas, se graban en paquetes que viajan o se depositan en discos duros que se graban con láser, pero todo es absolutamente material, tiene un soporte material y una existencia ontológica en el mundo.

El segundo el miedo del computador como nuevo Golem, que aparece citado una sola vez en el Antiguo Testamento, esto es, en Salmo 139, verso 16, allí se dice “inconcluso o esbozado me vieron tus ojos. Tus ojos vieron mi embrión, y en tu libro se escribieron todos los días que me fueron dados, cuando no existía ni uno solo de ellos”.

Ese embrión, según la interpretación, es el Golem, pero para otros Adán. En hebreo, idioma original del Antiguo Testamento, se coloca el origen de la figura del Golem, de donde la Qabbalh (tradición) busca sus significados.

Sí, vale la pena ocuparse de los peligros serios que han aparecido ya y que están siendo tratados; podemos llamarlos riesgos y son debidos al hecho que se trata de una metodología nueva a la cual la sociedad no ha tenido tiempo de habituarse. Los sistemas inteligentes no van a volver atrás, por lo tanto, la solución no es demonizarlos como si no existieran o fuéramos a desterrarlos sino ver cuáles son los riesgos que crean, diferenciarlos pues algunos son menores.

Por cierto, que las nuevas tecnologías agregan mucho potencial a las Administraciones, pero albergan no pocas insidias. El caso del derecho fiscal de los países bajos es un ejemplo: La vida de Chermaine Leysner cambió en 2012, cuando recibió una carta de la autoridad fiscal holandesa exigiéndole que devolviera su subsidio de

cuidado infantil desde 2008. Leysner, entonces un estudiante que estudiaba trabajo social, tenía tres hijos menores de 6 años. La factura fiscal superaba los 100.000 euros. “Pensé: ‘No te preocupes, esto es un gran error’. Pero no fue un error. Fue el comienzo de algo grande”, dijo.

El calvario duró nueve años de la vida de Leysner. El estrés causado por la factura de impuestos y el diagnóstico de cáncer de su madre llevaron a Leysner a la depresión y el agotamiento. Terminó separándose del padre de sus hijos. “Estaba trabajando como loca para poder hacer algo por mis hijos, como darles algunas cosas bonitas para comer o comprar dulces. Pero tuve momentos en que mi hijo pequeño tuvo que ir a la escuela con un agujero en el zapato”, dijo Leysner.

Leysner es una de las decenas de miles de víctimas de lo que los holandeses han denominado el “toeslagenaffaire” o el escándalo de los beneficios de cuidado infantil. En 2019 se reveló que las autoridades fiscales holandesas habían utilizado un algoritmo de autoaprendizaje para crear perfiles de riesgo en un esfuerzo por detectar el fraude de beneficios de cuidado infantil.

Las autoridades penalizaron a las familias por una mera sospecha de fraude basada en los indicadores de riesgo del sistema. Decenas de miles de familias, a menudo con ingresos más bajos o pertenecientes a minorías étnicas, fueron empujadas a la pobreza debido a las deudas exorbitantes con la agencia tributaria. Algunas víctimas se suicidaron. Más de mil niños fueron acogidos en hogares de guarda.

Las autoridades fiscales holandesas se enfrentan ahora a una nueva multa de 3,7 millones de euros del regulador de privacidad del país. En un comunicado publicado el 12 de abril, la agencia describió varias violaciones del reglamento de protección de datos de la UE, el Reglamento General de Protección de Datos, incluido no tener una base legal para procesar los datos de las personas y aferrarse a la información durante demasiado tiempo.

Aleid Wolfsen, el jefe de la autoridad de privacidad holandesa, calificó las violaciones como sin precedentes: “Durante más de 6 años, las personas a menudo fueron etiquetadas erróneamente como estafadores, con consecuencias nefastas ... algunos no recibieron un acuerdo de pago o usted no era elegible para la reestructuración de la deuda. Las autoridades fiscales han puesto vidas patas arriba”.

A medida que los gobiernos de todo el mundo recurren a algoritmos e IA para automatizar sus sistemas, el escándalo holandés muestra cuán completamente devastadores pueden ser los sistemas automatizados sin las salvaguardas adecuadas. La Unión Europea, que se posiciona como el principal regulador tecnológico del mundo, está trabajando en un proyecto de ley que tiene como objetivo frenar los daños algorítmicos.

Pero los críticos dicen que el proyecto de ley falla y no protegería a los ciudadanos de incidentes como lo que sucedió en los Países Bajos, pues esa práctica no tiene controles ni equilibrios.

El nuevo gobierno de Rutte se ha comprometido a crear un nuevo regulador de algoritmos bajo la autoridad de protección de datos del país. La ministra digital holandesa, Alexandra van Huffelen, quien anteriormente fue ministra de Finanzas a cargo de la autoridad fiscal, dijo a un medio local que el papel de la autoridad de datos será

"supervisar la creación de algoritmos e IA, pero también cómo se desarrolla cuando está allí, cómo se trata, asegurarse de que esté centrado en el ser humano y que se aplique a todas las regulaciones que están en uso".

Las Administraciones tiene mucho que revisar sobre los cambios que las nuevas tecnologías han introducido en la sociedad y por ende en el derecho y también los cambios que la propia producción procesal constitucional ha sufrido y está sufriendo por las nuevas tecnologías, sin temores, pero sin pausa, pues el trabajo a realizar llevará mucho tiempo y energía. Y no es procastinable.

Bibliografía

Cabrera Cabrera, Pedro J. (dir.), *Nuevas Tecnologías y exclusión social. Un estudio sobre las posibilidades de las TIC en la lucha por la inclusión social en España*, Madrid, Fundación Telefónica, 2015, www.ohchr.org/sites/default/files/Documents/Issues/CulturalRights/ConsultationEnjoyBenefits/UNESCONUEVAS_TECNOLOGIASyExclusionsocial.pdf.

Consoli, Gianluca, *Arte e cognizione. Rapporti tra estetica e intelligenza artificiale*, Milano, Bulzoni, 2006.

Consulta Pública ¿Qué dicen los expertos sobre eLAC 2010-2015? CEPAL, setiembre de 2010, www.eclac.cl/socinfo/noticias/noticias/3/40843/Consulta_publica.pdf.

Darwin, Charles, *The Descent of Man 1859*, Londres, Princeton University Press, 1981, vol. 1, Primera Parte, cap. 3.

Duhigg, Charles, *Cómo las empresas aprenden sus secretos*, NYT, 2012.

Elon Musk, *Neuralink*, proyecto visible en el link https://neuralink.com.

Floridi, Luciano (ed.), *The Blackwell Guide to the Philosophy of Computing and Information*, Blackwell, 2004.

Fukuyama, Francis, *State-Building: Governance and World Order in the 21st Century*, Corneil University Press, 2004.

Hinojo, Alex, *Hacia una nueva ética informativa*, "CCCBLab", 16/1/20, http://lab.cccb.org/es/hacia-una-nueva-etica-informativa.

Kant, Immanuel, *Fundamentación de la metafísica de las costumbres*, Austral.

Leibniz, Gottfried W. Freiherr von, *Ensayo de Teodicea. Acerca de la bondad de Dios, la libertad del hombre y el origen del mal*, Madrid, Abada Editores, 2019.

Lo, Edwin, *Entrevista: sobre Tecnodiversidad: una conversación con Yuk Hui*, 27/7/20, Seminario de Tecnologías Filosóficas, http://philosophyandtechnology.network/3939/entrevista-sobre-technodiversity-una-conversacion-con-yuk-hui.

Markus, Gabriel, *Yo no soy mi cerebro. Filosofía de la mente para el siglo XXI*, Barcelona, Pasado y Presente, 2016.

Martino, Antonio A. (ed.), *La giustifi cazione morale della dernocrazía*, Quaderndi ell'Istitutod i Scienza Politica Universitá di Genova, Genova.

Martino, Antonio A., *Lógica informática, derecho y Estado*, Lima, Grijley, 2021.

Martino, Antonio A., *Tecnologías innovadoras para la Justicia*, Bs. As., Astrea, 2021.

Refik, Anadol, *"Melting Memories" esculturas digitales en movimiento*, exposición en San Francisco, 1019.

Ross, David, *Fundamentos de ética*, Bs. As., Eudeba, 2003. El original inglés es de 1930.

Yuk, Hui, *On the Existence of Digital Objects*, Minessota, Electronic Mediations, vol. 48, 2020.

Umberto Eco, Lectio magistralis, celebrada como parte de la reunión de los 83 Ministros de Cultura reunidos en Expo Milano por el Ministro de Cultura Dario Franceschini, el 31 de julio y el 10 de agosto de 2015.

Unesco, *Recomendación sobre la Ética de la Inteligencia Artificial*, https://es.unesco.org/artificial-intelligence/ethics.

Wittgenstein, Ludwig, *Tractatus logico-philosophicus*.

Sistemi intelligenti tra etica e privacy. Quali sono le sfide che dobbiamo affrontare?

Por Nicola Fabiano

1. Premessa

In questo ciclo di conferenze si discute dell'impatto su persone organizzazioni sulla pubblica amministrazione della generale evoluzione tecnologica con particolare attenzione allo sviluppo del digitale che si impone sempre di più nella vita personale e lavorativa.

Indubbiamente, sono cambiate le abitudini di ciascuno di noi e conseguentemente le attività lavorative; tutti oggi utilizzano un device, che sia uno smartphone, un computer, un tablet. Abbiamo modificato le nostre abitudini e certamente anche la nostra vita che dipende in qualche modo dalla rete internet da questi device che ci consentono di comunicare e di lavorare.

Questo aspetto, peraltro, è stato accentuato ancora di più dalla pandemia, perché ovviamente essendo rimasti obbligati a non avere più quelle relazioni che eravamo abituati ad avere prima, si è stati costretti ad un maggiore utilizzo, ancora più intenso, di questi di questi dispositivi. Quindi il digitale è entrato ancora più profondamente nella nostra vita nelle nostre abitudini.

Ciò che vorrei evidenziare ancora in questa premessa è che l'approccio al tema del dei sistemi intelligenti e comunque all'intelligenza artificiale richiede, a mio modesto parere, un approccio multidisciplinare che coinvolge tecnici e giuristi. Molto spesso è capitato di ascoltare giuristi professati esperti di tecnologie e di intelligenza artificiale così come i tecnici spesso dichiarano di conoscere il diritto e i profili giuridici di alcuni istituti.

Probabilmente, però, non tutti i giuristi hanno un solido background tecnico e allo stesso modo molti tecnici non hanno conoscenze legali. Pertanto, è importante avere un approccio multidisciplinare a questo tema, in modo che si possa realizzare una convergenza delle singole specifiche competenze e quindi le professionalità vengano coinvolte intervenendo non in competizione tra loro, di una categoria professionale nei confronti dell'altra, o addirittura di primazia, ma in termini di piena collaborazione.

Il mio intervento sarà sempre in relazione alla protezione dei dati personali, anzi in relazione alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Ancora oggi alcuni considerano i robot o la robotica come espressione delle norme tecniche e come domini tipicamente di competenza esclusiva dei tecnici. L'esperienza comune, però, ci insegna che questi temi devono essere affrontati congiuntamente da chi possiede professionalità sia di estrazione tecnica sia legale, anche perché emergono aspetti che sono tipicamente legali.

Nella nostra prospettiva dovremmo affrontare questi argomenti, considerando prima ciascuno di essi come un singolo strato perché l'ibridazione cioè la parte ibrida delle competenze non significa assolutamente rinunciare alla sfera propria del giurista. Il giurista ha una visione dei fenomeni umani e può considerare la robotica e l'intelligenza artificiale come una derivazione estremamente innovativa. Questo primo passo ci consente di avere una visione generale di un singolo caso come un contesto multistrato dove ci sono più strati che vanno analizzati. Soltanto in questo modo possiamo avere chiaro in anticipo, quali domini dovremmo trattare e poi il passo successivo sarà quello di stabilire la procedura o i processi si adeguati a lavorare sull'intero contesto con il giusto approccio e ottenere il massimo risultato. Non è molto facile coniugare la parte tecnica, quindi la robotica intelligenza artificiale gli standard tecnici l'etica e la parte giuridica le leggi sulla protezione dei dati sulla privacy. Riteniamo, comunque che questo tutto questo possa coesistere se cambiamo mentalità e adottiamo un approccio diverso è il più innovativo.

Sono necessarie delle precisazioni.

Il tema della "protezione delle persone fisiche con riguardo al trattamento dei dati personali" è diverso da quello della privacy, anche perché in Europa la Carta dei diritti fondamentali dell'Unione Europea disciplina agli articoli 7 e 8 differentemente la riservatezza e la protezione delle persone fisiche con riguardo al trattamento dei dati personali.

L'attenzione va posta alla protezione delle persone fisiche con riguardo al trattamento di dati personali, la cui disciplina europea è contenuta nel Regolamento Europeo 2016/679. Quindi, non si tratta di protezione del dato.

Un altro assioma è quello secondo il quale la privacy è diversa dalla sicurezza.

Molti pensano che avere un sistema informatico sicuro corrisponda ad una conformità alla disciplina sulla protezione dei dati personali.

Quindi, protezione dei dati personali è un concetto diverso da quello della security e ciò può essere espresso con la seguente formula matematica: "Protezione dei dati personali ≠ Security".

2. La protezione delle persone fisiche con riguardo al trattamento di dati personali

In Europa la principale fonte normativa in materia di protezione delle persone fisiche con riguardo al trattamento di dati personali è il Regolamento Europeo 2016/79 Regolamento Generale sulla protezione dei dati (in inglese, General Data Protection Regulation - GDPR), ma non è l'unica.

In effetti, probabilmente molti ignorano che il GDPR deriva dalla Convenzione 108/1981 del Consiglio d'Europa sulla protezione delle persone fisiche con riguardo al trattamento automatizzato dei dati. La Convenzione 108 rappresenta il punto di riferimento dal quale si è avviato il processo di formazione del menzionato GDPR.

Peraltro, il mese di maggio del 2018 è stato molto importante per la protezione dei dati personali. In realtà, il 17 e 18 maggio del 2018 veniva approvata la versione

modernizzata della convenzione 108 che è tuttora in corso di ratifica da parte degli Stati aderenti al Consiglio d'Europa. Com'è noto, inoltre, dal 25 maggio si applica il GDPR.

Il GDPR disciplina la protezione delle persone fisiche con riguardo al trattamento dei dati.

Peraltro, la persona fisica assume un ruolo primario e decisivo, essendo essa un'entità che ha una propria dignità umana. Da qui scaturiscono altri aspetti che riguardano i diritti fondamentali.

Il GDPR ha sostituito e abrogato la Direttiva europea 95/46/CE che già disciplinava la protezione delle persone fisiche con riguardo al trattamento di dati personali. Si è realizzato, pertanto, un percorso evolutivo in materia di protezione dei dati personali avviato sin dagli anni novanta.

Quindi, il primo aspetto è certamente acquisire la necessaria consapevolezza che i tempi sono decisamente cambiati e conseguentemente è necessario essere pronti ad affrontare le sfide che abbiamo di fronte. Da tempo siamo entrati nella nuova era della protezione delle persone fisiche con riguardo al trattamento di dati personali e della privacy che non dipende strettamente dall'evoluzione tecnologica, ma è una vera e propria nuova fase che richiede un approccio basato su una mentalità aperta.

I tempi sono cambiati.

È necessario, pertanto, un nuovo approccio con il quale dovremmo cercare di cambiare la nostra mentalità verso una dimensione che viene definita open-minded, modificando le nostre abitudini o per lo più il nostro approccio al dominio della protezione delle persone fisiche con riguardo al trattamento di dati personali.

Tutto questo, ovviamente non significa non considerare o trascurare la disciplina normativa sulla protezione delle persone fisiche con riguardo al trattamento di dati personali o trascurare il GDPR e le altre fonti normative vigenti, ma semplicemente essere consapevoli che siamo in una nuova era. Il GDPR è sicuramente una rivoluzione e la maggior parte dei professionisti della privacy spesso fa fatica a entrare nella dimensione concettuale della protezione delle persone fisiche con riguardo al trattamento di dati personali.

È necessario continuare a lavorare in questo settore con un approccio non più obsoleto, focalizzato fondamentalmente solo sulle norme, trascurando altri aspetti rilevanti.

3. Intelligenza artificiale e sistemi di intelligenza artificiale

Tuttavia, bisogna riflettere, anche solo brevemente, su quella che è la storia dell'intelligenza artificiale. In effetti, riguardo ai metodi nella ricerca emerge la cosiddetta Symbolic Artificial Intelligence che è stata poi definita con l'acronimo GOFAI (Good Old Fashion Artificial Intelligence) da John Haugeland nel 1985.

Il percorso storico di questa simbolica artificial intelligence è caratterizzato da un'evoluzione dei cosiddetti paradigmi dominanti che sono stati individuati e poi evoluti e succeduti nel corso degli anni, dagli anni 50 a metà degli anni '90. Meritano di essere

menzionati: Cognitive simulation, Logic-based, Anti-logic or “scruffy”.

Negli anni ‘70 emerge il paradigma noto come Knowledge-based dal quale sono scaturiti i sistemi esperti, i cosiddetti Expert Systems.

Negli anni 90, è stato abbandonato l’approccio simbolico e ancora oggi la materia è oggetto di studio e di approfondimento.

È necessario fare riferimento agli agenti intelligenti, i cosiddetti “intelligent agents”, che, sostanzialmente, sono composti da hardware e software. I sensori, a seconda delle istruzioni che vengono fornite dal software, compiono determinate attività.

Riguardo ai sistemi intelligenti, i cosiddetti Intelligent Systems, ci si dovrebbe domandare cosa si intende per sistemi intelligenti.

Una parte della dottrina[42] ha definito i sistemi intelligenti facendo riferimento al concetto emerso nella tecnologia dell’informazione come un tipo di sistema che è derivato dalle applicazioni di successo dell’intelligenza artificiale attraverso il Machine Learning.

La definizione proposta dalla dottrina citata è la seguente: “Un sistema intelligente opera in un ambiente con altri agenti possiede abilità cognitive come la percezione, il controllo delle azioni, il ragionamento deliberativo o l’uso del linguaggio, segue principi comportamentali basati sulla razionalità e le norme sociali, e ha la capacità di adattarsi attraverso l’apprendimento”[43].

Quindi, è evidente che quando si parla di sistemi intelligenti si fa riferimento all’intelligenza artificiale.

Considerato quanto sin qui descritto, poiché il ciclo di conferenze del SAI è dedicato al rapporto del digitale con la pubblica amministrazione, si propongono di seguito alcuni esempi di sistemi intelligenti che potrebbero essere utilizzati dalla pubblica amministrazione:

- Intelligent Systems for Transport (ITS)
- Autonomous vehicles
- Business Intelligence (BI) - salute e sicurezza sul lavoro (SSL)
- Controlli generali di illuminazione
- Sistemi di comunicazione
- Controlli di sicurezza
- Controlli di accesso (spettacoli, ecc.)

---

[42] Molina, Martin, *What is an intelligent system?*, Universidad Politécnica de Madrid, february 2022; il testo citato in lingua originale è il seguente: “An intelligent system: *1*) operates in an environment with other agents, *2*) possesses cognitive abilities such as perception, action control, deliberative reasoning or language use, *3*) follows behavioral principles based on rationality and social norms, and *4*) has the capacity to adapt through learning”.

[43] NdR: la traduzione del testo è nostra.

• Controlli HVAC (Heating, Ventilation and Air Conditioning) - risparmio energetico.

Controlli esterni (contatori d'acqua avanzati, Meters) ... ed altro.

È, ovviamente, una elencazione meramente esemplificativa utile per presentare una panoramica di quelle che attualmente sono le tipologie di sistemi intelligenti. Non risulta che soluzioni di questo tipo siano state attuate nelle pubbliche amministrazioni, non soltanto in Italia, ma anche nel resto del mondo.

Dal tema dei sistemi intelligenti o sistemi di intelligenza artificiale scaturisce la questione più rilevante che è relativa alla definizione di intelligenza artificiale.

Autorevole dottrina[44] afferma che[45]: Storicamente, i ricercatori si sono dedicati a diverse versioni di IA. Alcuni hanno definito l'intelligenza in termini di fedeltà alla performance umana, mentre altri preferiscono una definizione astratta e formale di intelligenza chiamata razionalità - in parole povere, fare la "cosa giusta". Anche l'argomento stesso varia: alcuni considerano l'intelligenza come una proprietà dei processi interni di pensiero e ragionamento, mentre altri si concentrano sul comportamento intelligente, una caratterizzazione esterna. Da queste due dimensioni –umano vs. razionale e pensiero vs. comportamento– ci sono quattro possibili combinazioni, e ci sono stati aderenti e programmi di ricerca per tutti e quattro.

Dalla già menzionata citazione emerge con assoluta chiarezza che non è possibile fornire una definizione di intelligenza artificiale, in quanto è necessario considerare contesti e approcci che possono essere evidentemente variabili e non definibili a priori.

Il richiamo al testo contenuto nel volume di Norvig e Russel, pubblicazione molto nota e considerata un punto di riferimento importante in questo ambito, fa emergere come la definizione di intelligenza artificiale potrebbe cambiare a seconda del tipo di approccio.

Sempre nell'ambito dell'intelligenza artificiale, altro noto autore[46] afferma: Il sacro graal della ricerca sull'IA è la costruzione di una "IA generale" (meglio nota come "intelligenza artificiale generale" o IAG) della massima ampiezza: in grado di realizzare praticamente qualsiasi fine, compreso quello dell'apprendimento.

Inoltre, Tegmark aggiunge[47]: Anche il movimento dell'IA benefica la ritiene probabile in questo secolo, ma non pensa che un esito buono sia garantito, bensì che debba essere assicurato da un forte impegno sotto forma di ricerca sulla sicurezza dell'IA.

In sostanza, Tegmark definisce l'intelligenza come la "capacità di realizzare fini complessi" e l'intelligenza artificiale come "Intelligenza non biologica".

---

[44] Russell, Stuart - Norvig, Peter, *Artificial Intelligence. A Modern Approach*, 4 ed., 2020.

[45] NdR: la traduzione del testo è nostra.

[46] Tegmark, Max, *Vita 3.0*, Raffaello Cortina Editore, p. 66 y 67.

[47] Tegmark, *Vita 3.0*.

Nella ricerca su intelligenza artificiale Tegmark arriva a dire che "il disaccordo aumenta se si allarga l'orizzonte temporale e si parla di intelligenza artificiale generale (IAG), in particolare dell'IAG che arrivi al livello umano e lo superi", definendo la IAG come la "capacità di svolgere qualsiasi compito cognitivo almeno tanto bene quanto un essere umano".

Lo stesso Tegmark, peraltro, è promotore di "An Open Letter - Research priorities for robust and beneficial artificial intelligence", firmata anche da Stuart Russel.

In questa "Open Letter" vengono evidenziate le priorità di ricerca per un'intelligenza artificiale robusta e benefica e nel testo si legge[48]: La ricerca sull'intelligenza artificiale (AI) ha esplorato una varietà di problemi e approcci fin dal suo inizio, ma negli ultimi 20 anni circa si è concentrata sui problemi che circondano la costruzione di agenti intelligenti - sistemi che percepiscono e agiscono in qualche ambiente. In questo contesto, "intelligenza" è legata alle nozioni statistiche ed economiche di razionalità - colloquialmente, la capacità di prendere buone decisioni, piani o inferenze. L'adozione di rappresentazioni probabilistiche e decisionali e di metodi di apprendimento statistico ha portato a un ampio grado di integrazione e fertilizzazione incrociata tra l'IA, l'apprendimento automatico, la statistica, la teoria del controllo, le neuroscienze e altri campi. L'istituzione di quadri teorici condivisi, combinata con la disponibilità di dati e potenza di elaborazione, ha prodotto notevoli successi in vari compiti di componenti come il riconoscimento vocale, la classificazione delle immagini, i veicoli autonomi, la traduzione automatica, la locomozione su gambe e i sistemi di risposta alle domande… Questa ricerca è per necessità interdisciplinare, perché coinvolge sia la società che l'IA. Spazia dall'economia, la legge e la filosofia alla sicurezza informatica, i metodi formali e, naturalmente, vari rami dell'IA stessa.

Quindi, gli autori della "Open Letter" sono arrivati a prendere coscienza e consapevolezza che c'è un'interazione tra intelligenza artificiale e altri settori come, in particolare, le neuroscienze che è un ambito estremamente importante è attuale soprattutto per l'impatto sui dati personali. È interessante questa parte della "Open Letter" perché viene ribadito il principio della necessità di una interdisciplinarietà, così come abbiamo precisato all'inizio.

4. Sistemi intelligenti, Pubblica Amministrazione e protezione dei dati personali

Passando al rapporto tra sistemi intelligenti e pubblica amministrazione, ci si dovrebbe domandare quali soluzioni sono state adottate dalle pubbliche amministrazioni. In Italia, a seguito di un'indagine, il risultato è il seguente:

• SOGEI - Società Generale d'informatica del Ministero dell'Economia e delle Finanze.

Si occupa di diversi aspetti, come si può verificare sul sito web istituzionale. In effetti, SOGEI si occupa di giustizia digitale, di patrimonio pubblico, di intelligenza e

[48] NdR: la traduzione è nostra.

controlli, ecc.

• AgID –Agenzia per l'Italia digitale– Nel 2018 sul sito web istituzionale di AgID veniva pubblicato il "Libro bianco sull'intelligenza artificiale a servizio del cittadino". Tuttavia, si tratta di un documento risalente al 2018 che non risulta avere avuto applicazione concreta. In questo documento dell'AgID emerge la mappa dell'ecosistema dell'intelligenza artificiale in Italia nella quale emerge una cospicua presenza di poli universitari. Si tratta du una "fotografia" di quanto esistente nel 2018.

• Ministero dello Sviluppo Economico - Nel 2019 veniva lanciata la strategia nazionale per l'intelligenza artificiale. La citata strategia si articolava in quattro punti fondamentali. Il primo punto sottolineava l'esigenza di realizzare un'azione sinergica tra i Paesi membri dell'Unione Europea e da ciò emerge la consapevolezza circa la realizzabilità solo di azioni comuni e coordinate. Nel 2020 la strategia è andata in consultazione pubblica. Al momento non risulta ancora alcuna attuazione concreta

Intanto in Europa che cosa è accaduto?

In materia di intelligenza artificiale, in Europa si registra un percorso avviato nel 2015 che ha visto coinvolte alcune istituzioni europee, tra le quali anche il Comitato per la protezione dei dati personali (EDPB). Tale percorso è proseguito, intensificandosi, dal 2019 in poi.

Peraltro, dal documento del Comitato ad hoc sull'intelligenza artificiale (CAHAI) del Consiglio d'Europa dell'11 marzo 2021 dal titolo "Ad Hoc Committee on Artificial Intelligence (CAHAI) Policy Development Group" emergono informazioni interessanti proprio su questo argomento.

In particolare, il gruppo di lavoro del CAHAI nel documento su menzionato afferma[49]: "Attualmente, le agenzie del settore pubblico usano il processo decisionale automatizzato per lo più nella categoria dell'automazione assistita o condizionata.

In pochi casi vengono automatizzati processi o servizi completi.

Non ci sono sistemi completamente autonomi in uso nel settore pubblico.

Le basi legali per l'uso dell'ADM possono variare negli Stati membri.

Esempi sono la Germania e i Paesi Bassi. Secondo la legge tedesca, il processo decisionale automatizzato può essere usato solo quando non c'è margine di discrezionalità e quando la decisione da prendere è sì o no.

In tutti i casi, dovrebbe essere possibile rinunciare, rivalutare il processo e spiegare come è stata presa la decisione.

Nei Paesi Bassi, la situazione è la seguente: il principio di legalità richiede una base nella legge per il processo decisionale (con conseguenze legali/quando i diritti fondamentali sono in gioco), indipendentemente dall'uso o meno di sistemi di informazione".

Naturalmente, il trattamento dei dati personali è regolato dal GDPR e da altre

[49] NdR: la traduzione è nostra.

leggi sulla privacy/protezione dei dati.

Pertanto, il Consiglio d'Europa riconosce che nel settore pubblico viene utilizzato il processo decisionale automatizzato ma è esplicitamente affermato che che non ci sono sistemi completamente autonomi in uso nel settore pubblico.

Le considerazioni contenute nel documento citato assumono particolare rilievo per il settore pubblico, soprattutto con riferimento alla estensione del Consiglio d'Europa, posto che ne fanno parte non soltanto Paesi europei ma anche altri che non appartengono all'Unione Europea.

Lo stesso documento, poi, indica i tipi di applicazioni di intelligenza artificiale che potrebbero essere utilizzati nel governo e segnatamente i seguenti (NdR: la traduzione è nostra):

• Natural Language Processing (NLP) - Il campo di NLP è anche chiamato linguistica computazionale e presenta soluzioni nella comprensione delle lingue umane attraverso modelli e processi computazionali.

• Speech Recognition - Il riconoscimento vocale permette ad un computer di identificare le parole che una persona pronuncia in un microfono o in un telefono e di convertirle in testo scritto.

• Computer Vision - Le applicazioni AI di questa categoria utilizzano una qualche forma di riconoscimento di immagini, video o facciale per ottenere informazioni sull'ambiente esterno e/o l'identità di persone o oggetti specifici.

• Machine Translation - La traduzione automatica è un sottocampo della linguistica computazionale che si concentra sull'uso di software per tradurre testi o discorsi da una lingua all'altra.

• Robotics - La robotica è un campo interdisciplinare che integra l'ingegneria meccanica, l'ingegneria elettrica, l'ingegneria dell'informazione, la meccatronica, l'elettronica, la bioingegneria, l'ingegneria informatica, l'ingegneria di controllo, l'ingegneria del software, e che include la progettazione, la costruzione, il funzionamento e l'uso di robot.

• Rules-based systems - I sistemi basati su regole (conosciuti anche come sistemi di produzione o sistemi esperti) sono la forma più semplice di intelligenza artificiale. Un sistema basato su regole è un modo di codificare la conoscenza di un esperto umano in un'area abbastanza ristretta in un sistema automatizzato.

• Machine Learning - L'apprendimento automatico è un metodo di analisi dei dati che automatizza la costruzione di modelli analitici. È una branca dell'intelligenza artificiale basata sui sistemi che possono imparare dai dati, identificare i modelli e prendere decisioni con il minimo intervento umano.

Concludendo l'analisi del documento del CAHAI, emerge, infine, che[50]:

"Rispetto al settore privato, si potrebbe sostenere che il settore pubblico è attualmente in ritardo nell'adozione dell'IA.

[50] NdR: la traduzione è nostra.

Tuttavia, i governi stanno cercando di recuperare il ritardo e colmare il divario.

Secondo la mappatura iniziale dell'OCSE sull'IA, l'OCSE ha identificato 50 paesi (compresa l'UE) che hanno partecipato all'introduzione di strategie nazionali di IA, 36 di questi paesi hanno strategie specifiche per l'IA nel settore pubblico".

5. È possibile definire l'intelligenza artificiale?

La Commissione Europea, all'interno della strategia di ricerca di innovazione contenuta nell'Agenda per l'Europa, proprio sul tema dell'intelligenza artificiale e sulla robotica, ha evidenziato la necessità di realizzare partnership tra pubblico e privato da definire con interventi comuni.

Com'è noto, il 21 aprile 2021 è stata pubblicata la proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione.

In particolare, ciò che rileva, ai fini della nostra indagine, è l'articolo 3 della menzionata proposta perché viene fornita la definizione di "sistema di intelligenza artificiale" (sistema di IA), nei termini seguenti: "sistema di intelligenza artificiale" (sistema di IA): un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono".

Facendo riferimento a quanto affermato da Russell e Norvig in ordine alla difficoltà di individuare una definizione di intelligenza artificiale, il legislatore europeo interviene definendo il "sistema di intelligenza artificiale" (e quindi non l'intelligenza artificiale) come un software.

Ciò posto, non sono da escludere conseguenze di carattere etico, tecnico e giuridico, e di qui la difficoltà di individuare un approccio corretto nel rapporto tra intelligenza artificiale e protezione dati personali. Infatti, non si può prescindere dalle innovazioni dello sviluppo tecnologico, né tanto meno è possibile censurarle, ma –al contrario– vanno incentivate, trovando il corretto equilibrio nel rapporto tra protezione dei dati personali e intelligenza artificiale.

Del resto, l'approccio multidisciplinare, a cui si faceva riferimento in principio, è possibile e realizzabile in concreto e ciò è dimostrato –ad esempio– nello sviluppo dello "Ontological Standard for Ethically Driven Robotics and Automation System" di IEEE, ove il gruppo di lavoro, composto da tecnici e giuristi, ha terminato il lavoro con un risultato di successo che è stato anche premiato. Il tema principale è relativo alla ricerca di un comune equilibrio.

6. L'etica e i rischi

L'etica è, senza dubbio, un aspetto importante dal quale non possiamo assolutamente prescindere. In particolare, in materia di protezione dei personali non ci sono norme giuridiche sull'etica, ma essa è intrinsecamente espressa dai principi contenuti nella disciplina normativa e –con riferimento al GDPR– soprattutto

nell'articolo 5.

Peraltro, il nostro assunto è confermato dal contenuto della voce "Ethics of Artificial Intelligence and Robotics" della Stanford Encyclopedia of Philosophy, che evidenzia i temi sui quali si è generato un generale dibattito e segnatamente:

- Privacy & Surveillance
- Manipulation of Behaviour
- Opacity of AI Systems
- Bias in Decision Systems
- Human-Robot Interaction
- Automation and Employment
- Autonomous Systems
- Machine Ethics
- Artificial Moral Agents
- Singularity

Il tema dell'etica già evidenzia alcune criticità dell'intelligenza artificiale, ed è evidente che sussistono anche rischi concreti.

In effetti, di seguito si riporta un elenco esemplificativo e non esaustivo di alcuni dei rischi connessi all'intelligenza artificiale, dei quali si discute:

- rischi per la privacy
- bias e equità
- automazione del lavoro
- incidenti e considerazioni sulla sicurezza fisica
- responsabilità dei sistemi intelligenti
- uso malevolo dell'IA
- i livelli di rischio indicati nella proposta di regolamento UE

Peraltro, proprio sul tema dei rischi, è interessante il contributo di Benjamin Cheatham, Kia Javanmardian e Hamid Samandari, pubblicato da McKinsey & Company il 26 aprile 2019, dal titolo "Confronting the risks of artificial intelligence". Tale contributo evidenzia le conseguenze involontarie dell'intelligenza artificiale, raggruppate per Individui, Organizzazioni e Società, tra le quali è menzionata anche la privacy.

Queste risorse documentano una preoccupazione sull'impatto dell'intelligenza artificiale nei vari ambiti, incluso quello della protezione delle persone fisiche con riguardo al trattamento di dati personali e della privacy. Tuttavia, è possibile fare riferimento ai principi contenuti nell'articolo 5 del GDPR, tra i quali menzioniamo trasparenza ed etica.

Inoltre, non possiamo sottacere il riferimento ai principi "Protezione dei dati fin

dalla progettazione e protezione per impostazione predefinita" (Data Protection by Design and by Default) descritti nell'art. 25 del GDPR.

7. Le sfide

Dall'attuale scenario emerge che ci sono delle sfide da affrontare tra le quali, in primis, una adeguata consapevolezza della realtà in cui viviamo e degli strumenti che si hanno a disposizione. È necessario, pertanto, essere consapevoli dell'impatto che le risorse tecnologiche e il loro utilizzo hanno sulle persone e sulla società.

Il tema dell'intelligenza artificiale rappresenta una delle sfide tra le più importanti che va considerata unitamente all'etica. Al di là delle soluzioni tecniche adottate non si può prescindere dall'impatto che esse possono avere sulla protezione delle persone fisiche con riguardo al trattamento di dati personali, come –ad esempio– il riconoscimento facciale.

Ulteriore tema che non va trascurato è quello delle neuroscienze e neurobioscienze, ove si dovrebbero affrontare le questioni connesse all'impatto che possono avere determinate tecnologie sulle persone fisiche e sui loro dati personali.

Infine, merita di essere menzionato il modello relazionale DAPPREMO, acronimo di Data Protection and Privacy Relationships Model, basato sulla teoria degli insiemi e su alta matematica, il quale fornisce un approccio estremamente innovativo per affrontare gli aspetti connessi alla protezione delle persone fisiche con riguardo al trattamento di dati personali e alla privacy. Il logo di DAPPREMO esprime matematicamente un fibrato vettoriale, ove nel nucleo è rappresentato l'insieme della disciplina in materia di protezione delle persone fisiche con riguardo al trattamento di dati personali, privacy con il riferimento anche all'etica, e i punti di intersezione delle tangenti costituiscono gli insiemi che contengono gli "oggetti" (i singoli processi) presenti nella realtà. Si tratta di un modello multidimensionale che favorisce l'approccio alla realtà mediante l'analisi di tutti i processi, appunto con una visione a più dimensioni, conseguendo così un risultato molto ampio e non restrittivo come potrebbe accadere su un piano bidimensionale. DAPPREMO, quindi, consente di avere un approccio corretto ed esaustivo ai contesti in ambito protezione delle persone fisiche con riguardo al trattamento di dati personali, privacy (ma non solo).

EDITORIAL ASTREA

El derecho a una buena administración en un entorno de Administración pública digital

Reflexiones a partir del ejemplo de Italia

Por Diana-Urania Galetta

1. Premisa introductoria

Desde la adopción de la Carta de Derechos Fundamentales de la Unión Europea (CDUE), en el contexto de la Unión Europea, la buena administración se caracteriza como un nuevo derecho fundamental de la persona: el derecho a la buena administración, tal y como está escrito y detallado en el art. 41 de esa Carta (D.U. Galetta, 2018b; D.U. Galetta, B. Grzeszick, 2016).

Se trata de un derecho y no solamente de un "principio rector" de la acción administrativa (A. Zito, 2002); y su noción jurídica coincide con aquella idea filosófica según la cual una buena Administración pública es una administración que cumple sus propias funciones en el contexto de una democracia; y es una administración que está al servicio de la ciudadanía y que realiza su trabajo con imparcialidad y racionalidad, justificando sus acciones y orientándose continuamente al interés general (J. Rodríguez-Arana, 2013).

Como bien lo dice Rodríguez-Arana en su ensayo de 2013 sobre la buena administración como principio y como derecho fundamental "*Una buena Administración pública es aquella que cumple con las funciones que le son propias en democracia. Es decir, una Administración pública que sirve objetivamente a la ciudadanía, que realiza su trabajo con racionalidad, justificando sus actuaciones y que se orienta continuamente al interés general. Un interés general que en el Estado social y democrático de Derecho reside en la mejora permanente e integral de las condiciones de vida de las personas*" (J. Rodríguez-Arana, 2013, p. 26).

Creo que esta afirmación puede ser compartida. Cualquiera que sea el concepto de "mejorar las condiciones de vida" que se pretenda, sin importar el momento, la orientación, tampoco la ideología dominante al respecto en lugares y épocas históricas diferentes, tiene un sentimiento común.

Mi tesis que aquí expondré es que todavía –como voy a explicarlo–, en la era actual, la revolución relacionada con el uso de las modernas tecnologías de la información y la comunicación (TIC), y sobre todo el uso de la Inteligencia Artificial, puede ayudar, y mucho, a lograr el objetivo de la buena administración; e intentaré demostrarlo refiriéndome específicamente al caso de Italia.

2. La relación entre derecho a la buena administración y artículo 97 de la Constitución italiana

Según lo dispuesto en el art. 41, párrafo 2, de la Carta de los Derechos Fundamentales de la Unión Europea el derecho a la buena administración "incluye en particular:

- el derecho de toda persona a ser oída antes de que se tome en contra suya una medida individual que le afecte desfavorablemente,

- el derecho de toda persona a acceder al expediente que le afecte, dentro del respeto de los intereses legítimos de la confidencialidad y del secreto profesional y comercial,

- la obligación que incumbe a la administración de motivar sus decisiones".

Todavía, este listado no debe considerarse como exhaustivo de todo lo que puede incluirse en el concepto de buena administración.

El concepto más general de lo que se entiende por derecho a una buena administración se encuentra, en efecto, en el párrafo 1 del art. 41 CDUE: que se refiere al derecho de toda persona "*a que las instituciones y órganos de la Unión traten sus asuntos imparcial y equitativamente y dentro de un plazo razonable*".

Con relación a esta previsión normativa, hay una evidente correspondencia con lo previsto en el art. 97 de la Constitución italiana: donde se establece que "*Los cargos públicos se organizarán …de tal modo que queden garantizados su buen funcionamiento y la imparcialidad de la Administración*".

Las dos disposiciones mencionadas se complementan recíprocamente: es decir, que una administración cuyos cargos públicos estén organizados para que se asegure la imparcialidad de la administración (tal como exige el art. 97, párrafo 1 de la Constitución italiana), es también la única que puede garantizar el tratamiento imparcial y equitativo de los asuntos que afectan a los administrados.

Del mismo modo, una administración cuyos cargos públicos estén organizados de manera que aseguren el buen funcionamiento me parece como la única capaz de asegurar el cumplimiento del plazo razonable, al que el art. 41 CDUE también expresamente se refiere. Es decir que el principio de buen funcionamiento ciertamente engloba una exigencia de eficiencia de la Administración pública.

En el derecho italiano, la mejor expresión del principio de buen funcionamiento está representada por la Ley 241/1990 sobre el procedimiento administrativo (Ley 7 de agosto de 1990 n° 241, Nuevas reglas sobre el procedimiento administrativo y el derecho de acceso a los documentos administrativos), en consonancia con la idea expresada por la doctrina más influente (G. Berti, 1968) que sería necesario "procedimentalizar" el buen funcionamiento de los cargos públicos.

Desde los años noventa, todavía, los principios de imparcialidad y buen funcionamiento son puestos en relación también con la exigencia de modernizar la "máquina administrativa", también para llevar a cabo una adecuada reorganización del sistema administrativo.

Es precisamente en esta perspectiva que se evidencia el papel fundamental

que pueden desempeñar, actualmente, las tecnologías de la información y comunicación (TIC) en el contexto de la administración pública (D.U.Galetta, 2020a).

Entonces, si hay "instrumentos jurídicos" establecidos por la ley italiana del 1990 sobre el procedimiento administrativo que corresponden llenamente a la idea de buena administración tal como se describe en la Carta de los Derechos de la Unión Europea, hoy me parece necesario analizarlos también en una perspectiva de utilización de las TIC por parte de las administraciones públicas. Y eso es lo que pretendo hacer rápidamente aquí, seleccionando algunos ejemplos para explicar cómo esta revolución de la Administración 4.0 podría realmente actuarse (D.U. Galetta, J.G. Corvalán, 2019).

3. Buena administración, responsable del procedimiento y TIC

Entre los "instrumentos jurídicos" establecidos por la ley italiana sobre el procedimiento administrativo –y que no pueden separarse de la idea misma de la buena administración tal como nosotros en Italia ahora la entendemos– hay por cierto el responsable del procedimiento, que además es considerado como un *best practice* en el contexto de la Unión Europea (G. della Cananea, D.U. Galetta, 2016, p. XXI ss.).

Además, esta figura también representa el punto de unión esencial de la relación entre la digitalización de la Administración pública y el derecho a la buena administración: porque solo a través de una adecuada valorización de esta peculiar figura de funcionario público se podrá pasar del uso de las TIC como herramienta de mejora de la relación Administración pública-ciudadano reservada sólo a unos pocos, a las TIC como herramienta para mejorar la relación entre Administración pública y ciudadano de una perspectiva más general y que pueda corresponder a la idea de la buena administración (D.U. Galetta, 2020b).

En el derecho administrativo italiano las funciones del responsable del procedimiento son múltiples.

Desempeña, ante todo, una función esencial de "gobernanza del procedimiento", en lo que respecta a la organización y gestión del mismo. Tiene funciones investigativas, pero también funciones de impulso del procedimiento. Desempeña una función importante como interlocutor de las partes involucradas en el procedimiento. De hecho, su nombre se indica expresamente en la comunicación de inicio del procedimiento, de modo que los interesados puedan identificarlo, de inmediato, como su punto de referencia. Finalmente, el responsable del procedimiento tiene también importantes funciones de toma de decisiones.

En un contexto de Administración Pública que utiliza las TIC para brindar (mejores) servicios a la ciudadanía y también para superar las distancias físicas que a veces impiden que la ciudadanía acceda a los servicios prestados, el rol del responsable del procedimiento no se ve revaluado. Por el contrario, en un "entorno administrativo" dominado por el uso de las TIC, es evidente que esta figura puede jugar un papel aún más central (D.U. Galetta, 2018a).

En primer lugar, el responsable del procedimiento podría ser la figura clave para intentar cerrar esa nueva brecha entre los ciudadanos, que en la literatura del sector

ha sido bautizada como la brecha digital (*digital divide)*. Se trata de ese complejo de importantes desigualdades en el acceso a las tecnologías de la información y en la participación en las nuevas formas de comunicación e información que concierne a una parte bastante grande de los ciudadanos: los ciudadanos más pobres, pero también los ancianos (D. Donati, 2005).

Este fenómeno no concierne, como podría pensarse, solo a los países del Tercer Mundo o los países en desarrollo. Italia tiene, en verdad, problemas sustanciales a este respecto; y esto también surge claramente del Índice DESI (Índice de digitalización de la economía y la sociedad, en https://digital-strategy.ec.europa.eu/en/policies/desi).

Este documento, que proporciona una descripción general del progreso realizado por los estados miembros de la Unión Europea en la digitalización y detalles sobre las respuestas políticas de los estados miembros para abordar los desafíos específicos que esto implica, coloca a Italia un poco mejor que antes para el año 2021; es decir que Italia ocupa ahora el puesto 20 entre los 27 Estados miembros de la UE. Esto se debe a que, aunque el uso de tecnologías digitales por parte de las empresas y la prestación de servicios públicos en línea se acerca en realidad a la media de los demás Estados miembros de la UE, y que Italia ha hecho algunos progresos tanto en la cobertura como en la utilización de las redes de conectividad, Italia está muy por detrás de otros países de la UE en “capital humano”. De hecho, en comparación con la media de la UE Italia registra niveles muy bajos de habilidades digitales de los ciudadanos y, sobre todo, es la brecha tecnológica entre los distintos segmentos de la población el verdadero problema.

Por lo tanto, en un escenario de administración digitalizada que presta sus servicios sobre todo en línea, el derecho a una buena administración corre el riesgo también en Italia de romper trágicamente con el obstáculo de la ausencia de herramientas y habilidades digitales por parte de aquellos ciudadanos que más necesitan de los servicios que prestan las Administraciones públicas y que más dependen de la relación con ella en términos no solo de su bienestar (entendido como una mejora de sus condiciones de vida, en la perspectiva de J. Rodríguez-Arana, 2013) sino incluso de su propia supervivencia!

Si hoy es tarea de las Administraciones públicas permitir que los ciudadanos utilicen también aquellos servicios que se prestan digitalmente, en mi sentido debe ser tarea del responsable del procedimiento actuar como el “punto de contacto” del ciudadano con la Administración Pública, incluso de forma remota y de forma que se evite que la brecha digital se traduzca, en última instancia, en una actividad administrativa que sea todo lo contrario a los contenidos básicos del derecho a la buena administración. Y esto es cierto a fortiori cuando –como es el caso por Italia, tras la muy reciente reforma del art. 3 bis de la ley sobre el procedimiento administrativo por el decreto ley 76/2020 (el “decreto de simplificación”, decreto ley 16 de julio de 2020, n° 76, Medidas urgentes para la simplificación e innovación digital)– se aclara que existe una obligación concreta para las Administraciones públicas de actuar utilizando herramientas informáticas y telemática, para lograr una mayor eficiencia (D.U.Galetta, 2020a).

Evidentemente, esto implicará la necesidad de invertir en el responsable del procedimiento: también en cuanto a la formación adecuada de estas figuras, que

necesariamente deben ser fortalecidas y adecuadamente potenciadas.

Ahora, con el Plan Nacional de Recuperación y Resiliencia para Italia (www.governo.it/sites/governo.it/files/PNRR.pdf), autorizado por la Unión europea con el dinero del plan NextGenerationUE (https://europa.eu/next-generation-eu/index_es) y que pone a disposición el 27 % de los recursos globales (más de 54 millardos de euros) para la "transición digital" de la Administración pública italiana, este objetivo parece en todos los casos más factible que antes (D.U. Galetta, 2021).

4. Buena administración y decisión imparcial y equitativa

El término equidad puede adquirir un doble sentido en derecho administrativo: el de equidad sustancial y el de equidad procedimental.

El art. 41 de la Carta de los Derechos Fundamentales de la Unión Europea se refiere específicamente al segundo significado del término el de equidad procedimental. La disposición implica la idea de una Administración Pública capaz de ofrecer a los ciudadanos todas esas garantías de contradictorio, defensa, acceso a documentos, motivación de las decisiones, etc. que se enumeran en el párrafo 2 del art. 41 de la Carta. Lo que obviamente llama la atención sobre la importancia de una adecuada instrucción del procedimiento administrativo (F. Levi, 1967).

Al considerar un escenario caracterizado por la disponibilidad de tecnologías TIC, se pone bajo al reflector la exigencia de hacer uso de todas aquellas herramientas que permiten, hoy, a las Administraciones públicas adquirir fácilmente no solo documentos, sino también información obtenida desde sensores y herramientas de monitoreo de varios tipos (D.U. Galetta, 2019).

En cuanto al primer significado de equidad, interpretada como equidad sustancial, en este caso se perfila también una relación y, pero, no necesariamente una relación positiva entre las Administraciones públicas, las TIC y la decisión imparcial y equitativa. Pues si no será posible llegar a una organización de la actividad administrativa con las TIC de una forma que permita la superación de la brecha digital antes mencionada, en definitiva, lo que sería fuertemente cuestionado es también el cumplimiento de los dos importantes principios de la decisión imparcial y equitativa, que integran el derecho a la buena administración.

Desde este punto de vista, como ya he mencionado antes, la solución primaria consistiría en aprovechar al máximo todas las potencialidades inherentes a la figura del responsable del procedimiento: es decir, es el responsable del procedimiento quien debe actuar como "garante concreto" del cumplimiento de los principios de equidad e imparcialidad en la fase preliminar del procedimiento también en un escenario de administración digitalizada. Y debe hacerlo, por un lado, adoptando soluciones organizativas concretas que permitan evitar la discriminación entre los ciudadanos a consecuencia del diferente nivel de "alfabetización informática" y de la diferente disponibilidad de herramientas informáticas (y conexión a la red). Por otro lado, evitando que, en particular cuando la Administración pública recurra al uso de algoritmos de Inteligencia Artificial en la fase preliminar del procedimiento, pueda discriminar entre diferentes categorías de ciudadanos escondiéndose detrás del paradigma de la "neutralidad del algoritmo".

Desde este último punto de vista hay una conexión muy importante con un otro aspecto del derecho a una buena administración, el ultimo que voy a tratar aquí: el de la obligación que incumbe a la administración pública de motivar sus decisiones.

5. Buena administración y obligación que incumbe a la administración de motivar sus decisiones

En el contexto del Derecho de la Unión europea la obligación de motivación reviste una importancia crucial. No es casualidad que el art. 15 del Tratado sobre la Comunidad Europea del Carbón y del Acero (que se extinguió en 2002 una vez cumplido el periodo de vigencia de 50 años desde su firma) ya establecía que las decisiones, recomendaciones y opiniones de la Alta Autoridad tenían que estar motivadas ("Les décisions, recommandations et avis de la Haute Autorité sont motivés" - el texto oficial del Tratado constitutivo de la Comunidad Europea del Carbón y del Acero, fue firmado en París el 18 de abril de 1951 y fue redactado únicamente en francés).

La obligación de las Administraciones públicas de motivar sus decisiones es aún más importante en un contexto donde se utilizan las tecnologías TIC y, en particular, en relación con la llamada "decisión administrativa automatizada" (D. Marongiu, 2005).

Al respecto, el Consejo de Estado italiano ha especificado recientemente que el uso de "procedimientos robóticos" no puede ser un motivo para eludir los principios que conforman nuestro ordenamiento jurídico y regulan el desarrollo de la actividad administrativa (sentencia de 8 de abril de 2019, n° 2270, apartado 8.2., www.giustizia-amministrativa.it).

Por tanto, la opinión del Consejo de Estado italiano es que, cuando se recurre (legítimamente) a una automatización del procedimiento administrativo, resulta ser aún más importante cumplir con la obligación de motivar las decisiones administrativas: ya que "*la regla algorítmica debe ser no sólo cognoscible en sí misma, pero también sujeta al pleno conocimiento y a la revisión completa del juez administrativo*" ("*la regola algoritmica deve essere non solo conoscibile in sé, ma anche soggetta alla piena cognizione, e al pieno sindacato, del giudice amministrativo*". Consiglio di Stato, sentencia de 8 de abril de 2019, n° 2270, apartado 8.4, www.giustizia-amministrativa.it).

En general, la posición más reciente del Consejo de Estado italiano es, por un lado, claramente en el sentido de permitir a la Administración Pública hacer uso de las herramientas puestas a disposición por las tecnologías TIC, en la medida en que éstas resulten aptas para la realización de una acción administrativa más atenta a los estándares de imparcialidad y buen funcionamiento del art. 97 de la Constitución. Todavía el Consejo de Estado considera que la disposición constitucional sobre los principios de imparcialidad y buen funcionamiento condiciona también el uso de estas herramientas a la observancia del principio de transparencia, que se entiende aquí como pleno conocimiento tanto de la existencia de cualquier proceso automatizado de toma de decisiones como del algoritmo utilizado (D.U. Galetta, 2020; C. Coglianese, D. Lehr, 2019; P. Spano Tardivo, 2016).

Esta obligación de transparencia debe cumplirse, en primer lugar, mediante el

correcto cumplimiento de la obligación de motivar la decisión final adoptada.

De modo que, en conclusión, en un escenario de decisiones administrativas que usen herramientas de las TIC revolucionarias, tan como lo son los algoritmos de inteligencia artificial, la obligación que incumbe a la Administración pública de motivar sus decisiones, lejos de perder su sentido, sale absolutamente reforzada en su sentido esencial.

6. Conclusiones

Ya en su opinión de 2005 sobre el Código de Administración Digital de Italia (CAD - Decreto Legislativo 7 de marzo de 2005 n° 82), el Consejo de Estado italiano había observado cómo la presencia de nuevos medios para llevar a cabo la actividad administrativa requiere, cuando las innovaciones lo permiten, la finalización de operaciones para adaptar los instrumentos jurídicos existentes a las nuevas situaciones que se llevan a cabo ("*la presenza di nuovi mezzi di svolgimento dell'attività amministrativa impone, quando le innovazioni lo consentono, il compimento di operazioni di adattamento dei vecchi istituti alle nuove situazioni*". Consejo de Estado, opinión de 7 de febrero de 2005 n° 11.995, párrafo/apartado 7, www.giustizia-amministrativa.it).

Por parte de las Administraciones Públicas el uso de tecnologías TIC para sustentar sus actividades representa sin duda un elemento importante en la perspectiva de implementar tanto las disposiciones constitucionales italianas del art. 97 (en términos de mayor imparcialidad y buen funcionamiento) como de los diversos corolarios del derecho a una buena administración del art. 41 de la Carta de los Derechos Fundamentales de la Unión Europea.

Para alcanzar este objetivo es necesario, todavía, que también se consuma la transición desde un modelo informático documental (es decir, el uso de la telemática para la recogida, organización y comunicación digital de datos e información previamente contenidos en un soporte de papel), a un modelo informático meta-documental, en el cual el uso de herramientas informáticas permite la reproducción automática de ciertos procesos lógicos propios de la mente humana (G. Duni, 2008; M. D'Angelosante, 2016). Estamos hablando aquí del tema problemático y complejo –pero hoy aun central e ineludible– del uso de sistemas de inteligencia artificial (J-C. Heudin, 2017; J-C. Heudin, 2018) para apoyar la actividad administrativa (D.U. Galetta, J.G. Corvalán, 2019).

En segundo lugar, no solo es necesario proceder a una automatización real del procedimiento administrativo gracias a las TIC, identificando y explotando al máximo su potencial. También es necesario poder identificar los objetivos que se pueden alcanzar mediante la automatización de las actividades administrativas y, de manera más general, mediante el uso de las TIC.

Todavía, para que sea realmente un salto adelante también en la perspectiva de los arts. 97 de la Constitución italiana y 41 de la Carta de los Derechos Fundamentales de la Unión Europea es aún necesario que se tenga concienciación de la importancia de aquellas normas que necesariamente deben ser respetadas para que el sistema de garantías en el que se fundamenta el "estado de derecho" permanece intacto.

En esta perspectiva –y por eso concluyo– es necesario tener en cuenta que las garantías dentro del procedimiento administrativo son en sí mismas muy relevantes: en mi sentido al menos tanto como lo son los "intereses sustanciales" que la actividad administrativa pretende satisfacer (D.U. Galetta, 2005).

Bibliografia de referencia

Berti, Giorgio, *La Pubblica Amministrazione come organizzazione*, Padova, Cedam, 1968.

Coglianese, Cary - Lehr, David, *Transparency and Algorithmic Governance*, "Administrative Law Review", 2019.

D'Angelosante, Melania, *La consistenza del modello dell'amministrazione 'invisibile' nell'età della tecnificazione: dalla formazione delle decisioni alla responsabilità per le decisioni*, in Civitarese Matteucci, Stefano - Torchia, Luisa (a cura di), "La tecnificazione", Firenze, p. 156 y siguientes.

Della Cananea, Giacinto - Galetta, Diana U. e. a. (a cura di), *Codice ReNEUAL del procedimento amministrativo dell'Unione Europea*, Napoli, Editoriale Scientifica, 2016.

Donati, Daniele, *Digital divide e promozione della diffusione delle ICT*, in F. Merloni (a cura di), "Introduzione all'eGovernment: pubbliche amministrazioni e società dell'informazione", Torino, Giappichelli, 2005, p. 209 y siguientes.

Duni, Giovanni, *L'amministrazione digitale. Il diritto amministrativo nell'evoluzione telematica*, Milano, Giuffré, 2008.

Galetta, Diana U., *Technological Transition in response to COVID. Scattered Thoughts on the possibility of a (Technological) transition to a Digitalized Public Administration in Italy, with the help of the Recovery and Resilience Plan*, in CERIDAP, 4/2021, https://ceridap.eu, 16/11/21.

Galetta, Diana U., *Digitalizzazione e diritto ad una buona amministrazione (il procedimento amministrativo, fra diritto UE e tecnologie ICT)*, in C. Cavallo Perin, D.U. Galetta, "Il diritto dell'Amministrazione digitale", Torino, Giappichelli, 2020 (2020a).

Galetta, Diana U., *Algoritmi, procedimento amministrativo e garanzie: brevi riflessioni, anche alla luce degli ultimi arresti giurisprudenziali in materia*, "Rivista Italiana di Diritto Pubblico Comunitario", 2020/3(2020b).

Galetta, Diana U., *Public Administration in the Era of Database and Information Exchange Networks: Empowering Administrative Power or Just Better Serving the Citizens?*, "European Public Law", vol. 25(2), 2019, p. 171 y siguientes.

Galetta, Diana U., *Digitalización y transparencia: ¿un "responsable de la trasparencia" y su "asistente digital" como herramientas del buen gobierno del futuro?*, "Revista Jurídica de Buenos Aires", 96/2018 I, p. 159 y ss. (2018a).

Galetta, Diana U., *La Pubblica Amministrazione nell'era delle ICT: sportello digitale unico e Intelligenza Artificiale al servizio della trasparenza e dei cittadini?*, "Ciberspazio e Diritto", 2018/3, p. 319 y ss. (2018b).

Galetta, Diana U., *Il diritto ad una buona amministrazione europea come fonte di essenziali garanzie procedimentali nei confronti della Pubblica Amministrazione*, "Rivista Italiana di Diritto Pubblico Comunitario", 2005/3, p. 819 y siguientes.

Galetta, Diana U. - Corvalán, Juan G., *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, "Federalismi.it", n° 3, 6/2/19.

Galetta, Diana U. - Grzeszick, B., *Kommentar zu art. 41 Grundrechtecharta*, K. Stern/M. Sachs (a cura di), Europäische Grundrechtecharta. Kölner Gemeinschafts-Kommentar, Köln, 2016, 2ª ed., p. 618 y siguientes.

Heudin, Jean C., *Intelligence Artificielle. Manuel de survie*, Science-eBook, 2017.

Heudin, Jean C., *Comprendre le deep learning: Une introduction aux réseaux de neurones*, Paris, 2016.

Levi, Franco, *L'attività conoscitiva della pubblica amministrazione*, Torino, Giappichelli, 1967.

Marongiu, Daniele, *L'attività amministrativa automatizzata*, Rimini, Maggioli, 2005.

Rodríguez-Arana, Jaime, *La buena administración como principio y como derecho fundamental en Europa*, "Derecho y Ciencias Sociales", n° 6, 2013, p. 23 y ss., https://dialnet.unirioja.es/descarga/articulo/5167578.pdf.

Spano Tardivo, Pedro, *El principio de transparencia de la gestión pública in el marco de la teoría del bueno gobierno y la buena administración*, "Revista Digital de la Asociación Argentina de Derecho Administrativo", 2016/1, p. 226 y siguientes.

Zito, Alberto, *Il "diritto ad una buona amministrazione" nella Carte dei diritti fondamentali dell'Unione europea e nell'ordinamento interno*, "Rivista Italiana di Diritto Pubblico Comunitario", 2002, p. 427 y siguientes.

Una nueva era para la Administración pública: Posibles soluciones de inteligencia artificial

Por Natascia Arcifa

La Inteligencia Artificial[51] intenta emular la inteligencia humana mediante la creación de máquinas capaces de resolver problemas y realizar tareas y actividades típicas de la mente y las habilidades humanas. La inteligencia artificial y el aprendizaje automático se utilizan ahora en todos los ámbitos –comercial, gubernamental y empresarial– a través de servicios que logran controlar una gran cantidad de datos produciendo efectos sobre la sociedad.

La pandemia de Covid-19 y la situación de emergencia económica y social asociada han acentuado la atención de las empresas y las instituciones hacia soluciones digitales avanzadas basadas en la inteligencia artificial. El sector público, en particular, se ha enfrentado a nuevas necesidades y normas, abriendo el camino a soluciones innovadoras.

De hecho, el proceso de digitalización en la PA, incluida la introducción de soluciones basadas en la inteligencia artificial en la Administración pública, está demostrando ser fundamental para ofrecer servicios más democráticos, próximos a las necesidades de los ciudadanos. De esta manera, el ciudadano también participa indirectamente.

La digitalización en la PA aporta importantes beneficios en varios ámbitos: la reducción de costes, la mejora del rendimiento y la optimización de la asignación de recursos humanos a los objetivos estratégicos de las organizaciones.

Algunos ejemplos de Administración pública digital italiana son:

- SPID: los ciudadanos pueden acceder a los servicios en línea de la administración pública gracias a su identidad digital única;

- PagoPA: es el sistema de pagos a las administraciones públicas y a los operadores de servicios públicos en Italia.

¿Cómo implementar soluciones de Inteligencia Artificial dentro de la máquina administrativa-burocrática?

La Administración pública tiene una pluralidad de servicios y prestaciones a realizar, así como problemas a resolver que requieren la adopción de instrumentos sofisticados en las lógicas de diseño y realización. Las tecnologías que se utilicen para encontrar estas soluciones deben seguir un enfoque human-centered para

[51] Un grupo de expertos en IA de alto nivel, promovido por la Comisión Europea (2019), así define la Inteligencia Artificial: "Sistemas de software diseñados por el hombre que, dado un objetivo complejo, actúan en la dimensión física o digital percibiendo su entorno mediante la adquisición de datos, interpretando los datos estructurados o no estructurados recogidos, razonando sobre el conocimiento o procesando la información derivada de estos datos y decidiendo las mejores acciones a emprender para alcanzar el objetivo".

evolucionar los servicios públicos en función de las necesidades de las personas[52]. En particular, deben considerar los intereses desde el pequeño municipio hasta el gobierno central.

Los ámbitos de aplicación de los algoritmos de IA destinados a garantizar la eficacia de las actividades de la PA son múltiples: gestión de conjuntos de datos de gran tamaño; responder a preguntas sencillas o apoyar las decisiones de los operadores en las actividades de interacción con el ciudadano; predecir acontecimientos sobre series de datos históricos; desarrollar operaciones iterativas con entradas binarias/salidas; trabajar con imágenes, datos espaciales e información relacionada con el lenguaje natural.

En la lucha contra Covid-19, la digitalización de la Administración pública ha acelerado la carrera para ofrecer una serie de valiosas herramientas que permiten una respuesta rápida destinada, por ejemplo, a controlar el acceso a las oficinas públicas o a los consultorios médicos para garantizar la separación entre los usuarios dentro de los espacios cerrados. El éxito del esfuerzo global para utilizar las técnicas de IA depende del acceso suficiente a los datos[53].

He aquí algunos ejemplos de digitalización durante la pandemia de Covid[54]:

- *Ínter-Homines*: proyecto en fase de implementación en el URP del municipio de Módena. Utiliza servicios de inteligencia artificial y de ordenador visión para el cálculo en tiempo real de las distancias interpersonales y del nivel dinámico del riesgo de contagio en lugares públicos y de trabajo, localizando a las personas en el espacio 3D y reconociendo los Equipos de Protección Individual (EPI).

- *Covid-Skunk*: sistema de seguimiento e identificación en tiempo real de grupos de personas a través de redes celulares para prevenir la propagación del virus en entornos abiertos al público.

- *Openair*: sistema de detección automática del requisito de distanciamiento social en espacios abiertos que apoyan a la policía local y al transporte público.

¿Qué son los principales riesgos del uso de inteligencia artificial?

El uso de algoritmos en la actuación administrativa es una opción y no un imperativo, de hecho, el espacio para el uso de algoritmos debe ser identificado en un justo equilibrio[55] entre la eficacia y los derechos de los ciudadanos, regulando su uso.

---

[52] "Intelligenza artificiale e nuove forme di interazione tra cittadino e pubblica amministrazione" - Di Cristiana Benetazzo, www.federalismi.it/nv14/articolo-documento.cfm?Artid=43530.

[53] El *machine learning* y el *deep learning*, en particular, requieren grandes cantidades de datos y procesamiento para desarrollar nuevos algoritmos y arquitecturas de redes neuronales.

[54] "L'intelligenza artificiale nella pubblica amministrazione locale contro la pandemia" - Anna Francesca Pattaro, www.ai4business.it/intelligenza-artificiale/lintelligenza-artificiale-nella-pubblica-amministrazione-locale-contro-la-pandemia.

[55] La socióloga Elena Battaglini sostiene que "la omnipresencia de la tecnología implica un aumento de la responsabilidad humana en la que la dimensión del lenguaje y la palabra es fundamental en el injerto y desarrollo de procesos inclusivos en beneficio de la humanidad en su conjunto".

Los principales riesgos de la IA en las ciudades artificialmente inteligentes pueden ser los siguientes:

a) La vigilancia en masa. En la carrera por la supremacía de la IA compiten Estados Unidos[56] y China, que cuentan con la mayoría de las empresas de IA más importantes y bien financiadas del planeta. A ellos se suman otros países[57] que países usan exponencialmente el software de reconocimiento facial.

b) La discriminación automática de las características personales y de las preferencias del individuo (políticas, religiosas, sexuales, etc.).

En el ámbito del derecho, existen casos en los que el ejercicio del poder se efectúa mediante procedimientos automatizados que pueden dictar mediante un algoritmo con el riesgo de dejar la decisión a un programa informático en base a unos pocos datos[58]. Los sistemas de IA aplicados al ámbito jurídico[59] se dividen en tres áreas principales de interés: *1*) Sistemas de análisis jurídico, para la sucesión de un caso jurídico en un caso jurídico concreto; *2*) Sistemas de planificación jurídica; *3*) Sistemas de búsqueda de información jurídica que permitan buscar información conceptual - jurídica y no puramente semántica[60].

En Italia, la jurisprudencia[61] se ha ocupado de los casos en los que el uso de

---

[56] A través de una app –Clearview AI– que supuestamente recoge más de tres mil millones de imágenes de la web puestas a disposición de las fuerzas del orden para identificar a los delincuentes. Permite tomar una foto de una persona, subirla a Internet e identificarla a través de sus fotos públicas. Aun así, en 2018, el departamento de policía de Orlando comenzó a utilizar Rekognition, un programa de escaneo facial de Amazon que utiliza imágenes de cámaras de seguridad en directo.

[57] Australia está creando un sistema de reconocimiento facial para comprobar también los permisos de conducir y los pasaportes de todos los ciudadanos. India está siguiendo a China en el modelo de archivo biométrico total al planear la creación de un sistema de reconocimiento facial para las fuerzas del orden, que pretende crear un sistema centralizado vinculado también a los pasaportes, las huellas dactilares y otras bases de datos. También hay una tendencia en Europa a aumentar el uso del reconocimiento facial con fines de seguridad nacional y orden público, lucha contra el terrorismo y prevención de la delincuencia. En Alemania se han iniciado las primeras pruebas de uso del reconocimiento facial en las estaciones de tren.

[58] En los Estados Unidos, los jueces y oficiales de libertad condicional han utilizado algoritmos para evaluar la probabilidad de que un acusado delincuente reincida, descubriendo que los acusados negros tenían más probabilidades que los acusados blancos de ser juzgados erróneamente con mayor riesgo de reincidencia. Un análisis mostró que incluso durante el seguimiento de delitos anteriores, reincidencia futura, edad y sexo, los acusados negros tenían un 45% más probabilidades de recibir puntuaciones de riesgo más altas que los acusados blancos.

[59] Crisci, Stefano, *Intelligenza Artificiale ed Etica Dell'algoritmo*, "Foro Amministrativo", anno V, fasc. 10, 2018; Sartor, Giovanni, *Intelligenza artificiale e diritto. Un'introduzione*, Milano, Giuffrè, 1996.

[60] Un ejemplo es el modelo de tesauro de ITALGIURE (el sistema de documentación automática del CED del Tribunal Supremo de Casación). Este sistema, que va más allá de la tradicional búsqueda booleana mediante coincidencias exactas entre palabras, opera a nivel de semillas lingüísticas. Cada semilla contiene un conjunto de términos técnicos y de uso común que permite ampliar la búsqueda a todos los documentos que contienen palabras conceptualmente contiguas a la buscada.

[61] Chiarelli, Marina, *L'intelligenza artificiale nel procedimento amministrativo*, 10/4/20, www.diritto.it/lintelligenza-artificiale-nel-procedimento-amministrativo.

las nuevas tecnologías (algoritmos o programas informáticos) operan una elección de interés público, siempre que garanticen la transparencia de la forma y los criterios utilizados, en particular, se citan dos recientes sentencias del Consiglio di Stato Italiano:

- Sentencia 2270 de 2019[62]: el Consejo de Estado reconoció el uso de las nuevas tecnologías informáticas y algoritmos en los procedimientos administrativos, siempre que estén subordinados a los principios de eficacia y economía de la acción administrativa y sean coherentes con el principio constitucional del buen funcionamiento.

- Sentencia 8472 de 2019: el Consejo de Estado reconoció la posibilidad de confiar el procedimiento de formación de una decisión administrativa a un software que toma una decisión procesando los datos ciertos y comprobables.

c) La violación de la privacidad. La importancia de la protección de las personas está consagrada en la Declaración Universal de los Derechos Humanos (art. 3, 1948), "toda persona tiene derecho a la vida, a la libertad y a la seguridad de su persona". El más reciente Reglamento europeo de protección de datos personales (GDPR 2016/679), al centrarse en los métodos de tratamiento de datos, integra la disciplina ya contenida en la Directiva 95/46/CE con la intención de frenar el riesgo de un tratamiento discriminatorio para el individuo que encuentra su origen en una dependencia exclusiva del uso de algoritmos. En particular, los arts. 13 y 14[63] del Reglamento estipulan que el aviso de información al interesado debe notificar todo proceso de toma de decisiones automatizada, tanto si los datos se recogen directamente del interesado como si se recogen indirectamente. Además, el art. 22 estipula qua el interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos que le afecten o que afecte significativamente a su persona de manera similar. La utilización de algoritmos y procedimientos automatizados, como instrumentos procedimentales, podría constituir un "acto administrativo informático" –limitado al respeto de los principios de racionalidad, proporcionalidad, publicidad y transparencia– sujeto a las comprobaciones y al control pleno del juez administrativo, en cuanto expresamente previsto por la ley[64].

---

[62] Evoluzione tecnologica e trasparenza nei procedimenti algoritmici- Consiglio di Stato; sezione IV; sentenza 8 aprile 2019, n° 2270; Pres. Carbone; Est. Lamberti; M. A. e altri (Avv. Ursini) c. Ministero dell'Istruzione dell'Università e della Ricerca (Avvocatura Generale dello Stato).

[63] Los arts. 13 y 14 dispondrán que se informe al interesado de la posible ejecución de un proceso de toma de decisiones automatizada, tanto si la recogida de datos se efectúa directamente del interesado como si se efectúa indirectamente.

[64] La Comisión Europea tomó posición en el Libro Blanco 2020 reconociendo que la aplicación eficaz y segura del AI requiere la realización del llamado "ecosistema de confianza" en el cual se interviene en diferentes dimensiones: intervención humana y vigilancia; solidez técnica y seguridad; confidencialidad y gobernanza de los datos; transparencia; diversidad, no discriminación y equidad; bienestar social y medioambiental; y responsabilidad.

Las habilidades blandas y la ciberseguridad por diseño en la transformación digital del sector público

Por Jesús Cano Carrillo

1. Introducción

La ciberseguridad ha sido una disciplina que ha acaparado un extraordinario interés tanto a profesionales como a investigadores tradicionalmente, pero que ha venido en aumento, más si cabe, muy a propósito durante y tras las primeras olas de la pandemia mundial provocada por la Covid-19. De forma inusitada, gran parte de la sociedad se trasladó a sus hogares desde el trabajo, incluyendo a los trabajadores del sector público. El éxodo de la función pública, articulada por la necesidad básica de las personas de salvaguardar su integridad, paulatinamente se fue acompañando de mecanismos que habilitaran el trabajo a distancia (Cano, Covid-19 en la Guardia Civil: la tecnología como estrategia de respuesta rápida frente a la pandemia 2020). En una adaptación urgente y dependiendo de la capacidad de cada organización, se implantaría el acceso remoto y el teletrabajo, limando repentinamente resistencias organizativas y personales hacia el cambio digital.

El esquema de relaciones basado en la relación de la Administración Pública y los ciudadanos (Meier y Teran 2014), la figura del empleado público cobra un significado peculiar, a través del teletrabajo, ya que traslada las dependencias gubernativas a su domicilio particular. Ciertamente, esto es digno de una reflexión más profunda, especialmente porque debido a la situación de pandemia, la huida hacia el trabajo telemático nos ha dejado un escenario socio-tecnológico complejo o no fácilmente resolubles, ya que tiene imbricaciones íntimas con la brecha digital (Ballester- Espinosa 2021). Así, se observa que ha existido desigualdad en el acceso y el uso de las tecnologías de la información en distintos grupos de personas, desde un punto de vista profesional, social, e incluso criterios culturales, geográficos, políticos o de género, agudizado en los últimos tiempos, a posar de estar en primera línea de preocupación por organismos mundiales como ha mencionado la UNESCO ante el desarrollo de la sociedad del conocimiento (Bindé 2005).

La destreza individual en el uso de sistemas tecnológicos, llegado el momento de la contingencia de mantener la distancia interpersonal, como ha ocurrido en época de la pandemia global, se especializa más si cabe sobre una realidad inesperada para el usuario común: la implantación de escritorios remotos, videoconferencias y computación en la nube, junto con una serie de herramientas de ciberseguridad corporativas de cifrado de las comunicaciones, VPN, antimalware corporativo, restricción de privilegios administrativos, doble factor de autenticación 2FA, entre otros, que se suman a las medidas de seguridad básicas de cualquier usuario doméstico: antivirus, cortafuegos personales, si acaso, y actualización regular de sus equipos.

La aparición de brecha digital con respecto al teletrabajo ha demostrado la debilidad del puesto de trabajo tradicional y muestra un fenómeno, a veces imperceptible, de algo que podríamos llamar cinturón de miseria tecnológica. Esta comparación de términos comparte una cualidad que trae a colación este símil, desde el momento en que los cinturones de miseria en los núcleos urbanos ha sido objeto de estudio por la literatura científica como asentamientos informales e irregulares de personas en situación de pobreza y que se encuentran al borde las grandes ciudades, de tal manera se puede observar en la sociedad digital los asentamientos irregulares de personas que quedan marginadas por la causa electrónica, más si cabe con el despliegue de las modernas ciudades inteligentes o smart cities (Cano, Jiménez y Zoughbi 2015).

Los cinturones de miseria tecnológica, ante el éxodo domiciliario de la pandemia, ha dejado evidencias de esos asentamientos informales e irregulares que la definen: conocimientos, experiencias y equipos diferentes, no siempre compatibles, o inexistentes, que son barreras salvables o imposibles. Algunos autores han empezado a resaltar el fenómeno de los departamentos TIC en la sombra, donde trabajadores o incluso estamentos organizativos ajenos al departamento de informática han tomado la decisión de comprar e instalar dispositivos sin tomar en cuenta criterios de seguridad o sin supervisión técnica (Silic y Back 2014). La tormenta perfecta para comprometer la seguridad se presenta para el ciberdelincuente en ese traslado de la oficina al hogar.

Las nuevas modalidades de trabajo remoto, incluyendo el que se viene asumiendo de forma híbrida, unos días presencial y otros en casa, propone una revisión de los puestos de trabajo de los funcionarios públicos, desde el punto de vista de la disponibilidad, integridad y confidencialidad de la información sensible que manejan de la ciudadanía. A pesar de que es encomiable el carácter resiliente de la sociedad a nivel global frente a crisis basadas en la distancia social, quedan muchos retos propios de la organización y de la naturaleza humana, para hacer frente al oportunismo que ha supuesto la ciberdelincuencia.

2. La transformación digital: un enfoque multidisciplinar

Desde un punto de vista multidisciplinar, la idea de la transformación digital en el contexto del Gobierno electrónico pasa ineludiblemente por asumir la importancia que tiene la seguridad en el diseño de todo sistema informático de una Administración pública. El esquema clásico de relaciones entre ciudadanía y sector público está taraceado, en definitiva, por personas: de una parte, ciudadanos que participan de un servicio; de otra parte, empleados públicos que trabajan para dar ese servicio; en tercer lugar, las empresas o personas jurídicas, que se relacionan con la administración, que a su vez cierran el esquema circular con terceras personas.

En el ámbito de la tecnología de la información (TI), las habilidades, que tiene que ofrecer el personal que está detrás de los servicios públicos, se valoran por los conocimientos y experiencia que a nivel técnico acreditan. Dígase, por ejemplo, los ingenieros cuyas las habilidades técnicas vienen definidas por sus estudios y su progresión profesional. A esto se le suele llamar habilidades o capacidades duras o *hard skills*.

No obstante, existen una serie de habilidades que no son valoradas habitualmente, no por ello menos importantes, que son las habilidades blandas o *soft skills*. Tanto las habilidades duras como blandas, dentro del desarrollo de la Administración electrónica y de la efectividad de la transformación digital, influyen en la manera en que se presta el servicio público y, por ende, facilita y agiliza el desarrollo de la sociedad digital y de la nueva economía del conocimiento.

a. La supremacía de la realidad digital

Operada a través de Internet, según Castells, la nuestra es una sociedad red que reinterpreta las relaciones personales (2013). Los números respaldan esta realidad, ya que la mayoría de la población mundial es usuaria de Internet y tiene teléfono móvil, lo que supone que más de la mitad del mundo tiene vida virtual. Sin embargo, por poner un caso, más de la mitad de la población global no tiene acceso a la justicia (OCDE 2016).

Esta realidad se debería traducir en un principio impulsor básico que es importante, sobre todo a la hora de diseñar estrategias de cambio en la Administración a partir de las nuevas tecnologías. La supremacía de la realidad digital debe ser un elemento de arrastre del estado de derecho y del bienestar, una vez constatado que los propios gobiernos por vía electrónica han cambiado la forma de perseguir sus objetivos, como refleja la literatura académica sobre gestión pública desde sus inicios (Gascó 2003).

Abundando en ello, no es posible estar al margen para una buena gobernanza pública, sin considerar el hecho de que, a día de hoy, la gente usa más el teléfono móvil que los ordenadores y que es el dispositivo principal para navegar por Internet. Esto significa que la computación ubicua, donde el teléfono es protagonista, es la disciplina que se atisba para liderar un servicio electrónico bueno al ciudadano debe de contemplar que tal servicio sea respetuoso con el formato celular. A una era del metaverso que nos espera, encontramos los ciudadanos de las redes sociales, la aplicación WhatsApp, Facebook, Instagram y seguida por Twitter y TikTok, sin olvidar YouTube, lo que nos dirige a planificar servicios públicos en redes sociales y en los sistemas sociales que se van desarrollando.

En esta amalgama tecnosocial, de alguna manera, se retroalimentan dos componentes, que venimos observando de la huella que la sociedad va dejando en el uso de Internet: la edad de los usuarios y las plataformas informáticas. En todos los casos, existe una pérdida del control de su información personal, asumida en parte por el contrato tácito que hace el usuario frente a las compañías que ofrecen tecnología social, cuya primera obligación es aceptar irremediablemente el texto de aviso sobre responsabilidades jurídicas o exoneración por daños y perjuicios del uso de su red.

b. Ciberseguridad como norma cívica

La preocupación está en la calle, en esa sociedad red, que consume y participa de los servicios públicos, formando su identidad cívica digital. Nos recuerda al dilema

de la seguridad frente a la libertad individual reformulada para el ciberespacio: ¿más ciberseguridad o más libertad cibernética?

Empecemos por buscar una definición de partida de lo que se entiende por ciberseguridad. Para ello, la Unión Internacional de Telecomunicación (UIT) tiene una norma de recomendación, denotada X.1205, que habitualmente se utiliza como concepto de ciberseguridad. No es simplista, la UIT ha preferido describirla mediante una pléyade de once términos, cada uno de los cuales puede ser objeto de un capítulo o un libro completo en la materia (Carpio Cámara, y otros 2015).

Inicialmente, la ciberseguridad trata de proteger los activos de una organización, entre los que se incluyen también a los usuarios ad intra y en el ciberentorno. En primer término, se enuncian las dimensiones básicas que conforman la ciberseguridad: la tríada de la confidencialidad, la integridad y la disponibilidad, que ha pasado de ser un modelo de uso ingenieril a transponerse en los preámbulos y articulados de los distintos códigos legales. Es decir, que el modelo CIA, como se conoce por sus siglas anglosajonas, ha pasado de estar en los libros de Informática a estar inscrita en las normas actuales de convivencia cuando se habla de servicios electrónicos (Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas) (Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza).

Desgranándose en sus otros términos, la ciberseguridad aterriza en las organizaciones en forma de política de seguridad, como expresión del compromiso de la alta dirección para proteger sus activos. Más tarde, se materializan en directrices de seguridad donde esas políticas se concretan, y, además, a través de prácticas idóneas o recomendaciones de seguridad, como la típica variación de letras y números para crear una contraseña, o bien qué se debe hacer con un correo de destinatarios desconocidos que contienen enlaces o ficheros adjuntos, por poner algunos ejemplos. Así, la ley, la política, las directrices y las prácticas idóneas vienen a formar una especie de pirámide normativa de la ciberseguridad de cada una de las organizaciones.

Pero nos podríamos preguntar: ¿cómo de buena resulta ser esa pirámide de la ciberseguridad que estamos construyendo en nuestra organización? Un elemento crucial para dilucidar una respuesta para por analizar la situación, es decir, aplicar un estudio de los riesgos que están cubiertos por nuestro sistema de protección. Tener un método de gestión de riesgos quiere decir que hay que evaluar las amenazas que pueden afectar a cada uno de los activos de la organización. Hacerlo mediante un método asevera el abandono de la improvisación. De ahí que los sistemas de gestión de riesgos requieran de herramientas adecuadas, para definir un plan de acción, que incluya la aplicabilidad de salvaguardas, controles o medidas de seguridad (INCIBE 2020).

Por su trascendencia, por su carácter horizontal, la formación es la primera media que se nos puede venir a la cabeza para hacer frente a los problemas de ciberseguridad que afectan a los usuarios, que consigue mejorar la concienciación de la organización y alcanzar una cultura de ciberseguridad corporativa. La última de esas medidas que nos deja ante lo inasumible, constituye la contratación de seguros de riesgos, si es posible al caso, como salvaguarda final que garantice o compense un

daño de un ataque informático, cuando otros controles fracasaron o simplemente no pudieron aplicarse.

c. La vulnerabilidad humana

La sociedad cambia a la vez que las tecnologías y éstas retroalimentan a aquella. El factor humano es, de entre los activos, como hemos visto, sobre el que debemos parar nuestra primera mirada. La vulnerabilidad humana representa el mayor riesgo potencial para una empresa. Se manifiesta habitualmente por ser sujeto de engaño, negligencia, falta de adaptación tecnológica o impericia, o una colección aprovechada de varios de estos componentes. La técnica más conocida para engañar a un usuario es lo que se llama ingeniería social.

En esencia, lo que lo que ocurre, cuando recibimos un correo engañoso con un código malicioso, es que la pretensión es tomar posesión del equipo del usuario, acceder ilegítimamente a sus documentos y realizar acciones en su nombre. La doctrina toma en consideración este concepto como engaño suficiente, que resulta de la provocación de un error en la persona para injustamente disminuir su patrimonio.

Todos activos de una organización son objetivo potencial de un ciberataque, tanto si son personas, como dispositivos en sí, como si son aplicaciones que usan los usuarios o los administradores, como también los servicios ofrecidos: servicio de nóminas, correo, aulas virtuales, portal web, y un sinfín de facilidades. En este punto, es preocupante la incidencia sobre los canales de comunicación con la ciudadanía. La omnicanalidad como estrategia de relación cívica de las administraciones amplía la superficie de exposición, a cambio del incuestionable valor de servicio público que ofrece.

Nos encontramos con que la ciberseguridad resulta que puede ser un problema de gestión para una organización, basado en la evaluación de esas dimensiones básicas que definen a todos los activos: disponibilidad, la integridad y la privacidad. En ocasiones encontramos que el triángulo CIA se amplía, según el entorno, añadiendo parámetros, aunque de alguna manera derivadas. Es el caso del Esquema Nacional de Seguridad (ENS) en España, donde además se incluye la autenticidad y la trazabilidad, donde la norma considera que son de suficiente relevancia como para para elevarlo a la al mismo nivel que el modelo triangular para valorar cada dimensión de seguridad. Según el perjuicio que tiene sobre la organización, una amenaza cibernética podría provocar un impacto, consecuencia o daño de nivel bajo, si no afecta significativamente al normal funcionamiento de la organización; un nivel medio, que afecta sobre un activo, pero el trabajo puede seguir delante, aunque sea de forma contingente; o bien una afectación de nivel alto, cuando un activo se perjudica gravemente, de tal manera que no se puede seguir dando el servicio que se prestaba. Este esquema de consecuencias sobre la continuidad del negocio participa de un análisis de riesgo que propone una remediación del riego mediante el tratamiento de una serie de salvaguardas o medidas de seguridad (CCN-CERT 2021).

Por ejemplo, para no infectarse con malware se necesita tener en cada equipo un software cliente antivirus, lo que se constituye en una salvaguarda; si se quiere evitar fugas de información, o bien que no se establezcan puertas traseras por parte

de ciberdelincuentes desde el exterior, hay que tomar medidas con elementos cortafuegos; si no se quiere que la base de datos sean hackeadas, debe establecerse medidas de control de acceso lógico, como contraseñas reforzadas, o técnicas de huella digital (hashes) para controlar modificaciones indeseadas. Todas esas medidas son medidas de seguridad o salvaguarda que al final lo que pretenden es proteger la confidencialidad los datos personales, la integridad de la información y la disponibilidad de los sistemas. ¿Pero cuántos controles de seguridad hay que poner en una organización?

d. El aforismo del hacker protector

Se ha acuñado la idea popular, como aforismo pseudocientífico, que quizás lo ideal para una empresa es contratar a un hacker, con la idea de que como sabe cómo se ataca, debe entenderse que será el mejor defensor. La literatura técnica se ha hecho eco de este tema, distinguiendo entre el currículo necesario para la formación de un hacker y el currículo del ingeniero en computación.

No obstante, hay que hacer un inciso sobre la definición de voz inglesa hacker, porque podemos encontrarnos con distintas acepciones que nos condicionan el discurso en relación con la ciberseguridad. Según el diccionario Collins, se entiende como aquel que intenta romper los sistemas informáticos, especialmente para obtener información secreta. La Real Academia de la Lengua española, lo ha entendido tradicionalmente como un pirata informático: “persona que accede ilegalmente a sistemas informáticos ajenos para apropiárselos u obtener información secreta”. Sin embargo, consecuente con movimientos sociales de dignificación del hacking, desde 2018 se admite el sentido de “persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora” (EUROPAPRESS 2017). En cualquier caso, existen en el uso del idioma español ambos sentidos semánticos, por lo que según el contexto debemos distinguir entre el hacker malo (primer de ellas) y, digamos, el bueno (segunda acepción lingüística).

En el mundo de la Informática siempre se ha distinguido entre el hacker de sombrero blanco, para hacer referencia a ese buen samaritano tecnológico, y el hacker de sombrero negro, que es el malo malísimo que viene a señalar al pirata informático o ciberdelincuente. Lo curioso es que, entre el blanco y el negro, hay toda una colección de sombreros. Se llama hacker de sombrero gris a aquella persona que combina las características de ambos tipos, realizando intrusiones de seguridad sin consentimiento de la víctima, ansiando principalmente que le alaben sus conocimientos y le agradezcan o reconozcan sus ciberataques como un altruismo en pro de la ciberseguridad. Sin embargo, rara vez las empresas estarían de acuerdo en que, sin su consentimiento previo, forzaran sus sistemas de seguridad. En la discusión sobre los límites del hacker, a veces se traslada la idea de que podría incluir tanto el hacker blanco como el gris, cuestión que en ocasiones ha llegado a los tribunales.

La sensibilidad emocional hacia el altruismo que en los últimos años refleja el término hacker, en cierto modo, viene impulsada por la corriente de pensamiento neorromántica del ciberactivismo. También conocido como hacktivismo, pretende promover estrategias o políticas tales relacionadas con los derechos fundamentales, la

libertad de expresión y moral propia sobre la información. A finales del siglo pasado, la ética hacker surge como pensamiento colectivo con principios filosóficos propios, que en cierta manera intenta conectar con la ilusión de los primeros informáticos (Levy 1984). Le siguieron otros que fomentaron una visión positiva de la cultura hacker, como en el trabajo de Himanen (2002), donde el filósofo finés pone énfasis en comparar la ética hacker con pasión, creatividad, libertad y entusiasmo por lo que hace, alejándose de la visión criminológica y aproximándose a una definición generalista, que es aplicable a cualquier ciencia. Sin embargo, curiosamente, al hacker a veces se le ha retratado como un nerd, inteligente, concentrado en sus cosas y distraído de determinadas convenciones sociales.

En esa dinámica hackeriana, se resaltan, como vemos, habilidades blandas, como la pasión o creatividad. Llegados aquí, apelamos a buscar la respuesta a las preguntas con la intuición de dejarlas sin cerrar: ¿qué diferencia hay entre hacker o ingeniero en informática?, ¿un experto en ciberseguridad es un hacker?, ¿a todo el que se apasione por su trabajo se le podría llamar hacker? En cierta forma, sí, ¿no creen?

1) *Las habilidades blandas: de la bola de cristal al método*. Las habilidades blandas o, incluso, las duras, no elevan el arte de la clarividencia a ciencia en el ámbito de la ciberseguridad. La disciplina de la ciberseguridad, altamente especializada, requiere de un conjunto de características que se sobreponen a las propias de la ingeniería informática. Si no se dominan los fundamentos computaciones, rara vez puede acertarse en un buen diagnóstico y un tratamiento adecuado de la defensa tecnológica que se requiere en las organizaciones. Más allá de sacar una bola de cristal manejada por expertos, las metodologías para la gestión de los sistemas de información vienen formalizar las buenas prácticas y la exhaustividad en esta materia.

Los sistemas de gestión de la seguridad de la información son métodos bien estudiados para intentar que no se deje prácticamente nada al azar, a pesar de reconocer que la seguridad cien por cien no existe y que queda claro que siempre hay un riesgo residual que es necesario asumir. Pero asumir, con conocimiento de lo que se asume. De ahí que hayan surgido estándares, como la familia de normas ISO/IEC 27000, la más utilizada por la empresa para gestionar la seguridad (Ramos, y otros 2017). En el caso de la Administración pública en España hablamos del ENS, esquema que consiste en una metodología, que en el horizonte da un catálogo de salvaguardas posibles para intentar atender cualquier ciberataque.

Se han identificado 114 medidas de seguridad, conforme con el estándar 27002, en su versión revisada (2013), que dan respuesta a cualquier problema de ciberseguridad, que se clasifican en 14 tipos o dominios: políticas, organización, recursos humanos, gestión de activos, control de accesos, cifrado, seguridad física, seguridad operacional, comunicaciones, desarrollo, proveedores, gestión de incidentes, continuidad del negocio y conformidad legal. En el caso de la Administración pública española se han planteado 75 salvaguardas con el objetivo de crear una situación de confianza y protección para el ciudadano que se relaciona por medios electrónicos, que se agrupan en tres marcos: organizativo (org), operacional (op) en sentido general y de protección (mp) de activos concretos. El grado con que los productos que implementan cada una de las medidas de seguridad deben ser medibles, de tal manera que para ello se han creado un conjunto de criterios comunes (CC), que se vienen

utilizando en la industria desde los años 90. El estándar ISO/IEC 15408, ratificado en 2020, permite dar una evaluación de confianza para un dominio o categoría de productos que cubre las necesidades de seguridad común a varios usuarios, que va desde un primer nivel EAL 1 (funcionalidad básica) hasta EAL 7 (diseño verificado formalmente). Productos evaluados para su uso en entornos militares, por poner un caso representativo, exigiría unos niveles de evaluación entre EAL 5 y EAL.

En cada país que sigue los acuerdos CC existe un órgano acreditador que homologa los productos y son reconocidos por el resto de los países (en España, corresponde al Organismo de Certificación de la Seguridad de las Tecnologías de la Información, del Centro Criptológico Nacional). Ciertamente es un avance importante disponer de un consenso científico alrededor de los controles de seguridad que solucionan los problemas de ciberseguridad a nivel global, incluso poder examinar los productos concretos sobre criterios comunes. Sin embargo, a la hora de aplicarlas surge un proceso delicado: de entre esas medidas de seguridad hay que elegir las que mejor operen sobre nuestros sistemas. En una hipotética decisión de querer aplicar todas las posibles medidas, el elevado coste que supondría lo haría imposible (CSN 2019).

El cálculo del balance entre el coste de las medidas de seguridad y el grado de seguridad tiene una relación que ha preocupado siempre a los directivos de TI. El coste derivado del impacto provocado por un ciberincidente entra dentro del riesgo que se asume (riesgo residual) y disminuye conforme mayor es el número de salvaguardas que se toman. Por otro lado, el coste en prevención del riesgo (medidas adoptadas proactivamente) aumenta con el grado de seguridad. En la intersección de ambas curvas, coste reactivo y coste preventivo, se encontraría un punto óptimo de gasto en ciberseguridad. En la derivada de ambos comportamientos se debe encontrar el equilibrio donde un gasto adicional en seguridad no aporta un avance significativo en protección. En los procesos de fabricación de productos, tanto software como hardware, la tendencia de la industria y el interés del máximo beneficio del mercado, ha provocado que los procesos de la industria tecnológica liberen productos con esquemas de calidad precipitados.

2) *Inversión opex y soft skills*. En la inversión en ciberseguridad existe una tendencia a realizar el gasto en tecnología centrado en productos o activos reales, esto es, en CAPEX (capital expenditure). Se trata de invertir en capital o inmovilizado fijo, como nuevas herramientas, máquinas, plataformas o sistemas informáticos concretos, reponer los sistemas obsoletos, renovar su licenciamiento o expandir la cobertura de protección frente a amenazas en emergencia. Por el contrario, la estrategia de gastos operativos (OPEX), como es el hecho de gastar en empleados cualificados, que suponen capacidades solventes para gestionar esas nuevas herramientas, está bastante infrautilizada en este ámbito. La ratio CAPEX/OPEX en la Administración pública está doblemente influido, desde mi perspectiva, por el fenómeno de la pérdida de talento humano y la habilidad del sector público por retener el talento, ya que la fuga de profesionales en un organismo conlleva una pérdida de eficiencia en la función pública y la carencia de habilidades blandas agrava la situación.

En la disciplina de ciberseguridad deben valorarse las habilidades blandas, de la misma manera que para la ciberdelincuencia se valoran las cualidades para el engaño o la ingeniería social. Es necesario poner en valor se sexto sentido, que da un experto en tecnologías de la seguridad una combinación de destrezas sociales,

comunicativas, de empatía a los demás y una forma de ser proactiva, capaz de convertir y hacer efectiva la relación con otros.

De las soft skills o habilidades blandas debe ser obligatorio la habilidad de gestionar los conflictos, ya que los incidentes de seguridad tiene un componente muy propio de estos perfiles; también la destreza de gestionar el estrés, en lo que se suele llamar apagafuegos o bomberos tecnológicos; por ende, gestionar bien el tiempo; ser buenos comunicadores, tanto a nivel verbal como a nivel escrito, para transmitir a los usuarios los riesgos y poder determinar las medidas de contingencia adecuadamente; inteligencia emocional, que permita trabajar con un variopinto conjunto de personas; y la capacidad de cambio, en un entorno donde los ciberdelincuentes suelen ir por delante.

La comprensión del comportamiento humano, más allá de lo que trata la ingeniería de datos y el estudio estadístico, son capacidades blandas que se pueden adquirir desde la Psicología y que, a menudo, es obviado en los currículos técnicos. Ponerse en los zapatos del hacker, en su piel, es una cuestión superior para estar preparados para las amenazas y las vulnerabilidades que están por explotar, prevenidos para que no sobresalten las defensas de la red administrativa.

3. La industria del diseño de la seguridad

Hay una diferencia sustancial entre la forma tradicional de diseñar la seguridad de un sistema de información y el paradigma de la seguridad por diseño. En efecto, se reduce el coste del riesgo con la introducción de remedios tecno-organizativos, como venimos arguyendo, a posteriori, con la asunción de un riesgo residual que, a la postre, conlleva otro coste. En la economía de la información, la industria tecnológica va evaluando optimizaciones de coste-beneficio cada vez más refinados. Cuando el coste de desarrollo creativo de los ingenieros software supera el coste de mantenimiento posterior, los productos paran su ciclo de afinamiento y se fija la calidad final. Las compañías intentan reducir los ciclos de producción, sacar al mercado el nuevo producto y mantener la cuota de mercado en una sociedad cada vez más demandante de tecnologías. Digamos que los fabricantes tecnológicos aligeran en el proceso de desarrollo, en ocasiones sustrayéndolos del trabajo de los ingenieros en seguridad, que en la cadena de producción se suele incorporar en la fase final.

a. El diseño de la seguridad por diseño

La seguridad por diseño es una buena práctica que implica añadir control entre cada paso en el ciclo de desarrollo y, por lo tanto, añadir mayor esfuerzo en todas las fases, no sólo en la última. De ahí, que un producto con seguridad por diseño es un producto de calidad, menos propenso a errores. Lo contrario de la seguridad por diseño es hacer limitarse al final de un proyecto a hacer una serie de pruebas para chequear la seguridad y, luego, esperar que vayan surgiendo los fallos una vez puesto en el mercado. Los usuarios experimentando o no, en casa o en su empresa, va descubriendo fallos que se reportan como vulnerabilidades, que se solucionan con parches o hotfix. Paradójicamente, cuando hay un parche de seguridad, el fabricante

reconoce que lo ha hecho mal, que en un producto ha dejado un punto débil o defecto. Se constata que prácticamente podemos decir que todos los productos tecnológicos hoy son defectuosos. Posiblemente podamos hacer un acto de contrición alegando en primer lugar que es una creación humana, al fin y al cabo, pero acto seguido reconocer que no se aplican criterios de seguridad por diseño.

En el desarrollo de cualquier sistema informático la técnica de la ingeniería de la computación, tanto a nivel de software como hardware, se sigue un trabajo en cadena partiendo de un análisis o diseño del sistema, para después hacer el código y realizar pruebas. Es significativo que los defectos introducidos en las primeras fases del ciclo de desarrollo de un sistema de información producen mayor número de incidencias y de más difícil solución que las introducidas en las últimas fases. En el caso de la seguridad, se planifica el testeo de la seguridad para descubrir, a veces adivinar, las posibles amenazas que pueda haber con el objetivo de alcanzar un nivel de calidad preestablecido, que va a depender de los recursos, medidos en persona-tiempo fundamentalmente. Si ese producto final requiere un mantenimiento continuado, con parches y nuevos despliegues, denota que se han dejado escapar un volumen importante de vulnerabilidades e, indirectamente, significa que en el proceso de fabricación ha sido deficitario.

De hecho, el estudio de vulnerabilidades está a la orden del día y hay grandes organizaciones que se dedican a la investigación en la búsqueda de puntos débiles en los sistemas. Por su repercusión, se podría mencionar el software espía Pegasus, que aprovechaba tres vulnerabilidades, descubiertas en 2016, y que ha estado siendo explotada durante años. En concreto, la primera vulnerabilidad constituía la fuga de información en la memoria del dispositivo; la segunda que afectaba a sistemas iOS de 32 y 64 bits del fabricante Apple, que permitía al atacante liberar (jailbreak) en secreto el teléfono e instalar el software de vigilancia Pegasus; y, una tercera, sobre el navegador Safari que ponía en peligro el dispositivo simplemente cuando el usuario hace clic en un enlace. La empresa israelí NSO vendía la explotación de estas vulnerabilidades con el propósito, al menos inicialmente, de luchar contra el terrorismo y el crimen organizado, a pesar de que escandalosamente ha podido descubrirse otros usos abusivos para controlar a disidentes y periodistas. El caso Pegasus nos descubre la impresionante industria de la explotación de vulnerabilidades del software, que de forma organizada da trabajo a los expertos de sombrero negro, e incluso a los de sombrero gris, para desarrollar un programa para venderlo con un determinado fin (el color del sombrero pronostica la bondad de su utilización ulterior). Esto nos introduce el concepto de vulnerabilidades de día cero, cuando se detecta un fallo de seguridad para el que aún no existe un parche (Marczak, y otros 2018).

b. El desafío de la gestión de la administración electrónica

La Administración electrónica es un modelo de gestión pública basada en las TIC, que implica cambios organizativos y jurídicos, con el objetivo de mejorar los procesos internos en aras a la eficiencia, las relaciones interadministrativas y las relaciones con la ciudadanía, para lo que es imprescindible garantizar el aseguramiento de los activos que la constituyen.

La custodia de los derechos y libertades fundamentales obliga a diseñar una ciberseguridad pública por diseño, extremándolo si cabe en el sector de la justicia electrónica y, como extensión del concepto de gobierno abierto, el acceso universal que propone lo que se viene en llamar justicia abierta. De esta manera, la apertura por medios digitales de la Administración, acerca al ciudadano o, hablando en propiedad, acerca a los organismos de la Administración, poniendo al ciudadano en el centro. En esencia, el mantra que pretende de la Administración electrónica es que a los ciudadanos se les dota de un derecho universal a relacionarse de forma electrónica con los organismos públicos. Algunos autores han tildado el gobierno electrónico como un gigante de dos cabezas, una cabeza política y otra tecnológica.

A través de la de las nuevas tecnologías, se habilitan mecanismos de democracia electrónica para que las personas participen electrónicamente en la toma de decisiones a nivel gubernamental, aunque difiera entre un sector u otro de lo público (Estevez Mendoza y Cano 2019). Así, a veces resulta un problema técnicamente fácil y otras organizativamente complejas, como es el caso de la participación electrónica en las decisiones judiciales. La justicia en sí no se caracteriza por ser un mecanismo democrático, sino un poder del Estado de Derecho, que protege la legalidad. En el caso de la representatividad legislativa, la literatura ha ebullido con las posibilidades tecnológicas, con propuestas como la democracia directa, o la democracia líquida o revocable, que permitiría la posibilidad de delegar el voto de forma instantánea, gracias a su inmediatez electrónica, siendo a su vez revocable, flexibilidad que hace referencia a esa liquidez.

En España, la equivalencia entre la firma manuscrita y la electrónica supuso un hito importante para el avance digital gracias a una ley de finales de 2003. La Ley 59/2003, de 19 de diciembre, de Firma Electrónica, define la misma como el conjunto de datos en forma electrónica que pueden ser utilizados como medio de identificación del firmante. Junto a la organización administrativa del estado que se operó en la regulación de 1992, en el año 2007 se instituyó toda una serie de reformas para incorporar la Administración electrónica (Ley 11/2007, de 22 de junio). En un salto madurativo legal mayor, en 2015 se consolida la gestión administrativa electrónica con la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y por la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. En 2021, se perfecciona mediante el Reglamento de actuación y funcionamiento del sector público por medios electrónicos (Real Decreto 203/2021, de 30 de marzo).

4. Conclusiones

La urgente realidad nos muestra que los puestos de trabajo en ciberseguridad que se necesitan en la Administración pública no pueden cubrirse por falta de personal cualificado. La inversión en capital (CAPEX) no está acorde con el gasto público en personal (OPEX), ni la valoración de las habilidades duras (*hard skills*) son suficientes para enfrentarse a los riesgos producidos por los ciberdelincuentes.

Una nueva generación de ingenieros o de hackers buenos, en la segunda acepción moderna del término lingüístico, se necesitan con un puñado de destrezas que no son inherentes a la socialización de la persona. Son las habilidades blandas o *soft*

skills que son necesarios para afrontar los retos de la ciberseguridad que aspira a defender los derechos fundamentales de la ciudadanía digital.

La ciberseguridad es una disciplina que reivindica la incorporación de habilidades blandas en el personal dedicado a protegernos, como una práctica de seguridad por diseño, en este caso aplicada sobre los recursos humanos. Cada vez es más importante para la Administración pública, de la misma manera que tradicionalmente lo es para un policía en su misión de seguridad y el orden público. El avance de la ciberseguridad sigue los pasos de la propia naturaleza de la tecnología, de las olas tecnológicas, en la medida que surgen nuevas amenazas y acechan los ciberataques. Hay que mentalizarse para ello.

Referencias

Ballester-Espinosa, Adrián, *La transformación digital forzosa en la Administración pública*, "Telos", 2021, p. 146 a 151.

Bindé, Jérôme, *Hacia las sociedades del conocimiento: informe mundial de la UNESCO*, Ediciones UNESCO, 2005.

Cano, Jesús, *Covid-19 en la Guardia Civil: la tecnología como estrategia de respuesta rápida frente a la pandemia*, "Cuadernos de la Guardia Civil: Revista de Seguridad Pública", n° 1, 2020, p. 47 a 62.

Cano, Jesús - Jiménez, Carlos - Zoughbi, Saleem, *A smart city model based on citizen-sensors*, IEEE First International Smart Cities Conference (ISC2), 2015, p. 1 y 2.

Carpio Cámara, Manuel - León Antonio - Cano, Jesús - Jiménez, Carlos E., *Regulación y ciberseguridad: contribuciones al modelo de gobernanza*, en "La Gobernanza de Internet en España", España, IGF, 2015.

Castell, Manuel, *Power Communication*, Oxford University Press, 2013.

CCN-CERT, *Principios y recomendaciones básicas en Ciberseguridad. Recomendación*, Centro Criptológico Nacional, 2021.

CSN, *Estrategia Nacional de Ciberseguridad. Estrategia*, Madrid, Consejo de Seguridad Nacional, Administración General del Estado, 2019.

Estevez Mendoza, Lucana - Cano, Jesús, *Analysing dissenting votes through electronic justice from online posts to streets: a real case*, Sixth International Conference on eDemocracy & eGovernment, ICEDEG, Quito, IEEE, 2019, p. 64 a 68.

EUROPAPRESS, *La RAE añade una segunda acepción a la palabra "hacker" para resaltar su condición de experto en ciberseguridad*, 21 de diciembre de 2017.

Gascó, Mila, *New technologies and institutional change in public administration*, "Social Science Computer Review" 21, n° 1, 2003, p. 6 a 14.

Himanen, Peka, *La ética del hacker y el espíritu de la era de la información*, Finlandia, 2002.

INCIBE, *Buenas prácticas en el área informática*, Dosier, Instituto Nacional de Ciberseguridad, 2020.

Levy, Steven, *Hackers: Heroes of the computer revolution*, NY, Anchor Press, 1984.

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, BOE 236, 2 de octubre de 2015.

Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, BOE 298, 12 de noviembre de 2020.

Marczak, Bill - Scott-Railton, John - McKune, Sarah - Abdul Razzak, Bahr - Deibert, Ron, *Hide and Seek: Tracking NSO Group's Pegasus Spyware to operations in 45 countries*, University of Toronto, Citizen Lab Research Report n° 113, 2018.

Meier, Andreas - Teran, Luis, *eGovernment framework*, First International Conference on eDemocracy & eGovernment, Quito, ICEDEG, 2014, p. 9 a 11.

OCDE, *Leveraging the SDG's for Inclusive Growth: Delivering Access to Justice for all*, ISSUES Brief, 2016, p. 2.

Ramos, Yiner - Urrutia, Orlando - Bravo, Alberto - Ordoñez, Dayner, *Adoptar una política de seguridad de la información basados en un dominio del estándar NTC ISO/IEC 27002: 2013 para la Cooperativa Codelcauca*, Memorias de Congresos UTP, Popayán, Congreso Internacional AmITIC, 2017, p. 88 a 95.

Silic, Mario - Back, Andrea, *Shadow IT-A view from behind the curtain*, "Computers & Security" n° 45, 2014, p. 274 a 283.

BlockChain en la Administración pública. Más allá de la emisión de criptomonedas

Rafael Y. Cuartas Báez

Con el auge y creciente aplicación del protocolo BlockChain para el desarrollo de múltiplestecnologías en todos los sectores económicos, cuyo dinamismo tiene un evidente impacto en todos los ámbitos de la vida, la administración pública moderna o la función de gobiernoaplicada no puede ser ajena.

El protocolo BlockChain, como siguiente nivel de aplicación del concepto de Internet con potencialidad de acceso global virtualmente sin límites y la capacidad de generar valor, conresistencia a varios de los elementos negativos de la sociedad y el Estado de hoy; representauna gran oportunidad de modernizar las arcaicas instituciones de la administración públicay hacer realidad la transformación digital del Estado.

Al considerar los conceptos de Administración pública y BlockChain para encontrar puntos de contacto, en principio podríamos identificar una paradoja o cuando menos una contradicción al comparar los objetivos, orígenes filosóficos y políticos; y algunos elementosque son de la esencia de cada uno de estos conceptos.

En efecto, la teoría de la Administración pública denota por lo menos una parte importante de centralización, independientemente del modelo político imperante, mientras que el fundamento inicial de BlockChain se basa en la descentralización como garante de confianza, transparencia y no manipulación. Por otro lado, el modelo de Estado moderno evidencia la existencia recurrente de monopolios en diferentes aspectos del desarrollo como Nación, entre ellos la emisión de la moneda como elemento fundamental de la soberanía de los Estados; pero BlockChain por el contrario busca la democratización de estos aspectos, con la consecuente eliminación de monopolios e intermediarios; siendo suaplicación inicial orientada precisamente a la emisión de moneda sin la participación de unbanco central y la eliminación de los demás intermediarios financieros.

De igual forma, la permanente generación de medios normativos para el control social quees propia de los modelos de Gobierno actual, con independencia del enfoque político; donde la tecnología ha jugado un papel importante para llevarla a cabo. Todo lo cual es evidentemente rechazado por la corriente de pensamiento y el fundamento político-económico que dio origen a BlockChain.

En este punto, cabe recordar precisamente que BlockChain tiene sus orígenes en un movimiento Criptoanarquista denominado “CypherPunk”, que nace en la década de los años 80 en el corazón mismo de la naciente internet académica y pública, por unos apasionados de la criptografía y con ideales libertarios que rechazan el control social que genera el Estado. Este movimiento, cuyos referentes más notorios son Timothy C. May (autor del manifiesto criptoanarquista), Nick Szabo, Hal Finey y quienes están detrás del pseudónimo de Satoshi Nakamoto; entre otros; surge como una subcultura sustentada en aquel movimiento literario “Punk” de la primera mitad del siglo XX, cuyo principal referente es George Orwell con su renombrada novela “1984”, representativa de los modelos de sociedad distópica.

Desde el ámbito económico, la BlockChain se enmarca en la teoría de la escuela Austriaca de Carl Menger y F.A. Hayek, caracterizada por el individualismo metodológico, el subjetivismo y de talante antiintervencionista del Estado, en la que no existe la figura de un Banco central que tenga a su cargo la emisión de moneda nacional. Esta teoría propende precisamente por la libertad económica, sin manipulación estatal y con el trabajo como verdadero generador de valor; contrario al modelo económico imperante basado en la especulación financiera que le sirve de columna angular al sistema económico moderno.

Sin embargo, al margen de sus orígenes, las tecnologías basadas en BlockChain han mostrado en más de 13 años de existencia, un gran potencial como aliado de diferentes industrias, donde la gestión de gobiernos y administración pública, no son la excepción. No como modelo descentralizado y anárquico como en la idea original del protocolo, ni para la mera utilización como activo financiero como fue su primer uso; sino para resolver todas las oportunidades de mejora que representa la administración pública y que han sido la causa de la actual crisis de gobernanza que tiene la generalidad de las naciones en el mundo.

No es un secreto el nivel de desconfianza que alcanza en general la administración pública, especialmente en los países de la Latinoamérica, son muchos los índices que se usan hoy día y que evidencia una cada vez más crónica falta de confianza de los ciudadanos hacia sus gobiernos y las entidades estatales; desconfianza que se extiende a monopolios de interés público que son compartidos con privados, como es el caso de sector financiero, el cual no tiene cifras muy favorables de confianza por parte de los usuarios, producto de los altos costos de comisiones y las crisis de las últimas décadas; generadas en gran parte por la especulación y manipulación propia del modelo financiero global.

Entre los problemas más recurrentes para la Administración pública que reflejan los diferentes índices o encuestas que miden el nivel de confianza, se encuentran los temas de corrupción, falta de transparencia, gasto público excesivo, lentitud e ineficiencia, fallas de organización, burocracia, vulneración de derechos fundamentales y privacidad, precaria transformación digital; por mencionar solo las más relevantes. Aspectos que precisamente la teoría que sustenta el protocolo de BlockChain promete superar, generando bajos costos de implementación y menores costos de utilización, emisión monetaria eficiente sin los problemas del papel y el manejo de efectivo en la economía informal, seguridad, eficacia transaccional, transparencia y confianza, auditoria y no manipulación, modelos de identificación y autenticación; y hasta la “tokenización” de los activos de la nación con diferentes propósitos.

Dentro de los casos de uso puntuales de la Administración pública en los que se han desarrollado tecnologías basadas en el protocolo BlockChain, tenemos:

- Sistemas electorales y votación
- Emisión de monedas nacionales
- Transferencias intergubernamentales
- Sistema aduanero y control migratorio transfronterizo
- Control de presupuesto y gasto público

• Aseguramiento de bases de datos y calidad de la información oficial

• Gestión documental y trámites oficiales

• Gestión de información entre entidades gubernamentales

• Transparencia en procesos de contratación pública

• Eficiencia en el uso de infraestructura TI del Estado

• Gestión tributaria y cruce de fuentes de información

• Procesos de identidad digital segura y autosoberana

• Administración de justicia, aseguramiento de evidencia y proceso judicial digital

• Medición de eficiencia de recursos naturales de la nación y protección del medioambiente

• Gobernanza de sistemas de bienestar y salud a los ciudadanos

• Eficiente manejo de cambio de divisas para turismo y comercio internacional

• Gestión de registros públicos y notarías

• Medición imparcial y objetiva de indicadores críticos de gobierno

En cada uno de estos aspectos hay un universo de posibilidades de aplicación y alcance de desarrollos que seguramente beneficiarán y modernizarán la administración pública, que no podríamos abordar completamente en este artículo. Aplicaciones prácticas que ya no son simple teoría, sino que en muchos de los países más avanzados en desarrollo de TI son una realidad palpable y que ha permitido experiencias positivas para el mejoramiento de los sistemas aplicados a la administración de lo público.

En Latinoamérica ha habido algunas experiencias, entre las que se puede destacar la de Colombia, donde existe la Guía de Referencia de BlockChain emitida por el gobierno, para la adopción e implementación de proyectos en el Estado Colombiano. Puntualmente el Ministerio de las TIC, viene desarrollando proyectos para la implementación del protocolo BlockChain en el sector público, con el apoyo de empresas innovadoras y el BID, con quién firmó un memorando de entendimiento para este propósito[65].

Se destacan además proyectos oficiales del gobierno basados en BlockChain para combatir la corrupción que tanto afecta las sociedades de la región[66].

Otro de los proyectos que pueden destacarse en Colombia por que hacen parte de la problemática del conflicto armado que vive la nación desde hace décadas, es el relacionado con la titulación de tierras que fueron despojadas, producto de la degeneración del conflicto que causó miles de desplazamientos y refugiados al interior y el

---

[65] https://mintic.gov.co/portal/inicio/Sala-de-prensa/MinTIC-en-los-medios/178576:Implementaran-tecnologia- blockchain-en-sector-publico?utm_source=canva&utm_medium=iframely.

[66] https://mintic.gov.co/portal/inicio/Sala-de-prensa/179873:Colombia-avanza-en-la-implementacion-de-blockchain- para-combatir-la-corrupcion?utm_source=canva&utm_medium=iframely.

exterior del país; muchos de los cuales abandonaron sus tierras para huir de la violencia, viéndose en ocasiones obligados a entregar sus títulos de propiedad de manera irregular. Hoy con el proceso de paz firmado y el programa de restablecimiento de derechos a las víctimas, se usa la tecnología BlockChain para titular la restitución de esas tierras y hacer el seguimiento que evite que este despojo ilegal se vuelva a presentar. En este proyecto piloto participan la Agencia Nacional de Tierras - ANT, la Universidad Nacional de Colombia, el Ministerio TIC, y ViveLab Bogotá[67].

Un proyecto en el que apenas se inició su exploración y búsqueda de atención de los entes gubernamentales, es el relacionado con la trazabilidad y gestión de procesos con Niños institucionalizados, para evitar la vulneración de los derechos de niños, niñas y adolescentes que se encuentran a cargo o bajo custodia del Estado, que se pierden entre tanta tramitología y burocracia. Proyecto que originalmente surge en México producto de una tesis de Maestría de Beatriz Ornelas, quien como miembro del Semillero de Investigación en Derecho, Tecnología e Innovación de la Facultad de Derecho y Ciencias Políticas de la Universidad de Antioquia en Colombia[68], propone explorar su implementación en el ICBF (Instituto Colombiano de Bienestar Familiar), faltando hasta el momento la voluntad política tan necesaria en este tipo de iniciativas.

Otro de los aspectos que cobra especial relevancia en el contexto de la tecnología actual y su perspectiva a un futuro cercano, es el tema de la Identidad Digital, que con BlockChain permite interesantes formas de hacerla realidad aprovechando las características ya comentadas de la cadena de bloques.

La identidad digital tiene diferentes aproximaciones desde varios enfoques, generalmente asociada a la identidad generada por las redes sociales y las *Bigtech* por medio del uso de aplicaciones móviles y *web* que son casi de obligatorio uso hoy en día como la ofimática, además del inevitable uso de motores de búsqueda y la realización de todo tipo de transacciones en la red, que van generando un perfilamiento a través de potentes algoritmos y analítica con modernas técnicas de *bigdata* e inteligencia artificial. Sin embargo, este concepto es el que genera mayores efectos negativos y se hace con fines meramente económicos, sin que resulte en un verdadero beneficio para el usuario ni la administración pública, pues los réditos se quedan en el ámbito privado.

En este punto, es que BlockChain puede ayudar a la generación de una verdadera identidad digital autosoberana que permita superar escollos de autenticación, suplantación y protección de la privacidad, que no permiten los modelos de las *BigTech*. Cuando BlockChain se une con otros protocolos como el denominado ZKP (*zero knowledge proof*), o prueba de conocimiento cero; permite cumplir con las finalidades y objetivos que busca generar un modelo de identidad digital eficiente y global ajustado a la realidad mundial, pero sin poner en riesgo la seguridad y la privacidad del titular de los datos. Además, que le da al titular total control y gobernanza sobre sus datos personales, permitiendo decidir qué, cuánto y a quién comparte su información privada.

---

[67] https://impactotic.co/agencia-nacional-de-tierras-blockchain/?utm_source=canva&utm_medium=iframely.

[68] https://sites.google.com/udea.edu.co/semillero-dti.

Este modelo que se teorizó ya desde inicios de los años 80 del siglo pasado, sólo con el desarrollo de BlockChain pudo encontrar la forma de una aplicación práctica eficiente, siendo hoy usada en muchos modelos de autenticación financiera y en otros niveles con resultados eficientes. Basada en la teoría de juegos donde se puede probar que se conoce algo sin necesidad de revelar ese algo, simplemente iterando una prueba cuya probabilidad de manipulación del resultado es casi nula; es el medio más eficiente y seguro que hasta el momento existe, teniendo el potencial de resistir incluso a la naciente computación cuántica que amenaza la criptografía tradicional y asimétrica de doble llave.

Es indudable que los modelos de gobernanza que son innatos a las BlockChain, pueden ser un elemento que sirva para modernizar y replicar en algunos aspectos de la administración pública. Siendo el foco principal y su mayor potencialidad la capacidad de combatir la corrupción pública y privada que tanto impacta nuestros países, donde el gran reto recae en lograr la interoperabilidad con otros sistemas tanto públicos como privados, que permitan la integración de servicios. De igual manera, se encuentra en el orden del día la gestión normativa y regulatoria de los aspectos que se relacionan con históricos monopolios como el de emisión de moneda; y otros instrumentos financieros y del mercado de valores que requieren de habilitación estatal para su ejercicio.

A futuro, es previsible la existencia de Estados con servicios descentralizados en una BlockChain, pero bajo control estatal, con aplicación de modelos del denominado *OpenGoverment*, que requiere de una decidida voluntad política, el relevamiento cultural y modelos eficientes de formación y desarrollo de habilidades en TIC por parte de los funcionarios públicos y de la misma ciudadanía.

Smart City e Inteligencia Artificial entre enfoques evolutivos y perfiles problemáticos

Por Angelo Alù

1. El advenimiento de la Smart City como paradigma de diseño de una ciudad innovadora

Esta contribución pretende profundizar en la configuración estructural de la Smart City, también a la luz del impacto cada vez más central que la Inteligencia Artificial está teniendo en el desarrollo evolutivo de la arquitectura global de una ciudad innovadora.

En primer lugar, cabe señalar que, a pesar de la ausencia de una definición legislativa positivista a nivel normativo, de acuerdo con la definición aceptada pacíficamente a nivel internacional por Naciones Unidas, cuando hablamos de Smart City generalmente identificamos la existencia de una "ciudad innovadora que utiliza las TIC y otros medios para mejorar la calidad de vida, la eficiencia de las operaciones y servicios urbanos y la competitividad, asegurando la satisfacción de las necesidades ambientales, culturales, económicas y sociales en interés de las generaciones presentes y futuras"[69].

Los rasgos peculiares de la Smart City se perfilan, por tanto, en función de la disponibilidad de tecnologías innovadoras atribuibles a cualquier proceso innovador vinculado a la evolución digital que cada ciudad pueda adoptar en su misión programática de promoción del bienestar urbano a perseguir, según un amplio planificación con visión de futuro planificación, objetivos de crecimiento socioeconómico sostenible realizables en el interés general de la comunidad con una perspectiva de intervención que pueda configurarse en un horizonte temporal de medio-largo plazo que permita satisfacer, mucho más allá de las actuales necesidades contingentes conectadas únicamente a necesidades inmediatas. situaciones y extemporáneos, las demás instancias latentes aún no materializadas, como expectativas abstractas dignas de protección, de las que son portadoras las generaciones futuras.

A nivel funcional, el desarrollo de aplicaciones del modelo Smart City postula la combinación interoperable de 6 pilares tecnológicos integrados, divididos en: *1*) "Smart economy"; *2*) "Smart people"; *3*) "Smart governance"; *4*) "Smart mobility"; *5*) "Smart environment"; *6*) "Smart living"[70].

En particular, la noción de "Smart economy" incluye el complejo de servicios empresariales y procesos de producción atribuibles al paradigma innovador de los

[69] Cfr. *Sustainable Smart Cities*, UNECE (https://unece.org/housing/sustainable-smart-cities).

[70] Según la clasificación tradicional elaborada por "European Smart Cities", extraída del sitio www.smart-cities.eu.

llamados economía circular[71], funcional para promover el comercio urbano en condiciones de competitividad próspera y repartida gracias a la iniciativa de un tejido empresarial local capaz de competir en los mercados internacionales, generando un excedente global de beneficios sociales rentables para todo el territorio, como valor añadido general en concreto tangible que se puede gastar para toda la comunidad de referencia. Para medir la consistencia del capital humano dotado de habilidades adecuadas capaces de explotar las ventajas que ofrecen las tecnologías, se utiliza el concepto de "Smart people", que presupone, junto con la disponibilidad de infraestructuras tecnológicas accesibles, la existencia de un sustrato cultural digital que se encuentra en que la población urbana posea, como requisito indispensable de eficacia tecnológica, una capacidad real en el uso consciente de las herramientas digitales. El término "Smart governance" describe el sistema de cooperación institucional entre las autoridades públicas y los ciudadanos diseñado para promover, según un enfoque horizontal de interacción bidireccional, la participación activa de los usuarios en el proceso de toma de decisiones, a través de métodos transparentes de actuación administrativa. en el ámbito de un entorno relacional omnipresente destinado a favorecer una confrontación dialógica constante atribuible al modelo de la cd. OpenGov[72], potenciado por el uso masivo de tecnologías. En un nivel avanzado de desarrollo de los servicios públicos prestados por una ciudad innovadora, el sistema de "Smart mobility" se sitúa como un modelo de transporte alternativo "inteligente" altamente tecnológico para permitir movimientos ecológicos y eficientes en el tráfico, mediante el uso de medios económicos y compartidos. incluido el uso de proyectos experimentales autónomos[73].

Con el fin de conciliar la búsqueda de objetivos de crecimiento económico con la satisfacción de las necesidades generales de desarrollo sostenible, es posible lograr, según el modelo de "Smart enviroment", la explotación eficaz de los recursos naturales para salvaguardar la protección del medio ambiente, también mediante

---

[71] Para una visión general de la economía circular, consulte los documentos publicados por el portal institucional de la Unión Europea (www.europarl.europa.eu/news/en/headlines/economy/20151201STO05603/circular-economy-definition-importance-and-benefits).

[72] La reconstrucción aplicativa del modelo "OpenGov" se describe en el cd. "*Declaración de Gobierno Abierto*" proclamada por la organización "*Open Government Parthership*", teniendo en cuenta las indicaciones formalizadas por la OCDE en la Recomendación del Consejo sobre Gobierno Abierto, de 14 de diciembre de 2017.

[73] En términos de vehículos autónomos, la clasificación desarrollada por la Sociedad de Ingenieros Automotrices identifica cinco niveles diferentes de asistencia tecnológica que se pueden asociar con la conducción de un automóvil. En particular, el nivel 0 implica la ausencia de automatización ya que la conducción del vehículo está totalmente confiada a un conductor humano que controla manualmente todas las funciones del vehículo. El nivel 1 cobra protagonismo cuando existe una baja automatización que aún requiere el control de la conducción humana para el uso de aplicaciones que regulan la velocidad y el frenado del vehículo, a la par del nivel 2, que sin embargo ofrece al conductor mayores funciones de automatización (como, por ejemplo, por ejemplo, estacionamiento automático). El nivel 3, por otro lado, permite que los vehículos tomen decisiones con mayores capacidades de automatización del vehículo. A partir del nivel 4, se excluye cualquier interacción humana, que se requiere solo cuando ocurre una falla del sistema, mientras que el nivel 5, en modo de automatización completa, elimina por completo la guía humana: cfr. Shuttleworth, Jennifer, *SAE Standard News: J3016 automated-driving graphic update*, 1/7/19 (para un examen integral de estos aspectos, www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic#:~:text= The%20J3016%20standard%20defines%20six,graphic%20first%20deployed%20in%202016).

recogida selectiva, para garantizar la reducción de residuos y emisiones de gases de efecto invernadero[74]. Finalmente, la noción de "Smart living" promueve estilos de vida saludables y seguros capaces de garantizar el bienestar social, la calidad de los servicios públicos y la salud colectiva gracias a la amplia disponibilidad de servicios tecnológicos que pueden ser utilizados en el ecosistema urbano en su conjunto[75].

En comparación con la clasificación general de Smart City desarrollada para describir el funcionamiento general de una ciudad innovadora, un conjunto variado de procesos tecnológicos concretos que influyen en la operación de medidas de intervención sofisticadas destinadas a la transformación de sectores específicos del contexto urbano de referencia. En particular, de acuerdo con otro marco conceptual autorizado[76], es posible identificar las características distintivas de tres prototipos inéditos de ciudades: *1*) "Ciudad digital"; *2*) "Ciudad cibernética"; *3*) "Ciudad Inteligente". La "Ciudad Digital" se puede considerar como una ciudad basada en el uso de tecnologías IoT[77] y sensores que procesan Big Data para brindar servicios personalizados a los ciudadanos. En cambio, la estructura de la "Ciudad Cibernética" está orientada a salvaguardar altos estándares de seguridad y orden público gracias al uso generalizado de sistemas de seguimiento de identificación de personas con fines de control y prevención del delito. El tejido de ciudad construido según el modelo de "Ciudad Inteligente", pretende estimular el intercambio colaborativo y participativo de recursos a través de la adopción de sistemas co-creativos capaces de elaborar soluciones cívicas desde abajo que, en el contexto de una toma de decisiones procesar colectivamente de abajo hacia arriba, contribuir al bienestar social generalizado[78].

En la configuración concreta de una Smart City, las aplicaciones de la Inteligencia Artificial constituyen tecnologías emergentes de regeneración penetrante utilizadas para dar nueva vida al tejido urbano reconvertido de forma innovadora[79], hasta el punto de inducir recientemente a algunas ciudades a emprender, de forma

---

[74] Emblemático, en este sentido, el cd. "Plan UE 20-20-20" elaborado por la Unión Europea, a través de la formulación de un ambicioso paquete de reformas legislativas promulgadas para reducir, para 2020, las emisiones de gases de efecto invernadero a un nivel del 20%, al tiempo que aumenta el consumo de fuentes renovables en un 20% para llevar el ahorro energético a una cuota diferencial positiva del 20%, también en cumplimiento de los objetivos establecidos en el Protocolo de Kioto aprobado en 1997 en la Conferencia "COP 3" de aplicación de la Convención Marco de las Naciones Unidas sobre el cambio climático.

[75] La clasificación funcional de los paradigmas de aplicación de la Smart City descritos hace referencia al examen analítico elaborado por DalL'Ò, Giuliano, *Smart city*, Bologna, Il Mulino, 2014, p. 32 y siguientes.

[76] Cfr. Dameri, Renata P. - Giovannacci, Lorenzo, *Smart city e Digital city. Strategie urbane a confronto*, Milano, FrancoAngeli, 2015, p. 24 e 25.

[77] Un interesante estudio futurista sobre las perspectivas evolutivas de la tecnología IoT aplicada al desarrollo socioeconómico de los territorios lo proporciona Rifkin, Jeremy, *La società a costo marginale zero. L'Internet delle cose, l'ascesa del "commons" collaborativo e l'eclissi del capitalismo*, Milano, Mondadori, 2014.

[78] Cfr. Dameri - Giovannacci, *Smart city e Digital city. Strategie urbane a confronto*, p. 24 e 25.

[79] Sobre el tema ver Kirwan, Christopher - Zhiyong, Fu, *Smart Cities and Artificial Intelligence*, "Elsevier", 2020.

experimental, la tramitación de intervenciones normativas locales inéditas en la materia para asegurar el correcto funcionamiento de los sistemas de Inteligencia Artificial utilizados en la prestación de los diversos servicios públicos prestados a la comunidad en cumplimiento de sólidos principios éticos para salvaguardar la privacidad, seguridad y confiabilidad de las personas, evitando la riesgo de exponer a los usuarios a sesgos discriminatorios[80] codificados por los algoritmos instalados en los procesos automatizados de toma de decisiones[81].

Dentro del entorno urbano, los sistemas de Inteligencia Artificial están diseñados, por ejemplo, para la mejora de sensores capaces de procesar una cantidad significativa de datos personales en tiempo real, principalmente con el fin de gestionar el flujo del tráfico rodado[82], así como para la supervisión de seguridad pública[83] mediante la implementación de tecnologías de reconocimiento facial capaces de identificar los rostros humanos recogidos y rastrear las identidades de los usuarios, explotando el potencial de las aplicaciones de vigilancia biométrica[84] basadas en el funcionamiento –todavía aparentemente no del todo fiable[85]– de la Inteligencia Artificial.

Precisamente en consideración a estas implicaciones ha sido promovido recientemente por algunas ciudades[86] adheridas al llamado "*City Coalition for Digital Rights*"[87] (CC4DR), el cd. "*Observatorio Global de Inteligencia Artificial Urbana*"[88] (GOUAI): es una importante iniciativa de cooperación internacional multilateral destinada a elaborar, monitorear y actualizar los estándares técnicos definidos a través de lineamientos, acciones y políticas públicas a partir de los cuales se aplican modelos transparentes y responsables de Inteligencia Artificial a la entorno urbano de las ciudades, capaz de promover el desarrollo de una "gobernanza ética de los algoritmos en un contexto municipal"[89].

Dadas las especificidades que emergen en la práctica concreta, por lo tanto, la noción de Smart City expresa el paradigma principal del desarrollo urbano

---

[80] Para mayor información: Hardesty, Larry, *Study finds gender and skin-type bias in commercial artificial-intelligence systems*, "MIT News", 11/2/18 (https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212).

[81] Al respecto, un interesante análisis es realizado por Snow, Jackie, *Cities Take the Lead in Setting Rules Around How AI Is Used*, "The Wall Street Journal", 9/4/22.

[82] Baker, Francesca, *The technology that could end traffic jams*, "BBC", 12/12/18 (enlace: www.bbc.com/future/article/20181212-can-artificial-intelligence-end-traffic-jams).

[83] Ver Appleton, Joe, *The use of AI for Smart Urban Services in Smart Cities*, "Bee Smart City", 6/4/21 (https://hub.beesmart.city/en/solutions/the-use-of-ai-for-smart-urban-services-in-smart-cities).

[84] Cfr. Habersetzer, Nicola, *Moscow Silently Expands Surveillance of Citizens*, "HRW", 25/3/20 (www.hrw.org/news/2020/03/25/moscow-silently-expands-surveillance-citizens).

[85] Sobre el tema, ver el análisis de Lomas, Natasha, *Italy fines Clearview AI €20M and orders data deleted*, "TechCrunch", 9/3/22 (https://techcrunch.com/2022/03/09/clearview-italy-gdpr/).

[86] Las ciudades líderes del proyecto incluyen Barcelona, Londres y Ámsterdam.

[87] Sitio web: https://citiesfordigitalrights.org/cities.

[88] Sitio web: https://citiesfordigitalrights.org/presentation-global-observatory-urban-ai.

[89] Cfr. *Presentation of the Global Observatory on Urban AI*, cit.

estrictamente conectado al proceso de innovación digital omnipresente destinado a cambiar la forma actual de concebir el funcionamiento de las ciudades hasta el punto de determinar una transformación radical. proyecto justificado por las cambiantes necesidades climáticas, demográficas, medioambientales y socioeconómicas que están surgiendo en un futuro próximo según las previsiones elaboradas por el "Índice de Innovación Global 2020"[90].

El impacto de las tecnologías en la planificación urbana de las ciudades[91] es sin duda central a la luz de los desafíos anticipados de cambio que se pueden encontrar a nivel global, gracias a la implementación de soluciones eficientes y sostenibles que son posibles gracias al uso de sofisticados algoritmos, sistemas de inteligencia Dispositivos artificiales e IoT capaces de procesar una gran cantidad de Big Data, para interconectar estructuras públicas, calles, barrios y edificios equipados con sensores[92] con el fin de mejorar la calidad de vida de los ciudadanos[93].

Por tanto, se manifiesta el inicio de una profunda metamorfosis de las ciudades fuertemente acentuada por los efectos de la innovación digital, de la que dependerá la potencial capacidad innovadora de las primeras 600 ciudades del mundo para generar el 60% del PIB global[94], considerando que para 2027, se conectarán más de 41 mil millones de dispositivos IoT[95] (hasta alcanzar la cuota de 125 mil millones en 2030[96]).

Ante un alto valor de mercado global asociado al desarrollo de las Smart cities (cuantificado en unos 2 billones de dólares para 2025[97]), la Inteligencia Artificial[98] y el

---

[90] Este es el estudio publicado para la edición de 2020, editado por "World Intellectual Property Organization - WIPO" (www.wipo.int/global_innovation_index/en/2020/).

[91] Para mayor información, Ielo, Domenico, *L'agenda digitale: dalle parole ai fatti. Sanità, scuola, ricerca, start up, smart city, infrastrutture, appalti, anticorruzione, radiotelevisione*, Torino, Giappichelli, 2015.

[92] Sobre el tema ver, Nam Tuan Le - Hossain, Mohammad Arif - Islam, Amirul - Kim, Do-yun - Choi, Young-June - Jang, Yeong Min, *Survey of promising technologies for 5G networks*, "Mobile Information Systems", 2016.

[93] Ver comentarios de Rao, Sriganesh - Prasad, Ramjee, *Impact of 5G technologies on smart city implementation*, "Wireless Personal Communications", n° 100, 2018, p. 161 a 176.

[94] Cfr. Eggers, William D. - Skowron, John, *Forces of change: Smart cities*, "Deloitte", 2018 (www2.deloitte.com/us/en/insights/focus/smart-city/overview.html).

[95] Cfr. Newman, Peter, *Insider Intelligence The Internet of Things 2020*, "Business Insider", 6/3/20 (www.businessinsider.com/internet-of-things-report?IR=T).

[96] *Number of connected IoT devices will surge to 125 billion by 2030*, "Semiconductor Digest" (https://sst.semiconductor-digest.com/2017/10/number-of-connected-iot-devices-will-surge-to-125-billion-by-2030/).

[97] Cfr. Bourne, James, *Smart cities market value to hit $2 trillion by 2025, says Frost & Sullivan*, "IOTnew", 2018 (https://iottechnews.com/news/2018/apr/04/smart-cities-market-value-hit-2-trillion-2025-says-frost-sullivan/).

[98] Según el estudio titulado "*PwC's Global Artificial Intelligence Study: Exploiting the AI Revolution*" a cura di PWC está claro que la Inteligencia Artificial producirá importantes ingresos en los

blockchain[99] se encuentran sin duda entre las principales tecnologías emergentes destinadas a transformar el rostro actual de las ciudades, determinando también efectos significativos sobre el sistema de movilidad urbana, en implantación del modelo "Smart Mobility", con el consiguiente crecimiento en el sector de los coches autónomos inteligentes[100].

Tomando nota de estos cambios, teniendo en cuenta el progresivo crecimiento demográfico de la población mundial –cerca de alcanzar el umbral del 66% en las aglomeraciones urbanas para 2050 (equivale a unos 2.500 millones de personas más[101])– el programa internacional "United Smart Cities"[102] tiene como objetivo potenciar el desarrollo de las ciudades inteligentes sobre la base de una serie de objetivos prioritarios[103] desarrollados por Naciones Unidas[104], con el fin de favorecer el bienestar generalizado de la comunidad gracias a una mejora general de los servicios públicos digitalizados.

Siguiendo las mismas coordenadas trazadas a nivel internacional, también en el contexto de las políticas de cohesión de la Unión Europea[105], se enfoca la centralidad de la Smart City como emblema de la regeneración urbana de las ciudades, a través de la creación de espacios públicos funcionales de alta calidad, asegurar el fortalecimiento de la economía local en estrecha vinculación con la valorización de los barrios degradados, como parte de una acción coordinada e integrada entre los

próximos años cuantificables en más de 15 billones de dólares (el estudio se puede consultar en el siguiente enlace: www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html).

[99] Sobre los efectos de la tecnología blockchain, ver *Time for trust: How blockchain will transform business and the economy*, PWC (www.pwc.com/gx/en/industries/technology/publications/blockchain-report-transform-business-economy.html).

[100] Cfr. *Automotive IoT Market by Platform (Data Management), Component (Sensor, GPS, Bluetooth, Wi-Fi), Data Converter (ADC), Connectivity (Embedded), End User (OEM), and Application (ADAS, Fleet Management, Infotainment) Global Forecast to 2025* (www.meticulousresearch.com/product/automotive-iot-market-5071/).

[101] Cfr. "World Urbanization Prospects", Nazioni Unite, 2014 (más información en el sitio web: https://population.un.org/wup/publications/files/wup2014-highlights.pdf).

[102] Todos los detalles se pueden ver en el siguiente sitio web: https://sustainabledevelopment.un.org/partnership/?p=10009#:~:text=United%20Smart%20Cities%20is%20a,the%20OiER%20Secretariat%20in%20Vienna.

[103] *Collection Methodology for Key Performance Indicators for Smart Sustainable Cities*, Naciones Unidas.

[104] Como, por ejemplo, la iniciativa *Unidos por las Ciudades Inteligentes y Sostenibles* (U4SSC) impulsada por Naciones Unidas en colaboración con la Unión Internacional de Telecomunicaciones (UIT).

[105] Emblemática, en este sentido, es la "Carta de Lispia" sobre Ciudades Europeas Sostenibles de 2007 que constituye la base de reconocimiento de referencia que puede utilizarse para reconstruir el modelo de diseño de Smart City en cumplimiento de los compromisos formalizados en la Agenda territorial de la Unión Europea (más información puede consultarse en el siguiente sitio web: https://ec.europa.eu/regional_policy/archive/themes/urban/leipzig_charter.pdf).

distintos niveles institucionales[106] para asegurar el desarrollo territorial, económico y social de las comunidades inteligentes[107].

Para ello, la "*Agenda Urbana de la Unión Europea*"[108] –elaborada a instancias de la Comisión Europea[109]– se estableció con el Pacto de Ámsterdam en 2016[110], precisamente para potenciar, con respecto a los 12 retos urbanos[111] formalizados en la "Declaración de Riga"[112], el papel clave de las ciudades consideradas "centros de creatividad y motores del crecimiento europeo"[113].

2. Es la ciudad de Buenos Aires un prototipo de Smart City? El estado del arte de las principales iniciativas realizadas

El informe internacional "Smart City Index 2020", elaborado por el Institute for Management Development (IMD)[114] en colaboración con la Singapore University for Technology and Design (SUTD)[115], ofrece un panorama general de las realidades urbanas más innovadoras del mundo[116].

---

[106] Siguiendo estas coordenadas de aplicación, la Estrategia "Europa 2020" formaliza el compromiso de la Unión Europea de impulsar un crecimiento inteligente, sostenible e integrador destinado a perseguir 5 objetivos fundamentales (empleo, investigación y desarrollo, clima y energía, educación, integración social y reducción de la pobreza) que presupone la revitalización efectiva de las comunidades locales a través del desarrollo de estrategias políticas innovadoras que se adoptarán de acuerdo con un enfoque de gobernanza descentralizada multinivel basado en la cooperación sinérgica entre actores públicos, empresas y centros de investigación para favorecer la difusión general de tecnologías: ver Comunicación Comisión Europea, *Europa 2020: Una estrategia para un crecimiento inteligente, sostenible e integrador*, 3 de marzo de 2010.

[107] Como se desprende de la resolución del Parlamento Europeo de 9 de septiembre de 2015 sobre la dimensión urbana de las políticas de la UE (el documento se puede consultar en el siguiente enlace: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52015IP0307).

[108] Sitio web: https://ec.europa.eu/futurium/en/urban-agenda.

[109] Ver la Comunicazione della Commissione Europea, *The urban dimension of EU policies - key features of an EU Urban Agenda*, del 18/7/14.

[110] Sitio web: https://ec.europa.eu/regional_policy/sources/policy/themes/urban-development/agenda/pact-of-amsterdam.pdf.

[111] Los 12 desafíos urbanos son: *1*) inclusión de migrantes y refugiados, *2*) calidad del aire, *3*) pobreza urbana, *4*) vivienda, *5*) economía circular, *6*) empleos y competencias profesionales en la economía local, *7*) adaptación al cambio climático, *8*) transición energética, *9*) uso sostenible del suelo y soluciones basadas en la naturaleza, *10*) movilidad urbana, *11*) transición digital, *12*) contratación pública innovadora y responsable.

[112] Sitio web: https://eu2015.lv/images/news/2015_06_10_EUurbanDeclaration.pdf.

[113] Véase, Comunicado de prensa "La agenda urbana de la UE: implicar a las ciudades en el diseño de las políticas de la UE", 30/5/16 (El documento completo al que se hace referencia se puede consultar en el siguiente enlace: https://ec.europa.eu/commission/presscorner/detail/it/IP_16_1924).

[114] Sitio web: https://www.imd.org/.

[115] Sitio web: https://www.sutd.edu.sg/.

[116] Para más información sobre el Informe, puede consultar el siguiente enlace: www.imd.org/smart-city-observatory/smart-city-profiles/.

En particular, al esbozar interesantes reflexiones sobre los escenarios de desarrollo de las ciudades "inteligentes" de las que emerge el indudable potencial de lo digital, el estudio sitúa a Singapur (Singapur) en el primer puesto del ranking mundial, seguida de Zúrich (Suiza) y Oslo (Noruega) en comparación con 109 ciudades monitoreadas sobre la base de 5 indicadores clave (salud y seguridad, movilidad, actividades, oportunidades y gobernanza).

El top 10 también incluye Taipei (Taiwán), Lausana (Suiza), Helsinki (Finlandia), Copenhague (Dinamarca), Ginebra (Suiza), Auckland (Nueva Zelanda) y Bilbao (España).

Con especial referencia al contexto de América Latina, la ciudad que logra el resultado más alto en el índice general es Buenos Aires (Argentina) obteniendo la posición 98[117], mientras que Medellín (Colombia) se encuentra en el lugar 101 y Ciudad de México (México) en el puesto 108.

Aunque se ubica en la parte final más baja del ranking elaborado por el citado estudio, la capital argentina fue galardonada, con motivo de los "World Smart City Awards 2021"[118], como Smart City de 2021[119], una de las más avanzadas en el panorama sudamericano.

Entrando en el mérito de las valoraciones expresadas en apoyo al resultado alcanzado por Buenos Aires, se reconoce el constante crecimiento tecnológico de la ciudad como prototipo del desarrollo de un centro urbano de alta intensidad demográfica capaz de materializar el inicio concreto de una proceso de transformación digital que ha favorecido la mejora progresiva de los servicios públicos prestados en los sectores del transporte, la energía, los residuos y la seguridad, sin negar la presencia de problemas socioeconómicos –todavía existentes– particularmente arraigados en los barrios más populosos de la ciudad.

En este sentido, se potenció el "*Plan Municipal de Gestión de Residuos Sólidos*"[120] que, para mejorar la reducción de residuos, contempla, entre los principales objetivos de la estrategia, la recogida selectiva como parte integrante de un sistema general de economía circular sobre el que se fundamenta el pilar tecnológico de los llamados "Smart Economy", constituyendo uno de los rasgos peculiares de la arquitectura estructural de una ciudad innovadora.

En cumplimiento de la Estrategia Nacional para la Gestión Integral de los Residuos Sólidos Urbanos[121], desarrollada en el ámbito de las políticas públicas ambientales para perfilar un marco general homogéneo aplicable en todo el territorio con un

---

[117] Sin embargo, la capital argentina registró un empeoramiento de su desempeño respecto a la evaluación del año anterior, ya que Buenos Aires se ubicó efectivamente en el puesto 88 de la clasificación general. El informe completo se puede consultar en el siguiente sitio web: www.imd.org/smart-city-profile/Buenos%20Aires/2021.

[118] Sitio web: https://tomorrow.city/a/scewc2021-awards.

[119] Como Santiago de Chile, Panamá, Montevideo y San José.

[120] www.buenosaires.gob.ar/sites/gcaba/files/guia_para_alumnos_-_secundaria_-_gir.pdf.

[121] www.mininterior.gov.ar/municipios/pdfs/SAM_03_residuos_solidos.pdf.

horizonte temporal de largo plazo (fijado, como primera fase de seguimiento de la aplicación, en el 2025), la ciudad de Buenos Aires ha planificado el proceso de gestión de residuos industriales urbanos de acuerdo con el ciclo ordinario de recolección orgánica, transporte, procesamiento, reciclaje y compostaje, para proteger la salud pública y el ecosistema ambiental, en implementación de la llamada "5R"[122].

Buenos Aires, que es una de las áreas urbanas más grandes del continente, está desarrollando una serie de proyectos innovadores que promueven la inclusión social a través de la provisión de servicios públicos basados en el uso de tecnologías emergentes con miras a simplificar y modernizar los procesos administrativos, incluyendo mediante el uso de formas de experimentación flexibles y creativas.

Emblemático, en este sentido, es el "*Mapa de oportunidades de negocio*"[123], que permite a los usuarios adquirir en tiempo real la información necesaria para tomar las mejores decisiones de acuerdo a la posible apertura de actividades empresariales en la ciudad, al igual que el "*Mapa de la delincuencia*"[124] contener datos estadísticos fiables y actualizados sobre los fenómenos delictivos detectados en la ciudad, disponibles gracias a la recopilación de una gran cantidad de conjuntos de datos accesibles en formato OpenData[125].

La Secretaría de Innovación y Transformación Digital, como oficina encargada de desarrollar proyectos innovadores, ofrece a los ciudadanos de la capital argentina la oportunidad de descargar la aplicación "*BA WiFi*" que identifica los puntos de conexión a la red wifi pública y gratuita[126].

También cabe destacar una plataforma virtual[127] que, tras el registro de una cuenta personal asociada a los datos personales del usuario, permite, a distancia, realizar un seguimiento, a distancia, de todas las prácticas activas en las relaciones con las Administraciones Públicas de forma virtual, como proyecto significativo estrictamente ligado al uso de la aplicación "*Fila Cero*"[128] que monitorea los tiempos de espera en los trámites en línea para racionalizar los servicios públicos, así como realizar denuncias y reclamos directamente dirigidos a los responsables de las oficinas competentes[129].

Una colección de aplicaciones móviles oficiales[130] de la ciudad también está activa en línea para facilitar los viajes urbanos a través de la posibilidad de rastrear los sistemas de transporte público y taxis en base a las rutas viales solicitadas por los

---

[122] www.argentina.gob.ar/ambiente/contenidos/5R.

[123] https://mapa.seguridadciudad.gob.ar/.

[124] https://mapa.seguridadciudad.gob.ar/.

[125] https://data.buenosaires.gob.ar/dataset/.

[126] www.buenosaires.gob.ar/jefaturadegabinete/innovacion/aplicacionesmoviles/ba-wifi.

[127] www.buenosaires.gob.ar/tramites/tramites-distancia-tad.

[128] www.buenosaires.gob.ar/atencionygestionciudadana/fila-cero.

[129] www.buenosaires.gob.ar/jefaturadegabinete/innovacion/aplicacionesmoviles.

[130] www.buenosaires.gob.ar/jefaturadegabinete/innovacion/aplicacionesmoviles.

usuarios, incluida la posibilidad de identificar espacios de estacionamiento en tiempo real y encontrar actividades culturales, deportivas y gastronómicas.

Recientemente, la ciudad de Buenos Aires lanzó el "*Plan de Inteligencia Artificial*"[131] con el objetivo de estimular el uso generalizado de los beneficios que ofrecen las tecnologías emergentes, en cumplimiento de estándares éticos y legales adecuados, tomando nota del impacto significativo de la Inteligencia Artificial en la vida de las personas en todos los sectores públicos, lo que abre la oportunidad de impulsar un proceso concreto de transformación industrial local a través de la definición preventiva de un marco normativo adecuado a la dinámica evolutiva de la innovación.

Para ello, se creó el proyecto "*Chatbot*"[132] de la ciudad, que ofrece un servicio de asistencia virtual a los ciudadanos, fundamental para crear, a través del desarrollo de una plataforma de comunicación de conversación personalizada, una intervención concreta para simplificar los procedimientos y tiempos de la actividad administrativa gracias a una efectiva acción de digitalización automatizada que permita a los usuarios definir en línea las solicitudes relacionadas directamente desde su hogar, sin necesidad de acudir físicamente a las oficinas públicas de los sistemas administrativos competentes.

Recientemente, con el fin de racionalizar el flujo de pacientes ingresados en los hospitales, también se ha desarrollado un sistema de salud de Inteligencia Artificial[133] para detectar la propagación de la epidemia "Covid-19" a través del diagnóstico remoto, basado en algoritmos de aprendizaje automático capaces de examinar la tos de los usuarios, audios y sonidos respiratorios con alta precisión estadística igual a casi el 90% de confiabilidad.

3. El desarrollo problemático de la Smart City: ¿la brecha digital como desigualdad "crónica" de las ciudades inteligentes?

El desarrollo urbano de la Smart City, si bien en constante expansión a escala planetaria como un fenómeno generalizado en todos los continentes, gracias a la paulatina implementación de un prototipo de diseño cada vez más avanzado y sofisticado compartido a nivel mundial[134], no es sin embargo uniforme en todo el mundo debido al retraso tecnológico que se vive en determinados contextos geográficos, donde las condiciones desfavorables del atraso digital ralentizarán los beneficios de la innovación, obstaculizados por graves déficits culturales e infraestructurales, con el riesgo de alimentar nuevas formas de pobreza vinculadas a la Preocupante expansión de la

[131] www.buenosaires.gob.ar/sites/gcaba/files/plan_de_inteligencia_artificial_de_la_ciudad.pdf.

[132] www.buenosaires.gob.ar/jefaturadegabinete/innovacion/boti.

[133] www.buenosaires.gob.ar/jefaturadegabinete/innovacion/plan-de-inteligencia-artificial/iatos.

[134] En este sentido, se desarrolló la plataforma "*Virginia Smart community test center*" para desarrollar soluciones tecnológicas innovadoras de punta funcionales para incrementar el modelo de ciudad inteligente, a través del uso integrado de los servicios de seguridad pública, banda ancha y turismo y desarrollo económico, en cumplimiento con la disciplina de protección de datos personales, contemplando la experimentación de drones y sensores, así como herramientas de blockchain, IoT y realidad aumentada (sitio web: https://www.virginiaipc.org/smart-community-testbed).

brecha digital frente[135] a un porcentaje todavía demasiado elevado de la población residente excluida digitalmente[136].

Por lo tanto, a pesar de la mejora progresiva de la arquitectura innovadora que aumenta el nivel de eficiencia de un número creciente de "ciudades inteligentes", la implementación efectiva del pilar "Smart People" es aún insuficiente, en la medida en que existe un capital humano limitado personas con competencias digitales cualificadas, capaces de explotar los servicios tecnológicos disponibles. Esta es una criticidad muy significativa, más aún cuando se refiere a la disponibilidad de nuevas tecnologías emergentes (incluida la Inteligencia Artificial), que, además de los indudables beneficios que ofrece para optimizar el crecimiento económico gracias a procedimientos automatizados capaces de maximizar las líneas de montaje de las cadenas productivas , sin embargo, representan herramientas aún más sofisticadas e insidiosas en comparación con la posibilidad de generar efectos invasivos, a menudo imperceptibles, capaces de tener un impacto aún más generalizado en la vida de las personas.

Por ello, los problemas encontrados muestran la "doble cara" de las ciudades: esto es, entornos formales tecnológicamente avanzados (teniendo en cuenta el equipamiento infraestructural instalado en el territorio), pero esencialmente destinados a configurar comunidades desiguales que traen –extremadamente amplificadas– exclusiones masivas relacionadas con el retraso digital cultural.

La brecha digital es, de hecho, la principal fuente de discriminación en el acceso y uso de tecnologías[137] debido a la falta de habilidades básicas (alfabetización, numéricas e informáticas), agravada por los bajos niveles de escolaridad y educación, que se encuentran principalmente en sujetos de la tercera edad (denominada "brecha digital intergeneracional"), en mujeres desempleadas (denominada "brecha digital de género"), inmigrantes (denominada "brecha digital lingüístico-cultural") y, en general, en personas con discapacidad[138].

Con el advenimiento de la "Sociedad de la Información"[139] se hace necesario permitir que las personas adquieran un nivel adecuado de cultura digital (básica y especializada), como requisito indispensable no sólo para el correcto ejercicio de los derechos ciudadanos configurables en el espacio red virtual, donde las relaciones entre los usuarios y el sector público se intensifican, pero también a la luz del progresivo aumento de nuevas salidas profesionales que demanda el mercado laboral[140], de ahí

---

[135] Tal y como señala al respecto el estudio de la OCDE "*Digital Economy Outlook*".

[136] Está permitido ver Alù, Angelo - Longo, Alessandro, *Cos'è il digital divide, nuova discriminazione sociale (e culturale)*, Agendadigitale.eu, 13/3/20. El artículo se puede ver en el siguiente enlace: www.agendadigitale.eu/infrastrutture/il-digital-divide-culturale-e-una-nuova-discriminazione-sociale/).

[137] Di Maggio, Paul, *From the "Digital Divide" to "Digital Inequality": Studying Internet Use as Penetration Increases*, "Working Paper Series", n° 15.

[138] Cfr. Norris, Pippa, *Digital Divide: Civic Engagement, Information Poverty, and the Internet*, Cambridge University Press, 2001.

[139] Sobre el tema se puede ver el análisis de Beniger, James R., *Le origini della Società dell'Informazione. La rivoluzione del controllo*, Torino, Utet, 1995.

[140] Según las perspectivas del Foro Económico Mundial que desde hace tiempo, reconociendo el impacto significativo de las tecnologías en las ocupaciones dinámicas del mercado laboral, ha

la necesidad de asegurar la recualificación de fuerza de trabajo[141] de obra cada vez más ligada a la necesidad prioritaria de satisfacer las necesidades de la tecnología sector[142].

En esta perspectiva, las ciudades pueden desempeñar un papel fundamental para el crecimiento económico y el bienestar social, también en la implementación de los objetivos de desarrollo sostenible definidos por la Agenda 2030[143] de las Naciones Unidas, solo a condición de que se garantice una inclusión social efectiva a través de la mejora del nivel general de alfabetización digital.

De ello se deduce que el diseño de una ciudad inteligente verdaderamente innovadora no solo debe limitarse a la construcción de infraestructuras tecnológicas de punta para convertir la provisión general de servicios públicos en forma digitalizada, sino que, sobre todo, requiere el indispensable uso generalizado de las tecnologías, en condiciones generales de acceso sustancial de todas las personas con habilidades en TIC[144], para evitar cualquier forma de exclusión social que pueda comprometer el desarrollo efectivo de una ciudad inteligente próspera, sostenible e inclusiva.

previsto, entre otras cosas, la creación de 133 millones de nuevos puestos de trabajo relacionados con el sector TIC; cf. Informe "Future of Jobs Report 2018" (www.weforum.org/reports/the-future-of-jobs-report-2018).

[141] A la luz de lo que sostiene el informe "Digital Skill Insight" elaborado por la Unión Internacional de Telecomunicaciones, que destaca la necesidad de incrementar el nivel de cultura digital básica como requisito imprescindible no solo para poder aprovechar las próximas oportunidades laborales vinculadas a las TIC sectores, sino para llevar a cabo la gran mayoría de las actividades en un entorno digital (por más información ver sitio web: https://academy.itu.int/index.php/main-activities/research-publications/digital-skills-insights/digital-skills-insights-2020).

[142] La posesión de competencias digitales puede representar un factor concreto de recualificación laboral, estimulando la demanda con la consiguiente reducción de la tasa de desempleo, más aún en un contexto general de recesión económica, generada por la crisis mundial que data ya de 2008 y agravada aún más por la pandemia de Covid-19, como subraya en este sentido el informe "Employment Outlook 2020" elaborado por la OCDE que proyecta un aumento en el nivel de desempleo de casi el 10% en los países de la OCDE, además de una disminución relacionada del PIB de casi un 15%, con el riesgo concreto de graves repercusiones socioeconómicas en un futuro próximo incluso comparables a los tiempos de la "Gran Depresión". De ahí la necesidad de impulsar "la reconstrucción de un mercado laboral mejor y más resiliente, inversión esencial para las generaciones futuras": cf. Informe "Employment Outlook 2020", OCDE (www.oecd.org/employment-outlook/2020/).

[143] https://unric.org/it/agenda-2030/.

[144] La falta de una cultura digital básica puede, por tanto, representar un grave factor de discriminación destinado a agravar los problemas encontrados. Según el informe "Measuring digital development", editado por la Unión Internacional de Telecomunicaciones, de hecho, grandes sectores de la población, a nivel mundial, carecen de habilidades informáticas básicas (como, por ejemplo, copiar un archivo o enviar un correo electrónico con un archivo adjunto), con déficits aún más negativos en comparación con las "habilidades informáticas estándar" (a modo de ejemplo, usar una hoja de cálculo, descargar e instalar un nuevo software), y el nivel de habilidades informáticas es todavía demasiado bajo "Avanzado" (https://itu.foleon.com/itu/measuring-digital-development/resources/).

Ciudad Segura
Tecnología y seguridad pública

Por Vittoria Pistone

1. Ciudad inteligente y ciudad segura: conceptos y definiciones

El término “ciudad inteligente” tiene contornos borrosos y se presta a una gran variedad de usos, no siempre coherentes con el resultado. De hecho, no existe una expresión que pueda ofrecer una imagen completa del concepto, ni una definición válida para todos los estudiosos del fenómeno[145].

En la literatura, sin embargo, la ciudad inteligente suele definirse como: “la ciudad en la que las inversiones en capital humano y social y las tecnologías de la información y la comunicación (TIC) tradicionales y modernas impulsan un crecimiento económico sostenible y una alta calidad de vida, con una gestión prudente de los recursos naturales a través de una *governance* participativa”[146].

Algunos de los principales rasgos que caracterizan a la ciudad inteligente, identificados en la literatura dominante[147], convergen en la definición adoptada por la Comisión Europea, que entiende la ciudad inteligente como “el lugar donde las redes y los servicios tradicionales se hacen más eficientes mediante el uso de las tecnologías digitales y de la información y la comunicación (TIC)”[148].

El objetivo, según la Comisión, es utilizar las tecnologías para hacer un uso más sostenible de los recursos, reducir las emisiones nocivas, mejorar las infraestructuras urbanas y disponer de espacios públicos más seguros, mediante una *governance* promovida por las administraciones locales más interactivas y sensibles a las necesidades de la población.

Las definiciones muestran la importancia que se da al uso de las tecnologías de la información y la comunicación para el desarrollo y el funcionamiento de las ciudades inteligentes. Luciano Floridi señala hasta qué punto las TIC son un recurso esencial e indispensable para las sociedades actuales y futuras, e identifica una nueva etapa de la historia en la reciente relación de interdependencia entre el ser humano y

---

[145] Albino, Vito - Berardi, Umberto - Dangelico, Rosa M., *Smart Cities: Definitions, Dimensions, Performance, and Initiatives*, “Journal of Urban Technology”, vol. 22, fasc. 1, 2015, p. 3 a 21.

[146] Lacinák, Maroš - Ristvej, Jozef, *Smart city, Safety and Security*, “Procedia Engineering”, vol. 192, 2017, p. 522 a 527, www.sciencedirect.com.

[147] Ibidem.

[148] https://ec.europa.eu.

la tecnología. En sus palabras, la transición de la era de la historia a la de la hiperhistoria[149].

El uso de la innovación tecnológica en el contexto urbano, como se ha mencionado anteriormente, está dedicado a la consecución de objetivos destinados a mejorar la vida global del ciudadano. El uso de la innovación tecnológica en el contexto urbano, como se ha mencionado anteriormente, está orientado a la consecución de objetivos que pretenden mejorar la vida global del ciudadano.

A pesar de que en algunos estudios sobre el fenómeno de las ciudades inteligentes a veces se infravalora el ámbito de la seguridad pública, hay quienes, partiendo de la jerarquía de necesidades de Maslow, coinciden en que la seguridad es uno de los componentes cruciales para elevar la calidad de vida urbana y que, por tanto, se puede decir que toda ciudad inteligente es también una ciudad segura[150].

De forma aún más decisiva, otros autores consideran que la ciudad segura es una de las condiciones fundamentales y necesarias para la realización de una ciudad inteligente[151].

Entendiendo la interconexión entre los conceptos de ciudad inteligente y ciudad segura, que podríamos definir como ontológicamente interdependientes, es posible definir una ciudad segura como: "una ciudad en la que el uso de hardware y software, junto con la *governance* de la seguridad, permite salvaguardar de la mejor manera posible la seguridad de la población, minimizando la delincuencia y respondiendo con prontitud a las amenazas inesperadas al orden público, como la propagación de pandemias".

Por ello, la organización de la ciudad segura debe incluir las siguientes características: sistemas inteligentes de seguridad para la vigilancia, búsqueda, detección e identificación de posibles delincuentes, sistemas de alerta, seguimiento y previsión de emergencias sanitarias y medioambientales, *governance* participativa para la gestión de la seguridad urbana, unidades policiales centralizadas y sistema integrado de rescate, conexión segura a Internet y protección de datos, así como gestión inteligente del tráfico[152].

2. Un modelo italiano de governance de la seguridad pública

El análisis realizado en el apartado anterior revela la centralidad de la *governance* como principal característica de la ciudad segura. Amenazas como el terrorismo, la inmigración ilegal y, más recientemente, la necesidad de atención sanitaria

---

[149] Floridi, Luciano, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, Cortina, 2017, p. 2 a 20.

[150] Lacinák - Ristvej, *Smart city, Safety and Security*, "Procedia Engineering", vol. 192, 2017, p. 522 a 527, www.sciencedirect.com.

[151] Ristvej, Jozef - Lacinák, Maroš - Ondrejka, Roman, *On Smart City and Safe City Concepts*, "Mobile Networks and Applications", vol. 25, 2020, p. 836 a 845, www.springer.com.

[152] Ibidem.

ha llevado a los legisladores a ocuparse de la seguridad pública. El legislador italiano también sintió esta necesidad.

Para los desarrollos resultantes en términos de *governance* e innovación de los sistemas de vigilancia, un papel destacado sigue siendo el decreto-legge 14 de 20 de febrero de 2017, intitulado "Disposizioni urgenti in materia di sicurezza delle città"[153].

El decreto tiene por objeto poner en práctica las formas de coordinación entre los distintos niveles territoriales, previstas en el art. 118, párrafo 3, de la Constitución italiana, que esboza el paradigma de la seguridad integrada. Además de la competencia exclusiva del Estado en materia de orden público y seguridad, el decreto refuerza el papel de las administraciones locales, mediante la previsión de los llamados pactos para la aplicación de la seguridad urbana, en los que alcaldes y prefectos desempeñan un papel primordial[154].

Además, junto a ellos se creará un comité metropolitano cuya función es analizar, evaluar y debatir los problemas de seguridad urbana y fomentar la más amplia participación de los actores públicos y privados en el debate[155].

El legislador también da un amplio espacio al uso de la tecnología y, para ello, promueve la interconexión de las salas operativas de las policías locales, con especial atención al uso común de los sistemas tecnológicos de seguridad, esperando una mayor competencia de los operadores en el campo de la innovación tecnológica y promoviendo la instalación de nuevas cámaras de vídeo que se integren con las ya existentes para una completa cartografía de las ciudades[156].

Con este último fin, durante la conversión del decreto en ley, se añadió el apartado 1 bis al art. 7 del decreto, que anima a los particulares (por ejemplo, condominios y empresas) a instalar sistemas de vigilancia, equipados con software de análisis de vídeo con envío automático de alarmas a las comisarías[157].

Esta aportación legislativa pretende, por tanto, ampliar el control ambiental de la ciudad y reducir el gasto público necesario para actualizar los sistemas de videovigilancia existentes[158].

En aplicación de las disposiciones legislativas, según la "Relazione del Ministero dell'Interno sulle performance per l'anno 2019", se han firmado varios acuerdos y

---

[153] D.L. 20 febbraio 2017, n° 14 "*Disposizioni urgenti in materia di sicurezza delle città*", convertido con modificación con L. 18 aprile 2017, n° 48, y modificado L. 1° dicembre 2018, n° 132, www.gazzettaufficiale.it.

[154] D.L. 14/2017, art. 5.

[155] D.L. 14/2017, art. 6.

[156] L. 18 aprile 2017, n° 48 titulada "Conversione in legge, con modificazioni, del decreto-legge 20 febbraio 2017, n° 14, recante disposizioni urgenti in materia di sicurezza della città", www.gazzettaufficiale.it.

[157] Ibidem. La ley también prevé deducciones del impuesto municipal o de la tasa por servicios indivisibles en favor de quienes soportan los costes de la inversión.

[158] L. 18 dicembre 2018132 autorizó, para el año 2020, un gasto de 17 millones de euros para la adquisición de nuevos equipos de videovigilancia, www.interno.gov.it.

pactos para el fomento de la seguridad integral, además de otras iniciativas, como los protocolos de legalidad y los memorandos de entendimiento de "control de vecindad"[159].

El legislador italiano, a través del modelo de *governance* de la seguridad esbozado, confirma la centralidad de crear ciudades inteligentes que sean ante todo ciudades seguras, dotadas de una adecuada gestión de la seguridad urbana y de un mayor uso de la tecnología a través del incremento de los sistemas de videovigilancia, la interconexión de las salas de operaciones de las comisarías, la formación profesional de los operadores y, sobre todo, el ensayo de herramientas adicionales de seguimiento de la delincuencia.

3. Tecnologías para la seguridad urbana: la "new surveillance"

El ambicioso objetivo de crear ciudades seguras ha generado un verdadero "enamoramiento" tecnológico, en cuya onda, desde hace varios años, las administraciones públicas y las fuerzas policiales recurren cada vez más al uso de programas y dispositivos innovadores para hacer frente a los problemas de seguridad y desorden urbano.

El proceso de integración entre la informática y las telecomunicaciones, a través de las tecnologías de la información y la comunicación, ha aumentado la capacidad de los agentes de policía de ver, oír, reconocer, almacenar, conservar, cruzar, verificar, analizar y comunicar datos[160].

Por un lado, las nuevas tecnologías han ampliado la cantidad de informaciones disponible para los operadores, y por otro, mediante el uso de sistemas TIC, han permitido un acceso más rápido y sencillo a los datos, mayores posibilidades de almacenamiento y una mayor capacidad de análisis de estos[161].

En cuanto a la videovigilancia, que es especialmente popular, cabe señalar que en las últimas décadas se ha pasado de los sistemas analógicos a los digitales. Este cambio ha permitido integrar la grabación con herramientas de software para el tratamiento de la señal de vídeo, lo que ha tenido un impacto significativo en las actividades de control[162].

Entre estas herramientas de software, las más conocidas son los detectores de movimiento, el reconocimiento óptico de caracteres y el reconocimiento facial. Dado que se trata de instrumentos tecnológicos relativamente dúctiles, conviene precisar aquí su uso para la seguridad urbana.

---

[159] Ministero dell'interno, "Relazione sulla performance", 2019, www.interno.gov.it.

[160] A este respecto, se hace referencia a los comentarios de Nobli, Gian G., *Le politiche di sicurezza urbana in Italia: lo stato dell'arte e i nodi irrisolti*, "SINAPPSI-Connessioni tra ricerca e politiche pubbliche", vol. 2, 2020, p. 120 a 137.

[161] Ivi. p. 123.

[162] Ibidem.

El detector de movimiento es capaz de reconocer automáticamente situaciones de peligro, predefinidas por el usuario del sistema. Una vez identificado el riesgo (identificado, por ejemplo, como un movimiento específico), el software activa la conexión con el centro de operaciones de la policía, envía alarmas e imágenes y, si es necesario, activa las grabaciones o guarda las realizadas cíclicamente[163].

En la actualidad, la investigación pretende perfeccionar el detector de movimiento hasta el punto de que sea capaz de leer los movimientos más imperceptibles del cuerpo humano, de modo que incluso las acciones microcriminales, como el paso de drogas, puedan identificarse a través de los vídeos de las cámaras de seguridad[164].

También existe un software que puede dirigir las unidades de grabación de vídeo hacia fuentes de sonido reconocidas como peligrosas. Las cámaras panorámicas e inclinadas no sólo son "ojos", sino también "oídos inteligentes"[165].

El reconocimiento óptico de caracteres (OCR) es un software muy versátil, que se utiliza para clasificar el correo, leer cheques bancarios, verificar firmas, procesar automáticamente documentos impresos y como ayuda para los invidentes. En las actividades de vigilancia se utiliza para el reconocimiento automático de matrículas[166].

En las ciudades inteligentes italianas, como Milán, esta tecnología está especialmente en desarrollo por las ventajas que aporta en materia de tráfico, prevención y lucha contra las infracciones[167].

El reconocimiento facial, que utiliza una aplicación informática para analizar el rostro con el fin de definir o verificar la identidad personal, es una tecnología muy probada y debatida[168].

El reconocimiento facial es una herramienta valiosa en la lucha contra la delincuencia, ya que ayuda a las fuerzas del orden a reconocer, aunque con un margen de error, a los sujetos señalados como peligrosos entre los rostros captados por las cámaras de videovigilancia, a localizar a los fugitivos entre la multitud y a identificar a los terroristas que entran en el país. Más recientemente, el reconocimiento facial también se ha utilizado para contener el virus Covid-19, ya que es capaz, con suficiente precisión, de identificar a las personas que llevan mascarillas y, si se conecta a un sensor

---

[163] Ivi. p. 124.

[164] Mi, Yang - Zhang, Xingyuan et.al, *Dual-Branch Network with a Subtle Motion Detector for Micro Action Recognition in Videos*, "Ieee Transaction on Image processing", vol. 29, 2020, p. 1 a 99.

[165] Nobli, *Le politiche di sicurezza urbana in Italia*, cit., p. 123.

[166] Islam, Norman - Islam, Zeeshan - Noor, Nazia, *A Survey on Optical Character Recognition System*, "Journal of Information & Communication Technology-JICT", vol. 10, fasc. 2, 2016, p. 1 a 4.

[167] È stato siglato il protocollo d'intesa tra la questura e la polizia locale di Milano per la definizione delle modalità di gestione e di impiego della lettura targhe al sistema di videosorveglianza cittadina, www.comune.milano.it.

[168] Hamann, Kristine - Smith, Rachel, *Facial recognition technology*, "Criminal Justice", vol. 34, fasc. 1, 2019, p. 1 a 9.

para medir la temperatura corporal, de averiguar si la temperatura es de 38° o superior[169].

Un software diferente para la prevención de la delincuencia que se ha probado recientemente es Sweetie 2.0. Un bot de chat, utilizado por la organización de defensa de los derechos de los niños, Terre des Hommes (Países Bajos), en su evolución más reciente, casi completamente autónomo, para identificar a posibles pedófilos en la red[170]. Más concretamente, un personaje virtual, con las características de una niña filipina de diez años, identifica y recoge activamente información sobre sujetos potencialmente interesados en el turismo sexual infantil por webcam[171].

El entusiasmo con el que se ha acogido esta técnica de vigilancia y prevención de la delincuencia ha llegado a un punto muerto, sobre todo en los sistemas jurídicos europeos, como el italiano, en los que lo relevante penalmente es la acción delictiva y no la mera intención delictiva[172].

Este breve examen de algunos de los instrumentos más conocidos al servicio de la seguridad pública pone de manifiesto el grado de impacto de la tecnología en las actividades de vigilancia y el profundo cambio que se ha producido en cuanto al ámbito de aplicación, la omnipresencia, la eficacia y los riesgos que conlleva.

Gary T. Marx fue el primero en darse cuenta de este cambio. En 1986 resumió en nueve puntos las características que distinguen la nueva vigilancia de la tradicional[173].

Para resumir el pensamiento del autor, la vigilancia trasciende hoy en día la distancia, la oscuridad y las barreras físicas, ya que las nuevas tecnologías han permitido superar aquellos límites técnicos que impedían extender la vigilancia tanto fuera de las fronteras del Estado-nación como dentro de la vida íntima de los individuos, con la consecuencia de que la imposibilidad y la ineficacia técnicas ya no pueden considerarse como protectores, aunque incidentales, de la libertad y la privacidad[174].

A estas características podría añadirse la implicación directa del ciudadano en la actividad de vigilancia, un factor que parece predominar en la vigilancia actual.

---

[169] Ibidem.

[170] Siegel, Dina - Senol Sert, Deniz - Pacek, Małgorzata, *Towards a Better Future: Human Rights, Organized Crime and Digital Society*, International Scientific Conference, Center for Scientific Research at the Faculty of Law, Kiev- Bitola, 2020, p. 148 a 150.

[171] Schemer, Bart W. - Georgieva, Ilina - Van Der Hof, Simonem et al., *Legal aspects of Sweetie 2.0*, Leiden-Tilburg, Tilt, 2016, p. 148.

[172] Ibidem.

[173] La vigilancia tradicional se refiere a todas las técnicas de control caracterizadas por una actividad humana total o predominante (acecho, controles postales, colaboración con personas cercanas a la persona vigilada, etc.).

[174] Marx, Gary T., *The Iron Fist and the Velvet Glove: Totalitarian Potentials Within Democratic Structures*, 1986, http://web.mit.edu/gtmarx/www/iron.html.

Un ejemplo de ello son las ciudades inteligentes de China, en las que la vigilancia combina enfoques automatizados y manuales, utilizando por igual el capital humano y el tecnológico[175].

Así lo demuestra la reciente evolución del programa de vigilancia urbana Sharp Eyes, que confirma no sólo la omnipresencia de los actuales sistemas de vigilancia, sino también la tendencia a requerir la colaboración directa de los ciudadanos en la realización de actividades de control.

En la ciudad de Linyi, donde se originó el programa, se han instalado decodificadores de televisión por cable para que los ciudadanos puedan denunciar a distancia los delitos a través de sus televisores domésticos. Por ello, esta nueva versión de Sharp Eyes se anunció con el eslogan "mando a distancia en la mano, seguridad en el corazón"[176].

También confirma esta tendencia la ciudad de Jackson (Misisipi), donde los gobiernos locales han adoptado, a modo de prueba, un programa de vigilancia urbana que permite a los agentes utilizar cámaras de seguridad privadas y timbres inteligentes, accediendo al contenido en tiempo real y directamente desde el centro de operaciones de la policía[177].

Por lo tanto, podría decirse que, en la ciudad estadounidense, el ciudadano contribuye a la vigilancia aportando únicamente capital tecnológico, mientras que en la ciudad china, no sólo aporta dispositivos sino también actividad humana, lo que da lugar a una participación proactiva en la vigilancia urbana.

A la luz de las tecnologías disponibles y el consiguiente cambio en los sistemas de vigilancia, el debate actual sobre la seguridad pública no puede separarse de las reflexiones sobre el potencial y los riesgos que conlleva. La mayor seguridad de las ciudades seguras tiene como contrapartida la amenaza de una reducción de los derechos y libertades de los ciudadanos. Este riesgo se percibe no sólo en las grandes metrópolis chinas o americanas, sino también en las modernas e inteligentes ciudades europeas.

4. Límites europeos al uso de tecnologías para la seguridad pública

La necesidad de garantizar la seguridad mediante el uso de tecnología, como ya se ha mencionado, tampoco deja indiferente a Europa, que comparte con China y Estados Unidos la ambición de crear verdaderas ciudades seguras. De hecho, se han

---

[175] Peterson, Dahlia, *Designing Alternatives to China's Repressive Surveillance State*, "Center for Security and Emerging Technology", 2020, p. 1 a 31, https://cset.georgetown.edu/ publication/designing-alternatives-to-chinas-repressive-surveillance-state.

[176] Ibidem.

[177] www.nbcnew.com y www.eff.org/deeplinks/2020/11.

puesto en marcha programas de vigilancia masiva en Francia, Alemania y Gran Bretaña, que se considera uno de los países más vigilados del mundo[178].

En lo que respecta al desarrollo y la difusión de la tecnología, la Unión Europea parece adoptar un enfoque basado en el riesgo y en la centralidad del ser humano y el respeto a la intimidad y la dignidad[179].

Por otro lado, el tratamiento de datos biométricos, incluidas las imágenes faciales, podría atentar contra la dignidad humana al restringir la libertad de expresión, manifestación y asociación en los espacios públicos. Al estar sometido a continuas actividades de vigilancia, el famoso "Hermano Mayor", de hecho, corre el riesgo de comprometer la libertad de autodeterminación, una libertad fundamental para que se respete la inviolabilidad de la dignidad humana, tal como se establece en el art. 1° de la Carta de los Derechos Fundamentales de la UE.

También se utiliza un marco (basado en el riesgo) en relación con el uso de la tecnología para la seguridad pública, como demuestra el debate sobre el reconocimiento facial. De hecho, el debate en curso afecta directamente a Italia también, en la medida en que el reconocimiento facial parece estar actualmente en la disponibilidad operativa de las Fuerzas de Policía (por ejemplo, el Sistema de Reconocimiento Automático de Imágenes)[180].

La Agencia de Derechos Fundamentales de la Unión Europea ha señalado que el uso de esta tecnología conlleva el riesgo de que se violen la libertad de expresión, la libertad de reunión, el derecho a la no discriminación, la protección de los datos personales y de la intimidad, los derechos del niño, el derecho a una buena administración y la tutela judicial efectiva[181].

Estas preocupaciones han sido reiteradas por la Comisión Europea, que en su Libro Blanco sobre Inteligencia Artificial destaca los límites del tratamiento de datos biométricos con el fin de identificar de forma única a una persona física. De acuerdo con el GDPR y la directiva 2016/680, dicho tratamiento solo se permite por razones de interés público, si se lleva a cabo sobre la base del derecho de la Unión o del Estado miembro y está debidamente justificado, proporcionado y sujeto a garantías adecuadas[182].

El Consejo de Europa ha confirmado recientemente este enfoque basado en la evaluación del riesgo para el uso de tecnologías (como el reconocimiento facial) con fines de seguridad. En sus Directrices 2021, recomienda la promulgación de una

---

[178] Christakis, Theodore - Bouslimani, Katia, *National Security, surveillance, and human rights*, "Handbook on The International Law of Global Security", 2020, https://ssrn.com/abstract=3599994.

[179] European Commission, *White paper on Artificial intelligence*, Bruxelles, febrero 2020, https://ec.europa.eu.

[180] Pierre Paliotta, Achille, *Le politiche innovative di sicurezza nelle città tra tecnologie di riconoscimento e smart cities*, "SINAPPSI - Connessioni tra ricerca e politiche pubbliche", vol. 10, fasc. 2, 2020, p. 98 a 119.

[181] European Union Agency for Fundamental Rights, *Facial recognition technology fundamental rights considerations in the context of law enforcement*, 2019, https://fra.europa.eu.

[182] European Commission, *White paper on Artificial Intelligence*, cit.

legislación *ad hoc* que defina los parámetros que deben seguir las fuerzas del orden para crear la base de datos y desplegar el software sobre el terreno. Debido a la omnipresencia de esta tecnología, los organismos encargados de la aplicación de la ley deberían estar obligados a justificar la necesidad y la proporcionalidad de su uso en función de una serie de factores, como el lugar y el momento en que se utiliza la tecnología[183].

Así lo reitera la "Propuesta de Reglamento del Parlamento Europeo y del Consejo por lo que se establecen normas armonizadas en materia de inteligencia artificial (Ley De Inteligencia Artificial) y Se Modifican Determinados Actos Legislativos De La Unión", firmada en Bruselas el 21 de abril de 2021, cuyo objetivo es definir un marco jurídico uniforme para garantizar el desarrollo, la comercialización y la utilización de la inteligencia artificial de acuerdo con los valores del ordenamiento jurídico de la Unión Europea[184].

La propuesta de reglamento para establecer normas armonizadas también se ha beneficiado del trabajo del Grupo de Expertos de Alto Nivel sobre la IA y de las directrices que este grupo ha elaborado en materia de *Trustworthy AI* (8 de abril de 2019). Antes de su aprobación, la propuesta también se sometió a una evaluación de impacto por parte del Consejo de Control Reglamentario de la Comisión[185].

El largo trabajo que ha precedido a la elaboración de la propuesta confirma lo difícil que es para las instituciones crear una disciplina que pretenda regular de forma eficaz y realista el fenómeno de la IA y que, al mismo tiempo, sea capaz de equilibrar con precisión los diferentes intereses y concepciones. Si, por un lado, la legislación no debe inhibir la investigación y el desarrollo de la IA, para la que Europa espera inversiones económicas de 20.000 millones de euros, por otro, está llamada a afirmar y consolidar los principios del Estado de derecho; también debe ser flexible y adaptable a los cambios tecnológicos y a la rápida evolución que caracteriza a la tecnología, garantizando al mismo tiempo el grado de certidumbre y previsibilidad necesario para un ámbito tan estratégico y sensible. Por último, debe inhibir los posibles abusos en el uso de la IA (*abusus non tollit usum*), pero saber explorar con audacia dominios nuevos y beneficiosos, promoviendo y reforzando los derechos fundamentales de las personas y la salud de nuestro propio planeta[186].

Para alcanzar este ambicioso objetivo, la Comisión ha recurrido al instrumento reglamentario, que es el más adecuado para garantizar unas limitaciones uniformes y

---

[183] Council of Europe, *Guidelines on Facial Recognition. Consultative Committee of The Convention for The Protection of Individuals with Regard to Automatic Processing of Personal Data*, enero 2021, https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3.

[184] Propuesta de Reglamento del Parlamento Europeo y del Consejo por lo que se establecen normas armonizadas en materia de inteligencia artificial, Bruxelles, 2021, https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0006.02/DOC_1&format=PDF.

[185] Casonato, Carlo - Marchetti, Barbara, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale,* "BioLaw Journal", n° 3, septiembre, 2021, www.biodiritto.org/Pubblicazioni/BioLaw-Journal, p. 415 a 443.

[186] Ibidem.

directamente aplicables en todo el territorio de la Unión, estableciendo un marco reglamentario homogéneo y básicamente rígido para los Estados miembros.

Además de la uniformidad del marco normativo, también se hace hincapié en las características específicas de la IA, que dan forma a toda la normativa. Aunque el término "inteligencia artificial" se utiliza desde hace casi 70 años, no ha surgido ninguna definición universalmente aceptada[187]. La IA suele describirse, en términos generales, como cualquier software capaz, para un conjunto determinado de objetivos definidos por el ser humano, de generar resultados que influyan en el entorno con el que el mismo software interactúa. En realidad, la IA engloba técnicas y aplicaciones muy diferentes, cuyo funcionamiento se caracteriza por un grado variable de autonomía, imprevisibilidad y transparencia de los resultados, así como por diferentes niveles de riesgo[188].

Para comprender mejor la heterogeneidad de los sistemas de IA, conviene referirse, a modo de ejemplo, a los siete macroámbitos de los modelos de IA identificados por Ebers, a saber: "Autonomous Systems", "Patterns and Anomalies", "Hyperpersonalization", "Recognition", "Human Interaction", "Predictive Analytics", "Goal-driven system"[189].

Así, para adaptar la normativa a la ductilidad de la IA, la Comisión ha adoptado una clasificación de los sistemas de inteligencia artificial subdividida por clases de riesgo, confirmando el enfoque basado en el riesgo ya afirmado anteriormente en el marco institucional europeo.

El texto distingue, de hecho, diferentes niveles de riesgo relativos a las prácticas de IA, que pueden dividirse en cuatro categorías: *1*) riesgos inaceptables (Título II); *2*) riesgos elevados (Título III); *3*) riesgos limitados (Título IV); *4*) riesgos mínimos (Título IX)[190].

En cuanto al uso de la tecnología con fines de seguridad pública, lo importante es lo que dice el art. 5, letra d: la disposición prohíbe el uso de determinados sistemas biométricos "en tiempo real" en espacios accesibles al público por parte de las fuerzas del orden. Un ejemplo de este sistema podría ser una red de CCTV a gran escala combinada con un software de reconocimiento facial.

Su uso sólo se permite en casos específicos como: "la búsqueda selectiva de posibles víctimas de delitos específicos, incluidos los niños desaparecidos"; la "prevención de una amenaza específica, sustancial e inminente para la vida o la integridad física o de un atentado terrorista"; y la "detección, localización, identificación o

---

[187] Ebers, Martin, *Liability for Artificial Intelligence and EU Consumer Law*, "JIPITEC", n° 12, 2021, www.jipitec.eu/about-the-journal.

[188] Casonato - Marchetti, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale,* cit.

[189] Ibidem.

[190] Veale, Michael - Borgesius, Frederik, *Demystifying the Draft EU Artificial Intelligence Act. Analysing the good, the bad, and the unclear elements of the proposed approach*, "Computer Law Review International", 2021, www.degruyter.com/journal/key/cri/html.

enjuiciamiento" de un delincuente o sospechoso de un delito con una pena máxima de al menos tres años que permita la emisión de una Orden de Detención Europea[191].

Además, el uso de la IA debe medirse en función de la gravedad, la probabilidad y el alcance del daño causado no sólo por la no utilización del sistema, sino también por las consecuencias para los derechos y las libertades de todas las personas afectadas que se derivan del uso del sistema.

De ello se desprende que la autoridad judicial o administrativa competente emitirá la autorización de uso del sistema de inteligencia artificial sólo después de haber comprobado, sobre la base de pruebas objetivas, que la utilización del sistema de identificación biométrica a distancia "en tiempo real" es necesaria y proporcionada a la consecución de uno de los objetivos, a la situación para la que se solicita su uso y a las consecuencias que se derivan del mismo.

Del examen de la disposición se desprende que las excepciones a la prohibición se caracterizan por un cierto grado de vaguedad, lo que permite un considerable margen de maniobra al Estado y a sus autoridades, que están llamados a valorar, por ejemplo, si existen consecuencias perjudiciales derivadas del uso del reconocimiento facial y si éstas son de tal magnitud que justifiquen su uso, o si la valoración de la fiabilidad es proporcionada en relación con la conducta observada. La presencia de conceptos indeterminados e interpretables implica flexibilidad en la aplicación y, por tanto, margen de maniobra para los Estados miembros. Por otro lado, en ausencia de prácticas comunes de aplicación, el riesgo es que esta vaguedad también genere incertidumbre[192].

El enfoque *risk-based* no es la única característica que se desprende predominantemente de la lectura de la "Ley de IA"; de hecho, también se da amplio espacio a las obligaciones de transparencia y supervisión humana del funcionamiento de la IA. El considerando 47 y el apartado 1 del art. 13 establecen que los sistemas de IA de alto riesgo deben diseñarse y desarrollarse de forma que su funcionamiento sea comprensible para los usuarios. Éste debe ser capaz de: *a*) interpretar el resultado del sistema, y *b*) utilizarlo adecuadamente de forma que favorezca al individuo respetando las obligaciones de supervisión humana establecidas en los apartados 4 y 5 del art. 14[193].

Obligaciones que se vuelven aún más estrictas cuando el uso de la IA permite la identificación biométrica a distancia de las personas en tiempo real y a posteriori, para lo cual se exige que cada decisión sea verificada y confirmada por al menos dos supervisores[194].

---

[191] Propuesta de Reglamento del Parlamento Europeo y del Consejo por lo que se establecen normas armonizadas en materia de inteligencia artificial, cit.

[192] Casonato - Marchetti, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, cit.

[193] Sovrano, Francesco - Sapienza, Salvatore et al., *A Survey on Methods and Metrics for the Assessment of Explainability under the Proposed AI Act*, 2021, https://arxiv.org/abs/2110.11168v1.

[194] Casonato - Marchetti, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, cit.

Por lo tanto, es de agradecer que la “Ley de IA” haya previsto la planificación y el desarrollo de los sistemas de IA de manera que se garantice una supervisión humana eficaz destinada a prevenir y minimizar cualquier riesgo para la salud, la seguridad u otros derechos fundamentales.

Un análisis de algunos de los puntos más destacados de la propuesta muestra la intención de crear un equilibrio entre los instrumentos de apoyo y las medidas para garantizar los derechos fundamentales[195].

Desde un punto de vista crítico, se ha observado que la generalidad de las cláusulas, algunas de las cuales son herencia de experiencias normativas anteriores, requerirá una ardua tarea de interpretación para no comprometer la uniformidad de aplicación y no socavar los objetivos de armonización y certidumbre jurídica en los que se basa la fiabilidad del uso de la tecnología y sin los cuales se desencadenarían conflictos jurídicos insostenibles[196].

No se puede obviar que han surgido y surgirán otras cuestiones críticas en caso de que el reglamento entre en vigor. No obstante, se trata de una primera intervención que muestra un compromiso institucional encomiable, aunque perfectible, y un reto para los juristas y la clase dirigente de la *millennial generation*.

[195] Ibidem.

[196] Ibidem.

EDITORIAL ASTREA

Hate speech: brevi note su un percorso articolato tra la libertà di pensiero e il deplatforming

Por Alessandro Picarone

Introduzione

La libertà di manifestazione del pensiero merita di essere considerata come la "pietra angolare" di una democrazia[197]: ne consegue che qualunque interferenza con essa può comportare una indebita compressione di un diritto fondamentale costituzionalmente tutelato.

Tuttavia, esistono determinati ambiti in cui si può valutare se sia opportuna (se non addirittura auspicabile) una limitazione, che in questo caso non sarebbe da considerarsi impropria: il riferimento è ai discorsi d'odio[198] mentre non vi è dubbio sul fatto che non si possa effettuare alcuna limitazione sulla base di motivazioni etniche o sessuali o religiose.

Il primo punto da approfondire è relativo alla responsabilità delle piattaforme, tenendo conto soprattutto dell'evoluzione sociale e tecnologica, che potrebbe mettere in questione l'assunto per cui, con la c.d. *Good Samaritan clause*[199], sarebbe sensato esentare i proprietari delle piattaforme *web* dalla responsabilità dei contenuti condivisi dagli utenti. Da un lato, non si deve dimenticare che Facebook ha natura privata, ma dall'altro, l'esercizio privato di tale potere può essere potenzialmente pericoloso.

In fondo, si pensi al caso in cui un personaggio politico (come nel caso del Presidente Trump, qui in analisi) o in generale un personaggio noto, venga escluso da una o più piattaforme *social*: da un lato, potrà senza dubbio continuare a esprimersi ma, d'altro canto, la sua possibilità di comunicare sarà ridotta.

Ulteriormente ci si deve interrogare relativamente all'esenzione di responsabilità delle piattaforme rispetto ai contenuti condivisi dagli utenti: quest'ultima non ottiene l'effetto sperato di tutelare la manifestazione del pensiero ma, anzi, fa scaturire la conseguenza opposta di autorizzare le piattaforme a decidere se, come e

---

[197] Cfr. Corte Costituzionale, sent. 84/1969, in www.giurcost.org/decisioni/1969/0084s-69.html.

[198] Sulla sua tollerabilità in nome della libertà di manifestazione del pensiero, e sul confine tra pensiero legittimo e "odioso": Monti, Matteo, *Libertà di espressione e* hate speech *razzista: un'analisi mediante le categorie di* speakers, in https://dirittifondamentali.it, 9/7/15.

[199] Cfr. www.congress.gov/bill/104th-congress/senate-bill/314/. Nell'Unione Europea la norma è stata sostanzialmente riprodotta negli art. 12-15 della Direttiva 2000/31/EU (cfr. GUCE, *Direttiva 2000/31/CE sul commercio elettronico*, L. 178, del 17 luglio 2000, al link https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32000L0031&from=IT).

Più recentemente, con il *Digital Service Act* (https://ec.europa.eu/info/sites/info/files/proposal_for_a_regulation_on_a_single_market_for_digital_services.pdf) la Commissione europea mira a sottrarre alle piattaforme il potere di operare scelte potenzialmente in grado di condizionare l'esercizio di diritti fondamentali.

quando intervenire. Il problema non è di poco conto, se si considera che possono sussistere molte situazioni intermedie, nelle quali i pensieri espressi sono sgraditi ai gestori della piattaforma, pur non essendo illeciti. Inoltre, non va dimenticato che è bene che sia una autorità terza e indipendente a sancire che un fatto sia contrario a una norma vigente che esplicitamente lo vieti.

Più nello specifico, e con riferimento alle motivazioni del *deplatforming* di Donald Trump, sono molte le riflessioni che l'evento ha generato: principalmente, ci si deve domandare se sia una censura quella subita Trump, che, contestualmente, porta alla domanda *quis custodiet custodes*[200]?

Oltre alla possibilità di comprimere la libertà di manifestazione del pensiero, diviene fondamentale soprattutto individuare il soggetto, e i motivi che legittimamente lo autorizzerebbero a comprimere un diritto costituzionalmente tutelato[201].

In tale contesto, occorre approfondire la dicotomia pubblico-privato: il rischio da valutare è una possibile commistione dell'interesse pubblico con quello privato, in modo che quest'ultimo possa sfruttare grandi risorse economiche e tecnologiche per interferire con le scelte della vita pubblica. Quindi, quale prospettiva è più utile attuare?

1. Hate speech e responsabilità: la Good Samaritan clause

L'*hate speech*[202] va inteso come ogni forma di incoraggiamento o giustificazione dell'ostilità e dell'intolleranza contro persone o gruppi in base a fattori come l'etnia[203], l'età, il genere, l'orientamento sessuale e la religione[204].

Sebbene in tema di dibattito politico, un primo punto fermo proviene dalla giurisprudenza statunitense, la quale ha stabilito che il Primo emendamento non tutela

---

[200] Cfr. Giovenale, *Satire*, VI, 48-49, cit. in Platone, "Repubblica", III, 13.

[201] Attriti sottolineati in De Tullio, Maria F., *Uguaglianza sostanziale e nuove dimensioni della partecipazione politica*, Napoli, Editoriale Scientifica, 2020, p. 146 ss.

[202] Cfr. Caielli, Mia, *Punire l'omofobia: (non) ce lo chiede l'Europa. Riflessioni sulle incertezze giurisprudenziali e normative in tema di hate speech*, in "Genius. Rivista di studi giuridici sull'orientamento sessuale e l'identità di genere", 2 (1), p. 56 (p. 54-64). Si rimanda anche a Consiglio dell'Unione Europea, Decisione 008/913/GAI del Consiglio, sulla "lotta contro talune *forme ed espressioni di razzismo e xenofobia mediante il diritto penale*", del 23/11/08, in Guue, L 328, p. 55-58, del 6/12/08 in https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32008F0913&from=EN.

Con riferimento alla Corte Europea dei diritti dell'Uomo, cfr. T. McGonagle, *Freedom of Expression and Defamation. A study of the case law of the European Court of Human Rights*, Strasbourg, Ed. Onur Andreotti, 2016.

[203] Sulla distinzione tra etnia e razza: Gometz, Gianmarco, *L'odio proibito: la repressione giuridca dello hate speech*, in "Stato, Chiese e pluralismo confessionale", n° 32, 2017, www.statoechiese.it/contributi/lodio-proibito-la-repressione-giuridica-dello-hate-speech; Luzzati, Clau dio, *Princìpi e prìncipi. La genericità nel diritto*, Torino, Giappichelli, 2012 e Id., *La vaghezza delle norme. Un'analisi del linguaggio giuridico*, Milano, Giuffrè, 1990.

[204] Cfr. Raccomandazione del Comitato dei ministri del Consiglio d'Europa del 1997.

le espressioni oscene e calunniose che violano l'ordine pubblico, poiché queste "non sono parte essenziale di alcuna esposizione di idee"[205].

Anche alla luce delle recenti vicende legate a Donald Trump, ci si chiede quali possano essere i margini di intervento dei *social network* dinanzi ai discorsi d'odio, specie se pronunciati da chi riveste cariche pubbliche di rilievo.

Semplicisticamente, potrebbe essere possibile affermare che nel mondo *social* il gestore stabilisce le regole di casa propria, decidendo se e quando applicarle: la situazione, tuttavia, è più complessa e merita un'ulteriore analisi, a partire dal *Communication Decency Act*, che con la *Good Samaritan clause* offre una sorta di scudo legale ai proprietari delle piattaforme *web,* rispetto a quanto pubblicato *online* dagli utenti[206].

Questa regola, grazie alla quale è nato il *web* 2.0, fornisce carta bianca ai gestori dei *social* per intervenire in base agli interessi del momento, a prescindere dagli interessi collettivi. In sostanza, una regola nata per ampliare la libertà di manifestazione del pensiero ha affermato la legge del più forte economicamente, consentendo alle piattaforme di esercitare un "potere censorio tanto in nome proprio (sui messaggi che ritenevano dannosi per i propri profitti e/o la propria immagine), quanto in adesione alle richieste degli Stati autoritari, quanto, infine, nell'esercizio delle deleghe di sorveglianza che gli ordinamenti democratici sono stati via via indotti ad istituire, pur nella consapevolezza di non poterne controllare in modo soddisfacente le modalità di svolgimento"[207].

Nel maggio 2020, il dibattito sulla sezione 230[208] ha trovato una sponda con un *executive order*[209], che, nelle intenzioni del Presidente Trump, avrebbe equiparato le piattaforme *social* agli editori, rendendole responsabili per i contenuti pubblicati[210]: a tale modifica conseguirebbe un controllo dei contenuti più attento, ma più restrittivo, da parte degli stessi *social network*.

---

[205] Cfr. "Chaplinsky vs. New Hampshire", 315 U.S. 568 (1942), in https://supreme.justia.com/cases/federal/us/315/568/.

[206] Il testo recita: "nessun fornitore o utente di un servizio informatico interattivo dovrà essere trattato come l'editore o il responsabile di qualunque tipo di informazione pubblicata da un altro soggetto".

[207] Cfr. Manetti, Michela, *I nuovi diritti nascenti dal mercato: illusioni e delusioni*, in "Giurisprudenza Costituzionale", 6/12/19, p. 3383.

[208] Sula necessità di modificare tale previsione cfr. Keats Citron, Danielle - Wittes, Benjamin, *The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity*, University of Maryland Legal Studies Research Paper n° 2017-22, in https://ssrn.com/abstract=3007720. In Italia cfr. Allegri, Maria R., *Ubi social. Fondamenti costituzionali dei social media e profili giuridici della responsabilità dei provider*, Milano, Franco Angeli, 2018.

[209] www.whitehouse.gov/presidential-actions/executive-order-preventing-online-censorship.

[210] Cfr. Re, Albachiara, *Trump ha firmato un ordine esecutivo che potrebbe cambiare i* social network, in "Wired.it", del 29 maggio 2020, al link www.wired.it/attualita/politica/2020/05/29/trump-twitter-ordine-esecutivo/.

2. Il deplatforming di Trump e l'intervento dell'Oversight Board Charter

a. La decisione di Zuckerberg

Con un post apparso su Facebook[211], il 7 gennaio 2021, Mark Zuckerberg ha spiegato le ragioni del *ban* comminato al Presidente Trump: tuttavia non si è espresso su alcuni elementi fondamentali della questione.

Innanzitutto, nulla ha comunicato sulla definitività (o temporaneità) della sanzione e, in secondo luogo, non ha specificato se la decisione sia rivedibile o meno. In realtà, Nick Clegg, vice di Zuckerberg, in un suo post del 21 gennaio 2021[212], ha riferito che in attesa della decisione del *board* la sospensione sarebbe stata a tempo indeterminato.

A seguito del *ban*, Donald Trump ha richiesto un intervento dell'*Oversight Board Charter*[213] che, al suo art. 2[214], prevede una propria determinazione quando dagli utenti viene richiesta una revisione della decisione presa da Facebook.

Precisiamo subito che vi sono forti dubbi su quale sia la vera finalità perseguita dalla istituzione del *Board* e sul fatto che questa coincida con i propositi dichiarati (cioè proteggere la libertà di espressione, con decisioni indipendenti[215]). Va considerato che il codice di condotta di Facebook[216] indica che i dipendenti devono agire nel miglior interesse del *social*: è lecito supporre, difatti, che con il mandato di Trump che all'epoca dei fatti era in scadenza, e ufficialmente per favorire la transizione pacifica con Biden,

---

211 Precisamente ha scritto: "We believe the risks of allowing the President to continue to use our service during this period are simply too great. Therefore, we are extending the block we have placed on his Facebook and Instagram accounts indefinitely and for at least the next two weeks until the peaceful transition of power is complete" (www.facebook.com/zuck/posts/10112681480907401).

212 Cfr. Clegg, Nick, *Referring Former President Trump's Suspension from Facebook to the Oversight Board*, 21 gennaio 2021 al link https://about.fb.com/news/2021/01/referring-trump-suspension-to-oversight-board/.

213 Cfr. Titcomb, James - Boland, Hannah, *Facebook's Oversight Board Expected to review Donald Trump's Suspension*, "The Telegraph", 12 gennaio 2021, al link www.telegraph.co.uk/technology/2021/01/12/facebooks-oversight-board-could-review-donald-trumps-suspension/ e Smith, Ben, *Trump Wants Back on Facebook. This Star-Studded Jury Might Let Him*, "New York Times", del 24 gennaio 2021, al link www.nytimes.com/2021/01/24/business/media/trump-facebook-oversight-board.html.

214 Il testo completo è: "in instances where people disagree with the outcome of Facebook's decision and have exhausted appeals, a request for review can be submitted to the board by either the original poster of the content or a person who previously submitted the content to Facebook for review", https://about.fb.com/wp-content/uploads/2019/09/oversight_board_charter.pdf.

215 www.facebook.com/notes/mark-zuckerberg/a-blueprint-for-content-governance-and-enforcement/10156443129621634/?hc_location=ufi.

216 https://investor.fb.com/corporate-governance/code-of-conduct/default.aspx.

vi sia stata una minore tolleranza l'atteggiamento è mutato in un *ban* forse perpetuo e senza certezze, né parametri, su un eventuale ulteriore cambio di decisione[217].

b. Le decisioni dell'*Oversight Board* e le ulteriori perplessità

Le aspettative sulla tempistica di una revisione del *Board* si attestano sui 90 giorni circa[218]: nel maggio 2021, l'*Oversight Board* ha confermato il *ban,* e quindi le limitazioni all'accesso dell'(ormai ex) Presidente Trump alla pubblicazione di contenuti sui suoi *account* Facebook e Instagram[219], le cui linee guida delle rispettive *community* erano state violate dagli elogi espliciti verso le persone coinvolte in atti di violenza (di fatto avallando gli attacchi a Capitol Hill).

Inoltre, la condivisione ripetuta di diverse *fake news* relative a presunti brogli elettorali mai dimostrati, né ipotizzabili, ha contribuito in modo determinante ad aumentare il clima di tensione: difatti, "al momento della pubblicazione dei post, c'era un chiaro e immediato rischio di violenze e le parole di Trump a supporto delle persone coinvolte nelle rivolte hanno legittimato le loro azioni violente. In qualità di Presidente, Trump aveva un elevato livello di influenza".

L'unica nota 'critica' rivolta da parte del *Board* è relativa alla "sospensione a tempo indeterminato come sanzione non aderente agli Standard e non definita dal punto di vista temporale". Mi pare un aspetto sostanziale: una limitazione, peraltro sancita da un soggetto privato e non dalla pubblica autorità, oltre che emanata in assenza di contraddittorio, non può affatto essere priva di una iniziale determinazione temporale.

La reazione di Facebook, nelle parole di Nick Clegg: "While these recommendations are not binding, we actively sought the board's views on our policies around political figures and will carefully review its recommendations"[220]. Da questa reazione, scaturisce una domanda naturale e, per certi versi, obbligatoria: le decisioni del *Board* sono vincolanti? In realtà, nella sua nota del 21 gennaio 2021, Clegg aveva sostenuto esattamente l'opposto: "It is an independent body and its decisions are binding - they can't be overruled by CEO Mark Zuckerberg or anyone else at Facebook"[221].

---

[217] Sempre nel post del 21 gennaio 2021, Clegg parla di "a US president actively fomenting a violent insurrection designed to thwart the peaceful transition of power … In making our decision, our first priority was to assist in the peaceful transfer of power".

[218] Cfr. *Facebook Oversight Board announces first six cases for review*, "Euronews", 1 dicembre 2020, al link www.euronews.com/2020/12/01/facebook-oversight-board-announces-first-six-cases-for-review.

[219] https://oversightboard.com/news/226612455899839-oversight-board-upholds-former-president-trump-s-suspension-finds-facebook-failed-to-impose-proper-penalty.

[220] Cfr. Clegg, Nick, *Oversight Board Upholds Facebook's Decision to Suspend Donald Trump's Accounts*, 5 maggio 2021 visibile al link https://about.fb.com/news/2021/05/facebook-oversight-board-decision-trump/.

[221] Cfr. Clegg, Nick, *Referring Former President Trump's Suspension from Facebook to the Oversight Board*, 21 gennaio 2021 al link https://about.fb.com/news/2021/01/referring-trump-suspension-to-oversight-board/.

3. Il ban su Twitter e la dicotomia privato-pubblico

Il *deplatform* di Trump ha riguardato anche Twitter, che ha spiegato: "we assessed the two Tweets referenced above under our Glorification of Violence policy, …and determined that they were highly likely to encourage and inspire people to replicate the criminal acts that took place at the U.S. Capitol on January 6, 2021"[222].

Ulteriori spunti di riflessione provengono dalle parole di Jack Dorsey[223], cofondatore di Twitter, secondo cui, pur riconoscendo di aver creato un precedente pericoloso, specifica di aver compiuto la migliore scelta per Twitter, anche se l'attenzione era finalizzata alla pubblica sicurezza[224].

Proprio su questo punto si concretizza il rischio: la contaminazione dell'interesse personale con quello pubblico, in modo che quest'ultimo viene coinvolto soltanto quando a rischio è l'interesse di pochi privati con risorse economiche, e tecnologiche, tali da poter anche influire sulla vita pubblica con le loro scelte.

A maggior ragione, non è consigliabile utilizzare una prospettiva esclusivamente privatistica, che consenta di basarsi solo sul rapporto contrattuale tra le piattaforme e gli utenti.

La questione, quindi, va "inquadrata come un problema di bilanciamento tra autonomia privata (di Facebook) e libertà di espressione (degli utenti) ...[ed] è intrecciata con l'ulteriore questione del ruolo delle piattaforme nella lotta ai contenuti e alle condotte illegali o comunque riprovevoli poste in essere grazie all'utilizzo della piattaforma stessa"[225].

Sicuramente le piattaforme *social* hanno interesse a mantenere e sviluppare le interazioni tra gli utenti (che determinano anche la visibilità, e quindi il successo, di un contenuto rispetto ad altri). Se, da un lato, l'interesse privatistico può essere legittimo, ciò che è degno di valutazione è se possa prevalere sull'interesse pubblico.

Conclusioni

Citando Mark Thompson (ex AD del New York Times), la censura "è un'ingiunzione al governo a rispettare la libertà di espressione. Non un obbligo rivolto a soggetti privati a pubblicare qualsiasi cosa"[226].

---

[222] https://blog.twitter.com/en_us/topics/company/2020/suspension.html e anche https://blog.twitter.com/en_us/topics/company/2021/protecting—the-conversation-following-the-riots-in-washington--.html.

[223] https://twitter.com/jack/status/1349510769268850690?ref_src=twsrc%5Etfw.

[224] https://twitter.com/jack/status/1349510770992640001.

[225] Cfr. Thobani, Shaira, *L'esclusione da Fabebook tra lesione della libertà di espressione e diniego di accesso al mercato*, in "Persone e Mercato", 2021, 2, p. 428.

[226] Cfr. R. Staglianò, *Thompson Ha senso bandire Trump dai social ma non è la soluzione,* "La Repubblica", del 15 gennaio 2021, p. 17.

In realtà, pur condividendo un'accezione più estesa del termine, il *deplatforming* è un intervento censorio, effettuato da parte di soggetti che di fatto sono soggetti privati e con un ingente potere economico.

Ma non possiamo limitarci a considerare Internet e le piattaforme *social* solo come strutture private, in quanto, considerati gli interessi in gioco, "tali piattaforme sono un coacervo di pubblico e privato, [con la conseguenza che] …non è sufficiente il rispetto dei contratti, ma occorre che vi siano delle regole 'costituzionali' proprie di questi soggetti, che regolino l'accesso, il contenzioso, e in generale la tutela dei diritti legati all'uso (l'*habeas mentem*) che vanno ben al di là delle regole del diritto civile. Di fatto, queste regole costituzionali globali i gestori le hanno già, ma se le sono date da soli (come la *lex mercatoria* è la 'costituzione' degli affari che le imprese si sono date da sé a livello globale). Occorre un processo invece in cui il costituzionalismo significhi procedure pubbliche e trasparenti di affermazione di diritti"[227].

È, quindi, il caso trovare delle risposte alla domanda: chi decide la legge marziale del *web*?[228] Ancora non siamo in presenza di una risposta chiara, ma ciò che appare è che se agire seguendo l'interesse economico è legittimo, tuttavia la mera tutela dell'interesse privato mimetizzato da tutela dell'interesse pubblico è qualcosa di potenzialmente pericoloso.

Considerando superata l'impostazione della Rete come luogo privo di regole[229], non si possono assolutizzare le esigenze privatistiche, legate all'immagine e del ritorno degli investitori. Una tale risposta conferirebbe un'indebita prevalenza dell'aspetto economico sul fondamentale diritto a esprimere il proprio, seppur deprecabile e non condivisibile, pensiero.

Contestualmente, non si possono nemmeno sottovalutare le difficoltà "di individuare con precisione le fattispecie illecite può di fatto allargare l'area delle condotte la cui repressione è lasciata all'iniziativa delle piattaforme. In altre parole, i due casi (condotte illecite e condotte, forse lecite, ma contrarie agli standard della *community*) si avvicinano nella misura in cui, non essendo spesso chiaro se vi sia o meno un illecito, ci si chiede quanto il gestore della piattaforma possa cautelarsi rispetto al semplice rischio di illeciti, in un'ottica di prevenzione"[230].

Una possibile soluzione potrebbe essere quella di stabilire, preliminarmente, con una normativa, globale e concordata con gli operatori privati del settore, se le piattaforme sono soggette alla normativa degli editori, a una normativa speciale o alla

---

[227] Tedesco, Francescomaria, *Ban di Trump: i social sono pubblici o privati? La risposta non è così scontata,* reperibile al link www.ilfattoquotidiano.it/2021/01/12/ban-di-trump-i-social-sono-pubblici-o-privati-la-risposta-non-e-cosi-scontata/6062166.

[228] È l'interrogativo che si pone anche Massimo Gaggi e da cui prendo spunto: Gaggi, Massimo, *Attacco a Capitol Hill e Trump fuori dai social: chi decide la legge marziale del web?* Sul Corsera.it, leggibile al link www.corriere.it/esteri/21_gennaio_13/attacco-capitol-hill-trump-fuori-social-chi-decide-legge-marziale-web-72eb50fa-55e1-11eb-a877-0f4e7aa8047a.shtml.

[229] Cfr. Johnson, David - Post, David, *Law and Borders. The rise of law of Cyberspace*, in "Stanford Law Review", vol. 48, 1995-1996.

[230] Cfr. Thobani, *L'esclusione da Facebook tra lesione della libertà di espressione e diniego di accesso al mercato*, in "Persone e Mercato", 2021, 2, p. 433.

Good Samaritan clause. Ogni intervento censorio, nel menzionato significato, dovrebbe essere in qualche modo giudiziabile alla luce di regole predeterminate, che tengono conto della diffusione dei contenuti e delle conseguenze effettive[231].

A prescindere dalla scelta che si compirà, si può e deve rafforzare l'idea che ciò che è penalmente sanzionabile nella vita reale deve esserlo anche *online*[232] (quindi anche l'istigazione a delinquere o la diffamazione). Inoltre, occorre riflettere attentamente su cosa succederebbe se, al posto di Trump, ci fosse una minoranza discriminata in uno Stato governato da un dittatore che, magari, entra nelle grazie dei gestori dei *social*. Difatti, se si concorda con l'idea che la libertà di manifestazione del pensiero è un principio fondamentale, colonna portante di ogni sistema democratico, che può essere ridotta solo eccezionalmente, tassativamente, temporaneamente e per tutelare un'altra libertà costituzionalmente garantita, un'eventuale compressione abusivamente portata a termine, va sanzionata. È il caso che ognuno di noi partecipi a questa riflessione, perché il tema riguarda ognuno di noi.

[231] Sul tema si rinvia anche a Cassano, Giuseppe, *Il caso Trump, la cacciata dai social media ed il diritto positivo. Brevi note in tema di ostracismo nell'era digitale*, in "Diritto di Internet", 2021, 2, p. 215-225.

[232] Cfr. Melzi d'Eril, Carlo - Vigevani, Giulio E., *Difesa giuridica dal social-chiacchiericcio*, in "Il Sole 24 Ore", 2 aprile 2017.

Identificación digital en Uruguay

Por María José Viega

1. Introducción

La ley 18.600 de 21 de setiembre de 2009 reguló en Uruguay el documento electrónico, la firma electrónica, la firma electrónica avanzada, los prestadores de servicios de certificación y creó la Unidad de Certificación Electrónica (UCE), diferenciando los efectos jurídicos en los dos tipos de firma.

Esta ley ha permitido el uso generalizado de la firma electrónica en nuestro país, conteniendo nuestro documento de identidad una firma electrónica avanzada. De acuerdo con la normativa, es necesario que la persona cuente con un dispositivo físico que contenga el certificado electrónico (como, por ejemplo: token, tarjeta o cédula de identidad electrónica), así como, la utilización de una computadora o lector que pueda leer dicha firma.

Por el art. 28 de la ley 19.535 de 25 de setiembre de 2017, se incorporaron los arts. 31 a 33 a la ley 18.600, regulando a los prestadores de servicios de confianza, concretamente los de identificación digital y firma electrónica avanzada con custodia centralizada. El 19 de marzo de 2018 el Poder Ejecutivo aprobó el decreto 70/018 reglamentario de los mencionados artículos.

Las firmas electrónicas avanzadas con custodia centralizada (custodia de los certificados en servidores accesibles vía Internet, conocidas como firma electrónica en la nube) supone que los certificados de firma electrónica se alojen en un tercero que tiene su custodia.

Esto permite implementar soluciones de firma electrónica avanzada en dispositivos de uso masivo, como pueden ser smartphones o tablets, lo que flexibiliza su uso, por ejemplo, para realizar un trámite completamente en línea o consumir servicios que se brinden a través de Internet, de manera confiable.

Por otra parte, se reconoce legalmente el concepto de Identificación Electrónica, considerándola como el equivalente digital de la identificación presencial.

2. Prestadores de servicios de certificación

El Capítulo III de la ley 18.600 regula a los Prestadores de Servicios de Certificación Acreditados, en los arts. 16 a 20 y en el Capítulo IV a los Certificados reconocidos, emitidos por estos prestadores, en los arts. 21 a 24.

De acuerdo con la ley la firma electrónica puede consistir en usuario y contraseña, datos biométricos o criptografía asimétrica, proporcionando un concepto amplio de ésta.

Y consagra la firma electrónica avanzada, definiéndola como: “la firma electrónica que cumple los siguientes requisitos:

1) requerir información de exclusivo conocimiento del firmante, permitiendo su identificación unívoca;

2) ser creada por medios que el firmante pueda mantener bajo su exclusivo control;

3) ser susceptible de verificación por terceros;

4) estar vinculada a un documento electrónico de tal modo que cualquier alteración subsiguiente en el mismo sea detestable; y

5) haber sido creada utilizando un dispositivo de creación de firma técnicamente seguro y confiable y estar basada en un certificado reconocido válido al momento de la firma".

La firma electrónica avanzada utiliza criptografía asimétrica, emitida a través de un certificado electrónico reconocido, es decir, expedido por un prestador de servicios de certificación acreditado. Cuando el prestador no se encuentra acreditado, el certificado electrónico constituye una firma electrónica común.

Los prestadores de servicios de certificación deben acreditarse ante la UCE, cumpliendo con los requisitos establecidos en la ley. Una vez acreditados, la UCE comunica a la Unidad Certificadora Raíz a los efectos de realizar la ceremonia de claves o llaves del prestador.

3. Prestadores de servicios de confianza

La aprobación del art. 28 de la ley 19.535, al que ya hemos hecho referencia, agregó un capítulo a la ley 18.600 a los efectos de regular a los prestadores de servicios de confianza.

Este artículo fue reglamentado por el decreto 70/018, estableciendo en el art. 3 literal f la conceptualización de servicios de confianza, definiéndolos como: "los servicios electrónicos que permiten brindar seguridad jurídica a los hechos, actos y negocios realizados por medios electrónicos, entre ellos:

a) servicios de firma electrónica avanzada con custodia centralizada;

b) servicios de identificación digital;

c) servicios de sellado de tiempo;

d) otros servicios establecidos por la Unidad de Certificación Electrónica".

Nos referiremos en este trabajo solamente a los literales a y b, en virtud a que, para el funcionamiento de la Identidad Digital se necesita una firma electrónica avanzada.

a. Firma electrónica avanzada con custodia centralizada

La modificación introducida a la ley 18.600 se debió a varias razones. En el art. 2° lit. *k* se establece como uno de los requisitos de la Firma Electrónica Avanzada: "*haber sido creada utilizando un dispositivo de creación de firma técnicamente segura*

y confiable…" y en el art. 6° lit. *c* garanticen que ha sido creada usando medios que el signatario mantiene bajo su exclusivo control.

La firma en nube o firma con control centralizado implica que los dispositivos de creación de firma se alojan en un tercero denominado proveedor de servicios de confianza, su acceso se produce mediante factores de autenticación y el proveedor custodia el par de claves en instalaciones accesibles (la nube) y controla su acceso.

La firma en la nube no cumple con los dos requisitos establecidos en la ley. Por lo tanto, fue necesaria la ampliación de la norma, para facilitar la apropiación y el uso de la firma electrónica avanzada, pudiendo en esta nueva modalidad firmar desde cualquier dispositivo móvil, no siendo necesario portar e instalar un dispositivo físico que aloje el certificado y las claves.

El art. 32 de la ley regula específicamente la firma electrónica avanzada con custodia centralizada, estableciendo que: "La firma electrónica avanzada con custodia centralizada, realizada a través de un Prestador de Servicios de Confianza, si cumple con todos los requisitos legales tendrá la misma validez y eficacia jurídica que la firma electrónica avanzada".

El uso de la firma en nube implica que el titular no depende más de un dispositivo físico, tampoco es necesario un lector para la cédula. En lugar de comprar el token, se va realizar un contrato con el proveedor de confianza para que aloje el certificado, del cual van a surgir todas las obligaciones para el prestador en cuanto a la custodia y el uso que se va a hacer de éste. El proveedor puede coincidir con el prestador de servicios de certificación, tener las dos acreditaciones, de certificación y de confianza.

A los efectos de regular este nuevo escenario se aprueba el decreto 70/018 que regula únicamente a los prestadores de firma electrónica avanzada con custodia centralizada y a los de identificación electrónica o digital, tal cual lo establece el art. 1° al referirse al ámbito de aplicación objetivo de la norma.

El art. 3° define en el literal b a la primera de ellas como: "la firma electrónica avanzada en la cual la clave privada del firmante se encuentra en custodia de un prestador de servicios de confianza acreditado, que realiza la firma bajo orden expresa del firmante".

El art. 4° establece las competencias de la UCE: acreditar y controlar los servicios prestados por los prestadores de servicios de confianza, establecer las especificaciones técnicas, normas y procedimientos respecto a los servicios de confianza y definir nuevos servicios de este tipo.

Los servicios de confianza de firma electrónica avanzada con custodia centralizada podrán consistir en la generación, almacenamiento y firma con certificados de firma electrónica avanzada de personas físicas y jurídicas.

Por tanto, es posible distinguir las siguientes situaciones:

a) El prestador que genera el certificado, almacena y firma, para los casos de personas físicas y jurídicas.

b) El prestador que solo almacena y firma, esta hipótesis aplica solo a personas jurídicas, como por ejemplo en los casos de certificados de personas jurídicas para facturación electrónica.

El art. 9° del decreto establece la prohibición de migrar la clave privada para la firma avanzada de persona física, entre los diferentes prestadores de servicios de confianza, ni modificar el medio de almacenamiento dentro del mismo prestador de servicios de certificación. Por tanto, aquellas firmas que se hayan emitido en dispositivos seguros de almacenamiento deben permanecer en ellos y el usuario deberá adquirir una nueva firma electrónica avanzada para utilizarla desde la nube.

El capítulo V del decreto establece en el art. 10 los requisitos para ser considerados prestadores de confianza, en el art. 11 sus obligaciones, el art. 12 establece los requerimientos técnicos y de gestión y el art. 13 remite, en cuanto a la responsabilidad, a lo previsto en el art. 20 de la ley 18.600 respecto a los prestadores de servicios de certificación.

En el capítulo VI se establece cual es el procedimiento de acreditación de los prestadores de servicios de confianza. El art. 14 establece los tres tipos de servicios de confianza que pueden brindarse, ellos son:

a) Generación, almacenamiento de certificados y firma de personas físicas y jurídicas.

b) Almacenamiento de certificados de personas físicas o jurídicas.

c) Identificación digital de personas físicas con niveles de seguridad equivalentes a la identificación presencial.

Los requisitos para cada uno de ellos se encuentran regulados en los arts. 15 y 16 respectivamente.

El art. 15, para los casos de prestadores de generación, almacenamiento y firma, remite a lo establecido en la ley 18.600 y su decreto reglamentario 436/011 de 8 de diciembre de 2011.

Para el caso de los prestadores que solo den servicio de almacenamiento y firma, el art. 16 establece que no será necesario que se acrediten, teniendo la UCE facultades para controlar en cualquier momento la regularidad de los servicios prestados. Sí establece la obligación de que cuenten con procedimientos de acceso y resguardo de certificados, cláusulas contractuales y todo lo que establezca la UCE en las políticas específicas.

Al igual que para los prestadores de servicios de certificación se exige una garantía de solvencia económica, mediante la constitución de un seguro de responsabilidad por daños y perjuicios que pudiera ocasionar la prestación del servicio.

La resolución de acreditación tiene los siguientes efectos: la incorporación del prestador en el Registro de prestadores de servicios de confianza acreditados y la habilitación para prestar el servicio en el cual se acredite.

Los arts. 23 al 27 regulan la suspensión y revocación de la acreditación de los prestadores de servicios de confianza, tanto de los prestadores de firma electrónica

avanzada con custodia centralizada como para los prestadores de identificación digital, así como el cese de las actividades de éstos.

En el capítulo VII se regula el control y supervisión de los prestadores de servicios de confianza acreditados, remitiendo al art. 14 numeral 5° de la ley 18.600 referente a las potestades sancionatorias de la UCE.

El art. 30 establece el deber de colaboración en los siguientes términos: "Los prestadores de servicios de confianza tienen la obligación de facilitar a la UCE toda la información y elementos necesarios para el ejercicio de sus funciones, así como la de permitir al personal inspector el acceso a sus instalaciones y la consulta de toda la documentación relevante".

En forma complementaria a lo establecido en el art. 30, el art. 31 prevé el relacionamiento entre prestadores de servicios de certificación y prestadores de servicios de confianza, estableciendo que los primeros deberán informar a la UCE la existencia de acuerdos y convenios que suscriban con prestadores de servicios de confianza para la prestación de los servicios que se regulan.

Finaliza el artículo haciendo la referencia a que "Dicha obligación se considerará cumplida mediante la entrega a la UCE del listado de los prestadores participantes. La UCE garantizará la confidencialidad de la información entregada".

El art. 31 le permite a la UCE conocer quiénes son los prestadores que brindan servicios de almacenamiento y firma, que, si bien no están acreditados, posee el cometido de controlarlos.

La UCE aprobó la política de Firma electrónica avanzada con custodia centralizada versión 1.0 por resolución 3/2018 y por resolución 6/2018 de 15 de agosto de 2018 la versión 1.1.

b. Identificación digital

La identidad digital es el conjunto de informaciones publicadas en Internet sobre una persona y que componen la imagen que los demás tienen de ésta: datos personales, imágenes, noticias, comentarios, gustos, amistades, aficiones, etc. Todos estos datos nos describen en Internet ante los demás y determinan la reputación digital, es decir, la opinión que los demás tienen en la red. Esta identidad puede construirse sin que se corresponda exactamente con la realidad. Sin embargo, lo que se hace bajo esa identidad digital tiene sus consecuencias en el mundo real y viceversa.

Como se puede observar el uso de Internet cada día va en aumento, por lo que la sociedad ha evolucionado considerablemente para formar comunidades en medios intangibles que se manifiestan día con día.

En este contexto es importante la identificación de la identidad ya que la información vertida directa e indirectamente por sí o por tercera persona puede producir efectos positivos y negativos en el mundo real. Un ejemplo de esta tendencia es

cuando personas y empresas navegan por las redes sociales para investigar la identidad digital de un candidato y tomar decisiones sobre él/ella[233].

Como las contraseñas son incómodas y difíciles de recordar, para su eliminación la FIDO Alliance y W3C, los consorcios que regulan los estándares en el uso de la web están trabajando en WebAuthn, el nuevo estándar que regulará la autenticación de los usuarios y eliminará las contraseñas.

Este nuevo estándar cuenta con el respaldo de Google, Mozilla y Microsoft y, en lugar de la contraseña, apuesta por sistemas de identificación biométricos a los que los usuarios de móviles de última generación están más habituados. El nuevo estándar va a permitir que un usuario pueda identificarse de forma inequívoca en un sistema o navegador empleando la huella digital o su propio rostro, o bien confiar su identidad a un segundo dispositivo (un móvil, tableta o pendrive USB).

En materia de identificación electrónica el Reglamento de la UE parte de la importancia de asegurar la interoperabilidad transfronteriza en el seno de la UE, de las identificaciones nacionales, así como el reconocimiento y aceptación mutuos entre los Estados Miembros de los medios de identificación electrónica. Objetivo básico del Reglamento es garantizar la identificación y la autenticación electrónicas seguras para el acceso a los servicios transfronterizos en línea ofrecidos por los Estados miembros, pero preservando la libertad de los Estados respecto a la gestión de la identificación electrónica y las infraestructuras conexas[234].

El art. 33 de la ley 18.600 en la redacción dada por la ley 19.535 establece la equivalencia funcional de la identificación digital. “La Unidad de Certificación Electrónica definirá los niveles de seguridad que proporcionen a la identificación digital el mismo valor y efecto jurídicos que la identificación presencial”.

Por su parte, el decreto 70/018 define en el art. 3°, en el literal a la autenticación electrónica como el proceso de identificar a una persona a través de un sistema informático mediante uno o más medios de identificación digital. En el literal *c* establece los medios de identificación electrónica o digital como: “la unidad material o inmaterial, procesable por un sistema informático, con una parte en control del sistema y otra en exclusivo control de la persona, ya sea mediante: su conocimiento; un dispositivo físico o lógico; algún rasgo físico o comportamental”.

Define además en el literal *e* el Registro de identificación digital y en *g* los servicios de identificación digital, como aquellos que realizan registros de autenticación electrónica de personas para su verificación por terceros.

En el Capítulo III del decreto se encuentran regulados los servicios de identificación digital. Estableciendo el art. 5° que éstos pueden contar con diversos niveles de seguridad, otorgándole competencias a la UCE para definir las condiciones para determinarlos, debiendo considerar el procedimiento de registro de identificación, los

---

[233] Molina Martínez, Laura, *El reconocimiento de la identidad digital a través de la firma electrónica avanzada*, p. 106.

[234] De Miguel Asencio, Pedro, *Unificación en la UE del régimen de los servicios de confianza para las transacciones electrónicas*, https://pedrodemiguelasensio.blogspot.com/2014.

medios de identificación digital y el proceso de autenticación. Y siendo este organismo quien definirá los niveles de seguridad que proporcionen a la identificación digital el mismo valor y efectos jurídicos que la identificación presencial. Para que exista esta equivalencia, los prestadores de servicios de confianza que brinden este servicio deberán estar acreditados.

El art. 7° establece que es responsabilidad de quien utiliza el servicio de identificación digital definir cuál es el nivel de seguridad que necesita, obviamente en virtud del servicio que se está brindando.

En el proceso de identificación digital tenemos que tener en cuenta el nivel de registro de la identificación digital, los medios de identificación digital y el nivel de autenticación electrónica.

Para el caso del Registro, podemos encontrar la existencia de 3 o 4 niveles, que van desde niveles muy bajos de seguridad hasta el nivel equivalente al presencial. Sin lugar a dudas, en nuestro país, un alto nivel de identificación y por tanto equivalente al presencial requerirá al momento del registro la instancia presencial, pudiendo el proceso comenzar en línea, pero siendo necesaria la presencia física de la persona que solicita la acreditación de su identidad a los efectos de vincularla con medios digitales. Será necesaria la captura de datos biométricos del suscriptor y el tipo de medio digital asociado al solicitante es un certificado de firma electrónica avanzada, otorgado dentro de la infraestructura de certificación electrónica de Uruguay.

Los medios de identificación electrónica digital que pueden ser considerados durante la etapa de autenticación son los siguientes:

a) Nombre de usuario y contraseña.

b) Lista de contraseñas, en soporte papel que posee el reclamante. Consiste en una lista de códigos a menudo en combinación con una contraseña estática o PIN dentro del sistema de autenticación.

c) Dispositivo de contraseña de un solo uso: es un dispositivo de hardware personal que genera una contraseña de "una sola vez", el cual es válido para una sola sesión de autenticación.

d) Certificado en software: es una clave criptográfica que normalmente se almacena en un disco, dispositivo USB u otro medio de dispositivo de comunicación. La autenticación se realiza probando la posesión y el control de la clave.

e) Certificado en hardware: es una tarjeta inteligente o medio similar que contiene una clave criptográfica protegida. La autenticación se realiza probando la posesión del dispositivo y el control de la clave.

f) Certificado electrónico reconocido de persona física: certificado de firma electrónica avanzada emitido por un prestador de servicios de certificación acreditado ante la UCE.

El tercer paso del proceso, la autenticación electrónica, como ya hicimos referencia, se encuentra definida en el art. 3° literal *a* del decreto como “el proceso de identificar a una persona a través de un sistema informático mediante uno o más medios de identificación digital”.

El nivel de confianza que se puede plantear en un mecanismo de autenticación remota depende del nivel de seguridad que posea, los cuales están muy relacionados con los tipos de ataques y el medio de identificación digital utilizado durante el proceso de autenticación.

Las amenazas dentro de los procesos de autenticación pueden ser:

a) Fuerza bruta: es un ataque donde se intenta adivinar el secreto de la comunicación, por ejemplo, una clave.

b) Eavesdropping: consiste en una escucha secreta o sigilosa. En la red, consiste en observar los mensajes que pasan por un canal de comunicación. Esos mensajes se almacenan para realizar un análisis fuera de línea de la información, obteniendo por ejemplo metadatos, que son utilizados para lanzar ataques sucesivos.

c) El secuestro: es un ataque que consiste en hacerse cargo de una sesión ya autenticada por un atacante y para aprender información sensible.

d) Retransmisión**:** es una forma de ataque donde una entidad maliciosa repite o retrasa previamente mensajes interceptados para obtener acceso a información confidencial.

e) *Man-in-the-middle*: es una forma de espionaje activo consiste en introducirse en la comunicación entre dos equipos para que todo el tráfico pase por él y poder así desencriptar sus datos, contraseñas, etc.

El nivel de seguridad del protocolo de autenticación lo hace o no susceptible de determinados ataques, por tanto, el nivel de seguridad dependerá de a qué tipo de riesgos se encuentra expuesto.

De acuerdo a los niveles definidos durante el procedimiento es que se definen los niveles de seguridad de la identificación digital.

La UCE aprobó por resolución 4/2018 de 8 de agosto de 2018 la política de identificación digital.

Los servicios de Identificación Digital podrán contar con diversos niveles de seguridad. La política define: especificaciones técnicas, normas y procedimientos para determinar los niveles de seguridad de los servicios, considerando: el procedimiento de registro, los medios de identificación y el proceso de autenticación electrónica.

Los niveles de seguridad de Identificación Digital considerados son:

Nivel 0 (Muy bajo): no requiere presencia física del solicitante, no se verifican los datos proporcionados. Se utiliza en los servicios en línea cuando no se requiere confianza en la ID.

Nivel 1 (Bajo): no requiere presencia física del solicitante, se realiza validación de los datos proporcionados.

Nivel 2 (Medio): se requiere la presencia de la persona durante la etapa de registro de ID. Los medios de ID asociados a la persona durante el registro y el proceso de autenticación, son considerados robustos.

Nivel 3 (Alto): identidad digital equivalente a la presencial. Igual que en el nivel 2, pero además se capturan y validan datos biométricos del solicitante. La autenticación se realiza utilizando un certificado electrónico reconocido de persona física.

El procedimiento de registro de Identificación Digital está determinado por el procedimiento de identificación de la persona y el proceso de emisión y asociación de los medios digitales a ésta. En este sentido se considera:

Nivel 0 (Muy bajo): no requiere presencia física del solicitante. El registro puede ser realizado en línea. No ser realiza verificación de los datos.

Nivel 1 (Bajo): no requiere presencia física del solicitante, se realiza validación de los datos proporcionados.

Nivel 2 (Medio): se requiere la presencia de la persona durante la etapa de registro de ID y asociar medios digitales a su ID. Se requiere la exhibición de un documento nacional de identidad. Se entrega en la instancia presencial un código QR, PIN o contraseña para activación del medio digital en línea

Nivel 3 (Alto): se requiere la presencia de la persona durante la etapa de registro de ID y asociar medios digitales a su ID. Se realiza verificación biométrica. El medio de identificación es un Certificado electrónico reconocido de Persona Física.

Los niveles de identidad digital podemos visualizarlos en forma más sencilla en el siguiente cuadro.

		Nivel de seguridad en el proceso de autenticación electrónica de una identidad digital			
		AE0	AE1	AE2	AE3
Procedimiento de registro de identificación digital	RID0	NIVEL DE IDENTIDAD DIGITAL 0	NIVEL DE IDENTIDAD DIGITAL 0	NIVEL DE IDENTIDAD DIGITAL 0	NIVEL DE IDENTIDAD DIGITAL 0
	RID1	NIVEL DE IDENTIDAD DIGITAL 0	NIVEL DE IDENTIDAD DIGITAL 1	NIVEL DE IDENTIDAD DIGITAL 1	NIVEL DE IDENTIDAD DIGITAL 1
	RID2	NIVEL DE IDENTIDAD DIGITAL 0	NIVEL DE IDENTIDAD DIGITAL 1	NIVEL DE IDENTIDAD DIGITAL 2	NIVEL DE IDENTIDAD DIGITAL 2
	RID3	NIVEL DE IDENTIDAD DIGITAL 0	NIVEL DE IDENTIDAD DIGITAL 1	NIVEL DE IDENTIDAD DIGITAL 2	NIVEL DE IDENTIDAD DIGITAL 3

4. Conclusiones

La aprobación de las normas analizadas ha proporcionado a Uruguay un marco jurídico completo y garantista a los efectos de la utilización de la firma electrónica avanzada con custodia centralizada y la identificación digital.

El objetivo de la normativa es asegurar que el dispositivo de creación y almacenamiento de firmas electrónicas sea confiable y que el firmante tenga el acceso exclusivo a su clave de firma electrónica avanzada de persona física con una custodia centralizada, con un alto grado de confianza.

Como se mencionó en la introducción, los servicios permitirán firmar documentos evitando utilizar dispositivos adicionales para la firma como los token o los lectores de cédula de identidad, facilitando el proceso a los usuarios.

El otorgar la equivalencia de la firma en nube con la firma electrónica avanzada y de la identidad digital con la identidad física constituye, sin lugar a dudas, dos herramientas poderosísimas para el avance de la seguridad en el ciberespacio.

Al momento actual existen dos prestadores de servicios de confianza acreditados en Identidad Digital: Abitab (privado) y Antel (compañía de telecomunicaciones del Estado).

Bibliografía

Molina Martínez, Laura, *El reconocimiento de la identidad digital a través de la firma electrónica avanzada*, "Hacia una Justicia 2.0", Actas del XX Congreso Iberoamericano de Derecho e Informática, vol. II, 2016.

Rico Carrillo, Mariliana, *La entrada en vigencia de la regulación europea sobre servicios de confianza y su impacto en el comercio electrónico*, Actas del XX Congreso iberoamericano de Derecho e Informática, Salamanca, España, 2016.

Viega Rodriguez, María José, *Derecho Informático e Informática Jurídica I*, Montevideo, Fundación de Cultura Universitaria, octubre, 2017.

Viega Rodriguez, María José - Hernandez Varela, María Jimena, *Derecho Informático e Informática Jurídica II*, Montevideo, Fundación de Cultura Universitaria, marzo, 2018.

Viega Rodriguez, María José - Rodriguez, Beatriz, *Documento y firma. Equivalentes funcionales en el mundo electrónico. Ley 18.600, Decreto 436/2011*, Editorial CADE, junio 2012.

Formato electrónico

Canal TIC. Educación. Tecnologías de la información y comunicación, http://canaltic.com/internetseguro/manual/3_mi_identidad_digital.html, página visitada el 17/4/18.

Canut, Pedro J., *El prestador cualificado de servicios de confianza. Seguridad jurídica en Internet*, www.blogespierre.com/2015/11/27/el-prestador-cualificado-de-servicios-de-confianza-seguridad-juridica-en-internet.

De Miguel Asencio, Pedro, *Unificación en la UE del régimen de los servicios de confianza para las transacciones electrónicas*, https://pedrodemiguelasensio.blogspot.com/2014.

El fin de las contraseñas está aquí: llega WebAuthn, www.cromo.com.uy/el-fin-las-contrasenas-esta-aqui-llega-webauthn-n1223243?utm_source=planisys&utm_medium=Cromo-Titularesdelasemana&utm_campaign=Cromo-Titularesdelasemana2018&utm_content=27&ns_campaign=Cromo-

Titularesdelasemana2018&ns_source=planisys&ns_linkname=27&ns_mchannel=Cromo-Titularesdelasemana.

Prestadores de servicios electrónicos de confianza, www.minetad.gob.es/telecomunicaciones/es-es/servicios/firmaelectronica/paginas/prestadores.aspx.

Sheldon, Robert, *Qué buscar en un proveedor de almacenamiento en nube*, http://searchdatacenter.techtarget.com/es/consejo/Que-buscar-en-un-proveedor-de-almacenamiento-en-nube.

Viega Rodriguez, María José - Rodriguez, Beatriz, *Documento electrónico y firma digital. Cuestiones de seguridad en las nuevas formas documentales*, Libro electrónico: www.viegasociados.com, Montevideo, 2005.

Winkler, Vic (J.R.), *Informática en nube: problemas legales y reglamentarios*, https://technet.microsoft.com/es-es/library/hh994647.aspx.