

Título: El derecho administrativo en el entorno digital. Las relaciones entre los sistemas informáticos y la función administrativa

Autor: Nielsen Enemark, Carlos A.

Publicado en: RDA 2022-139, 03/02/2022, 16

Cita: TR LALEY AR/DOC/3484/2021

Sumario: I. Introducción.— II. El campo de conocimiento científico jurídico en materia de TIC.— III. Características de los sistemas.— IV. Características de los procedimientos administrativos electrónicos.— V. Características de los actos administrativos automáticos.— VI. El sistema del dinero electrónico. La posibilidad de implementarlo como servicio público.— VII. Conclusiones.

(*)

I. Introducción

Existen numerosos desarrollos jurídicos sobre las tecnologías de la información y las comunicaciones (TIC), en asuntos vinculados al derecho administrativo [\(1\)](#). En ellos se exhiben diferentes relaciones entre los sistemas informáticos y la función administrativa. Estos trabajos, con muy buena conciencia de lo que persiguen y de las hipótesis que intentan demostrar, abordan las temáticas de manera intensiva, es decir, se analizan en detalle, de cerca, su objeto de estudio.

Desde luego, estos son los modos científicos a través de los cuales es posible dar soluciones fundadas a los problemas que se encuentran en el estudio de estos aspectos del derecho administrativo.

Sin embargo, al momento, no se ha efectuado una taxonomía de las cuestiones de derecho administrativo implicadas en el uso de las TIC junto a un abordaje sistémico de la totalidad; no existe un mapa donde se puedan identificar ámbitos de conocimiento de derecho administrativo que pudieran estar comprometidos en la aplicación de razones científicas ajenas a lo jurídico.

Este documento busca mostrar el campo de conocimiento científico jurídico de la función administrativa en lo digital, es decir, escenario desde lejos. Y, sin ánimo de dar precisiones sobre los institutos, sí intenta dar un panorama general de los asuntos de TIC donde el Estado se encuentra involucrado y el derecho administrativo aparece con posibilidades de dar una respuesta, o en aquellos donde necesita nutrirse de aspectos técnicos para emitir algún producto jurídico.

En esa comprensión, este documento no será un documento definitivo y estático, sino que es una propuesta modificable y dinámica, como base de trabajo para otros desarrollos doctrinarios, ya que los avances en las ciencias relacionadas a la tecnología, desde luego, se dan separados del derecho y con una evolución propia de aquellas.

La epistemología que se propone para abordar este problema tendrá por objeto determinar los límites en los cuales se puede producir válidamente el derecho administrativo en uso de tecnología, en la medida en que, por la ejecutoriedad y ejecutividad subyacente en los actos administrativos estatales, la tecnología utilizada por el Estado acarrea, por sí misma, la potestad de asignar, modificar o detraer unilateralmente los derechos de los particulares, y los particulares quedan obligados a su cumplimiento. Incluso más, se intentará demostrar que existe una estrecha vinculación entre la función administrativa y la utilización del dinero electrónico. Primero, ello incide sobre un aspecto central del individuo: su patrimonio. En segundo término, la ejecución presupuestaria, prácticamente en su totalidad, se ejecuta con actos y procedimientos administrativos que se enmarcan en un ecosistema digital.

De allí que sea socialmente necesario comprender las razones protectorias propias del derecho administrativo que se dan en el contexto de las TIC, no solo como aplicación en justicia de un espectro poco labrado, sino también como manera en que el derecho administrativo pueda proponer espacios válidos donde receptor demandas sociales, lo que sirve de método de aproximación a institutos jurídicos, así como forma de encontrar legitimación continua a favor de su propia razón de ser.

En ese entendimiento, el método será ir tratando cuestiones generales, desde la epistemología que pueda generar productos jurídicos válidos, hasta el contenido y significado, al día de hoy, de los temas que podrían considerarse relevantes para el derecho administrativo en asunto de TIC. Para ello, se separaron áreas temáticas en capítulos, y dentro de los capítulos, apartados.

II. El campo de conocimiento científico jurídico en materia de TIC

II.1. El derecho administrativo frente a las demás ciencias técnicas

Una de las primeras cuestiones radica en que el derecho administrativo recepta lo dicho por otros ámbitos científicos, a veces, sin posibilidad de indagar la validez de la producción científica dada en esos espacios, los

que, por cierto, no necesariamente tienen al derecho como perspectiva en la elaboración de sus productos.

Por ejemplo, se utiliza la inteligencia artificial para resolver un problema jurídico. Desde luego, el uso de esta tecnología será idóneo para atender el fin propuesto, aunque los inconvenientes jurídicos se dan al momento en que el programador deba tomar decisiones que se hacen, habitualmente, con base en normas de índole legal, impropias de la programación.

Este dilema se da ya que si bien, las distintas ciencias involucradas (por ejemplo, estadística y derecho administrativo) buscan un mismo objetivo, el resultado, por momentos, puede aparecer disímil en una y otra, en razón de que su campo científico, no necesariamente coincide en un mismo resultado.

En detalle, podemos identificar que, en una distribución normal (2), hay resultados estadísticos que pueden ser aceptados, e incluso, dan pautas para la toma de decisiones con un racional de fondo certero; en tanto, en el derecho administrativo, la juridicidad obligará a mirar con indiferencia a los problemas de curtosis (3).

Ahora, la programación plasmará, en líneas de código, la decisión que se fuera a adoptar con base a datos estadísticos y jurídicos, de donde surgirá el resultado a aplica.

Por ello, deben darse comprensiones recíprocas entre las ciencias, de manera que pueda ser posible la construcción de una juridicidad válida para las TIC.

En esto, aparece relevante reconocer que la naturaleza científica del derecho es muy distinta a la propia de la matemática, la estadística y la programación. En estas últimas existe una homogeneidad y un sentido unívoco en la producción del conocimiento y de los resultados válidos. Pero el derecho no necesariamente coincide con ellas: la finalidad instrumental de unas y otras es diferente, sirven para cosas distintas.

De ahí que vincular los diferentes espacios (derecho y ciencias duras) sea un desafío, acarree complejidades específicas, necesite de comprensiones, hasta este último tiempo, inexistentes, y solicite el planteo de preguntas cuyas respuestas se desconocen.

Eso sí supone un trabajo de elaboración jurídica novedosa, pero jamás puede tornarse una concesión hacia lo desconocido; no es posible admitir que las protecciones del derecho administrativo cedan ante lo incomprendido del álgebra, la estadística o de la programación.

Por el contrario, el derecho administrativo autónomo, es decir, el que es elaborado bajo condiciones socio-jurídicas válidas, debe tener un conocimiento acabado de las decisiones que se toman en el núcleo de las otras ciencias, no solo a riesgo de reducir su propio campo científico, sino también a costa de los derechos de las personas.

En el derecho administrativo se aplican las prerrogativas derivadas de las normas, que son una traducción jurídica del deber ser ético social que propone el Congreso a través de productos, las leyes. Ahora, las ciencias duras necesariamente tendrán que ajustar sus soluciones a las pautas jurídicas, bajo pena de ser, naturalmente, soluciones antijurídicas. Dicho de otra forma, ante la existencia de nuevas formas científicas, si es que no se hizo un ajuste hacia lo normativo, es posible que la ciencia haga un retorno forzado hacia el absolutismo, por tomar una decisión en lo matemático y plasmarlo en un algoritmo.

Este problema va a requerir que existan modificaciones en la formación de los operadores jurídicos y en los programas académicos. De no llevarse esto a cabo se corre el riesgo de convertir, al derecho administrativo, en una herramienta para prohibir lo desconocido, y así, cercenar todo tipo de avance; o bien, en el otro extremo del absurdo, volverlo una ciencia que no debe intervenir sobre el contenido técnico de lo analizado, poniendo en juego los derechos individuales y colectivos.

Ni lo uno ni lo otro aparece como razonable. Por el contrario, sí es posible pensar en procesos dialécticos entre las ciencias, en la integración recíproca y en la comprensión de fondo de cada uno de los problemas que cada ciencia pretende resolver. De no hacerlo, el derecho administrativo pondrá en juego su propia legitimación científica, por autoinhibirse de dar soluciones jurídicas específicas.

Por eso, las ciencias duras y el derecho administrativo, por principio, deben integrarse y complementarse, en una comprensión recíproca sobre el fondo de cada asunto, lo que importa una nueva formación de los operadores jurídicos y de los programas de estudio.

De esta forma, es posible dar un resguardo a los principios de tutela de las libertades ya concedidas y a la completitud del abordaje en lo técnico y en lo estrictamente legal.

II.2. Gobierno digital

Es interesante el abordaje de Bonina (4), al respecto de involucrar diferentes ámbitos conceptuales para llevar adelante las transformaciones digitales. El autor las califica como "disciplinas" a lo que denomina legal

design (diseño legal), legal project management (administración de proyectos legales) y legal operations (operaciones legales).

A pesar de utilizar una terminología inespecífica a partir del cual se crea un ámbito de conocimiento cuyas condiciones de producción no pueden ser fácilmente conocidas o replicadas, es interesante la referencia a un documento de la OCDE, donde se define al gobierno digital como "el uso de las tecnologías digitales como parte integral de las estrategias de modernización de los gobiernos con el fin de crear valor público. Esto se basa en un ecosistema de gobierno digital constituido por los actores estatales, organizaciones no gubernamentales, empresas, asociaciones de ciudadanos y personas encargadas de la producción y acceso a los datos, servicios y contenidos a través de interacciones con el gobierno" (5).

En ese sentido, el gobierno digital involucra las actividades de los tres poderes del Estado (y, naturalmente, de los órganos llamados extrapoderes), donde la interacción con los administrados pasa a ser el objeto del desarrollo.

Dicha interacción debe complementarse con la tecnología jurídica lograda a lo largo de la historia, de modo que los avances sobre los sistemas no supongan anegar los conductos que conoce el derecho, mediante incrementos de velocidades, replicaciones múltiples o soluciones algorítmicas. Es decir, las doctrinas jurídicas labradas en el tiempo no desmerecen las transformaciones digitales, ni las transformaciones digitales pueden ser disfuncionales a las doctrinas jurídicas existentes.

Antes bien, ese gobierno digital, y en lo que hace a asuntos de derecho administrativo, debe atender, en particular, a cuestiones de sistemas, procedimiento administrativo, de actos administrativos y de dinero electrónico.

Estos son los campos de conocimiento que más se pueden resentir con la introducción de nuevas tecnologías de información y comunicación.

II.3. Adaptabilidad

La adaptabilidad puede ser predicable de las personas y de la infraestructura.

Por un lado, en cuanto a infraestructura, las necesidades pueden ser cambiantes, tanto por dimensión de las instalaciones, como por ubicación de estas.

A su vez, los operadores necesitan ir capacitándose continuamente, e incluso, algunos empleados públicos deban ir adquiriendo capacidades que anteriormente no tenían.

Esto hace que ciertos contratos de empleo público necesiten contemplar estas alternancias de ubicación y capacitación, lo que no ocurre para todos los agentes. Es decir, esos contratos pueden mudar sustancialmente en su objeto, lo que no deja de ser menor, en cuanto a que el ecosistema técnico, en los hechos, puede tener mayor incidencia que la norma aplicable en sí.

Estas complejidades se incrementan y profundizan si se habilita la posibilidad de desarrollar trabajo remoto, lo que importa nuevos y mayores desafíos para el Estado en su rol de empleador. Por ejemplo, refiere la profesora Ivanega, con certeza, que, ante la aparición del teletrabajo, existe "la necesidad de articular los objetivos públicos institucionales y los derechos tanto de los ciudadanos como destinatarios de la función pública como de los empleados público". De ello, apunta conclusiones sobre el tipo de función a realizar en forma remota, los modos de selección, la capacitación, el tiempo de las tareas, las condiciones del servicio, las responsabilidades, la supervisión y las formas de comportamiento específicas (6).

Incluso, en un trabajo más reciente aún, la autora identificó que es necesario un desarrollo en los aspectos de las faltas disciplinarias, el derecho a la desconexión, así como aquellos derivados de la invisibilidad del empleado y los riesgos de la precariedad a la que pueden quedar sujetos los empleados en el trabajo remoto (7).

De esta manera, es necesario que estas adaptaciones sobre aspectos de empleo público tengan una mirada sobre los asuntos de derecho colectivo del trabajo que pudieran verse implicados, a los fines de dar las participaciones del caso, no solo por los empleados en sí, sino también por la réplica que ello tiene en los administrados.

Es interesante ver los dictámenes de la Procuración del Tesoro de la Nación para realizar audiencias por videoconferencias. Ellas serían excepcionales, y solo podrían ser realizadas si es que la situación epidemiológica lo impidiera y ello fuera invocado fundadamente por el particular (8).

Ahora bien, la adaptabilidad de los usuarios no puede ser una variante de ajuste, sino solo funcionar a favor de los administrados, no en contra. Por eso, las mejores posiciones suponen la posibilidad de tener capacitación simple y completa y la posibilidad de volver a utilizar los sistemas tradicionales si es que el derecho al que están intentando acceder está en juego o queda comprometido por la falta de posibilidades de adaptación.

III. Características de los sistemas

III.1. Interoperabilidad

La interoperabilidad o interoperatibilidad aparece como "la habilidad de dos o más componentes de software de cooperar a pesar de las diferencias en lenguaje, interface y plataforma de ejecución" (9), lo que también fue definido como en estos términos: "La interoperatibilidad entre componentes de sistemas distribuidos de gran escala es la habilidad de intercambiar, entre ellos, servicios e información" (10).

Estos intercambios se basan en acuerdos entre emisores y receptores de información, sobre protocolos de envíos de mensajes, nombres de procedimientos, códigos de errores y tipos de argumentos. Para que todo ello tenga sentido, es necesario que exista una interoperatibilidad semántica (11).

Se debe entender que existen varios niveles de interoperabilidad, de modo que sea posible el intercambio entre diferentes expertos (12).

Ello debe ser considerado a los fines de que el derecho administrativo genere válidamente su propia estructura conceptual (en aspectos técnicos), lo que luego, podrá ser receptado en otros ámbitos técnicos, para permitir la interoperatibilidad entre sistemas y operadores.

Ello, porque la interoperabilidad no solo ocurre como un espacio científico donde intercambian o interoperan diferentes sistemas en un mismo momento, sino que ello es necesario a los fines de atender el problema de la interoperatibilidad intertemporal.

Esto supone establecer reglas para evitar que la heterogeneidad de sistemas lleve a mayores dificultades en cuanto a su producción o mantenimiento (13), cuestión que aumenta su dificultad, en caso de que se pretenda introducir algún tipo de descentralización, como blockchain (14) (15).

De allí que sea necesario que, a lo largo del tiempo, los sistemas nuevos puedan leer y operar sobre sistemas más antiguos. De no ser así, los particulares pueden perder garantías en estos avances o en los cambios de tecnología. Ello es posible a través de un "marco de interoperabilidad (interoperability framework)", para lo que, en términos de robustez y escalabilidad, se propuso el lenguaje XML (16).

Por eso, los principios que pueden mirarse sobre este ámbito estarán vinculados a la integración, la componibilidad a nivel conceptual (17), la intrascendencia de la imposición, el centralismo y la colaboración.

Ello aparece como una búsqueda del art. 7º de la ley 27.446 (18) y del art. 2º del dec. 182/2019 (19), donde se indica que la interoperatibilidad documental se debe instrumentar a través del módulo de Interoperabilidad (IOP) del GDE.

Sin embargo, a pesar de lo referido, el formato elegido para trabajar asuntos de interoperabilidad es JSON (20), que sería más simple y rápido que XML, aunque cada lenguaje tiene fortalezas singulares (21). Por ejemplo, existe literatura que indica que XML tiene mayor escalabilidad (22), aunque JSON es más útil para vincular un software con navegadores nativos o una aplicación móvil (23).

La razón de utilizar este lenguaje, según los considerandos de las normas, atiende a que sea posible vincular "sistemas informáticos y bases de datos" de distintos organismos, "facilitando así el intercambio de información entre ellos, y posibilitando una respuesta rápida, segura, con información actualizada, y con valor jurídico, en un marco de seguridad y confianza" (24).

No hay mayores explicaciones sobre la causa de esta elección, lo que hubiera sido necesario para un asunto con esta relevancia. Por eso, esta norma parece escasa ante los dilemas que supone la interoperabilidad.

III.2. Especificidad técnica y normativa de los sistemas

Existen numerosos sistemas, plataformas, módulos, aplicaciones, interfaces y servicios que utiliza el Estado Nacional para llevar adelante sus procedimientos administrativos.

Podemos identificar los siguientes: Escritorio Único, Expediente Electrónico, Trámites a Distancia, Legajo Único Electrónico, Locación de Obras y Servicios, Registro Legajo Multipropósito, Comunicaciones Oficiales, Generador de Documentos Electrónicos, Comprar, Firma Digital, Autenticar, Plataforma de Autenticación Electrónica Central, Registro Integral de Destinatarios, Gestor de Asistencias y Transferencias, Porta Firma y Registro de Audiencias de Gestión de Intereses, entre otros.

Estos sistemas, plataformas, módulos, aplicaciones y servicios se enraízan en el Plan de Modernización del Estado, aprobado por el art. 1º del dec. 434/2016.

Dicho Plan de Modernización, entre otras cosas, dio origen a la implementación del Sistema de Gestión Documental Electrónica (GDE), mediante el dec. 561/2016, el que se configura como un sistema integrado de caratulación, numeración, seguimiento y registración de movimientos de actuaciones y expedientes (art. 1º).

Este Sistema o Plataforma, fue declarado como Infraestructura Crítica de Información del Estado, mediante la res. de la Secretaría de Innovación Pública 36/2020. La inclusión de este sistema en el concepto de Infraestructura Crítica de Información constituye un requisito esencial para la elaboración de "las normas, políticas y planes para la protección de las Infraestructuras que respaldan servicios críticos, permitiendo la identificación de sistemas, equipamiento y actores involucrados, entre otros aspectos" (25). Es decir, este sistema goza de una protección y una atención específica que otros sistemas no poseen, atento a su carácter crítico.

A su vez, por dec. 1063/2016 se aprobó la Plataforma de Trámites a Distancia, integrada por el módulo "Trámites a Distancia" (TAD), como medio de interacción del ciudadano con la administración, a través de la recepción y remisión por medios electrónicos de presentaciones, solicitudes, escritos, notificaciones y comunicaciones, entre otros (art. 1°).

A través de esta plataforma se efectúan presentaciones de escritos en sede administrativa, con fecha y cargo digital (art. 9°), así como que la Administración efectúa notificaciones a los usuarios en domicilio especial electrónico (arts. 4°, 7° y 8°).

Además, se contempla la posibilidad de suscribir documentos con firma digital en el Sistema de Gestión Documental Electrónica (art. 13).

Todo ello se hace expresamente como mecanismo alternativo al Reglamento para Mesas de Entradas, Salidas y Archivo, aprobado por el dec. 759/1966 (26) (art. 16), el que se encontraría vigente.

El Escritorio Único es una interfaz en la cual se centraliza el acceso a los distintos módulos del Sistema GDE.

Los principales módulos del Sistema GDE, y más utilizados por todos los usuarios son los que se aprobaron por la res. 3/2016 de la ex Secretaría de Modernización Administrativa (27), que son los denominados "Comunicaciones Oficiales" (art. 1°), "Generador de Documentos Electrónicos Oficiales (GEDO)" (art. 2°) y "Expedientes Oficiales" (art. 3°). A través de estos módulos se confeccionan documentos, que se firman digitalmente, produciendo idénticos efectos jurídicos a sus versiones impresas (art. 5°).

Es interesante que en esta norma se definen los términos "documento" y "expediente electrónico" (art. 4°). Para definir al documento, la norma dice: "Constituye documento, cualquiera sea su soporte, una entidad identificada y estructurada que comprende texto, gráficos, sonido, imágenes o cualquier clase de información". A su vez, el expediente electrónico es el "[c]onjunto de documentos electrónicos o actuaciones administrativas, originados a solicitud de parte interesada o de oficio y ordenadas cronológicamente, en el que se acumulan informaciones, dictámenes y todo otro dato o antecedente relacionado con la cuestión tratada, a efectos de lograr los elementos de juicio necesarios para arribar a conclusiones que darán sustento a la resolución definitiva".

Estas son las principales normas donde se enroscan los sistemas del Estado nacional. Existen muchas otras normas de detalle, e incluso, algunas normas que tuvieron muchas adaptaciones a lo largo del tiempo hasta lograr una adaptación específica a lo que pretendían resolver.

En cuanto a la terminología utilizada por las normas, se puede mencionar que existen diversos usos de menciones que aparecen como análogas. Por momentos, los sistemas se identifican con las plataformas. Los módulos o aplicaciones son subsistemas o también, sistemas dentro de los sistemas. Las interfaces sirven a la fácil exposición de los módulos dentro de los sistemas, y los servicios, que son mecanismos internos de un sistema que cumple una finalidad específica (por ejemplo, el servicio de autenticación, que tiene por "finalidad brindar servicio centralizado de información respecto de la acreditación en entornos virtuales de la identidad de los usuarios de sistemas informáticos a través de una red" (28).

Cada uno de los sistemas, plataformas, módulos, aplicaciones, interfaces o servicios debe contar con respaldo normativo, el que debe ser publicado. Las normas y los productos digitales que estas crean deben seguir todos los parámetros de validez de la actividad administrativa y como tales, son plenamente controlables judicialmente.

Ahora, en cuanto a la literatura técnica utilizada para el desarrollo de estos sistemas, no existen rastros en los decretos, lo que supone una deficiencia y un alto riesgo para generar posteriores interoperabilidades.

III.3. Los canales de intercambio y los servidores

Todos los sistemas de gestión digital se montan sobre las redes de internet y sobre distintos servidores. Es decir, son una tecnología que dependen de otras tecnologías y sistemas.

En algún punto en de la historia, internet era una forma de intercambio de datos entre tan pocas personas que no era un sistema desarrollado o significativo. Desde luego, con el paso del tiempo, dicha exclusividad mutó a una generalidad, y no solo a eso, sino que la generalidad comenzó a utilizar internet y los canales digitales que

esta provee, como modo de acceder a recursos vitales y estratégicos.

Ahora bien, esa evolución llevó a una generalización y estandarización transversal del uso de internet, cambio que se aceleró con la aparición de la pandemia. Los sistemas necesarios para la actuación de los tres poderes del Estado hacen que sean necesarias las redes de internet. Lo mismo ocurre con la educación, la salud, las comunicaciones, el comercio, las finanzas, los sistemas bancarios, la seguridad, la energía, los transportes de personas y cargas, el entretenimiento, etc. Es decir, actividades públicas y privadas se montan sobre internet y, consecuentemente, sobre los servidores que son necesarios para esta actividad.

Es así como estos servicios de tecnologías de la información y las comunicaciones, con el paso del tiempo, se tornaron estratégicos, útiles y centrales para el desarrollo de la vida en sociedad. En lo que a este trabajo interesa, con distintos acontecimientos normativos, se generó la posibilidad de iniciar un procedimiento administrativo por medios digitales.

Con ese trasfondo se dictó el dec. 690/2020, modificatorio de la ley 27.078, donde se estableció: "los Servicios de las Tecnologías de la Información y las Comunicaciones (TIC) y el acceso a las redes de telecomunicaciones para y entre licenciatarios y licenciatarias de servicios TIC son servicios públicos esenciales y estratégicos en competencia".

Además, se dictaron ciertas disposiciones en ENACOM, a los fines de resolver cuestiones de detalle.

Con ese escenario, la Sala II de la CNCAF, en una causa promovida por Telecom Argentina SA dictó, como medida precautoria, "la suspensión de los efectos de los arts. 1º, 2º, 3º, 4º, 5º y 6º del dec. 690/2020 y de las resoluciones ENACOM 1466/2020, 1467/2020 y 204/2021, y su consiguiente inaplicabilidad con relación a la firma accionante" (29).

Ahora, como perspectiva, no sería irrazonable que el Estado se incline a desarrollar sus propias redes y servidores sobre los que montar actividades que le resulten de interés, espacio sobre el que el derecho administrativo debería proyectar sus soluciones (naturaleza estratégica de la información, vías de acceso a estos canales, autoridades y estructura de control interno, derechos de los administrados, transparencia, reglas técnicas internas, etc.).

Por otra parte, es interesante conocer la experiencia dada en la Unión Europea, en la que se buscó reglamentar el principio de neutralidad tecnológica en internet, de manera que los usuarios finales puedan tener libertad de optar entre diferentes tipos de equipos terminales y lograr la convergencia de precios en la provisión de itinerancia, de modo de evitar el trato discriminatorio a usuarios de internet en razón de las tarifas (30).

III.4. Ciberseguridad

Este tópico va adquiriendo mayores complejidades con el paso del tiempo, en cuanto se identifican mayores amenazas.

Es interesante poder tratar la problemática que se dio al respecto en el gobierno norteamericano, ya que, por su posición a con respecto a otros países y por su actividad de política internacional, es un objetivo apetecible de ciberataques a nivel global.

En 2009, luego de estudios referidos a los asuntos estratégicos en el gobierno norteamericano (31), se emitió la Ley de Ciberseguridad. En esa ley, la problemática se abordó bajo la perspectiva de las relaciones intergubernamentales de todos los niveles de Estado, del sector privado y de los ciudadanos, como manera de generar una política de ciberseguridad satisfactoria (32) (33).

Otros estudios llevaron a poner en análisis el compromiso a la ciberseguridad gubernamental que se da por la implementación de la tecnología IoT (Internet of Things, Internet de las cosas) (34).

Andreasson indica que los desafíos estarán en la administración de la información, en la adecuada gestión del "M-Government" (Gobierno Móvil) y en el control de las amenazas de ciberespionaje, terrorismo y de la guerra digital con consecuencias online y offline (35).

En Argentina, con el dec. 577/2017 (36), se creó el Comité de Ciberseguridad. Dicho comité fue modificado por el dec. 480/2019. Este comité está integrado por representantes de diferentes unidades organizacionales (37), y su objetivo central es la elaboración de la Estrategia Nacional de Ciberseguridad.

Mediante el art. 1º de la res. 829/2019 (38) de la ex-Secretaría de Gobierno de Modernización se aprobó la Estrategia Nacional de Ciberseguridad. Esta estrategia tiene un abordaje similar a la ley de ciberseguridad norteamericana, en cuanto involucra a todos los actores de gobierno, al sector privado y a la sociedad civil. Se establecen principios rectores de la ciberseguridad y objetivos específicos (39).

La doctrina tuvo un tratamiento favorable al respecto del contenido de la mencionada Estrategia (40).

Además, existe la Dirección Nacional de Ciberseguridad, actuante en el ámbito de la Jefatura de Gabinete de Ministros, que entiende "en los aspectos relativos a la ciberseguridad y a la protección de las infraestructuras críticas de información, así como también a la generación de capacidades de prevención, detección, defensa, respuesta y recupero ante incidentes de seguridad informática del Sector Público Nacional", según las previsiones de la Decisión Administrativa 1865/2020 (41).

Dicha Dirección Nacional es la encargada de verificar el cumplimiento de las disposiciones de la Decisión Administrativa 641/2021 (42), norma que tiene por objeto contribuir a que "paulatinamente se incorporen controles que permitan una gestión más responsable, segura y transparente de la información que es tratada por ciertas áreas del Sector Público Nacional" (consid. 25), razón por la que se aprobaron los "Requisitos Mínimos de Seguridad de la Información para los Organismos del Sector Público Nacional" (art. 1°).

El objetivo general de dicho documento es "[e]stablecer los lineamientos generales y mínimos para los organismos del Sector Público Nacional comprendidos en el inc. a) del art. 8° de la ley 24.156, con el fin de proteger los activos de información, frente a riesgos internos o externos, que pudieran afectarlos, para así preservar su confidencialidad, integridad y disponibilidad". Luego, se determina la forma de revisión y actualización y las directrices sobre la política de seguridad del organismo; aspectos organizativos de la seguridad; seguridad informática y Recursos Humanos; gestión de activos; autenticación, autorización y control de accesos; uso de herramientas criptográficas; seguridad física y ambiental; seguridad operativa; seguridad en las comunicaciones; adquisición y mantenimiento de sistemas de información; relación con proveedores; gestión de incidentes de seguridad; aspectos de seguridad para la continuidad de la gestión; y el cumplimiento de la normativa aplicable.

En suma, existen avances en ciberseguridad, y las producciones normativas fueron receptadas favorablemente por la doctrina. Sin embargo, la norma central, en particular, la Estrategia Nacional de Ciberseguridad, en su objetivo tercero, acusa que es necesario el desarrollo del marco normativo.

No deja de ser un desafío, no deja de ser un riesgo constante, pero los lineamientos aparecen asentados adecuadamente, sobre lo que es necesario mantener un desarrollo continuo, atento a la amenaza permanente derivada de la innovación tecnológica.

IV. Características de los procedimientos administrativos electrónicos

IV.1. Expedientes electrónicos

Esta es una temática central, objeto central del Plan de Modernización del Estado y del expediente electrónico del ámbito judicial. Toda la normativa referida a la digitalización y despapelización del Estado apuntaba a volver digitales las actuaciones administrativas y judiciales.

Lo que se intentó con la digitalización de los expedientes administrativos y la depapelización del procedimiento administrativo (43) y del proceso judicial, es que estos fueran armándose sobre soportes digitales, sin cambiar su estructura protectoria. Es decir, el procedimiento administrativo seguía siendo, en el fondo, el mismo, aunque con documentos digitalizados. De igual forma ocurrió con el proceso judicial: en el fondo, las reglas son iguales a las existentes para el formato papel, aunque el soporte pasó a ser, casi en su totalidad, digital (44).

Ahora bien, más allá de estos logros, lo cierto es que la digitalización sin una actuación del funcionario más profunda e intensa puede acarrear algunos riesgos relevantes, ya que la digitalización de los canales, per se, importa una separación del individuo con el funcionario (judicial o administrativo). El administrado o justiciable pierde el contacto con el funcionario que gestionará su asunto. De modo que la contracara de la digitalización es que el agente (administrativo o judicial) queda implícitamente obligado a comprender, solo desde la lectura, lo que anteriormente podría considerar en una entrevista o en un intercambio interpersonal.

Es por eso por lo que la digitalización debe acompañarse de técnicas para sistematizar los procesos e identificar el grado de actuación y la relevancia de los asuntos que pudieran llegar a conocimiento de los despachos y los estrados. No todos los asuntos son iguales (tal como se pueden presentar en una pantalla), ni todos los funcionarios se desempeñan con igual nivel de especialización en todos los temas.

Así, queda en cabeza de los poderes que opten por un procedimiento digital y tienen un intercambio directo con los individuos, la obligación de mejorar su actuación de oficio, ya que, la abstracción y despersonalización de lo digital tiene potencia suficiente para sacar, de manera muy sencilla, a diferentes personas del trámite o de generar demoras de difícil resolución (45).

Esto, en la práctica, se debe traducir en un compromiso del funcionario para actuar efectivamente según las competencias para las que fue designado, ya que, los medios digitales, no se constituyen como instrumentos para excluir a los individuos del procedimiento o someterlos a demoras que los acaban desalentando, sino, antes

bien, para facilitar el acceso y gestionar de manera rápida y eficaz los intereses de los individuos.

Además, a nivel sistémico, los expedientes electrónicos deben garantizar, por lo menos, los mismos niveles de seguridad que tienen los expedientes en soporte papel. Es por eso por lo que, en el desarrollo de los expedientes digitales se deben considerar las cuestiones que se anotan a continuación:

i. Accesibilidad

Esta característica supone que se deben facilitar todos los medios y formatos de acceso al procedimiento administrativo, entre los que se encuentran los medios digitales y los medios físicos, ya que, el ecosistema digital, al no ser completo y total o cuando no es posible decir que toda la población dispone de los implementos técnicos necesarios, al momento, el procedimiento administrativo convive y necesita de integrarse con los medios tradicionales. Si bien la perspectiva de involucrar todos los procedimientos a un ecosistema digital todavía es un desafío lograr la conectividad en todo el territorio nacional.

Las normas, si bien obligaron a actuar en el ecosistema digital (46), con buen tino, se mantuvo vigente el régimen de trámites existente. En efecto, el art. 16 del dec. 1063/2016 indicó que no se aplican las pautas del dec. 759/1966, referido a la actividad de las mesas de entradas, así como que por el art. 11 del dec. 561/2016 se advirtió que no se aplican las pautas del dec. 333/1985 y sus normas complementarias y modificatorias al sistema del GDE. Es decir, tanto el dec. 759/1966 como el dec. 333/1985 no fueron privados de efectos. Esta última norma fue, sin embargo, modificada por el dec. 336/2017, en cuyos considerandos se anota que, al momento, subsiste la gestión en soporte papel en el Sector Público Nacional.

Ahora bien, si bien el dec. 1131/2016 obligó a la digitalización de lo existente en papel, no prohibió la actuación administrativa ante la existencia de documentos en papel. De esta manera, es posible pensar que sigue existiendo la posibilidad de que se presente quien pretenda instar un procedimiento por los mecanismos pensados para el soporte en papel.

En España, se elaboró un documento interesante que no tiene carácter normativo, pero sí tiene una impronta descriptiva, prospectiva y asertiva. Se denomina "La Carta de Derechos Digitales". Considera a estas cuestiones como "derecho a la igualdad y a la no discriminación en el entorno digital", de modo que sea factible garantizar el acceso efectivo a todas las personas a los servicios y oportunidades que dan los entornos digitales, advirtiendo que se debe garantizar el derecho a la no exclusión digital (47).

ii. Seguridad

Aquí trataremos de la seguridad o ciberseguridad específicamente del expediente electrónico, más allá de que es necesaria la implementación de una Política de Ciberseguridad, como se refirió anteriormente.

En tal sentido, este aspecto involucra a la seguridad de la gestión o administrativa, de las comunicaciones, de la seguridad informática, la seguridad ambiental y la seguridad física (48).

Además, implícitamente, y algunas veces, explícitamente, existe un deber de la Administración de preservar la seguridad de los datos que le proveemos para llevar adelante el procedimiento administrativo. Al momento en que el expediente se desarrollaba en papel, ese deber de seguridad se garantizaba conservando las actuaciones dentro de un edificio. En el expediente electrónico, la seguridad se da en dos momentos. Por un lado, evitando y/o mitigando los accesos no autorizados con los mecanismos técnicos disponibles (49); por otro, al momento en que el usuario protege sus credenciales de acceso. Es decir, existen responsabilidades compartidas entre la Administración y los administrados.

En cuanto al deber de la Administración, es razonable que se construyan arquitecturas de seguridad informática y un conjunto de políticas sobre seguridad, de modo que, en primer lugar, se conozcan las vulnerabilidades (50); luego, que se generen políticas para mitigar y evitar ataques informáticos; tercero, admitir metodologías de forensia informática que aseguren "que se pueda determinar adecuadamente el qué, quién, cuándo y cómo sucedió el incidente de seguridad, así como también ocuparse del correcto aseguramiento y preservación de los datos recolectados" (51).

Con ese esquema, es posible desarrollar las políticas de seguridad que sean necesarias según el tipo de gestión informática que se esté desarrollando.

iii. Inalterabilidad e integridad

Se puede decir que la inalterabilidad significa que el documento digital o electrónico no sea alterado en su contenido. En cuanto a su integridad, que este disponga de la totalidad de la extensión o de los elementos que lo integraron en su creación. Estas cualidades deben estar garantizadas por los sistemas de los expedientes digitales, en cuanto a que no sea posible modificar el contenido de los documentos digitales que los componen; ni tampoco, modificar o alterar el contenido del expediente digital sin que quede rastro de ello.

La ley 25.506 de Firma Digital, en su Anexo, vincula ambos conceptos, al definir integridad. Dice así: "Integridad: Condición que permite verificar que una información no ha sido alterada por medios desconocidos o no autorizados". De esa forma, es posible evitar el repudio del documento (52).

Existen interesantes trabajos de la doctrina extranjera donde se estudia la posibilidad de involucrar la tecnología de cadena de bloques (blockchain) para aspectos legales (53), de modo de lograr la inalterabilidad de documentos digitales. Allí se trata, sobre todo, la posibilidad de reemplazar la actividad notarial por dicha tecnología, aunque no deja de ser útil el documento a los fines considerar supuestos de descentralización en la conformación de documentos ciertos, y su consecuente inalterabilidad e integridad.

IV.2. Identidad, certificaciones y firma digital

Uno de los aspectos centrales sobre el desarrollo del procedimiento administrativo fue la validación de la identidad de los usuarios de los sistemas y de la utilización de firma digital.

Ello fue resuelto a través del art. 14 del dec. 1063/2016, por el que se modificó el art. 36, dec. 2682/2002. Allí se estableció que las Autoridades de Registro, que son las entidades facultadas por los Certificadores Licenciados, tienen el encargo de validar la identidad de quienes vayan a ser suscriptores de certificados, de modo de actuar en el ecosistema de la Infraestructura de Firma Digital de la República Argentina, donde existen diferentes actores que llevan a cabo actos y certificaciones diversas, en los términos de la res. de la Secretaría de Innovación Pública 649/2021 (54) (55).

A partir de esa certificación es posible suscribir documentos con firma digital, en los términos de la ley 25.506 y su dec. regl. 182/2019 (56), entre las que podemos identificar a la firma digital remota, a la firma digital con dispositivo criptográfico externo y a la firma digital con certificado del sistema (57).

Si bien ya contaba con la validez del art. 9º de la ley 25.506, se indicó específicamente, para la necesidad de firmas certificadas en el ámbito de la Administración Pública Nacional, que "[l]a firma digital de un documento electrónico satisface el requisito de certificación de firma establecido para la firma ológrafa en todo trámite efectuado por el interesado ante la Administración Pública Nacional, centralizada y descentralizada" (art. 2º del dec. 182/2019).

A su vez, en el art. 11 de la ley 25.506 se establece la calidad de original de todos los documentos electrónicos firmados digitalmente, así como sus reproducciones digitales a partir de originales. De allí que puede haber varios originales de un mismo documento firmado digitalmente, algo impensado en el papel.

Es interesante la doctrina de la Procuración del Tesoro de la Nación, donde se indicó, con fundamento en los antecedentes parlamentarios, lo siguiente: "La Ley 25.506 de Firma Digital incorpora el reconocimiento, con fuerza legal, de los distintos modos de expresión de consentimiento o declaraciones de conocimiento que puedan realizarse sobre soporte electrónico, aunque con distintos efectos. Entre ellos, la firma digital permite tener certeza de la identidad del firmante y de la integridad y no alteración del documento electrónico al que acompaña. La certeza se obtiene de la combinación de un mecanismo de creación en poder del firmante y de un mecanismo de verificación en poder de un tercero de confianza (p. ej., Certificador), que certifica identidad y contenido, y otorga plena seguridad e inviolabilidad de las expresiones volcadas en ese soporte. Las obligaciones que la ley impone al certificador garantizan que la sociedad pueda confiar en quienes obtienen una autorización del Estado para funcionar" (58).

IV.3. Aspectos de gestión del procedimiento administrativo electrónico. Posterior implementación de blockchain al procedimiento administrativo

Otra de las interesantes propuestas que conlleva un procedimiento administrativo electrónico es la digitalización de los expedientes existentes en soporte papel, de la constitución de domicilios electrónicos (a través del uso de correos o direcciones electrónicos) y, consecuentemente, la posibilidad de efectuar notificaciones digitales en dichas ubicaciones virtuales. Además, se facilita la toma de vista a distancia por medios electrónicos.

Estas mejoras fueron introducidas por la modificación realizada al dec. 1759/1972, reglamentario de la Ley Nacional de Procedimientos Administrativos, a través del dec. 894/2017 (59).

Es interesante ver que estos métodos digitales sirven para reducir las distancias físicas, pero en sí, no sustituyen los intercambios interpersonales. Es decir, facilitan la gestión y solucionan el inconveniente de tiempo y espacio, siempre y cuando, las presunciones y las obligaciones que las anteceden se hayan dado regularmente.

Además, otra mejora que supone la digitalización de los intercambios digitales es la precisión de fecha y hora.

Estas mejoras, en sí mismas, actualmente, solo atienden a resolver el inconveniente de la producción del documento en papel, del diligenciamiento, del acarreo del documento y de su acceso remoto.

Sin embargo, estas decisiones son un punto de partida necesario y fundacional para implementar, en un futuro, la certificación descentralizada que puede proveer la tecnología de blockchain u otras similares que la continúen.

Esta tecnología es capaz de proveer seguridad y certeza sin que intervengan terceros: Una vez que un documento se ingresa a una red descentralizada que opere bajo los parámetros de blockchain, la inalterabilidad depende de las verificaciones que provean los mismos usuarios de la red [\(60\)](#).

Aquí se pondrá en juego la toma de una decisión fundamental: si el Estado permite que los expedientes administrativos pasen a ser custodiados por los individuos de manera descentralizada, o si mantiene la custodia para sí. Sería una forma de despojarse del poder que significa poseer un expediente y no sería errado analizarlo en legislaciones futuras.

IV.4. Sistematización

Una carencia que no fue resuelta al momento, a pesar de los numerosos avances en materia de procedimiento y expedientes electrónicos, es que no se efectuó una sistematización de los circuitos administrativos.

La digitalización supone una abstracción que pone una barrera entre los hechos y las personas. Si bien los documentos en formato papel también distancian a las personas de los hechos, se transforman en una entidad en sí misma. De allí que sea posible la objetivación de cada asunto administrativo cuando se utiliza papel.

Ahora, la digitalización y la utilización de procedimientos electrónicos rompe con esa representación visual subyacente en un expediente en papel, y con ello, rompe con la representación de las personas involucradas. Eventualmente, los asuntos se transforman en un dato en algún disco rígido, y se ven, solo si se enciende la pantalla y el operador decide positivamente mirarlo. Además, la presentación digital saca al administrado de las ventanillas donde anteriormente interactuaba con los agentes.

Es decir, ahora, la actuación de oficio adquiere otras formas. Una de ellas es la sistematización, en el entendimiento que la actuación de oficio no solo importa el impulso de las actuaciones por parte de la administración, sino también de la implementación de mejoras para ponerse al servicio de la comunidad, en la medida en que la Administración no es una entidad aislada, sino que se da una interdependencia de la Administración con los administrados: cuando ambos operan por correlación de intereses, ambos se fortalecen; por el contrario, cuando uno intenta superar al otro, se genera una externalidad negativa para ambos, lo que siempre va a repercutir negativamente en el valor común que pudieran crear si cooperaran entre sí.

Existen estudios interesantes referidos a las técnicas de sistematización de los procesos internos de las organizaciones. Al respecto, es posible pensar en que replicar estudios de otras ciencias para analizar las maneras en los que se puede implementar una actuación de oficio. Para eso, es interesante ver la Teoría General de los Sistemas, sobre la que diferentes autores advirtieron distintas maneras. Katz y Kahn indican que existen subsistemas que llevan adelante el funcionamiento organizativo, que son los subsistemas de producción, de apoyo, de mantenimiento, de adaptación y de dirección. Kast y Rosenzweg indican que los subsistemas de los entes organizados son los subsistemas de metas y valores, técnico, estructural, psicosocial y administrativo [\(61\)](#).

Con tales parámetros, la Administración puede darle forma a la actuación de oficio, la que, por la incorporación de sistemas informáticos, no alcanza con solo impulsar las actuaciones que reciba de los particulares. En materia de organización administrativa luego de la aparición de los expedientes electrónicos y el trabajo a distancia, es necesario organizar la gestión interna para operar con eficacia y con sentido de finalidad, lo que puede ser plasmado en las normas.

V. Características de los actos administrativos automáticos

V.1. Cuestiones de la inteligencia artificial con respecto al acto administrativo

V.1.a. Nota introductoria

Con respecto al uso de la inteligencia artificial en el acto administrativo, se puede afirmar que todavía existe una distancia severa entre las normas y los datos que sean necesarios generar para plasmar en los algoritmos. Actualmente, si se pretendiera utilizar la inteligencia artificial para efectuar declaraciones sobre los derechos de los particulares, se van a encontrar comprometidos seriamente los elementos del acto, lo que afectaría su validez [\(62\)](#).

Ahora, no menos cierto es que mucha actividad administrativa está siendo desarrollada a través del uso de la inteligencia artificial. Y sobre eso, es apropiado evaluar que los ecosistemas son más potentes que los institutos

en sí mismos. En nuestro caso, el ecosistema de intercambio se encuentra en pleno desarrollo, por lo que los institutos de derecho administrativo, en muchos casos, deben ser repensados. Aunque, naturalmente, esa revisión se debe dar contemplando las protecciones históricas que logró el derecho, y como se dijo anteriormente, no ceder ante la técnica.

Por eso, en este apartado, se tratarán los factores determinantes de la inteligencia artificial en el derecho administrativo, y puntualmente, en el acto administrativo.

Bonina (63) hace un interesante estudio sobre las distintas conceptualizaciones involucradas al momento de la utilización de la inteligencia artificial en el derecho. Indica que inteligencia artificial es "[c]ualquier técnica que permita a las computadoras imitar la inteligencia humana. Incluye a machine learning"; en tanto, machine learning es "[u]n sub-conjunto de IA que incluye técnicas que permiten a las computadoras mejorar en la ejecución de tareas a partir de la experiencia. Incluye deep learning"; y al concepto de deep learning lo considera como "[u]n sub-conjunto de machine learning basado en redes neuronales que permite que una máquina se entrene a sí misma para realizar una tarea". Concluye con que la implementación de estas técnicas supone el inicio de una etapa de transformación en los modelos, pero nada dice sobre la juridicidad de la técnica de Inteligencia Artificial.

En un abordaje similar, Corvalán, Sá Zeichen y Albertsen (64) dividen en seis los niveles de automatización algorítmica, a saber: asistencia algorítmica básica, moderada, y fuerte; automatización restringida, moderada y fuerte. A partir del cuarto nivel, indican los autores, "comienzan los problemas", ya que en esa división que elaboran y a partir de esa categoría, se reemplaza la voluntad del funcionario.

Ambos trabajos, si bien muy profundos y fundados, de lectura recomendada, no llegan a pronunciarse sobre la ruptura que produce la utilización de la inteligencia artificial en materia de acto administrativo, con respecto al art. 7° de la ley 19.549. Sin embargo, advierten complejidades y dan cuenta de que no existe una réplica lineal del razonamiento que realiza el funcionario público (para verificar el cumplimiento de los elementos del acto), por parte del algoritmo.

V.1.b. Algoritmos

Un algoritmo es una serie de reglas que acarrearán un cálculo. Este cálculo puede ser hecho a mano o, usualmente, mediante una máquina o una computadora. Normalmente, la ejecución de un algoritmo no involucra intervención humana (65).

Totaro et al. indicaron que el uso de algoritmos es útil a los fines efectuar cálculos de lo que los autores llaman separaciones de distanciamiento físico o de espacio y tiempo, pero no para hacer cálculos que conllevan en sí interacciones sociales, porque el algoritmo, supone la eliminación de la comunicación entre los actores, en contra de las reglas de dichos procesos interactivos entre humanos.

En tal sentido, enfatizan que existe una "aplicación obstinada de la lógica del cálculo al factor humano" que genera que se produzca "una suerte de cálculo circular", de modo tal que no se logre el resultado que se persigue (66).

Hay veces donde se puede generar un algoritmo que resuelva inconvenientes sociales, reduciendo las distancias físicas, y que podría resolverse en el plano de la realidad. Por ejemplo, la intermediación en los mercados financieros modernos a través del uso de dinero electrónico. Ese dinero podría ser llevado físicamente al agente, el agente extender un recibo, y luego, adquirir el producto financiero que le fue encargado. Dicho proceso, en la actualidad, se resuelve mediante algoritmos que se basan en cálculos estrictamente matemáticos.

El segundo tipo de algoritmos, y que son los que importan al derecho administrativo, Totaro et al. los denominaron algoritmos burocráticos. Este tipo de algoritmos dificultan la interacción social, no por la distancia que se genera entre las personas, pero sí porque eliminan la comunicación para conectarlos en las reglas de un proceso matemático iterado.

Incluso afirman que "[e]l algoritmo burocrático (...) no genera un problema externo, sino intrínseco a la propia lógica de las organizaciones que se basan en él. La encapsulación de individuos dentro de pasos algorítmicos está implícita en el concepto de burocracia. Por tanto, en este caso, el algoritmo [burocrático] es la causa del problema y, por tanto, no puede ser su solución. Los seres humanos no pueden utilizar el algoritmo burocrático para resolver el problema porque ellos son las herramientas del algoritmo, no al revés" (67).

V.1.c. Redes neuronales artificiales. Su arquitectura

Las redes neuronales son un método de aproximación. Son formas de representar un cálculo complejo, en el que existe un dato de ingreso, y luego de varias operaciones, se emite un dato de salida. Son más complejas que los algoritmos, porque dentro de cada neurona de la red neuronal, pueden existir —aunque no necesariamente—

algoritmos que generen soluciones para cada proceso.

Su nombre deriva de la intencionalidad de replicar la estructura del razonamiento humano, para conformar un método estadístico a través de la interrelación de funciones matemáticas propias en cada neurona, para así obtener una solución al problema planteado.

La complejidad de la red neuronal se explica porque estas permiten hacer estadística no lineal, con base en la técnica de backpropagation o propagación hacia atrás. Esto importa que el cálculo efectuado por cada neurona se evalúa comparándolo con el resultado una la iteración ya dada, de donde surge el costo de cada operación, lo que busca ser minimizado en un nuevo cálculo, repitiéndose el proceso hasta obtener el menor costo posible de las iteraciones, según los valores que se hayan establecido para la red.

A partir de este método, se dice que existen redes neuronales de aprendizaje, porque utilizan información ya recibida, de la que se recogió un error, el que sirvió para generar una nueva iteración a menor costo.

La arquitectura de la red neuronal va a ser tal según la necesidad que se tenga, ya que la clasificación será mejor en unas que en otras, con base al problema que se intenta resolver. En ese sentido, se puede mencionar existen diversos tipos de redes neuronales, entre las que se pueden encontrar redes Feedforward, las que utilizan distintas funciones: Squasher Functions, Radial Basis Functions, Ridgelet [\(68\)](#).

Una de las más utilizadas es red Feedforward (Figura 1), donde x_1 , x_2 y x_3 son los datos de ingreso; n_1 y n_2 son las neuronas, cada una con funciones de entrada, de activación y de salida; el dato de salida está identificado con la letra y .

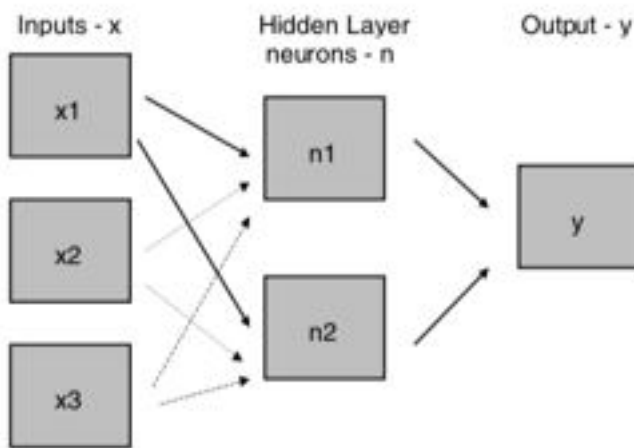


Figura 1: Red Feedforward. Fuente: McNeils, Paul [\(69\)](#).

Las funciones se activan cuando se dan, en los hechos de la realidad, los valores que les sean asignados a cada uno de ellos. De esa manera, el espectro numérico dado por el dato de entrada va a admitir o no la activación de la neurona.

Las activaciones de las neuronas se dan utilizando funciones. A modo testigo, la función sigmoidea logarítmica, en la que podemos ver que en las abscisas (x , línea horizontal), los valores de -5 a 5 son los parámetros que recibe la función; y las ordenadas (y , línea vertical), los valores de 1 a 0 indican la activación de la función [1] o la no activación de la función [0]. De esa manera, según se den los valores seleccionados arbitrariamente para las abscisas, se activará o no la función.

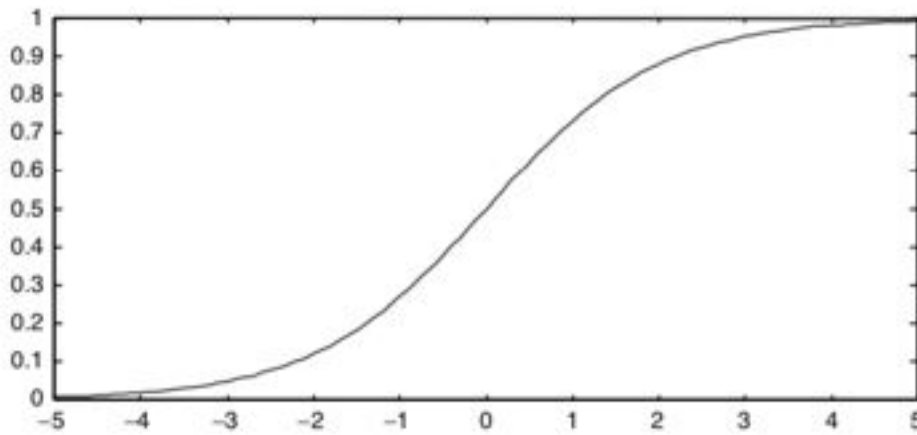


Figura 2: Función sigmoide logarítmica. Fuente: McNeils, Paul (70).

Por ejemplo, si quisiéramos hacer una función sigmoide logarítmica para identificar un acto nulo por vicio en la competencia, podríamos decir que la función de nulidad se activa (adquiere el valor de 1) si el acto administrativo fue dictado con incompetencia material (en nuestro ejemplo, el acto debía ser emitido por el Poder Judicial y lo emitió la Administración: eso sería una incompetencia material). Para eso, deberíamos parametrizar en números, el hecho incompetencia material, estableciéndole valores de -5 a 5. De esa forma, la red neuronal puede diferenciar los actos nulos si se activa la función, y los actos regulares si la función no se activa. Naturalmente, estos parámetros no pueden surgir de un programador, sino que tienen que ser establecidos por una norma.

El interrogante decisivo para implementar el uso de actos administrativos automáticos es si todos los vicios del acto y sus excepciones pueden ser parametrizadas (71).

Hay otras arquitecturas de redes como la denominada Feedforward con conexiones salteadas, que tiene el siguiente diagrama:

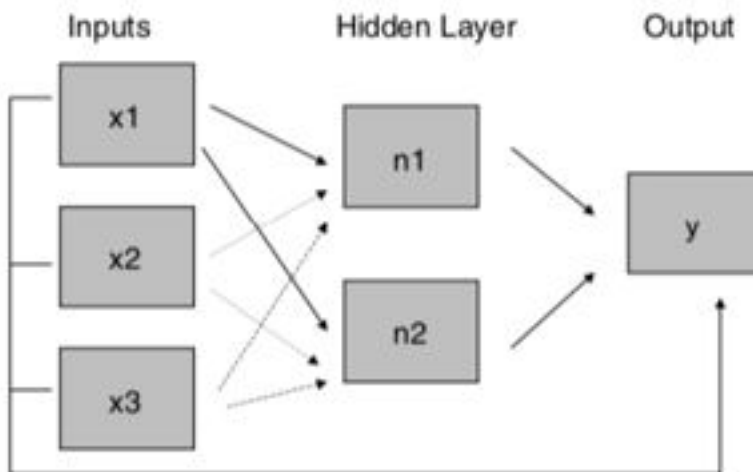


Figura 3: Red Feedforward con conexiones salteadas. Fuente: McNeils, Paul (72).

También existe la denominada Feedforward con múltiples capas:

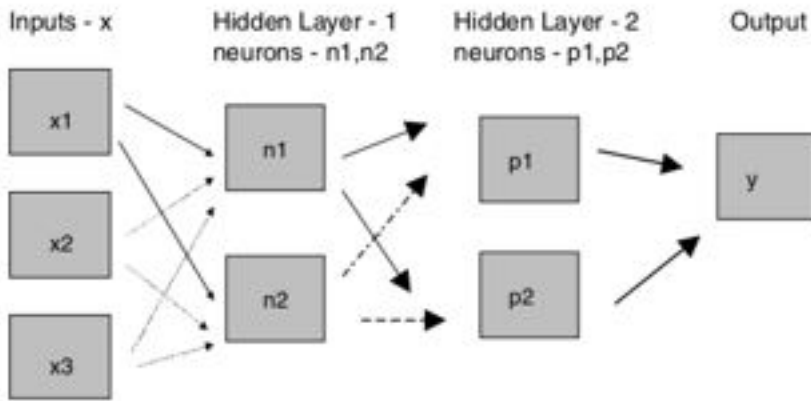


Figura 4: Red Feedforward con múltiples capas. Fuente: McNeils, Paul (73).

Otra arquitectura, las redes denominadas recurrentes:

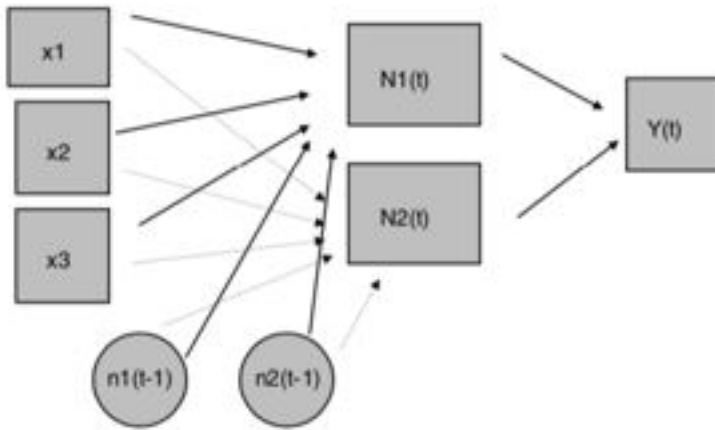


Figura 5: Red Recurrente. Fuente: McNeils, Paul (74).

Y, por último, las redes con múltiples salidas:

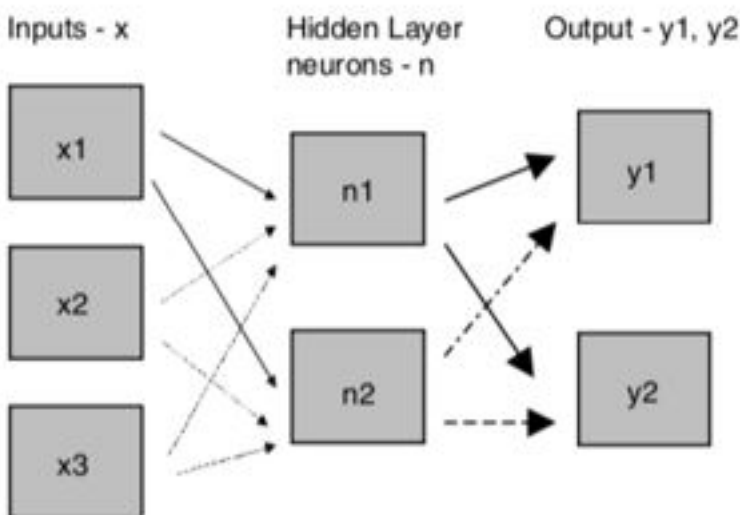


Figura 6: Red con múltiples salidas. Fuente: McNeils, Paul (75).

Además, vale advertir, a cada una se le agrega la cantidad de neuronas según el espectro de datos que se intenta cubrir. La diferencia entre ellas radica el diseño de los pasos de cálculo y las funciones de activación de las neuronas (76).

Ahora bien, este modo de segmentar la realidad y abstraer los procesos en funciones matemáticas y arquitecturas de redes, como se dijo, separa a la Administración de los administrados, y los instrumentaliza como parte del cálculo de la red o del algoritmo.

A pesar de ello, no deja de ser cierta la posibilidad de que las administraciones busquen aplicar algoritmos y redes neuronales artificiales a problemas de los seres humanos. Por eso, es relevante entender que las redes neuronales y los algoritmos son útiles cuando buscan reducir la distancia física, cuando atemperan y modelan el problema espacio-tiempo. Pero no son útiles cuando buscan reemplazar las relaciones humanas, porque el problema que intentan resolver (la relación con el hombre) es una de las mismas variables que el método utiliza.

Esto nos lleva a requerir que estos métodos de cálculo sigan algunas reglas de diseño: que no intenten reemplazar las intervenciones humanas, sino que solucionen problemas físicos, que no estén ideologizadas, que se diseñe apropiadamente la red, que existan reglas de testeo y performance, que el lenguaje de programación admita una adaptación transgeneracional, que exista un criterio de evaluación de datos, que se pueda hacer una revisión visual de la muestra.

En cualquier caso, a pesar de que se invoque que las decisiones de inteligencia artificial no son controlables, sí lo son las reglas de diseño, las que deben ser determinadas para cada caso en particular, para cada problema específico.

Eventualmente, ello puede seguir el esquema conocido por el derecho administrativo: existen pliegos de bases y condiciones generales que establecen las reglas de los pliegos de bases y condiciones particulares. Entonces, un acto general de carácter normativo establece los parámetros a los que se sujetará el acto general no normativo, el que es utilizado para el caso concreto. Quizás ello pueda ser una aproximación a la solución del abordaje normativo en asunto de redes neuronales y algoritmos.

V.1.d. Sesgos

En el uso de la inteligencia artificial aparecen los sesgos. Puede ocurrir que una gran base de datos no sea fácil de entender antes de introducirla en una red neuronal. En ese proceso de análisis, puede existir un dato no visto o sesgado, y el analista extravía esa categoría en el diseño de la red.

Este es un riesgo muy posible en un sistema donde las normas existen con pautas interpretables, de modo que un ángulo no visto de un artículo o una jurisprudencia no considerada por el diseñador puede generar un resultado errado en el uso de inteligencia artificial.

Otro sesgo en el trabajo con inteligencia artificial es el de information retrieval o de recuperación de información (77). Este inconveniente se puede identificar como aquel que surge por utilizar una base de datos incompleta, por efectuar una selección de casos que no es representativa del universo total de casos o por errar en el método de obtención de datos para su uso.

Esto puede impactar en el aprendizaje de una red neuronal, de modo que los resultados finales estén sesgados por utilizar un universo irreal de casos.

Existen otros sesgos, pero estos dos pueden ser tratados como los más posibles para el caso del uso de la inteligencia artificial en asuntos de derecho administrativo.

V.1.e. Derechos en juego

La inteligencia artificial, al ser una buena herramienta de gestión, tiene la idoneidad de afectar transversalmente a todos los derechos involucrados en asuntos de derecho administrativo.

Sin embargo, como todo riesgo, puede ser controlado o mitigado, siempre y cuando, se lo dimensione y evalúe con ecuanimidad.

Una de las primeras maneras de hacerlo es estableciendo reglas de uso de inteligencia artificial, en las que se consideren las siguientes pautas: 1) Que no se aplique inteligencia artificial de manera omnimoda en el proceso decisional; es decir, deben existir reductos de humanidad, en la medida de lo posible, de modo que existan chances de hacer evaluaciones humanas intermedias. 2) Que haya una determinación de reglas para los programadores. 3) Que haya una determinación de reglas para el desarrollo de normas generales y abstractas a ser utilizadas. 4) Que haya una determinación de reglas sobre el régimen de invalidez, impugnación y notificación. 5) Que haya una determinación de reglas para solución de problemas en el uso de redes neuronales (qué ocurre ante la parálisis de la red —los algoritmos no convergen y van a buscar números muy grandes—, mejores funciones a implementar, solución de la contradicción, optimización y reemplazo de algoritmos, etc.).

Trabajar con redes neuronales o con algoritmos sin estas determinaciones previas es extremadamente riesgoso y no debería admitirse la juridicidad de los resultados que estos puedan generar.

V.1.f. Principios jurídicos específicos en el uso de la inteligencia artificial en asuntos de derecho administrativo

La prudencia en el uso de inteligencia artificial requiere que se verifique la idoneidad de la herramienta para atender el problema, si el compromiso a los derechos no sugiere una solución menos gravosa, que se merezca el costo y el beneficio de utilizarlo, que analicen las variantes de riesgo, los escenarios en caso de fallas, la probabilidad de la ocurrencia de fallas y una ponderación revisada de las decisiones que configuraron el algoritmo o la red neuronal, con registro específico de cada uno de los momentos decisionales.

Debe existir un uso responsable de la inteligencia artificial, definiéndose un elenco de situaciones cuyas características deban ser tratadas con esta herramienta, en la consideración a que la inteligencia artificial separa a la Administración del administrado.

El uso de la inteligencia artificial tiene que estar guiado por el principio precautorio, a partir del cual, la inteligencia artificial no puede generar daño, tanto por quitar derechos como por no concederlos a quien se debe por normas.

Se tiene que considerar la trazabilidad de las decisiones involucradas en situaciones de uso de inteligencia artificial, y de los resultados parciales que se puedan ir obteniendo, ya que, una vez que la red inicia el cálculo iterado, no es posible identificar singularmente cada uno de los procesos de cálculo dentro de las neuronas. De hecho, la utilidad de este tipo de herramientas es manejar de forma rápida grandes bases de datos, cuya administración con algoritmos o redes supone una complejidad matemática elevada, siendo su trazabilidad, prácticamente imposible; o, de hacerse, prácticamente inútil por la cantidad de información generada: para leerla, sería necesaria otra red neuronal, la que también debería ser trazada.

En cuanto a la transparencia, los administrados tienen derecho a conocer la información descriptiva y técnica utilizada para desarrollar la red neuronal y/o los algoritmos con los que se administren sus derechos.

Las decisiones tomadas por y con inteligencia artificial deben ser auditables, de modo que, con posterioridad a su uso, se admita verificar si las reglas que condicionaron a la inteligencia artificial se cumplieron. En particular, las reglas referidas a que existan evaluaciones humanas intermedias, sobre programadores, sobre reglamentos (si existen), sobre invalidez, impugnación y notificación en cada caso, y sobre la solución de problemas.

Debe existir una reserva de humanidad y de retroacción de la decisión algorítmica, en cuyo caso, deberá analizarse si eso opera con efectos suspensivos o devolutivos.

En la medida de lo posible y según cada caso, debe atenderse el principio de no exclusividad de la decisión algorítmica, el que apunta a que no se deje a que los sistemas algorítmicos o redes neuronales tomen decisiones autónomamente. En la medida de lo posible, siempre tiene que existir un decisor humano.

Por naturaleza, los algoritmos y las redes neuronales sirven para separar conjuntos según categorías. Si bien, difícilmente en la Administración Pública se establezca un reglamento algorítmico que haga una discriminación indebida, pueden darse supuestos de discriminación por no contemplar u omitir categorías de manera involuntaria. De ahí que este principio de no discriminación algorítmica sea un espacio importante en la programación.

Por último, en cuanto a los principios, la cognoscibilidad importa la necesidad de dar a conocer la existencia de procesos automatizados en la toma de decisiones.

V.1.g. Cuestiones éticas en el uso de inteligencia artificial

Uno de los principios, el precautorio, supone el deber de no dañar en asuntos de derecho administrativo. Si bien es una verdad evidente, no menos cierto es que la falta de claridad en la impugnabilidad o en la extinción de un acto administrativo automático puede suponer un retroceso severo en materia iusadministrativa.

Por eso, la ética no deja aparecer como subyacente en el trasfondo de todas las decisiones por las que se implemente la inteligencia artificial en las administraciones. Por ejemplo, la denegatoria de inscripción en un registro, decidida por un algoritmo, puede suponer un daño severo al particular.

De ahí que se deba considerar un elenco de herramientas protectorias al momento de implementar decisiones mediante inteligencia artificial.

En líneas generales, todavía esta tecnología se encuentra en una etapa exploratoria y de desarrollo, y que, si bien opera con notables resultados en muchos campos, todavía no es una tecnología profundamente conocida por todos los operadores jurídicos. De ahí que, si se pretende utilizar, deba ser implementada paulatinamente, formando a los operadores, desarrollando la norma y promoviendo la participación ciudadana a través de audiencia pública y en forma previa, cuando la dimensión lo amerite, de modo que exista un control suficiente

antes de que se eche a correr el proceso iterativo de una red neuronal.

Por esas consideraciones, el juicio técnico debe estar muy justificado, y cada una de las elecciones, debe estar fundamentada, no solo para analizar la razonabilidad de la decisión en forma previa por las autoridades y los administrados, sino también, para permitir el control judicial posterior.

En esto, no deja de ponerse en tela de juicio la axiología subyacente en las decisiones referidas al uso de la inteligencia artificial: ¿qué valores pesan o se ponderan en la IA? ¿Existe una mirada a favor de la dignidad, intimidad, privacidad, libertad, legalidad, justicia, diversidad, perspectiva de género, protección de humanidad, no discriminación, protección a grupos minoritarios (ancianos, niños, enfermos)?

Estos interrogantes aparecen porque la inteligencia artificial tiene vocación de aborarlo todo. De modo que el todo que considera el derecho administrativo, también debe ser considerado por los operadores de la inteligencia artificial.

Un tema esencial es el referido a la captura de información y la dignidad humana: El ser humano no puede ser considerado como una mina de la que se extrae información. Más allá de que existan corporaciones que —tras fronteras— intenten hacerlo y lo logren, la Administración, por constituirse como ser ético por excelencia, no puede instrumentalizar a los seres humanos, o utilizar su intimidad o su espacio de datos sensibles, como un medio para obtener una finalidad, por más altruista que esta sea. Estos datos sensibles, en puridad, en la actualidad, son más que los que propone la Ley de Protección de Datos Personales (78): por ejemplo, ahora se recolectan datos sobre los gustos, las preferencias de toda índole, las ubicaciones, las sensibilidades, las amistades, los momentos en los que miramos el teléfono, las compras, las conversaciones, etc. Estos también deberían ser considerados como datos sensibles. El Estado, antes bien, debe tratar este escenario resguardando los derechos en juego.

Ahora bien, con estos canales de comunicación, herramientas digitales y sistemas tecnológicos que conforman un ecosistema relativamente nuevo, cabe preguntarse cuál es el plexo social subyacente: ¿Hay un modelo de negocios detrás? ¿el derecho administrativo tiene las herramientas para detectar si ese modelo es pernicioso y así regularlo? Son interrogantes éticos, cuya respuesta signará las decisiones a tomar sobre este campo.

V.2. Tramitación automática

Un interrogante práctico emerge cuando es necesaria la emisión de actos de respuesta inmediata. Tomaremos como caso de estudio la habilitación de circulación que otorga la aplicación "Cuid.AR" (79).

La Subsecretaría de Gobierno Abierto y País Digital, mediante disp. 432/2020 (80) aprobó el Repositorio de Versiones de los Términos y Condiciones de la Aplicación Cuid.AR.

En esta aplicación, el usuario ingresa unos datos, se hace un autodiagnóstico sobre cuestiones de salud, y en caso de que no existan parámetros de restricción, surge una pantalla que dice, entre otras cosas, "Certificado único de circulación. Habilitado".

Esta aplicación da por resultado un acto favorable o de gravamen, de respuesta inmediata.

La juridicidad de este tipo de decisiones automáticas va a estar signada por la juridicidad y razonabilidad utilizadas para desarrollar las reglas de programación de la aplicación. Desde luego, el acto favorable no traerá consigo hipótesis de conflicto. Ahora, en caso de que se emita un certificado que impida circular, surgirán numerosas cuestiones referidas al régimen de validez del certificado, a su notificación, a sus formas de impugnación y a su posterior control judicial, lo que acarrea una potencialidad de saturar las oficinas administrativas.

De allí que no existen inconvenientes cuando sea necesaria la emisión de actos administrativos automáticos de carácter favorable, aunque ello tiene una contracara, que la no emisión o su denegación expresa, supone desplegar una serie de chances procedimentales que no pueden cercenarse. Atentarían contra la tutela administrativa efectiva.

Por eso, este tipo de soluciones —a instancias de atender a las razones de justicia que siempre tienen los administrados— deben contar con un apartado para interponer, por la misma vía, las impugnaciones a partir de las cuales se revise, por un operador humano, el acto automático de gravamen.

V.3. Certificación y presunciones

Los medios digitales, al transformar los hechos de la realidad en documentos digitales, necesitan utilizar presunciones para poder operar.

En términos del diseño de los sistemas, es fundamental presumir que quien utiliza ciertas credenciales de

acceso es el usuario que fue habilitado para ello, que las personas identificadas digitalmente son quienes poseen las credenciales de acceso, que el usuario no cedió las credenciales, que la firma digital impuesta en un documento a través de la introducción de una contraseña significa la voluntad de obligarse, y que los documentos digitalizados se corresponden con los documentos existentes en formato papel.

Es decir, hay una presunción de que lo representado digitalmente guarda un correlato con lo ocurrido en el plano real o físico.

Estas presunciones operan como tales en forma de obligaciones: se obliga a no ceder la clave, se obliga a subir digitalmente un papel existente, se obliga a aceptar términos y condiciones en las cuales se identifican conductas que causan efectos.

Esto supone una mirada jurídica, en tanto a que tales presunciones, transformadas en obligaciones o no, en primer lugar, deben tener origen normativo, y no pueden presuponerse si no existe una advertencia específica. En segundo término, el Estado debe facilitar la digitalización del medio si es que ello es necesario para operar en términos digitales, o bien, admitir la posibilidad de la utilización de medios convencionales, como el papel.

Estos modos de actuar pueden no operar así en el ámbito privado, pero la sujeción que propone el derecho público obliga al propio Estado en establecer reglas para efectuar este tipo de efectos en las conductas de los particulares, así como facilitar todos los canales de acceso al procedimiento administrativo.

VI. El sistema del dinero electrónico. La posibilidad de implementarlo como servicio público

Existe un icónico trabajo de Chaum et al., donde se establecieron los lineamientos y protocolos que dieron origen al dinero electrónico. Allí se escribió un protocolo para su emisión y uso, con dos caracterizaciones especiales: la incondicional imposibilidad de rastrearlo, a menos que, mediante un fraude, se utilice doblemente por la misma persona; y su múltiple uso por usuarios sucesivos (81).

Con las tarjetas de crédito y la digitalización de las cuentas bancarias, el dinero electrónico fue extendiéndose en los usuarios del sistema bancario, hasta tornarse relevante en cuestiones de interés público y, en la actualidad, con un interesante impacto en la función administrativa.

Valencia advierte que la evolución de las telecomunicaciones móviles y, sobre todo, el acceso inalámbrico a internet trajo aparejado un desarrollo relevante en el uso del dinero electrónico, con la potencialidad de transformarse en un servicio público de bajo costo, en miras a lograr la inclusión financiera y económica (82).

En Argentina, con la modificación a la Carta del Banco Central del 2001, se introdujo el dinero electrónico en la legislación argentina. Con la ley 26.739 (83) se indicó, como facultad de la Superintendencia de entidades financieras y cambiarias del Banco Central de la República Argentina, la siguiente: "f) Aplicar las disposiciones legales que, sobre el funcionamiento de las denominadas tarjetas de crédito, tarjetas de compra, dinero electrónico u otras similares, dicte el Honorable Congreso de la Nación y las reglamentaciones que en uso de sus facultades dicte el Banco Central de la República Argentina".

Además, el dinero electrónico tuvo tratamiento normativo en la res. ANSeS 39/2019 (84), y en la res. de la Unidad de Información Financiera 300/2014 (85).

Es interesante referir a que, en cuanto a esta última resolución, para el organismo antilavado, en el art. 2° de la norma citada, se exhibió una distinción entre monedas virtuales y dinero electrónico (86), haciendo una afirmación anticipada, que con el paso del tiempo, se tornó imprecisa, ante la aparición de las GovCoins (monedas emitidas por los gobiernos), en cuanto a que estas sí se encuentran emitidas por un país y adquieren la relevancia de mover el poder desde los individuos al Estado, alterar la geopolítica y cambiar cómo se distribuye el dinero, por vincular directamente a los individuos con los bancos centrales (87).

Luego del desarrollo de las finanzas descentralizadas (donde Bitcoin es la más prominente, seguida por monedas, billeteras e intermediarios financieros), el paso siguiente puede ser la emisión de monedas digitales por los gobiernos, lo que conlleva la potencialidad de concentrar fuertemente el poder en los Bancos Centrales, por permitir así manejar la política económica sin los bancos minoristas, así como por poder actuar sin el costo de su intermediación a través de productos bancarios (88).

Ello adquiere suma relevancia, en tanto configurará la manera en que el Gobierno se exhiba a los administrados, quienes podrán confiar o no en ese dinero electrónico como medio de intercambio, de reserva de valor y de unidad de medida. Por su parte, esta tecnología pone en cuestionamiento si los gobiernos podrán trazar cada una de las unidades de dinero electrónico, y si podrán retirarlo sin más o devaluarlo, si así fuera de su interés (89).

Lo expuesto no solo es un asunto que atañe a la regulación del sistema financiero y a la política monetaria, financiera, cambiaria y económica de un país, sino que también estos extremos tienen que ser considerados

necesariamente por el derecho administrativo como ciencia, en cuanto a que el control de tales actos acabará siendo dado, naturalmente, en el fuero contencioso administrativo.

Además, todos los asuntos administrativos de los tres poderes del Estado que conlleven el pago o la percepción de dinero necesitarán embeber, en su objeto, una determinación con respecto al dinero electrónico involucrado. Es decir, muchas veces, la última acción relevante que ocurre en un expediente administrativo es un envío de dinero (pago de salarios y jubilaciones, pago de multas, asignación de subsidios, cobro de cánones, etc.), razón que llama a integrar los expedientes administrativos con el dinero electrónico y elaborar técnicas optimizadas de sistematización. En suma, se podría afirmar que la ejecución presupuestaria, prácticamente en su totalidad, se ejecuta mediante expedientes y dinero electrónico.

Ahora bien, en cuanto al uso de monedas gubernamentales y de dinero digital, tiene un rol prominente el Congreso de la Nación, en cuanto a que las normas a ser aplicadas por el Banco Central son aquellas que dicte el Poder Legislativo.

Sin embargo, las protecciones que se deben dar en la filosofía propia de cada norma serán las que protejan los derechos de los particulares, en cuanto a que la tecnología tiene la potencialidad de anteponerse, con alto grado de sofisticación, a los derechos de los individuos, siendo inadmisibles, aquellas que supongan alterar los derechos fundamentales, la dignidad humana y el principio *pro personae*.

Entonces, al darse un avance en materia tecnológica, al existir un fuerte incremento de los pagos electrónicos alrededor del mundo y al aparecer en el espectro las monedas gubernamentales, es posible analizar el establecimiento de un sistema de dinero digital de bajo costo, como servicio público, como una acción positiva del Estado en favor de los individuos.

VII. Conclusiones

En este trabajo se intentó realizar una taxonomía de los asuntos referidos a tecnología de información y comunicaciones que involucran al derecho administrativo, desde que el particular tiene una necesidad para instar una actuación hasta que se genera una consecuencia patrimonial para el particular o para la Administración.

Se trataron asuntos que aparecen tratados normativamente, y se buscó dar un abordaje técnico y explicativo del porqué de cada uno de ellos.

El uso de la inteligencia artificial ya es moneda corriente en los despachos administrativos. La arquitectura de las redes neuronales artificiales y demás características de los actos automáticos deben ser considerados con carácter normativo. Además, se puede afirmar que nada impide que el uso de la inteligencia artificial sea bajo principios específicos, con una mirada ética en favor del ser humano.

Como consecuencia de estos análisis, se observa una relevancia central y estratégica de los canales de intercambio y de los servidores, de la ciberseguridad y de la necesidad de que el derecho administrativo tenga un enfoque sobre la posibilidad de tratar como servicio público al sistema de dinero electrónico, más allá de que alguna vez se implementen (o no) monedas digitales emitidas por los gobiernos.

El aporte que puede hacer un derecho administrativo autónomo en aspectos de derecho administrativo digital es perseguir mejoras para los individuos, buscando las razones de justicia y equidad en los modos de establecer las relaciones, a los fines de lograr la creación de valor común, y que, de esa manera, se construya un derecho administrativo más empático y cercano a la sociedad.

(A) Abogado por la Universidad de Buenos Aires, magíster en Derecho Administrativo por la Universidad Austral y maestrando en Finanzas por la Universidad de San Andrés. Publicó diferentes trabajos de investigación y es autor del libro "Teoría General del Derecho Administrativo". Fue profesor invitado en diferentes universidades y actualmente enseña Derecho Administrativo en la carrera de grado en la Universidad de Buenos Aires.

(1) AA.VV., "Tratado de Inteligencia Artificial y Derecho", Ed. La Ley, Buenos Aires, 2021, t. II; LAMBER, Néstor D., "Reconocimiento automático de validez y eficacia del documento electrónico por la interoperabilidad en los sistemas de gestión documental de los poderes del Estado", TR LALEY AR/DOC/2768/2019; DELPIAZZO, Carlos E., "Lo nuevo y lo permanente de la actuación administrativa a través del procedimiento administrativo electrónico", TR LALEY AR/DOC/8768/2012; VALCÁRCEL FERNÁNDEZ, Patricia, "La técnica al servicio del derecho: la categoría del documento administrativo electrónico. Un estudio desde el Derecho español", publicado en: RDA 2010-74 , ps. 943 y ss., cita: TR LALEY AR/DOC/9954/2012; FERNÁNDEZ ESCUDERO, Josué, "Compensación electrónica de medios de pago (apuntes descriptivos del régimen argentino. aspectos jurídicos y operativos)", publicado en JA 1999-II-895, cita: TR LALEY 0003/000138.

- (2) Función para realizar una distribución de probabilidades de eventos (función gaussiana). MARTÍNEZ BENCARDINO, Ciro, "Estadística Básica Aplicada", Ecoe Ediciones, 4ª ed. (2012), p. 333.
- (3) La curtosis es una medida de la altura de la curva de la campana de Gauss, lo que importa una forma específica de distribución, donde se pueden identificar hechos ("outlayers") que se dan con poca o mucha frecuencia. V. MARTÍNEZ BENCARDINO, C., ídem, p. 200.
- (4) BONINA, Nicolás, "Abogacía 4.0. Transformación digital de la profesión. Legal management, legal design & legal operations", publicado en LA LEY del 31/08/2020, ps. 13 y ss.
- (5) OCDE, "Revisión del gobierno digital en Argentina. Acelerando la digitalización del sector público", 2018, informe online disponible en <https://www.oecd.org/gov/digital-government/digital-government-review-argentina-key-findings-2018-es.pdf> (último acceso: 29/11/ 2021), publicado en BONINA, N., ídem.
- (6) IVANEGA, Mirian M., "El teletrabajo en el empleo público", publicado en: El Teletrabajo en el Ordenamiento Jurídico Argentino. Volumen I, Posibilidades y Oportunidades del Teletrabajo, con fecha 24 de agosto de 2020, Cita: IJ-CMXXIII-660.
- (7) IVANEGA, Mirian M., "Nuevamente... dudas y certezas del teletrabajo en el empleo público", en El Teletrabajo en el Ordenamiento Jurídico Argentino. Volumen II - Posibilidades y Oportunidades del Teletrabajo, Publicado en IJ Editores, con fecha 26 de abril de 2021, Cita: IJ-MVI-761.
- (8) La PTN, en Dictámenes IF-2021-63738609-APN-PTN del 15-7-2021, se dijo: "si excepcionalmente ... la persona citada invocase fundadas razones que imposibilitasen su traslado y/o el riesgo para su salud que esto implicaría, quedando a su cargo alegar y acreditar dicho impedimento, podría ... el órgano responsable de la instrucción de la actuación sumarial, de considerar atendibles las razones esgrimidas, disponer la realización de teleconferencias, respetando las pautas sentadas por esta Casa...".
- (9) WEGNER, Peter (1996), "Interoperability", ACM Computing Surveys (CSUR), 28[1], 285-287.
- (10) HEILER, Sandra (1995), "Semantic interoperability", ACM Computing Surveys (CSUR), 27[2], 271-273.
- (11) HEILER, S., ídem.
- (12) TOLK, Andreas — MUGUIRA, James A. (2003, September). "The levels of conceptual interoperability model". In Proceedings of the 2003 fall simulation interoperability workshop (vol. 7, ps. 1-11). Citeseer.
- (13) MARGARIA, Tiziana — CHAUDHARY, Hafiz Ahmad Awais — GUEVARA, Ivan — RYAN, Stephen — SCHIEWECK, Alexander (2021, October), "The interoperability challenge: building a model-driven digital thread platform for CPS", In International Symposium on Leveraging Applications of Formal Methods (ps. 393-413). Springer, Cham.
- (14) BELCHIOR, Rafael — VASCONCELOS, André — GUERREIRO, Sérgio — CORREIA, Miguel, (2021), "A survey on blockchain interoperability: Past, present, and future trends", ACM Computing Surveys (CSUR), 54[8], 1-41.
- (15) Se puede ampliar sobre las formas y las tecnologías subyacentes en blockchain en HEREDIA QUERRO, Sebastián, "Smart Contracts: Qué son, para qué sirven y para qué no servirán" (2020). Disponible en <https://ssrn.com/abstract=3875645> (última consulta: 04/12/2021).
- (16) MARTÍNEZ USERO, José Ángel (2004), "La necesidad de interoperabilidad de la información en los servicios de administración electrónica: xml, una posible solución", In Tecnimap 2004. e-Cooperación en la Administración Pública, 28/09/2001 — Oct. 2004, Murcia, publicado en <https://eprints.ucm.es/id/eprint/5653/> (última consulta al 29/11/2021).
- (17) Tolk y Muguirra lo anotan como "composability of the underlying conceptual models is a necessary requirement". V. TOLK, A. — MUGUIRA, J. A., ídem.
- (18) BO 18/06/2018.
- (19) BO 12/03/2019.
- (20) Res. ex Secretaría de Modernización 19/2018 (BO 05/03/2018).
- (21) NURSEITOV, Nurzhan, et al., "Comparison of JSON and XML data interchange formats: a case study", Caine, 2009, vol. 9, ps. 157-162.
- (22) TRUICA, Ciprian-Octavian, et al. "The Forgotten Document-Oriented Database Management Systems: An Overview and Benchmark of Native XML DODBMSes in Comparison with JSON DODBMSes", Big Data Research 25, nro. 100205, disponible a partir del 26 de enero de 2021.
- (23) PRENSA CAMBIO DIGITAL ONLINE, "JSON: qué es, cómo usarlo y con qué herramientas", publicado en <https://cambiodigital-ol.com/2019/10/json-que-es-como-usarlo-y-con-que-herramientas/> (último acceso: 04/12/2021).
- (24) Res. ex Secretaría de Modernización 19/2018, BO 05/03/2018.
- (25) V. Consid. 8º de la res. 1523 de la ex Secretaría de Gobierno de Modernización (BO 18/09/2019).
- (26) BO 10/02/1966.
- (27) BO 22/04/2016.

- (28) Res. del Ministerio de Modernización 216/2018.
- (29) Ver causa "Telecom Argentina SA c/ EN-ENACOM y otro s/medida cautelar (autónoma)" (Expte. CAF 12.881/2020), voto de los Dres. José Luis López Castiñeira y Luis María Márquez.
- (30) Diario Oficial de la Unión Europea (ES), del 26/11/2015, "Reglamento (UE) 2015/2120 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, por el que se establecen medidas en relación con el acceso a una internet abierta y se modifica la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas y el Reglamento (UE) no 531/2012 relativo a la itinerancia en las redes públicas de comunicaciones móviles en la Unión".
- (31) "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure", citado en HARKNETT, Richard J. — STEVER, James A. (2009), "The cybersecurity triad: Government, private sector partners, and the engaged cybersecurity citizen", *Journal of Homeland Security and Emergency Management*, 6[1].
- (32) HARKNETT, Richard J. — STEVER, James A. (2009), "The cybersecurity triad: Government, private sector partners, and the engaged cybersecurity citizen", *Journal of Homeland Security and Emergency Management*, 6[1].
- (33) Debe considerarse también que en Estados Unidos de América existen otras dos leyes que complementan el sistema de ciberseguridad. La denominada "Cyber Intelligence Sharing and Protection Act" (H.R.3523) y la "Cybersecurity Information Sharing Act of 2014" (S.2588). La primera de ellas apunta a identificar los crímenes y los riesgos que se pueden generar al gobierno y a la población a través del ciberdelito. La segunda, tiene por objeto que agencias federales compartan datos de los ciudadanos, con la finalidad de evitar amenazas.
- (34) CHATFIELD, Akemi Takeoka — REDDICK, Christopher G., "A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in US federal government", *Government Information Quarterly*, nro. 2, 2019, vol. 36, ps. 346-357.
- (35) ANDREASSON, Kim J., "Cybersecurity: public sector threats and responses", Taylor & Francis, 2011, ps. 327 a 337.
- (36) BO 31/07/2017.
- (37) Este comité está compuesto por representantes de las siguientes unidades organizacionales: ex Secretaría de Gobierno de Modernización (actual Secretaría de Innovación Pública), Secretaría de Asuntos Estratégicos de la Jefatura de Gabinete de Ministros, Ministerio de Defensa, Ministerio de Seguridad, Ministerio de Relaciones Exteriores y Culto y del Ministerio de Justicia y Derechos Humanos.
- (38) BO 28/05/2019.
- (39) Es interesante ver el objetivo 3), que involucra interesantes aspectos para el derecho administrativo: "Objetivo 3) Desarrollo del marco normativo. Adecuar y generar las normas jurídicas, marcos regulatorios, estándares y protocolos, para hacer frente a los desafíos que plantean los riesgos del ciberespacio, asegurando el respeto de los derechos fundamentales. "Para ello será necesario: Actualizar el marco jurídico tomando en cuenta la necesidad de principios comunes mínimos con la comunidad internacional. Actualizar el marco normativo técnico en línea con las normas técnicas y las buenas prácticas reconocidas internacionalmente".
- (40) VANINETTI, Hugo A., "La ciberseguridad como política de estado. Estrategia nacional de ciberseguridad. Decreto 829/2019 (sic). Protección de los datos e intimidad personal". Publicado en: *Sup. Esp. LegalTechII* 2019 (noviembre), p. 103. Cita: TR LALEY AR/DOC/3582/2019.
- (41) BO 16/10/2020.
- (42) BO 28/06/2021.
- (43) Dec. 1131/2016. Allí se consideró originales a los documentos electrónicos (art. 1º), a la vez que se obligó a digitalizar lo que se encuentre en papel (arts. 2º y 5º).
- (44) Molina Quiroga, en 2011, hizo un trabajo que bien puede ser tomado como referencia histórica de un momento donde reinaba la imprecisión conceptual y autores tratando temas relacionados al ecosistema digital con imprecisión técnica e inopia de fundamentos, en el que solo se evidencia la doxa y la opinión electiva. Ampliar en MOLINA QUIROGA, Eduardo, "Ley de Expedientes Digitales y Notificaciones Electrónicas", *Diario LA LEY* 2011-C-1224 - AR/DOC/1996/2011.
- (45) Por ejemplo, es difícil resolver una petición no contestada que fue efectuada por correo electrónico; o bien, es difícil instar un procedimiento que no se encuentra en TAD o cuyas instrucciones de presentación no están publicadas en las plataformas. Lo que antes se resolvía presentándose en una mesa de entradas, hoy puede diluirse en la abstracción y en la despersonalización de lo digital. Si bien existen mecanismos jurídicos para conjurar estos inconvenientes, ello supone una sofisticación legal que acaba siendo implícitamente exigida a los individuos que necesitan de las administraciones o del Poder Judicial.
- (46) Art. 2º, dec. 561/2016 y art. 3º del dec. 1063/2016, entre muchos otros.
- (47) En las palabras preliminares se puede apreciar: "La Carta no tiene carácter normativo, sino que su objetivo es reconocer los novísimos retos de aplicación e interpretación que la adaptación de los derechos al entorno

- digital plantea, así como sugerir principios y políticas referidas a ellos en el citado contexto". Documento publicado en https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf (último acceso: 29/11/2021).
- (48) TUGNARELLI, Mónica D. — FORNAROLI, Mauro F. — SANTANA, Sonia R. — JACOBO, Eduardo — DÍAZ, Francisco J., "Análisis de metodologías de recolección de datos digitales", exposición en el evento XIX Workshop de Investigadores en Ciencias de la Computación (WICC 2017, ITBA, Buenos Aires), abril de 2017, ps. 1000 a 1004, publicado en <http://sedici.unlp.edu.ar/handle/10915/62613> (último acceso: 29/11/2021).
- (49) Ídem.
- (50) CERVANTES MORENO, M. A., "Desarrollar un análisis de vulnerabilidades en cooperativa alianza, para la identificación y corrección de las vulnerabilidades y accesos no autorizados a los diferentes sistemas de información". Publicado en <http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8583/Desarrollar%20un%20análisis%20de%20vulnerabilidades%20en%20cooperativa%20alianza%20para%20la%20identificación%20y%20corrección%20de%20las%20vulnerabilidades%20y%20accesos%20no%20autorizados%20a%20los%20diferentes%20sistemas%20de%20información> (último acceso: 29/11/2021).
- (51) TUGNARELLI et al, ídem.
- (52) JARA, Miguel L., "La Ley de Firma Digital en Argentina. Análisis del marco normativo nacional y sus problemáticas", *Ratio Iuris. Revista de Derecho Privado*, 7[2], 156-197.
- (53) MENDOZA MUNAR, Lainiver — RIASCOS DIAZ, Andrés en "Aspectos Jurídicos de la Tecnología Blockchain", en la obra *Revista de Direito, Estado e Telecomunicações*, nro. 1, vol. 13, ps. 131 a 142.
- (54) BO 24/09/2021.
- (55) Ampliar en GUINI, Leonor, en "Actualización de normativa de firma digital. Análisis de la res. 946/2021 sobre procedimientos y pautas técnicas complementarias del Marco Normativo de firma digital para Certificadores Licenciados", publicado el 19/10/2021, accesible en www.saij.gov.ar, Id SAIJ: DACF210185 (último acceso: 29/11/2021).
- (56) BO 12/03/2019.
- (57) Art. 13 del dec. 1063/2016.
- (58) PTN, Dictámenes 309:190.
- (59) BO 02/11/2017.
- (60) Ver HEREDIA QUERRO, S. ídem.
- (61) HERNÁNDEZ Y RODRÍGUEZ, Sergio, "Introducción a la Administración. Teoría general administrativa: origen, evolución y vanguardia", Ed. McGraw-Hill, 4ª ed., ps. 150-151.
- (62) NIELSEN ENEMARK, Carlos A., "El uso de la inteligencia artificial en el acto administrativo", publicado en *Revista de Derecho Administrativo*, Abeledo Perrot, ReDA 135, Buenos Aires, mayo de 2021, ps. 184 y ss.
- (63) BONINA, Nicolás, "Inteligencia artificial y derecho ¿Las máquinas van a remplazar a los abogados?", *Diario LA LEY* del 24/11/2020.
- (64) CORVALÁN, Juan G. — SÁ ZEICHEN, Gustavo — ALBERTSEN, Lihué María, "Actividad Administrativa Automatizada. IA, potestad reglamentaria algorítmica, delegación algorítmica, acto administrativo automatizado y reserva de humanidad", en AA.VV., *Tratado de Inteligencia Artificial y Derecho*, Ed. La Ley, Buenos Aires, 2021, t. II, ps. 193 a 240.
- (65) BRASSARD, Gilles — BRATLEY, Paul, "Fundamentals of algorithmics", Prentice-Hall Inc., 1996, ps. 2 y ss.
- (66) TOTARO, Paolo — NINNO, Domenico, "The concept of algorithm as an interpretative key of modern rationality", *Theory, Culture & Society*, nro. 4, 2014, vol. 31, p. 42.
- (67) TOTARO et al, ídem. Allí se lee: "The bureaucratic algorithm, (...) does not generate an external problem, but one that is intrinsic to the very logic of organizations based upon it. The encapsulation of individuals within algorithmic steps is implicit in the concept of bureaucracy. Thus, in this case the algorithm is the cause of the problem, and hence cannot be its solution. Human beings cannot use the bureaucratic algorithm to solve the problem because it is they who are the tools of the algorithm, not vice versa" (lo anotado arriba es traducción libre del autor).
- (68) MCNELIS, Paul D., "Neural Networks in Finance: Gaining Predictive Edge in the Market", Elsevier Academic Press, (2005), ps. 21 a 40.
- (69) MCNEILS, P., ídem, p. 22.
- (70) MCNEILS, P., ídem, p. 26.
- (71) Como se postulará más adelante, parecería que es difícil pensar en una norma general del acto automático, aunque sí se podrían pensar normas para efectuar actos automáticos favorables, para situaciones de respuesta inmediata.
- (72) MCNEILS, P., ídem, p. 31.
- (73) MCNEILS, P., ídem, p. 32.

- (74) MCNEILS, P., ídem, p. 35.
- (75) MCNEILS, P., ídem, p. 37.
- (76) MCNEILS, P., ídem, p. 22.
- (77) GROSSMAN, David A. — FRIEDER, Ophir, "Information retrieval, Algorithms and Heuristics", 2ª ed., Springer (2004).
- (78) El art. 2º de la ley 25.326 enumera datos sensibles a los siguientes: "[d]atos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual".
- (79) <https://www.argentina.gob.ar/aplicaciones/coronavirus>, consultado al 03/12/2021.
- (80) BO 21/05/2020.
- (81) CHAUM, David — FIAT, Amos — NAOR, Moni, "Untraceable electronic cash", en Conference on the Theory and Application of Cryptography. Springer, New York, NY, 1988, ps. 319-327.
- (82) VALENCIA, Fausto, et al., "Sistema de dinero electrónico, un medio de pago al alcance de todos", CEMA Bulletin, 2015, ps. 255 a 269. Allí se menciona que, para el caso de Ecuador, aún no ha sido explorada la posibilidad, pero es posible plantear un sistema de dinero electrónico constituido como "servicio público de fácil acceso para las personas, sin necesidad de teléfonos sofisticados, internet o datos móviles, de bajo costo para los usuarios y para los actores económicos, sin importar su tamaño ni condición socioeconómica". Vale destacar que hay estudios que indican que, en dicho país, este mecanismo fracasó en algunos estratos de la sociedad (VÁSQUEZ, John Campuzano — CRUZ, Gonzalo Junior Chávez — IÑIGUEZ, José Maza, "El fracaso del dinero electrónico en Ecuador", 3C Empresa: Investigación y pensamiento crítico, nro. 3, 2018, vol. 7, ps. 82-100.). Sin embargo, por otra parte y en otro sentido, en África Oriental, Egipto, India, América Latina, Indonesia, Malasia, Singapur, Filipina y China se ha verificado un crecimiento del uso de pagos electrónicos (FROST — GAMBACORTA — HUANG — SHIN — ZBINDEN, "BigTech and the changing structure of financial intermediation", p. 12, disponible en <https://www.bis.org/publ/work779.pdf>. Último acceso: 04/12/2021).
- (83) BO 28/03/2012.
- (84) BO 04/02/2019.
- (85) BO 10/07/2014.
- (86) El art. 2º de la Res. UIF 300/2014 dice así: "Art. 2º — A los efectos de la presente resolución se entenderá por 'Monedas Virtuales' a la representación digital de valor que puede ser objeto de comercio digital y cuyas funciones son la de constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor, pero que no tienen curso legal, ni se emiten, ni se encuentran garantizadas por ningún país o jurisdicción. En este sentido las monedas virtuales se diferencian del dinero electrónico, que es un mecanismo para transferir digitalmente monedas fiduciarias, es decir, mediante el cual se transfieren electrónicamente monedas que tienen curso legal en algún país o jurisdicción".
- (87) The Economist, diario del 8 de mayo de 2021, "The digital currencies that matter. Get ready for Fedcoin and the e-euro" Autor: D'URBINO, Luca. Accesible en <https://www.economist.com/leaders/2021/05/08/the-digital-currencies-that-matter> (Último acceso: 04/12/2021)
- (88) The Economist, ídem.
- (89) Es interesante el trabajo de Heredia Querro, donde se observa que la tecnología de blockchain aparece como una actividad criptográfica para generar confianza en los intercambios por fuera de las protecciones que puede generar un gobierno. (HEREDIA QUERRO, S., ídem).