Desafíos Jurídicos de la Industria 4.0

Mg. Abog. Maria del Carmen Becerra[2], Abog. Pedro Zarate[1,2],
Mg. Lic. Sandra Oviedo[13], Mg. Lic. Daniel Díaz[1,2]

[1] Instituto de Informática – FCEFN-UNSJ.
[2]Departamento de Informática FCEFN-UNSJ.
[3]Proyecto Transformación Digital en tiempos de la industria 4.0
Código Nº 21/E1172-CICITCA/UNSJ

Abstract: La cuarta revolución industrial es una revolución digital, que implica la desaparición de las líneas que dividen las esferas que pronostican la transformación de los sistemas de producción, administración y gobernanza. En este trabajo se aborda una estrategia digital compuesta por objetivos, habilidades y recursos, donde se identifican las tecnologías innovadoras que requieren disponer de una estrategia frente a los riesgos legales. Este paradigma implica identificar nuevos retos concretos y difíciles para todos los operadores jurídicos planteando cuestiones sobre cómo adoptar buenas prácticas en esas áreas carentes de regulación. Por ello resulta oportuno abrir espacios de discusión sobre los desafíos que propone la Cuarta Revolución Industrial en términos de saber hacer, con respecto a la regulación jurídica, protección de derechos individuales, modelos de organización empresarial, sistemas productivos y de propiedad industrial.

Keywords: **Industria 4.0. Transformación Digital. Disrupción tecnológica en el contexto jurídico. Amenazas y Riesgos. Estrategia técnica -jurídica**

1 Introducción

Los aspectos legales relacionados con la Industria 4.0 no suelen estar definidos en la legislación, siendo escasa la doctrina y la jurisprudencia [1]. Por ello los fabricantes y empresas usuarias deben identificar y documentar los riesgos potenciales para, en su caso, poder demostrar que se ha procedido a la minimización de los riesgos. Así según el estado actual de la técnica y la normativa legal aplicables se puede evaluar el nivel de riesgo legal. El riesgo legal en el que incurrirán las empresas digitalizadas dependerá de los pilares involucrados y el grado de implantación de los mismos.
Comprender el proceso de transformaciones es fundamental para proyectar y mejorar el desarrollo de las organizaciones en el marco de las denominadas Industria 4.0. Se plantea una estrategia técnico jurídico que pueda ayudar a fortalecer estrategias de negocio, de igual manera una profundización de las áreas de TI que pueden fortalecer ideas innovadoras y de algunas políticas nacionales en materia de tecnología de las cuales se pueda sacar provecho para que las tecnologías disruptivas cambien las empresas de manera positiva [2].
En nuestra provincia, a partir del año 2018 para la Agencia Calidad San Juan (sociedad de economía mixta, entre el Gobierno de la Provincia de San Juan y las cámaras comerciales e industriales) es un tema de interés por parte del gobierno, del sector empresarial y de universidades, especialmente potenciado con el Programa Producción 4.0 que trata de una política orientada a brindar herramientas que permitan a las

adfa, p. 1, 2011.

empresas, incorporar nuevos modos de producir y de trabajar adaptados a las reglas que impone el avance tecnológico a nivel global.

La Ley de Economía del conocimiento promulgada en el año 2019 puede ser vista como una ampliación de la previamente aprobada Ley de Promoción de Software. Ambas buscan seguir la tendencia mundial de potenciar la industria de conocimiento, que en Argentina representa el 20% de PBI, porcentaje que no ha aumentado desde 2011, mientras que a nivel mundial el promedio es del 40%. Uno de los riesgos que conlleva la adopción de estas tecnologías emergentes es la seguridad de la información y ciberseguridad, esta última se incrementó conforme al Informe de Riesgos Globales 2022 desarrollado por el Foro Económico Mundial. En este contexto, ya no es novedad que las organizaciones han experimentado una rápida digitalización, los trabajadores han cambiado al trabajo remoto siempre que sea posible, y al mismo tiempo, las amenazas a la ciberseguridad se han incrementado. En 2020, los ataques de malware y ransomware aumentaron en un 358% y 435% respectivamente, superando la capacidad de las organizaciones y las personas para prevenir o responder a ellos. Los gobiernos, las sociedades y las empresas confían cada vez más en la tecnología para administrar todo, desde los servicios públicos hasta los procesos comerciales. Las plataformas, herramientas e interfaces tecnológicas conectadas a través de Internet están creando a la vez un panorama de amenazas cibernéticas más complejo y un número creciente de puntos críticos de falla. A medida que la sociedad continúa migrando hacia el mundo digital, la amenaza del delito cibernético está más presente y les cuesta a las organizaciones decenas, incluso cientos, de millones de dólares [3].

Es necesario seguir avanzando en la institucionalidad y el marco normativo para generar confianza sobre el comercio electrónico. Para fomentar la confianza en esto, los factores institucionales son cruciales. La región muestra diferentes grados de avance en la adopción de marcos normativos relevantes para este tipo de actividad. En particular, se observa un grado de avance menor en la legislación asociada a la protección del consumidor en línea y la protección de los datos personales [4].

La revolución digital obligó a todas las organizaciones a reinventarse, o al menos a replantearse la forma en que se hacen los negocios. La mayoría de las grandes empresas han invertido una cantidad considerable de efectivo en los que generalmente se denomina transformación digital. Si bien se prevee que esas inversiones superen los 6,8 billones de dólares para 2023 a menudo se hacen sin ver beneficios de ROI (Retorno de Inversión) claros[5].

En este trabajo abordaremos la transformación digital identificando las nuevas tecnologías digitales y los efectos disruptivos que provocan. La propuesta consiste en minimizar el riesgo mediante una estrategia digital técnico jurídico donde se desarrollen habilidades y capacidades digitales basadas en leyes y estándares que protejan los datos de las personas y de las empresas.

La metodología a emplear, será de carácter cualitativa en su mayor parte, se basará de un análisis crítico, a través de la recopilación de datos y evaluación del material.

Creemos que es de suma importancia aportar al conocimiento de este proceso socio-económico en nuestra región que ya se da de manera relevante en varios países del mundo, cuya experiencia puede ser útil comparativamente con nuestro país.

2 Estrategia Digital para la Industria 4.0

El término ‘Industria 4.0' se acuñó por primera vez en la Feria de Hannover en 2011, y desde ese entonces ha atraído gran atención de académicos, profesionales, funcionarios gubernamentales y políticos de todo el mundo. A partir de los enfoques planteados, la Industria 4.0 se define como un nuevo modelo industrial para la autoorganización y la autogestión de sistemas de producción totalmente automatizados, que aprenden autónomamente y que son interactivos, en los que el núcleo son las nuevas tecnologías digitales y las tecnologías de Internet, y el papel de los humanos está limitado a su inicio, control y mantenimiento técnico, lo que requiere nuevas competencias de especialistas industriales modernos y está acompañado de cambios sociales [6].
El término "Industria 4.0" se usa para denotar el proceso de transformación en las cadenas globales de creación de valor. La Industria 4.0 incluye procesos de negocios en la industria que contemplan la organización de redes de producción globales sobre la base de las nuevas tecnologías de la información y las comunicaciones, y tecnologías de Internet, con la ayuda de las cuales se lleva a cabo la interacción de los objetos de producción [7].
Según el artículo, Requirements for Digital Transformation, el hecho de tener una estrategia digital clara, coherente y compartida desencadena y despliega el proceso de transformación digital. La estrategia digital estará compuesta por objetivos, habilidades y recursos. Los objetivos estratégicos de un proceso de transformación digital pueden ser algunos (o todos) de los siguientes:

1. mejorar la experiencia/compromiso del cliente (personalización de la oferta, personalización de la relación con el cliente, omnicanalidad, aplicaciones móviles, etc.);
2. mejorar la eficiencia (mejoras operativas, automatización de tareas y procesos, ganancias de productividad y agilidad, etc.);
3. mejorar la toma de decisiones (a nivel estratégico, operativo y táctico);
4. mejorar la innovación (nuevos productos y servicios, nuevas experiencias, productos aumentados, digitalización del proceso de I+D)
5. Transformar el modelo de negocio (estrategias disruptivas que cambian la naturaleza de los productos y servicios, el sistema operativo que los produce y entrega, y su monetización) [8].

Liderar una transformación digital es mucho más que integrar nuevas tecnologías. Se trata de crear una cultura de apertura e innovación que aproveche el poder de los datos y haga más con ellos. A medida que las empresas maduran digitalmente, esa transformación se vuelve más vital para la estrategia comercial y requiere más liderazgo encabezado por el director ejecutivo [9]. Según Schallmo, las habilidades que deberán tener las personas que lideren un proceso de TD son las siguientes [10]:

1. Conectar: ser capaz de conectar procesos, humanos (partes interesadas), objetos/productos, sistemas a través de redes inalámbricas;
2. Generar inteligencia: poder captar la información resultante de estas interacciones sin intervención humana;
3. Analizar: ser capaz de transformar esta información en conocimientos profundos y planes de acción.

Por lo tanto, para iniciar un proceso de transformación digital, es necesario definir una estrategia digital, Figura 1., que considere el "querer hacer" planteando objetivos bien claros y medibles, el "saber hacer" desarrollando capacidades y habilidades de líderes y equipo y el "poder hacer" estableciendo de qué recursos se dispone en cuanto a inversión y tecnologías a emplear.

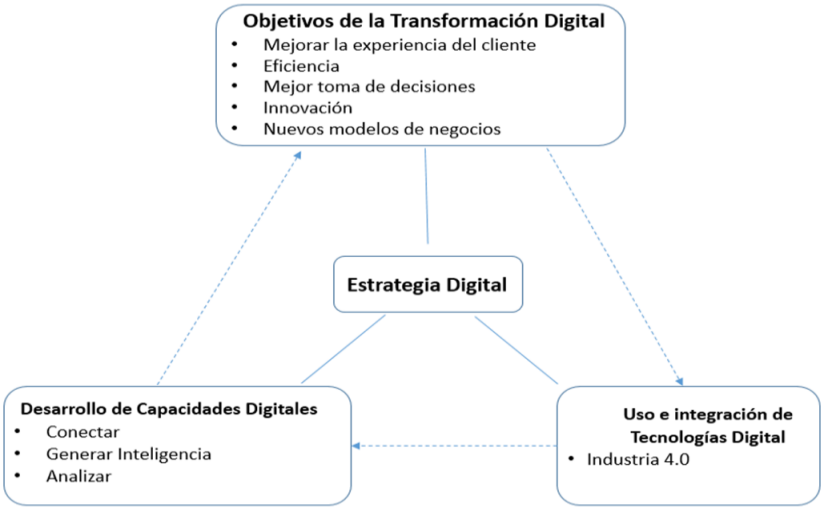

Figura 1. La estrategia digital. Fuente Ponsignon, F., S. Kleinhans, and G. Bressolles

Respecto a las tecnologías habilitadoras de la TD (transformación digital), son las llamadas Tecnologías de la Industria 4.0, diferentes autores las presentan organizadas de diferentes maneras [11], [12], en [10] se presenta una tipología de nueve familias de tecnologías, a saber:

- Tecnologías colaborativas: Habilitan la comunicación y la colaboración en tiempo real con socios externos/internos. Redes sociales, wikis, groupware.
- Tecnologías móviles: Permiten el acceso remoto a la información a través de redes inalámbricas y conexiones 3G/4G/5G. Computadoras portátiles, tabletas, teléfonos inteligentes, dispositivos de navegación GPS.
- Soluciones de Big Data y Analítica de datos: Permiten el análisis de datos masivos (textuales y encriptados, estructurados y no estructurados) de diversas fuentes. Algunos usos son: seguimiento de rastros, flujo de clics desde la web, contenido de redes sociales, datos de video, datos del centro de llamadas, transacciones bancarias, etc. Se aplican para: predicciones, optimización,

innovación de productos/servicios, personalización, detección, resolución de problemas, cumplimiento, toma de decisiones.

- Inteligencia Artificial: Métodos e ingeniería que permiten la realización de máquinas y programas capaces de simular la inteligencia humana. Objetivo: producir máquinas autónomas capaces de realizar tareas complejas. Ejemplos: aprendizaje automático, aprendizaje profundo, agente conversacional (chatbot), reconocimiento automático de voz (voz a texto), automatización robótica de procesos (RPA).
- Servicios de Computación en la Nube. Habilita la entrega de recursos y servicios bajo demanda a través de Internet. SaaS "Software como servicio", PaaS "Plataforma como servicio", IaaS "Infraestructura como servicio".
- Soluciones de trazabilidad y visibilidad. Se destacan RFID (Radio Frequency Identification o identificación por radiofrecuencia), NFC (Near Field Communication o comunicación de campo cercano), códigos QR (Quick Response o de respuesta rápida, GPS/geolocalización.
- Realidad virtual y realidad aumentada. Realidad virtual: sustituye a la realidad física por un entorno virtual generado por un software de ordenador. Realidad aumentada: superpone información digital (imágenes, datos, sonidos, videos, etc.) en el mundo físico. Aplicaciones: dibujo, diseño, mantenimiento, montaje, pilotaje, robótica y telerrobótica, implementación, estudio de impacto, etc.
- Juegos serios. Software que combina una intención "seria" –de tipo educativo, informativo, comunicacional, de marketing, ideológica o formativa– con motivaciones lúdicas. Ejemplos: Advergaming (juegos publicitarios), juegos de entretenimiento educativo (con fines educativos), juegos de edumarket (utilizados para comunicación corporativa), juegos comprometidos (o desviados) y juegos de capacitación y simulación.
- La tecnología Blockchain. Permite el almacenamiento y transmisión de información a un costo mínimo, seguro, transparente y operando sin un órgano central de gestión. Se refiere por extensión a una base de datos segura y distribuida de todas las transacciones realizadas. Aplicaciones: criptomonedas, contratos inteligentes que permiten el intercambio de todo tipo de bienes o servicios, reducción de costos de pago y transacción, seguros entre pares.

3 Amenazas y Riesgos

El uso de tecnologías innovadoras implica que se debe disponer de una estrategia frente a los riesgos, incluidos los riesgos legales, que se pueden materializar de acuerdo a la Familia de Tecnologías asociadas, como describe la siguiente tabla.

	Familias de Tecnologías	Riesgos Legales
1	Tecnologías colaborativas	● Robo de Información ● Violación de los Derechos relativos a la propiedad intelectual ● Problemas de Seguridad en las TIC
2	Tecnologías móviles	● Privacidad-confidencialidad
3	Soluciones de Big Data y Analítica de datos	● Privacidad- ● Pérdida de datos personales
4	Inteligencia Artificial	● Lesiones a las Personas ● Violación de los derechos de los trabajadores-Derecho de igualdad ● Privacidad
5	Servicios de Computación en la Nube	● Privacidad de los datos
6	Soluciones de trazabilidad y visibilidad	● Privacidad-Pérdida de Información
7	Realidad virtual y realidad aumentada	● Lesiones a las Personas ● Daños a la Propiedad
8	Juegos Serios	● Riesgo en el Trabajo
9	La tecnología Blockchain	● Incumplimientos contractuales- Defensa al consumidor ● Privacidad ● Lavado de activos

Los nuevos modelos de organización de los negocios surgen de la mano de nuevas innovaciones de garaje, de nuevas conectividades 5G, de nuevas plataformas colaborativas, de nuevos esquemas de trabajo freelance, de nuevos prototipados de productos, de nuevos desafíos para el financiamiento de la seguridad social y la adaptación de fiscalidades.

El robo cibernético sería otra amenaza peligrosa, el problema no es individual, y esto costará sustancialmente a los fabricantes e incluso podría dañar su reputación. Por lo tanto, la seguridad es un tema crucial que debe abordarse seriamente. Al igual que pasa en otros sectores productivos, el robo de información es una amenaza creciente en el entorno de la Industria 4.0. La disrupción tecnológica implica la disrupción de tradicionales modalidades de trabajo, tanto a nivel del management y de la dirección, como al nivel de las tareas de apoyo y de base.

La digitalización también desafía las leyes de la propiedad; dado que nuevos desarrollos tecnológicos construidos sobre conocimiento previo, o por la convergencia de varias tecnologías conocidas, reabre la discusión sobre los derechos de propiedad y sobre la efectividad de instrumentos como patentes y registros de marcas. Al mismo tiempo, el desarrollo de nuevos materiales y el avance en las técnicas de las ciencias biológicas como la edición de genes que desafían la ética humana.

Finalmente, la privacidad no solo es una preocupación del cliente, sino también del fabricante. En una red de Industria 4.0 interconectada, los fabricantes deben recopilar y analizar una gran cantidad de datos. Para las empresas, esto puede parecer una amenaza a su seguridad corporativa. Para los clientes puede considerarse una invasión en su privacidad personal. Reducir la brecha entre el consumidor y el fabricante será un gran desafío para ambas partes [13]

La creciente dependencia de los sistemas digitales ha acelerado la adopción de plataformas y dispositivos que permiten compartir datos confidenciales con terceros: servicios en la nube, interfaces de programación de aplicaciones (API) y otros intermediarios. Estos sistemas, si bien son herramientas poderosas para datos y procesamiento, agregan una capa adicional de dependencia de los proveedores de servicios. Los usuarios deberán navegar por las vulnerabilidades de seguridad inherentes tanto a la mayor dependencia como a la creciente fragmentación en este tipo de tecnologías complejas, a menudo caracterizadas por la descentralización y la falta de medidas de seguridad estructuradas.

La robotización del trabajo adquiere características poliédricas: abarca tareas insalubres y riesgosas (como en la industria del petróleo y minería); decisiones estratégicas (como en el trading algorítmico); y hasta irrumpe en el plano emocional (como en el neuromarketing y la economía del comportamiento aplicada a los servicios globales).

La inteligencia artificial tiene su impacto en el mundo jurídico, los sistemas expertos. Existe también el sistema de soporte de decisiones. Los datos relativos a todo el proceso productivo de una compañía se han vuelto uno de los elementos fundamentales para lograr el éxito comercial, con los años se han ido incorporando los avances de la tecnología informática para brindar las herramientas necesarias en la creación de sistemas de información confiable y eficaz. Sin embargo, en la actualidad aún existen empresas que observan con recelo la posible implementación de Sistemas de Información en sus procesos, debido a que implican un enorme cambio en las estructuras organizativas e institucionales de las organizaciones. En ocasiones, los Sistemas de Información pueden llegar a fallar, no por errores tecnológicos originados en el aspecto informático, sino por visiones culturales opuestas a la incorporación de este tipo de herramientas.

Hay una preocupación por como es el desplazamiento laboral implícito que es una constante en las revoluciones industriales, dado que el desaforado avance tecnológico de las últimas décadas afecta a todas las profesiones. La inteligencia artificial sumada al desarrollo de otros avances tecnológicos, generan consecuencias en todas las actividades humanas y producción de bienes y servicios. Dichos procesos generan mejores condiciones e información para poder satisfacer la demanda de clientes de manera eficiente, un control en línea constante de la situación de la empresa, con redes informáticas que permiten tener un mejor control de todas las operaciones. El surgimiento de la inteligencia artificial constituye un nuevo factor de producción, al crear una realidad ciber-física de trabajo virtual, en parte humana, en parte desarrollado

por máquinas inteligentes, que merced a la capacidad de análisis algorítmico cada vez más sofisticada y al desplazamiento de trillones de datos a súper velocidad, permiten un aprendizaje y autoaprendizaje exponencial. Asistimos en dicho contexto a la posibilidad de incrementar la productividad regional, sin dejar de apreciar el surgimiento de una reconfiguración de las clásicas cadenas globales de valor (el offshoring da paso al reshoring, por caso) en las cuales de la mano de la inteligencia artificial irrumpen modalidades tecnológicas igualmente disruptivas, como la internet de las cosas, la biología sintética y la fabricación aditiva y 3D, que hacen implosionar las distinciones rígidas entre bienes y servicios y convocan a reinventar las reglas básicas del comercio mundial.

La tecnología y los sistemas de información demandan el abordaje de nuevos problemas de ética, tanto para los individuos y grupos de la organización, como para las sociedades ya que provocan situaciones de cambio, muchas veces no previstas, las que impactan en forma positiva o negativa [14]. En este sentido, es necesario analizar que los avances de la tecnología de información son una fuente de beneficios para los usuarios de sistemas, al facilitar el acceso, el uso y la circulación de la información. Sin embargo, surgen nuevas amenazas de la seguridad y de la privacidad, planteando un dilema ético entre los asuntos y la información relacionada que deben ser resguardados y a aquellos que se puede acceder libremente. Con los modelos de negocio peer-to-peer (P2P), las empresas proporcionan la infraestructura técnica que comparten o alquilan.

Quizás el aspecto más desafiante de implementar Industria 4.0 es el riesgo de seguridad de TIC. La Industria 4.0 requerirá la integración en línea entre varias entidades, y esta integración en línea dará lugar a posibles violaciones de seguridad y fugas de datos [13]. Sin dudas, este nuevo modelo de procesos hace más eficiente la industria; pero de igual forma, aumenta los riesgos en lo relativo a la seguridad informática. Las empresas montadas en la ola de la Industria 4.0 deben estar conscientes de la vigencia de los ciberataques y los costosos riesgos regulatorios.

El uso de blockchain plantea una serie de riesgos, que no solo se manifiestan por los más conocidos como son la posibilidad de generar códigos errados, sino que en el caso del blockchain como tecnología de la cuarta revolución industrial, los riesgos asociados al ecosistema de las criptomonedas quedan de manifiesto. Los últimos fallos producidos en nuestro país señalan que las criptomonedas están teniendo impacto en todo tipo de relaciones humanas; los delitos no son la excepción a ello. Si algo tiene valor para una persona, existirá otro individuo que estará interesado en hacerse de ello contra la voluntad del legítimo titular [15].

Conforme la reflexión de la autora “con el fin de comprender, analizar y responder al desafío de monedas virtuales y su uso como vehículos para el lavado de dinero, el intercambio de bienes y servicios ilegales y la financiación de actividades de grupos terroristas, los gobiernos deberán hacer una inversión en investigación y entrenamiento, a los fines de construir grupos de expertos que puedan abordar el seguimiento de las transacciones” [16].

Como suele suceder ante toda disrupción tecnológica, emerge la idea del riesgo que generan estas nuevas máquinas y estas nuevas tecnologías, en este trabajo referidas a la Inteligencia Artificial (IA) y a la Propiedad Intelectual (PI). Se abre de esta forma un nuevo capítulo para el derecho de Daños, en el marco de la responsabilidad civil, todas estas innovaciones generan una crisis de la legislación que queda evidentemente desactualizada, toda vez que fue dictada sin tener en cuenta estas novedades.

Uno de los principales problemas con el que nos enfrentamos es la inexistencia de una normativa propia y específica que aborde las peculiaridades que presenta la robótica. Al respecto, el documento anexo a la comunicación de la Comisión Europea titulada "Inteligencia Artificial para Europa", destaca que la combinación entre el autoaprendizaje y la autonomía conlleva a que el comportamiento de las nuevas tecnologías sea difícil de predecir [21].

Esta situación podría plantear cuestiones relativas a la responsabilidad, en situaciones donde el daño causado por un robot que opera con autonomía, dado que son sistemas más complejos y que tienen capacidad de aprender, adaptarse al medio y tomar decisiones. Por ende, sus acciones son impredecibles. La responsabilidad de los robots por lo tanto, actuando con la normativa vigente, sería del dueño y/o guardián del mismo, por tratarse la robótica de una actividad riesgosa contemplada en los arts. 1757 y 1758 del C.C.C.

Se entiende que los daños derivados de la inteligencia artificial y nuevas tecnologías, tales como los casos que analizamos de vehículos autónomos y de robots autónomos quedan comprendidos en los arts. 1769 norma que regula los daños ocasionados por la circulación de vehículos automotores. La responsabilidad es objetiva y responde el dueño y guardián concurrentemente [22]. La IA pone en jaque el derecho de autor. ¿Será la autoría humana un requisito previo para obtener la protección? Estas cuestiones fueron tratadas por la Oficina de Derechos de Autor de los Estados Unidos, a través de su Comité de Revisión, el pasado 14 de febrero con un rotundo “no”. La Oficina fue contundente en su respuesta, negando la aplicabilidad de tales derechos a este tipo de obra, teniendo en cuenta que la legislación en materia de derechos de autor tan solo protege los frutos del trabajo intelectual de la mente humana. En este sentido se pronunció el Tribunal de Justicia de la Unión Europea (TJUE), en el caso Painer (asunto C-145/10) donde determinó que, se reportará como original aquella obra que sea “una creación intelectual del autor que refleje su personalidad y que se manifieste por las decisiones libres y creativas del mismo al realizarla”. Por lo tanto, la originalidad sólo puede extraerse de las aportaciones creativas que realice un autor persona física. Así pues, si la obra es creada íntegramente por un sistema de IA, y se constata que no hay decisiones libres y creativas del autor, porque en sí, no existe autor más allá del procesamiento algorítmico, el resultado no podrá ser protegido por derechos de autor. De la misma forma, si la intervención humana no es más que técnica o mecánica, y quien realiza el trabajo “creativo” es un sistema automatizado y sin intervención humana, el resultado, nuevamente, no podrá ser dotado de protección. [23]

El marco regulador de la IA propuesto desde las instituciones europeas subraya la necesidad de adoptar directrices para una IA fiable [24] a partir, principalmente, de evaluar los riesgos que conllevan este tipo de herramientas. Las herramientas de IA pueden generar un distinto impacto y riesgo para la protección de los derechos fundamentales, especialmente la protección de los datos personales y de la privacidad y la no discriminación, así como un riesgo para la seguridad y el funcionamiento eficaz del régimen de responsabilidad civil.

Con relacion a la Realidad Virtual y Realidad Aumentada AR/VR [del inglés, augmented reality/virtual reality], como dice Jose Manuel Mercado [25]. En un entorno virtual, pero ligado a la realidad, existen muchos riesgos digitales, pero no son los únicos. Entre los riesgos se pueden mencionar:

- Falta de precisión. La exactitud de los entornos virtuales depende de la exactitud de los datos. Un error o una desviación en un videojuego puede no ser muy importante, pero los riesgos se disparan cuando hablamos de la precisión que requiere, por ejemplo, un tratamiento médico.
- La seguridad de los datos. Como en todo entorno digital, los usuarios finales y las empresas exponen su información en una red que puede llegar a ser muy vulnerable, sobre todo, en el caso de aplicaciones o dispositivos en los que el ahorro de costes es una prioridad. Así, se dispara el riesgo de filtraciones (intencionadas o no) de información privada o confidencial.
- Manipulación de la identidad. Mención aparte merece la posibilidad de robar o suplantar las identidades digitales. En muchos entornos virtuales, los usuarios interactúan a través de avatares o representaciones digitales de sí mismos. Estas identidades pueden ser objeto de robo, manipulación o reemplazo con intenciones maliciosas [26].

4 Estrategia Técnico –Jurídica

Cuando se trata de proyectos con grandes volúmenes de datos, toca definir estrategias de desarrollo de capacidades técnico jurídicas para asegurar la confidencialidad, integridad y disponibilidad de la información; en ese sentido los Estándares de seguridad se están enfocando en controles de cara a la ciberseguridad, es el caso de la Norma ISO 27001, cuyos controles de apoyo (Anexo A) están en proceso de actualización y considerará temas como Inteligencia de Amenazas, Seguridad para Servicios en la Nube, Enmascaramiento de Datos, Filtrado Web, entre otros.
El conocimiento de los estándares de TI genera calidad en las estrategias de negocio que puedan aplicar las empresas, la ausencia de dichos estándares impide que las tareas sean realizadas ordenadamente siguiendo fases de planeación, organización y control, además de muchos otros factores que estos estándares otorgan.
El derecho debe ocuparse de estas tecnologías disruptivas a fin de colocar a buen resguardo aquellos derechos consagrados por el Derecho Internacional de los Derechos Humanos [12]. “La palabra disruptiva es de origen francés “disruptif” y del inglés “disruptive”, y se utiliza para definir un cambio determinante o brusco. Luego, aquella tecnología que propicia cambios profundos en los procesos, productos o servicios es una tecnología disruptiva y generalmente conlleva una estrategia de introducción, penetración y uso que la consolida y desplaza la tecnología anterior lo que la convierte en una innovación disruptiva”. “El término “disruptivo” fue introducido por el catedrático de la escuela de negocios de la Harvard Business School, Clayton Christensen en 1997, y es descrito como un proceso por el cual un producto o servicio se lleva al mercado, mediante aplicaciones sencillas para luego ganar ese mercado desplazando a otros competidores. Esta teoría es válida, no sólo para la gestión empresarial sino para cualquier sector social”. Algunas tecnologías pueden ser claramente entendidas como disruptivas, aunque no fueron consideradas así en sus comienzos, como la propia Internet, que trajo impactos profundos en la sociedad, en la forma de actuar, de interacción con el otro, ser vivo o máquina, y en la gestión de la propia vida de cada uno [17].

COBIT- La misión de Cobit es investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado y aceptado internacionalmente, para la adopción, por parte de las empresas y el uso diario, por parte de gerentes de negocio, profesionales de TI (ITGI, 2007) En el artículo se recomienda este estándar partiendo de que una de sus características es que las empresas deben medir dónde se encuentran y dónde se requieren mejoras, e implementar herramientas gerenciales para monitorear dicha mejora; lo que va de la mano de la tarea de hacer frente a la disrupción tecnológica para generar innovaciones que proyecten la organización hacia un modelo de negocio diferente con mayores ventajas. ISO 38500- proporciona un marco de principios para que la dirección de las organizaciones lo utilice al evaluar, dirigir y monitorear el uso de TI y obtener resultados que apoyen la toma de decisiones de manera mucho más acertada [18].

ITIL- Es el conjunto de conceptos y mejores prácticas para la administración de servicios de TI. Todos los estándares mencionados en este documento van dirigidos a proporcionar herramientas para una buena toma de decisiones que es lo que se requiere cuando se necesita transformar modelos de negocio y eficiencia de las plataformas digitales radica en el uso de datos obtenidos a partir de los usuarios. Éstas generan y obtienen constantemente datos respecto de sus usuarios: hábitos de consumo, prácticas sociales, preferencias, movilidad, etc. información de enorme valor para compañías que quieren conquistar nuevos espacios y oportunidades para sus negocios. Por lo tanto, éstas deben resguardar la privacidad de los datos de las personas que utilizan las plataformas. Sin embargo, al no estar constituidas en el país, reducen las posibilidades de exigir el cumplimiento de la Ley de Protección de Datos.

La ley de Protección de Datos Personales (2000) es un instrumento normativo necesario para proteger la privacidad de las personas respecto al tratamiento que puedan dar otros en relación a su información personal. Sin embargo, en este contexto, la ley es incompleta e insuficiente, generando grandes desafíos en las áreas de protección de los datos e información personal. En ese sentido, Argentina está al debe con los estándares internacionales como el Reglamento General de Protección de Datos Europeo. Se hace por lo tanto necesario una actualización y modificación de la ley de tal forma que incorpore los nuevos escenarios digitales, contemplando una estipulación clara que las solicitudes de datos de las plataformas a usuarios no excedan aquellos vinculados a la prestación del servicio [19].

Finalmente se debe tener en cuenta la Carta de Derechos Digitales, que se publicó en el año 2021 que es un documento que “ofrece un marco de referencia para garantizar los derechos de la ciudadanía en la nueva realidad digital” y que nace con el objetivo de “reconocer los retos que plantea la adaptación de los derechos actuales al entorno virtual y digital”.

La carta recoge derechos de privacidad, relaciones laborales o igualdad en entornos digitales. La Carta de Derechos Digitales es un documento no vinculante (es decir, no es una ley ni una obligación) en el que se muestran posibles derechos futuros en materia de protección digital. A medida que ‘lo digital’ ha ido entrando en la vida de las personas se ha ido comprobando cómo las normas se han ido quedando obsoletas porque no cubren las nuevas tecnologías. Esta nueva publicación trabaja sobre cinco grandes bloques de derechos digitales [20]:

En la figura 2, se representan los grandes bloques que componen la Estrategia Técnico Jurídica propuesta que asociada a una Estrategia Digital, se presenta como guía del

"Saber hacer" para el desarrollo de habilidades y capacidades orientadas por instrumentos jurídicos, que alienten a las empresas y organizaciones a encarar una transformación digital donde el "Poder hacer" mediante el uso e integración de tecnologías esté guiado por estándares y normas siempre cuidando que la regulación no signifique la asfixia de la innovación

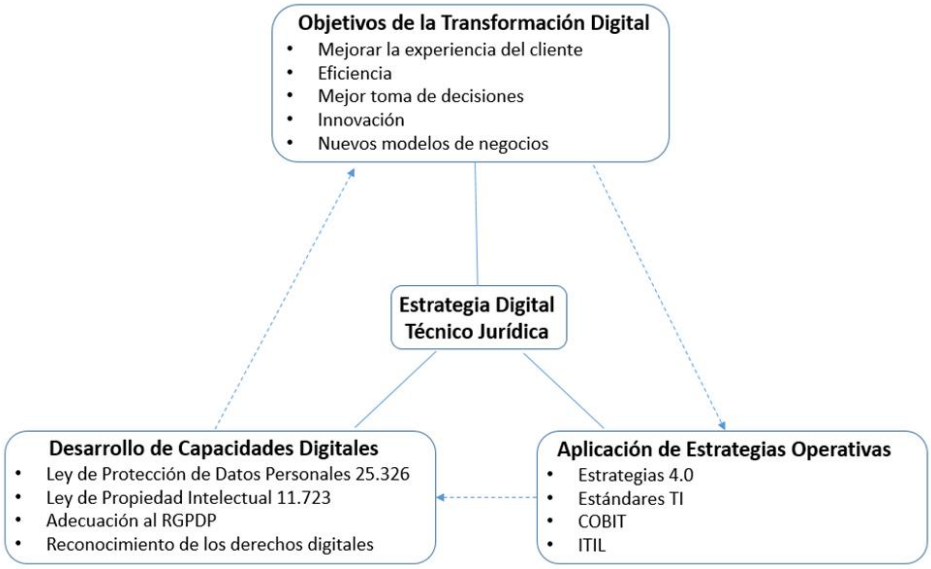

Figura 2. La estrategia digital. Fuente de elaboración propia

5 Conclusiones

En este trabajo se presentó un detalle de las familias de tecnologías involucradas. Además, para cada familia, se hizo un relevamiento de los riesgos legales posibles a los que se exponen las empresas adoptantes y usuarios en general. Siendo los principales riesgos relevados los relacionados con la privacidad de los datos y pérdida y robo de información en general.

También, se propuso una estrategia técnico-jurídica como referencia. Dicha estrategia considera alineado con los objetivos de la Transformación Digital, un componente denominado Desarrollo de Capacidades Digitales, fundado en el conocimiento de la legislación sobre protección de datos personales, propiedad intelectual y derechos digitales. Asimismo, la estrategia tiene otro componente relacionado con la aplicación de estrategias operativas basada en estándares y normas vinculadas a la gobernanza de datos.

Se requiere una nueva gobernanza, normas e instituciones ágiles que acompañen la transformación digital en todas sus dimensiones, cuidando los derechos de las personas, garantizando la inclusión tecnológica y social, priorizando tanto el acceso como el desarrollo de las habilidades.

6 Referencias

[1] www.osalan.euskadi.eus

[2] Facundo Paesano, Fratini, Joaquin. El impacto de la Industria 4.0 en Argentina.2021.https://ri.unsam.edu.ar/bitstream/123456789/1423/1/TFPP%20EEYN%202021%20PF-FJ.pdf

[3] https://es.weforum.org/agenda/2022/02/informe-de-riesgos-globales-2022-lo-que-debes-saber/

[4]https://repositorio.cepal.org/bitstream/handle/11362/46766/S2000991_es.pdf?sequence=1&isAllowed=y

[5]Tomas Chamorro- Premuzic.Los componentes esenciales de la transformación digital

[6] Sukhodolov, Y. A. (2019). The notion, essence and peculiarities of Industry 4.0 as a sphere of industry. En: Popkova, E.G. et, al. (2019). Industry 4.0: industrial revolution of the 21st Century. Warsaw, Poland: Springer-Verlag

[7] KANE, G.C., et al., Strategy, not technology, drives digital transformation MIT Sloan Manageemnt Review. , 2015.

[8] Lyon, O., 7 Requirements for Digital Transformation. 2020.

[9] Ponsignon, F., S. Kleinhans, and G. Bressolles, Vers la qualité 4.0 : Apports croisés de la fonction qualité et de la transformation digitale. AFNOR, 2018.

[10] Schallmo, D., C. Williams, and L. Boardman, Digital Transformation of Business Models. Best Practice, Enablers and Roadmaps. International Journal of Innovation Management, 2017. 21(8).

[11] Abolhassan, F., The Drivers of Digital Transformation. Springer, 2017.

[12] Horacio Granero. Inteligencia artificial y derecho, un reto social.El Dial.2020

[13] Sung, T. K. (2018). Industry 4.0: A Korea perspective. Technological Forecasting and Social Change, 132, 40-45.

[14] Calvo, P. (2020). Etificación, la transformación digital de lo moral. Kriterion: Revista de Filosofía, (60), 671-688.

[15] La Ley *https://www.udesa.edu.ar/sites/default/files/cetys_criptomonedas.pdf*

[16] Faliero, Johanna. Criptomonedas: La nueva frontera regulatoria del derecho informático.AD Hoc-Bs.As.2017

[17] GS Rodríguez · Tecnologías disruptivas: contexto jurídico Político, Desafíos y oportunidades en Latinoamérica.2021

[18] ISO 38500, 2009) ISSN: 1692-7257 - Volumen 2 – Número 34 - 2019 Universidad de Pamplona I. I. D. T. .(A. 27 Revista Colombiana de Tecnologías de Avanzada).

[19] http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

[20] https://edri.org/files/WePromiseCharter_booklet_ES.pdf

[21] Comission Staff Working Document, Liability for emerging digital technologies, SWD (2018) 137, Brussels, 25/04/2018

[22] https://repositorio.uca.edu.ar/bitstream/123456789/10922/1/danos-derivados-inteligencia-artificial.pdf (CAPÍTULO II)

[23] https://www.cuatrecasas.com/es/latam/articulo/internacional-inteligencia-artificial-y-derechos-de-autor

[24] https://op.europa.eu/es/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1

[25] file:///C:/Users/Usuario/Downloads/insights-techtalk-augmented-virtual-mixed-realities-the-risk-chain-grows-more-complex-wtw.pdf

[26] https://willistowerswatsonupdate.es/ciberseguridad/realidad-virtual-aumentada-mixta-riesgos/