N°2, 2024 diciembre
JURIS STUDIA
Revista especializada en ciencias jurídicas

Artículo científico

COMPLIANCE DIGITAL Y GOBERNANZA: EL DIÁLOGO INTERDISCIPLINARIO EN LA ERA DIGITAL

DIGITAL COMPLIANCE AND GOVERNANCE: INTERDISCIPLINARY DIALOGUE IN THE DIGITAL ERA

JOSÉ LUIZ DE MOURA FALEIROS JÚNIOR
https://orcid.org/0000-0002-0192-2336
josefaleirosjr@outlook.com

RESUMEN

Este artículo explora los conceptos clave del compliance digital y la gobernanza, y sus implicaciones en el contexto de la rápidamente evolucionante era digital. La discusión destaca la distinción entre ética y moral, enfatizando la necesidad de que las organizaciones alineen los valores individuales con las normas sociales para garantizar un comportamiento responsable en el ámbito digital. Se resalta la importancia de establecer códigos de ética y pautas integrales para abordar conflictos de interés, fomentar la confianza y mantener estándares éticos. Además, se examina el concepto de compliance digital como un esfuerzo multidisciplinario que involucra conocimientos legales, técnicos y éticos para garantizar el cumplimiento de marcos legales, prácticas de la industria y políticas internas. También se subraya la importancia de la gobernanza digital para gestionar de manera efectiva los procesos relacionados con la tecnología, proteger los datos y alinear las iniciativas digitales con los objetivos organizativos. Las prácticas de gobernanza efectivas son fundamentales para mantener la integridad, mitigar riesgos y promover el uso responsable de los recursos digitales. En conclusión, la intersección entre el compliance digital y la gobernanza presenta desafíos complejos para las organizaciones en la era digital. Al adoptar principios éticos, cumplir con las regulaciones e implementar prácticas sólidas de gobernanza, las organizaciones pueden superar estos desafíos, generar confianza y prosperar en el siempre cambiante panorama digital.

Palabras clave: Compliance digital. Gobernanza digital. Ética y moral. Comportamiento responsable. Enfoque multidisciplinario.

ABSTRACT

This paper explores the key concepts of digital compliance and governance and their implications in the context of the rapidly evolving digital era. The discussion highlights the distinction between ethics and morals, emphasizing the need for organizations to align individual values with societal norms to ensure responsible behavior in the digital realm, emphasizing the importance of establishing comprehensive codes of ethics and guidelines to address conflicts of interest, foster trust, and uphold ethical standards. It further examines the concept of digital compliance as a multidisciplinary effort that involves legal, technical, and ethical expertise to ensure adherence to legal frameworks, industry practices, and internal policies. Additionally, it underscores the significance of digital governance in effectively managing technology-related processes, safeguarding data, and aligning digital initiatives with organizational objectives. Effective governance practices are essential to maintaining integrity, mitigating risks, and promoting responsible use of digital resources. In conclusion, the intersection of digital compliance and governance presents organizations with complex challenges in the digital era. By embracing ethical principles, adhering to regulations, and implementing robust governance practices, organizations can navigate these challenges, build trust, and thrive in the ever-changing digital landscape.

Keywords: Digital compliance. Digital governance. Ethics and morals. Responsible behavior. Multidisciplinary approach.

Revisado: 02/09/2024. **Aceptado:** 18/10/2024.
Citado: de Moura Faleiros Júnior, J. L. COMPLIANCE DIGITAL Y GOBERNANZA: EL DIÁLOGO INTERDISCIPLINARIO EN LA ERA DIGITAL *Juris Studia,* 1(2), 145–158. https://doi.org/10.52428/12345678.v1i1.1091

Introducción

La falta de frenos morales que impidan la violación de los derechos de autor en el entorno virtual plantea cuestiones sobre la necesidad de marcos regulatorios específicos para Internet. Mientras que la gravedad y las consecuencias del homicidio son ampliamente conocidas y repudiadas por la sociedad, la violación de los derechos de autor en el mundo digital a menudo se percibe como un acto menos ofensivo, cuyas consecuencias son menos tangibles y perceptibles.

La amplia difusión de contenido digital en Internet, como música, películas y juegos, contribuye a la normalización y banalización de la descarga ilegal. La facilidad de acceso a estos archivos, junto con la sensación de impunidad que impregna el entorno virtual, crea una cultura de intercambio indiscriminado, donde la violación de los derechos de autor a menudo se justifica como una forma de democratizar el acceso a la cultura. El término "*compliance* digital" se refiere al conjunto de prácticas, políticas y controles adoptados por una organización para garantizar que sus actividades en el entorno digital cumplan con las leyes, regulaciones y estándares éticos aplicables.

Sin embargo, es importante reconocer que la violación de los derechos de autor no solo es una cuestión moral, sino también una violación de los derechos legales de los creadores y titulares de derechos de autor. La protección de los derechos de autor es fundamental para fomentar la creatividad, la innovación y la producción cultural, y la falta de una regulación adecuada en el entorno digital puede comprometer estos principios.

En este contexto, es necesario establecer marcos regulatorios específicos para Internet que equilibren la protección de los derechos de autor con la promoción de la libertad de expresión y el acceso a la cultura. Estos marcos deben abordar cuestiones como la responsabilidad de los proveedores de servicios en línea, los mecanismos de supervisión y lucha contra la piratería digital, y la concienciación de la sociedad sobre la importancia de respetar los derechos de autor.

Las empresas que operan en el sector de la distribución de contenido digital deben implementar mecanismos de *compliance* digital para garantizar el respeto de los derechos de autor y evitar la comercialización de material protegido sin autorización. Esto puede incluir la implementación de sistemas de gestión de derechos digitales, la adopción de prácticas de monitoreo y eliminación de contenido ilegal, y la celebración de acuerdos de licencia con los titulares de derechos de autor.

Además, el *compliance* digital también abarca aspectos relacionados con la protección de datos personales, la seguridad de la información y la privacidad de los usuarios. Las organizaciones deben adoptar medidas de ciberseguridad para garantizar la confidencialidad, integridad y disponibilidad de los datos, así como el cumplimiento de las leyes de protección de datos vigentes, como el Reglamento General de Protección de Datos (RGPD, o GDPR en inglés) en la Unión Europea.

Es fundamental promover una mayor conciencia sobre las consecuencias de la violación de los derechos de autor en el entorno virtual. La educación y difusión de información sobre los daños causados por la piratería digital pueden contribuir al fortalecimiento de los frenos morales y éticos en el uso de Internet, fomentando la adopción de comportamientos más responsables y respetuosos con los derechos de autor.

La investigación utilizará el método de enfoque deductivo, con la implementación de substratos obtenidos en investigaciones bibliográficas y doctrinales sobre el fenómeno

Revista JURIS STUDIA Diciembre de 2024
ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212

del tema-problema. Por último, se realizarán consideraciones finales destinadas a la exposición de puntos que permitan una comprensión más precisa de la necesidad de establecer parámetros contextuales para la comprensión de lo que se entiende por *compliance* digital.

1. El desafío de la libertad en la era digital: reflexiones sobre la sociedad de la información y el derecho en el ciberespacio

La razón detrás del fenómeno descrito en estas notas introductorias podría residir en el estudio de las necesidades humanas, definidas por Abraham Maslow (1970) y perfectamente enmarcadas en el contexto de la sociedad de la información actual, en la cual es necesario convivir con un nuevo entorno llamado ciberespacio, donde la tecnología actúa como un poderoso componente del ambiente de automejora.

En este contexto, los medios deben ser utilizados consciente y enfocadamente. En principio, los substratos presentes en el ciberespacio no representan ni perjuicios ni beneficios, pero pueden llegar a serlo dependiendo de cómo se utilicen. Un punto crucial en relación con esta sociedad de la información es la dicotomía entre los criterios de interioridad (moral) y exterioridad (derecho), que sirven como mecanismos diferenciadores de lo que es o no relevante para el universo jurídico.

Ahora bien, el mero pensamiento humano no tiene la relevancia necesaria para tener consecuencias jurídicas. Sin embargo, su manifestación puede tener algún tipo de consecuencia, sin importar el medio de exteriorización, ya sea un gesto, una palabra o en el entorno virtual. Blaise Pascal (2003), filósofo francés del siglo XVII, expresaba esta conclusión con mucha claridad de que si todos los hombres supieran lo que dicen unos de otros, "no habría cuatro amigos en este mundo" (PASCAL, 2003, traducción libre). Y este ideal de libertad se remonta a las bases mismas del Estado Liberal, muy bien explicado en las obras de John Stuart Mill (2016) y Benjamin Constant (2015), entre otros.

En la actualidad, la exteriorización del pensamiento es mucho mayor debido a la existencia de Internet, lo que ha llevado al surgimiento del Derecho Digital, que, aunque no se considera una rama jurídica autónoma, irradia sus efectos de forma duradera en todas las áreas del Derecho.

En el pasado, la exteriorización verbal en un entorno sonoro se perdía simplemente porque no se registraba lo que se decía. Sin embargo, con la aparición de las redes sociales, este paradigma cambió y muchas personas parecen no darse cuenta de que todo lo que dicen se expone al mundo entero.

El brocardo latino "*Verba volant, Scripta manent*" (las palabras vuelan, lo escrito permanece) revela exactamente lo que se enfrenta actualmente para prevenir la mala interpretación de la exposición inmediata de un pensamiento. En este punto, también cobra relevancia el estudio de los límites de la libertad de expresión, que aparece con los registros virtuales de todo lo que se dice en línea. Sin duda, se debe pensar mucho antes de hacer cualquier declaración en las redes sociales, ya que el pensamiento expresado perdurará en Internet, que a menudo no permite el derecho al arrepentimiento.

La difusión de rumores también sirve como válvula para represalias y acciones inapropiadas, lo que genera un enorme vacío legal en cuanto al mal uso de Internet para difundir información falsa (*fake news*). (PAESANI, 2000)

ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212

La falsa sensación de comodidad y seguridad al utilizar Internet hace que las personas decidan actuar de manera imprudente, acusando, denunciando, juzgando y condenando sin pensar en las repercusiones de sus actos para otras personas. (ASCENSÃO, 1999)

Lo mismo ocurre con el mal uso de la herramienta de compartir noticias y publicaciones, que ya ha sido objeto de decisiones judiciales en las que se consideró que hay responsabilidad de quienes "comparten" mensajes y de quienes opinan de manera ofensiva, por las consecuencias de las publicaciones. El uso de este medio de comunicación debe ser abordado con mayor seriedad y no con el carácter informal que suele emplearse para tales acciones.

Surge entonces la pregunta sobre el derecho al olvido en relación al pasado digital de las personas. En agosto de 2010, Eric Schmidt, ex CEO de Google, declaró al periódico *The Wall Street Journal* que teme que los jóvenes no entiendan las consecuencias de tener tanta información personal disponible sobre ellos en Internet, y predice que en el futuro los jóvenes tendrán el derecho de "cambiar de nombre automáticamente" (SCHMIDT, 2010) para dejar atrás las travesuras de la juventud almacenadas en los sitios de redes sociales.

Por su parte, el semiólogo italiano Umberto Eco (2015), en una entrevista para la revista Veja, señaló que Internet da voz a todo tipo de opiniones descalificadas. Según él, con el auge de las redes sociales, el "imbécil" comienza a opinar sobre temas que no comprende. Internet lo recuerda todo, no olvida nada, y por eso es necesario distinguir, filtrar y analizar la información.

Paralelamente a todo esto, es necesario recordar la evolución de la computación en tiempos recientes. El aumento de las capacidades de almacenamiento tangible, que pasó de los megabytes a los gigabytes y terabytes, ahora está siendo reemplazado por la computación en la nube. El bien más tangible del ser humano quizás sea el dinero en efectivo, pero incluso el dinero está cada vez más virtual, registrado en sistemas informáticos bancarios en los que se confía gracias a la existencia de un entorno virtual seguro.

La computación en la nube obviamente presupone la seguridad de los datos, pero también es en la seguridad jurídica donde se basa esta mayor confianza de los consumidores en los sistemas informáticos. El mismo razonamiento se aplica a la información publicada en la *World Wide* Web, ya que los contenidos sensibles a menudo se confían a sistemas no confiables. Ante estas breves notas, surge la reflexión: ¿existe realmente libertad en el uso de Internet?

2. La evolución de Internet y los desafíos legales en la era digital

En los primeros días de Internet, el intercambio de datos era pequeño, con pocas imágenes, textos y gráficos en un sistema aún rudimentario y poco interconectado, lo que dificultaba determinar la relevancia jurídica del tema en esta etapa llamada "web 1.0". Fue con la aparición de la llamada "*web 2.0*" que la relevancia jurídica de Internet tomó forma debido a la intensificación del intercambio de datos. El volumen de información creció de manera abrumadora, generando situaciones como las descritas en los párrafos anteriores.

Sin embargo, este fenómeno no se detuvo ahí, ya que hay muchos otros cambios que se están iniciando en este contexto virtual y que se implementarán a corto y medio

Revista JURIS STUDIA Diciembre de 2024
ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212

plazo. Se trata de la llamada "*web 3.0*", que equivale al presente período de la sociedad de la información, que avanza rápidamente hacia el contexto de Internet de las Cosas (*Internet of Things*, o IoT), también conocida como "*web 4.0*" o incluso Internet de Todo (*Internet of Everything*, o IoE).

En un contexto en el que Internet está fuertemente presente, el comportamiento del "no he leído y acepto" de los usuarios de diversos servicios y sistemas se vuelve de crucial importancia en el estudio del *compliance* digital. Antes de adherirse a un servicio en línea, es común que se presenten al usuario las condiciones de uso (los "Términos de Uso"). Sin embargo, es innegable que la gran mayoría ni siquiera los lee ni acepta, lo que deja margen, en el ámbito contractual, para la implementación de todo tipo de abusos.

Precisamente en este contexto se han promulgado importantes regulaciones en Brasil, siendo la primera de ellas la Ley Nº 12.965, de 23 de abril de 2014 (conocida como "Marco Civil de Internet") y posteriormente el Decreto Nº 8.771/2016, que la reglamentó. Más recientemente, este movimiento resurgió con la promulgación de la Ley Nº 13.709, de 14 de agosto de 2018 (la llamada "Ley General de Protección de Datos Personales").

La identificación de personas, realizada a partir de datos personales, ya no se limita a una sola variable que pueda ser esencialmente única, como la biometría, el escaneo de voz o retina, o incluso los *tokens*. En la web, la recopilación de datos de diversos tipos permite la creación de filtros y la delimitación de perfiles.

Es precisamente esta recopilación de datos la que a menudo se descuida por parte de los usuarios que no prestan atención a los Términos de Uso de un determinado servicio. (DONEDA, 2006) Existen en el entorno virtual contratos interpersonales (de persona a persona), interactivos (de persona a sistema) e inter-sistémicos (de sistema a sistema). Por eso surge el tema de la Gobernanza de Internet (o *Compliance* Digital), que actúa de "punta a punta".

Básicamente, la red es estática y no "sabe" para qué fines se está utilizando o se utilizará. Las nuevas ideas se prueban sin la necesidad de convencer previamente a ninguna persona, lo que resulta en un entorno generativo. Con esto, las nuevas aplicaciones solo necesitan estar conectadas a Internet para funcionar, lo que permite una innovación continua y permanente en su entorno.

Esta libertad de uso es la llamada neutralidad de la red, cuya preservación constituye uno de los principios establecidos en el Marco Civil de Internet (artículo 3, inciso IV). Es el extremo opuesto de lo que ocurre, por ejemplo, en China, donde existen organismos que regulan los contenidos que se pueden ofrecer a los usuarios.

Han surgido varios manifiestos a favor de la neutralidad total de la red, como la "Declaración de la Independencia del Ciberespacio", escrita por John Perry Barlow (1996), que aboga por la completa ausencia de interferencia estatal en la web en una visión algo idealizada del asunto.

ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212

2.1. La regulación de la *web* y la protección de los bienes jurídicos en la era digital desde la Escuela de la Arquitectura de la Red

Lawrence Lessig (2001) fue el creador de la llamada Escuela de la Arquitectura de la Red, que resaltó la necesidad de regular la web mediante la creación de mecanismos para limitar ciertos usos. Para ejemplificar, al igual que tener una ley que prohíba la alta velocidad en las zonas escolares no es suficiente para evitar abusos y se instala un resalto en el lugar, es necesario tener algoritmos que frenen los usos indebidos de la red. Ante esto, es imperativo que haya coherencia entre el algoritmo utilizado y la legislación vigente que regula el uso de la web.

El tema cobró fuerza después de los ataques terroristas del 11 de septiembre de 2001 en los Estados Unidos, lo que desencadenó dos eventos importantes: (i) la creación de la NSA (Agencia de Seguridad Nacional); (ii) la promulgación del "*Patriot Act*" (Ley Patriota) por el Congreso estadounidense el 11 de octubre de 2001, y su sanción el 26 de octubre de 2001.

El "*Patriot Act*" estableció algunas directrices interesantes: (i) proporcionar herramientas adecuadas y necesarias para interceptar y obstaculizar actos terroristas; (ii) autorizar la interceptación de comunicaciones relacionadas con actividades terroristas; (iii) permitir al Gobierno solicitar a los proveedores de servicios de comunicación los registros con detalles sobre el uso específico del servicio por parte del cliente; (iv) extensiones en 2006 de su aplicación y ampliación de su alcance para combatir el narcotráfico y otros delitos, con el objetivo de salvaguardar las libertades civiles de los estadounidenses.

Sin embargo, el 9 de junio de 2013, Edward Snowden (2013) reveló públicamente que casi todo esto era falso, exponiendo una gran falta de legitimidad en el propósito invocado para la recolección de datos personales de diversos tipos, incluso para el espionaje entre países.

En Brasil, por ejemplo, existe legislación que autoriza la interceptación telemática de comunicaciones (Ley Nº 9.296/1996) en situaciones específicas. Sin embargo, ha habido varios casos en los que el intento de interceptación se ha visto obstaculizado a través de la aplicación "*WhatsApp*", que utiliza cifrado de extremo a extremo, generando una censurable discordancia entre el sistema y la ley.

Por otro lado, se plantea el tema de la eliminación de contenido por medio de hash mediante el procedimiento de "*content ID*" (identificación de contenido), como lo hace YouTube en respuesta a una reclamación de derechos de autor, lo que puede resultar en el bloqueo de un video, la desactivación del audio o el bloqueo de algunas plataformas.

En este contexto de regulación de Internet, surge la pregunta de si se han creado nuevos bienes jurídicos que deben ser protegidos por el Derecho. La interrogante es relevante, pero aún no tiene una respuesta definitiva.

El decálogo de principios de gobernanza de Internet desarrollado por el Comité Gestor de Internet en Brasil (CGI.br) es un repositorio muy importante de postulados de los cuales se pueden extraer conclusiones relevantes sobre el tema. Sin embargo, no se percibe con absoluta claridad la existencia de bienes jurídicos distintos de aquellos ya protegidos por el ordenamiento, pero sí se observa la irradiación de efectos derivados de una nueva dinámica sobre los bienes jurídicos existentes y debidamente tutelados.

Revista JURIS STUDIA Diciembre de 2024
ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212

2.2. El *compliance* normativo y su relación con la gobernanza corporativa y la gestión de riesgos: un enfoque histórico y global

El estudio del cumplimiento normativo está intrínsecamente relacionado con temas de Gobierno Corporativo, Gestión de Riesgos, Ética y Moral (ASSI, 2012). En términos históricos, el gobierno corporativo surgió en el transcurso del siglo XX con la expansión de las transacciones financieras a escala global y el cambio en el modelo de propiedad. (ANDRADE; ROSSETTI, 2009)

Con la transición del modelo "concentrado" al modelo "difuso", la figura del propietario o accionista de la empresa fue reemplazada por agentes especializados (administradores). Ante esta innovación, el término "*compliance*" fue acuñado en Estados Unidos por la *Securities and Exchange Commission* (SEC), que comenzó a exigir a las empresas la contratación de Oficiales de *Compliance*.

Posteriormente, ocurrieron algunos eventos que consolidaron el término en relación con el gobierno corporativo: (i) el caso Watergate en 1974, que llevó a la renuncia del presidente Richard Nixon; (ii) en 1976, la creación de la Teoría de la Firma o del Agente Principal de Jensen y Meckling (1976), que estableció la necesidad de conciliar los intereses; (iii) la promulgación del Acta de Prácticas Corruptas en el Extranjero (FCPA) en 1977, la ley estadounidense contra la corrupción.

Además de estos eventos ocurridos en Estados Unidos, se produjeron otros a nivel internacional que demostraron la expansión del tema: (iv) en 1980, la actividad de *compliance* se extendió a diversas actividades financieras en Estados Unidos; (v) en 1988, se estableció el Primer Acuerdo de Capital de Basilea; (vi) en 1990, la *Financial Action Task Force* emitió 40 recomendaciones sobre lavado de dinero (las llamadas "buenas prácticas").

A su vez, el tema llegó a Brasil y a otros países del mundo a fines del siglo XX: (vii) en 1992, se promulgó la Ley de Improbidad Administrativa brasileña (Ley Nº 8.429/92); (viii) en 1995, se publicó "Basilea I", que estableció reglas para el mercado financiero; (ix) en 1997, se promulgó la Convención de la OCDE sobre el Combate de la Corrupción de Funcionarios Públicos Extranjeros en Transacciones Comerciales Internacionales, ratificada por Brasil y promulgada internamente mediante el Decreto Nº 3.678/00; (x) en 1998, se publicó en Brasil la Ley Nº 9.613/98, que definió los delitos de lavado y ocultación de bienes y creó el COAF; (xi) también en 1998, se publicó la Resolución Nº 2.554/98, que estableció la implementación de sistemas de controles internos.

En el año 2002, se promulgó el *Sarbanes-Oxley Act* en Estados Unidos, que estableció normas y estándares de auditoría, control de calidad e independencia, y otorgó mayores responsabilidades a los directores ejecutivos y financieros, así como mayor responsabilidad a los abogados para informar cualquier indicio de violaciones legales a los directores y al comité de auditoría. En Brasil, se publicó la Resolución Nº 3.198/03 del Consejo Monetario Nacional, que trató sobre auditoría independiente y reguló la creación del Comité de Auditoría con funciones similares a las establecidas por el *Sarbanes-Oxley Act*.

El tema avanzó mucho en la primera década del siglo XXI, culminando con la promulgación del Pacto Mundial contra la Corrupción de las Naciones Unidas en 2004, lo que a su vez llevó a la creación de los Principios Mundiales de Gobierno Corporativo y la *International Corporate Governance Network* (ICGN) en 2005.

ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212

Además, en 2009, el Banco Central de Brasil publicó la Circular Nº 3.461, que consolidó todas las normativas relacionadas con la prevención del lavado de dinero. En el año 2012, se promulgó la Ley Nº 12.683 en Brasil, que introdujo importantes cambios en la ley de lavado de dinero. Ese mismo año se promulgó la ley anticorrupción rusa.

También es importante destacar la promulgación de la Ley de Defensa de la Competencia (Ley Nº 12.529/11) y la Ley Anticorrupción brasileña (Ley Nº 12.846/13) y su Decreto reglamentario (Decreto Nº 8.420/15).

Finalmente, en 2016, el Consejo Administrativo de Defensa Económica (CADE) de Brasil publicó su Guía de *Compliance*. (ASSI, 2012) El término proviene del verbo inglés "*to comply*", que significa cumplir, actuar de acuerdo con la norma; es decir, cumplir con las leyes, marcos reguladores y normas internas y externas del mercado. Sin embargo, algunas empresas se centran en regulaciones internas sin alinearlas con cuestiones jurídicas. (ANDRADE; ROSSETTI, 2009)

La sigla "GRC" ha ganado peso en todos los estudios relacionados con el *compliance* normativo. (MATTAROZZI; TRUNKL, 2008) La "G" representa la Gobernanza y se relaciona con el control, supervisión y gestión de una empresa, involucrando análisis, organización, metas, procesos y objetivos. La "R" se refiere a los riesgos existentes inherentes al negocio y otros que puedan surgir debido a factores internos o externos, lo que implica un trabajo preventivo de mapeo para evitar conductas indeseables. La "C" se ocupa del *compliance* normativo, que abarca cuestiones de diversas materias y no solo financieras, jurídicas o contables. (SILVA, 2005)

Existen numerosas normativas técnicas, como las llamadas "ISO", cada una de las cuales se ocupa de estandarizar un determinado tipo de proceso interno, basándose en el método "*plan*, *do*, *check* e *act*" o "PDCA" (planificar, hacer, verificar y actuar), que merece un enfoque más específico. (ASSI, 2012)

2.3. *LICRA vs. Yahoo!* y los desafíos de la jurisdicción en Internet: el derecho al olvido y la aplicación de la legislación brasileña

El precedente *LICRA vs. Yahoo!* del año 2000[1], en Francia, representó el inicio del debate sobre los límites en Internet en relación con el proveedor francés Yahoo.fr, que fue prohibido de vender ciertos productos en ese país, aunque los usuarios franceses aún podían comprar a través del sitio internacional Yahoo.com.

Asimismo, el llamado "derecho al olvido" se enfrenta al tema de la jurisdicción y se presenta como un corolario del derecho al olvido al imponer restricciones de acceso a los resultados de búsqueda mediante la desindexación.

En cuanto a la aplicación de la legislación brasileña, el Código Penal establece el principio de territorialidad, previsto en el artículo 5º, y señala la aplicabilidad de la ley brasileña, sin perjuicio de convenciones, tratados y normas de derecho internacional, al delito cometido en territorio nacional, considerando que el delito se comete en el lugar

1. Se trata de un precedente de la jurisprudencia francesa que involucró a la *Ligue Contre le Racisme et l'Antisémitisme* en litisconsorcio activo con la *Union des Étudiants Juifs de France* contra las empresas *Yahoo! Inc.* y *Société Yahoo! France*, estas últimas en litisconsorcio pasivo. Se determinó la competencia del Poder Judicial francés para imponer restricciones a la comercialización, a través de Internet, de objetos de colección del período nazi y se discutió la aplicabilidad de la legislación francesa a Internet, trascendiendo los límites territoriales.

Revista JURIS STUDIA Diciembre de 2024
ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212

donde ocurrió la acción u omisión, en su totalidad o en parte, así como donde se produjo o debería haberse producido el resultado (artículo 6º).

El Marco Civil de Internet, en su artículo 11, establece que en cualquier operación de recopilación, almacenamiento, custodia y tratamiento de registros, datos personales o comunicaciones por parte de proveedores de aplicaciones de Internet, cuando al menos uno de estos actos ocurra en territorio nacional, se debe respetar obligatoriamente la legislación brasileña. (LONGHI, 2014)

Existe la misma disposición para los datos recopilados en territorio nacional y para el contenido de las comunicaciones, siempre que al menos uno de los terminales esté ubicado en Brasil, incluso si las actividades son realizadas por una entidad jurídica con sede en el extranjero, pero que ofrece servicios al público brasileño o si al menos una entidad del mismo grupo económico tiene una presencia en Brasil.

Dado que todos los proveedores de aplicaciones, inevitablemente, recopilan, almacenan, custodian y/o tratan datos personales y registros electrónicos, deben respetar la legislación brasileña, incluso si son extranjeros, siempre que dirijan sus servicios ("*targeting*") también al público brasileño, incluso si no tienen una entidad económica en el país.

3. *Compliance* digital y la confianza en los medios de prueba electrónicos: un desafío para el proceso judicial electrónico

Los substratos obtenidos en línea no siempre tienen la misma confiabilidad que los documentos materiales. Impresiones, capturas de pantalla, IPs, registros y otros documentos electrónicos se han vuelto parte de la vida diaria de las personas y, a menudo, son los principales (¡o únicos!) medios de prueba disponibles para resolver ciertas cuestiones.

Para admitir dichos elementos como medios de prueba, el Código de Procedimiento Civil de 2015 incluyó algunas regulaciones ya existentes, a saber: a) el principio de la convicción motivada del juez (art. 371, CPC); b) el principio de la atipicidad de los medios de prueba (art. 369, CPC); c) la validez de las reproducciones electrónicas de hechos o cosas (art. 225, CC).

En este contexto, se incluyeron varios medios de prueba, como el testimonio personal (artículos 385 a 388), la confesión (artículos 389 a 395), la presentación de documentos o cosas (artículos 396 a 404), pruebas documentales (artículos 405 a 429), documentos electrónicos (artículos 439 a 441), prueba testimonial (artículos 442 a 463) y prueba pericial (artículos 464 a 480).

En cuanto a los documentos electrónicos, el artículo 384 del CPC establece la posibilidad de utilizar actas notariales, que otorgan fe pública a todo lo que se explicita en ellas después de la certificación por parte de la autoridad competente (el oficial responsable del Registro Público).

Este mecanismo representa un avance importante en términos de medios de prueba y la posibilidad de presentar cierta información al juez que no tendría el mismo valor probatorio si proviniera de documentos electrónicos.

ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212

Sin embargo, no siempre se observa el uso de este instrumento para llevar al conocimiento del juez ciertos hechos ocurridos en el entorno virtual, ya que el incumplimiento del requisito técnico (certificación) resta fuerza probatoria a una simple fotografía o captura de pantalla, que son susceptibles de edición y manipulación digital.

En este sentido, surge la discusión sobre el *compliance* digital en cuanto al papel que todos los actores del proceso, especialmente los abogados, desempeñan en cuanto a la confiabilidad de las pruebas que presentan al juicio. Aunque la forma correcta de presentación de estas pruebas no sea estrictamente el acta notarial, ya que se permite la certificación en un documento escrito por el certificador y dos testigos, es evidente que una simple imagen no tiene la misma fuerza probatoria.

Surge así un imperativo de conformidad procedimental esencial para operar en un universo donde el proceso judicial electrónico es una realidad ya predominante.

4. Los desafíos del *compliance* digital en la presentación de pruebas electrónicas en el proceso judicial

Los elementos obtenidos en línea no siempre tienen la misma confiabilidad que los documentos físicos. Impresiones, capturas de pantalla, direcciones IP, registros y otros documentos electrónicos se han vuelto parte del día a día de las personas y, muchas veces, son los principales (¡o los únicos!) medios de prueba disponibles para resolver ciertos asuntos.

Para admitir tales elementos como medios de prueba, el Código de Procedimiento Civil (CPC) de 2015 incluyó algunas regulaciones existentes, a saber: a) principio de convicción razonada del juez (art. 371, CPC); b) principio de atipicidad de los medios de prueba (art. 369, CPC); c) validez de las reproducciones electrónicas de hechos o cosas (art. 225, Código Civil). En este contexto, se incluyeron diversos medios de prueba, como el testimonio personal (arts. 385 a 388), la confesión (arts. 389 a 395), la exhibición de documentos o cosas (arts. 396 a 404), pruebas documentales (arts. 405 a 429), documentos electrónicos (arts. 439 a 441), testimonio de testigos (arts. 442 a 463) y prueba pericial (arts. 464 a 480).

En cuanto a los documentos electrónicos, el art. 384 del CPC establece la posibilidad de utilizar actas notariales, las cuales otorgan fe pública a todo lo que se haya explicitado después de la certificación por parte de la autoridad competente (el oficial a cargo de la oficina notarial).

Este mecanismo representa un avance importante en cuanto a los medios de prueba y la posibilidad de presentar al juez cierta información que no tendría el mismo valor probatorio si proviniera de documentos electrónicos.

Sin embargo, no siempre se observa la utilización de este instrumento para poner en conocimiento del juez ciertos hechos ocurridos en el entorno virtual, ya que el incumplimiento del requisito técnico (la certificación) disminuye el valor probatorio de una simple fotografía o captura de pantalla, las cuales son susceptibles de edición y manipulación digital.

En este contexto, cobra relevancia la discusión sobre el *compliance* digital en relación con el papel que todos los actores del proceso, especialmente los abogados, desempeñan en cuanto a la confiabilidad de las pruebas que presentan ante el tribunal. Aunque la

Revista JURIS STUDIA Diciembre de 2024
ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212

forma correcta de presentar dichas pruebas no sea estrictamente el acta notarial (ya que se admite la certificación en un documento escrito por el notario y dos testigos), es evidente que la mera imagen no tiene el mismo valor probatorio.

Surge así un imperativo de conformidad procedimental fundamental para actuar en un universo donde el proceso judicial electrónico es una realidad predominante.

Conclusión

¿Es posible saber la diferencia entre el bien y el mal, es decir, entre lo permitido y lo prohibido, lo correcto y lo incorrecto? Evidentemente, la idea de Ética está relacionada con la apreciación de la conducta humana y está vinculada a normas y principios aceptados por una sociedad. En términos generales, se trata de los valores humanos perseguidos, como la honestidad.

La Moral, por otro lado, está relacionada con los valores de un individuo, sus hábitos, que son juzgados por la sociedad y se consideran correctos, siempre y cuando haya una conducta moral adecuada y se respete la ética. Cuando existe un conflicto de intereses, ¿cuál será la conducta adoptada por un determinado profesional?

Esta pregunta plantea situaciones de desviaciones de conducta, prácticas perjudiciales para la competencia, violaciones de los Derechos Humanos, divulgación de información confidencial, corrupción y fraudes, entre otros.

Para definir estas situaciones, las empresas deben establecer Códigos de Ética o de Conducta que busquen alinear el perfil del profesional con el perfil de la organización, de modo que se puedan resolver algunas cuestiones que puedan generar conflictos de interés, por ejemplo.

Se vive en un momento de poca conducta moral, negligencia ética y falta de confianza interpersonal. Por lo tanto, cuando ocurre un conflicto de intereses, la tendencia es que la conducta profesional sea objeto de análisis por parte del Derecho, lo que conduce a la necesidad de cumplimiento normativo (*compliance*), que abarca diversas cuestiones como el cumplimiento de las leyes, las prácticas de mercado, los reglamentos internos, las reglas de conducta y comportamiento, y los temas de publicidad y concienciación. A su vez, la Gobernanza de TI implica cumplir con marcos regulatorios, servicios, integración de tecnologías, seguridad de la información y la relación entre TI y el negocio.

Indudablemente, el *compliance* digital surge como una especie de Gobernanza que involucra el análisis jurídico y técnico que trasciende el Derecho, imponiendo un diálogo transversal e interdisciplinario.

Revista JURIS STUDIA Diciembre de 2024
ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212

REFERENCIAS BIBLIOGRÁFICAS

ANDRADE, A. de, & ROSSETTI, J. P. (2009). *Governança Corporativa*: fundamentos, desenvolvimento e tendências. São Paulo: Atlas.

ASCENSÃO, J. O., et al. (1999). *Sociedade da informação*: estudos jurídicos. Coimbra: Almedina.

ASSI, M. (2012). *Gestão de riscos com controles internos*: ferramentas, certificações e métodos para garantir a eficiência dos negócios. São Paulo: Saint Paul.

BARLOW, J. P. (2015). *A Declaration of the Independence of Cyberspace*. Recuperado de https://eff.org/cyberspace-independence

BRASIL. (1988). *Constituição da República Federativa do Brasil*. Brasília: Senado Federal. Recuperado de http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

BRASIL. (1940). *Decreto-Lei nº 2.848, de 07 de dezembro de 1940*. Código Penal. In Diário Oficial da República Federativa do Brasil. Brasília, DF, 31 dez. 1940. Recuperado de http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm

BRASIL. (1990a). *Lei nº 8.078, de 11 de setembro de 1990*. Dispõe sobre a proteção do consumidor e dá outras providências. In Diário Oficial da República Federativa do Brasil. Brasília, DF, 12 set. 1990. Recuperado de http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm

BRASIL. (1990b). *Lei nº 8.078, de 11 de setembro de 1990*. Dispõe sobre a proteção do consumidor e dá outras providências. In Diário Oficial da República Federativa do Brasil. Brasília, DF, 12 set. 1990. Recuperado de http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm

BRASIL. (1992). *Lei nº 8.429, de 02 de junho de 1992.* Dispõe sobre as sanções aplicáveis aos agentes públicos nos casos de enriquecimento ilícito no exercício de mandato, cargo, emprego ou função na administração pública direta, indireta ou fundacional e dá outras providências. In Diário Oficial da República Federativa do Brasil. Brasília, DF, 03 jun. 1992. Recuperado de http://www.planalto.gov.br/ccivil_03/LEIS/L8429.htm

BRASIL. (1996). *Lei nº 9.296, de 24 de julho de 1996.* Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. In Diário Oficial da República Federativa do Brasil. Brasília, DF, 25 jul. 1996. Recuperado de http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm

BRASIL. (1998). *Lei nº 9.613, de 03 de março de 1998*. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências. In Diário Oficial da República Federativa do Brasil. Brasília, DF, 04 mar. 1998. Recuperado de http://www.planalto.gov.br/ccIVIL_03/leis/L9613.htm

Revista JURIS STUDIA Diciembre de 2024
ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212

BRASIL. (2011). *Lei nº 12.529, de 30 de novembro de 2011*. Estrutura o Sistema Brasileiro de Defesa da Concorrência; dispõe sobre a prevenção e repressão às infrações contra a ordem econômica, altera diversos dispositivos e dá outras providências. In Diário Oficial da República Federativa do Brasil. Brasília, DF, 1º nov. 2011. Recuperado de http://www.planalto.gov.br/CCIVil_03/_Ato2011-2014/2011/Lei/L12529.htm

BRASIL. (2013). *Lei nº 12.846, de 1º de agosto de 2013*. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. In Diário Oficial da República Federativa do Brasil. Brasília, DF, 02 ago. 2013. Recuperado de http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm

BRASIL. (2013). *Lei nº 12.850, de 02 de agosto de 2013*. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei no 9.034, de 3 de maio de 1995; e dá outras providências. In Diário Oficial da República Federativa do Brasil. Brasília, DF, 03 ago. 2013. Recuperado de http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm

BRASIL. (2014). *Lei nº 12.965, de 23 de abril de 2014.* Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. In Diário Oficial da República Federativa do Brasil. Brasília, DF, 24 abr. 2014. Recuperado de http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

BRASIL. (2018). *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais – LGPD. Publicado no DOU de 15.8.2018. Recuperado de http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

BRASIL. (2019). *Lei nº 13.853, de 8 de julho de 2019*. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Publicado no DOU de 15.8.2018. Recuperado de http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm

BRASIL. (2018). *Medida Provisória nº 869, de 27 de dezembro de 2018*. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Publicado no DOU de 28.12.2018. Recuperado de http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm

CONSTANT, B. (2015). *A liberdade dos antigos comparada à dos modernos* (E. Garcia, Traducción.). São Paulo: Atlas.

DE LUCCA, N. (2008). *Direito e Internet*: aspectos jurídicos relevantes (Vol. II). São Paulo: Quartier Latin.

DONEDA, D. (2006). *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar.

ECO, U. (2015). *A conspiração dos imbecis* [Entrevistador: E. Wolf]. Veja, Milão. Recuperado de https://veja.abril.com.br/brasil/a-conspiracao-dos-imbecis

ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212

JENSEN, M. C., & MECKLING, W. H. (1976). *Theory of the firm: managerial behavior, agency costs and ownership structure.* Journal of Financial Economics, 3. Recuperado de https://doi.org/10.1016/0304-405X(76)90026-X

LESSIG, L. (2001). *The Future of Ideas*: the fate of the commons in a connected world. Nova Iorque: Random House.

LONGHI, J. V. R. (2014). *Marco Civil da Internet no Brasil*: breves considerações sobre fundamentos, princípios e análise crítica do regime de responsabilidade civil dos provedores. In G. M. Martins (Ed.), Direito privado e Internet. São Paulo: Atlas.

MASLOW, A. H. (1970). *Motivation and personality* (2nd ed.). Nova Iorque: Harper & Row.

MATTAROZZI, V., & TRUNKL, C. (2008). *Sustentabilidade do setor financeiro*: gerando valor e novos negócios. São Paulo: Senac.

MILL, J. S. (2016). *Sobre a liberdade* (D. Bottmann, Trans.). São Paulo: L&PM Editores.

MINTZBERG, H. (2003). *Criando organizações eficazes*: estruturas em cinco configurações (2nd ed.). São Paulo: Atlas.

NEGRÃO, C. L., & PONTELO, J. de F. (2015). *Compliance, controles internos e riscos*: a importância da área de gestão de pessoas. Brasília: Senac.

PAESANI, L. M. (2000). *Direito e Internet*: Liberdade de Informação, Privacidade e Responsabilidade Civil. São Paulo: Atlas.

PASCAL, B. (2003). *Pensamentos* (Pietro Nassetti, Traducción). São Paulo: Martin Claret.

SCHMIDT, E. (2010, August). *Google and the search for the future*. Entrevistador: H. W. Jenkins Jr. The Wall Street Journal. Recuperado de https://on.wsj.com/2y977yO

SILVA, A. L. C. da. (2005). *Governança Corporativa e Decisões financeiras no Brasil* (2nd ed.). Rio de Janeiro: Mauad Editora.

SNOWDEN, E. (2013). *Edward Snowden: the whistleblower behind the NSA surveillance revelations.* Entrevistadores: G. Greenwald, E. MacAskill, & L. Poitras. The Guardian. Recuperado de https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

UNIÓN EUROPEA. (2016). *Regulamiento n.º 2016/679, de 27 de abril de 2016.* Regulamento Geral Sobre A Proteção de Dados. Recuperado de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT

Revista JURIS STUDIA Diciembre de 2024
ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212