Revista Eletrônica de Direito Processual – REDP. Estrato A2 Qualis.
Rio de Janeiro. Ano 17. Volume 24. Número 3. Setembro a Dezembro de 2023
Periódico Quadrimestral da Pós-Graduação *Stricto Sensu* em Direito Processual da UERJ
Patrono: José Carlos Barbosa Moreira (*in mem.*). ISSN 1982-7636. pp. 316-345
www.redp.uerj.br

CIBERSEGURIDAD Y ATAQUES INFORMÁTICOS A LOS PODERES JUDICIALES: UNA MIRADA DESDE EL DERECHO PROCESAL[1]

CYBERSECURITY AND CYBERTTACKS ON THE JUDICIARY: A PERSPECTIVE FROM PROCEDURAL LAW

CIBERSEGURANÇA E CIBERATAQUES NO JUDICIÁRIO: UMA PERSPECTIVA DO DIREITO PROCESSUAL

Ignacio M. Soba Bracesco[2]

RESUMEN: La ciberseguridad o seguridad digital es un deber para las cortes o tribunales y un derecho para las personas. El sistema de justicia no es inmune a las ciberamenazas, como ha quedado en evidencia en los últimos tiempos, en los que los ciberataques han proliferado y han mostrado las vulnerabilidades. Por eso es importante priorizar el tema en la agenda, para prevenir que estas amenazas impacten en los procesos concretos, en temas sensibles como la reserva de actuaciones, la pérdida de información y de pruebas, los plazos procesales, etc.

PALABRAS CLAVE: Ciberseguridad; ciberataque; independencia judicial; justicia electrónica.

ABSTRACT: Cybersecurity or digital security is a duty for courts and a right for individuals. The justice system is not immune to cyber threats, as has become evident in recent times, when cyber-attacks have proliferated and vulnerabilities have been exposed. It is therefore important to prioritize the issue on the agenda, in order to prevent these threats from impacting on specific processes, on sensitive issues such as the confidentiality of certain proceedings, the loss of information and evidence, procedural deadlines, etc.

KEYWORDS: Cybersecurity; cyberattack; judicial independence; e-justice.

RESUMO: A segurança cibernética ou digital é um dever dos tribunais e um direito dos indivíduos. O sistema judiciário não está imune às ameaças cibernéticas, como ficou evidente nos últimos tempos, quando os ataques cibernéticos se proliferaram e as vulnerabilidades foram expostas. Por isso, é importante priorizar o tema na agenda, a fim de evitar que essas ameaças tenham impacto em processos específicos, em questões sensíveis como a confidencialidade de determinados procedimentos, a perda de informações e provas, prazos processuais etc.

[1] Artigo recebido em 19/09/2023, sob dispensa de revisão.

[2] Profesor de derecho procesal y de litigación en cursos de pregrado, posgrados, especialización y maestrías en distintas universidades iberoamericanas. Profesor adjunto y Profesor adscripto de derecho procesal en la Facultad de Derecho de la Universidad de la República. Miembro de la Asociación Internacional de Derecho Procesal y del Instituto Iberoamericano de Derecho Procesal. Presidente honorario del Foro Uruguayo de Derecho Probatorio. Director del Anuario de Derecho Probatorio. Contacto: ignacio.soba@fder.edu.uy. Uruguay. @IgnacioSoba

Revista Eletrônica de Direito Processual – REDP. Estrato A2 Qualis.
Rio de Janeiro. Ano 17. Volume 24. Número 3. Setembro a Dezembro de 2023
Periódico Quadrimestral da Pós-Graduação *Stricto Sensu* em Direito Processual da UERJ
Patrono: José Carlos Barbosa Moreira (*in mem.*). ISSN 1982-7636. pp. 316-345
www.redp.uerj.br

PALAVRAS-CHAVE: Segurança cibernética; ataque cibernético; independência judicial; justiça eletrônica.

1. INTRODUCCIÓN: EL VELAR POR LA CIBERSEGURIDAD

El sistema de justicia, a nivel internacional (en mayor o menor medida según las posibilidades locales), se ha volcado a lo digital. Y son muchas las decisiones vinculadas a la tecnología y a lo digital que tienen que tomar a diario por quienes dirigen desde el punto de vista administrativo-institucional el sistema de justicia[3].

El funcionamiento de la oficina judicial y la sustanciación de los procesos jurisdiccionales se vincula, cada vez más, con el entorno y la infraestructura digital. Se abandona la tramitación del expediente físico, en papel, propia de la administración de justicia hasta el siglo veinte, y con ello se abandonan algunos riesgos, mientras otros aparecen.

Muchos datos e información -alguna sumamente valiosa- de los jueces, litigantes, fiscales, defensores, auxiliares del tribunal, funcionarios, etc., son registrados, sistematizados, tratados en bases de datos de tipo electrónico, que cuentan con distintos niveles de seguridad. No se puede desaprovechar la oportunidad de resguardar debidamente esos activos, que en ocasiones resultan muy apetecibles. Hay que aprovechar la oportunidad de que, en gran medida, los desafíos que provocan las ciberamenazas y los ciberataques recién comienzan (en términos históricos, se podría decir que llevan sólo algunas décadas). Son desafíos que, como sostengo en el presente artículo, pueden adquirir ribetes particulares en los sistemas de justicia (en donde han comenzado a visualizarse con mayor frecuencia).

Se espera o aspira que el sistema de justicia sea previsible, brinde seguridad jurídica y confianza desde el punto de vista institucional. Si el servicio de justicia no ofrece estos atributos, su legitimidad probablemente sea cuestionada.

[3] Decisiones que van desde cuestiones que pueden parecer banales (pero que no lo son tanto) como qué redes sociales utilizar oficialmente y cómo interactuar en esos espacios digitales con las personas, hasta cómo diseñar el expediente y la oficina digital, qué reconocimiento darle a la resolución de conflictos en línea (ODR), a la inteligencia artificial, etc.

En el plano digital sucede algo similar: se requiere previsibilidad y confianza a la hora de interactuar digitalmente y se necesita proteger la infraestructura y datos mediante estrategias de ciberseguridad.[4]

No es extraño entonces que desde hace algún tiempo se haya comenzado a hablar y reflexionar también por los juristas acerca de un derecho y un deber relacionado con la ciberseguridad.

Tal como se plasma en el punto VI de la Carta de Derechos Digitales (2021) española, toda persona tiene derecho a que los sistemas digitales de información que utilice para su actividad personal, profesional o social, o que traten sus datos o le presten servicios, posean las medidas de seguridad adecuadas que permitan garantizar la integridad, confidencialidad, disponibilidad, resiliencia y autenticidad de la información tratada y la disponibilidad de los servicios prestados. Si bien la Carta no tiene carácter normativo vinculante, sirve como uno de los estándares de referencia en la materia, al cual se aspira -en ese caso- que el Gobierno español se ciña, adoptando las disposiciones oportunas en el ámbito de sus competencias, para garantizar la efectividad de lo dispuesto en la propia Carta.

Además, en el citado punto VI se añade que los poderes públicos -y esto entiendo es perfectamente aplicable a la administración del sistema de justicia (el punto XXVII de la Carta agrega que se promoverá la garantía de los derechos reconocidos en la misma, en el marco de las relaciones con la Administración de Justicia)- tienen el deber de velar por la ciberseguridad, de modo proporcional a los riesgos a los que se esté expuesto en cada caso.

[4] El Reglamento de la Unión Europea 2019/881, define -en su art. 2- la ciberseguridad como «todas las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas». Ciberamenzas, en tanto, se considera «cualquier situación potencial, hecho o acción que pueda dañar, perturbar o afectar desfavorablemente de otra manera las redes y los sistemas de información, a los usuarios de tales sistemas y a otras personas». La Directiva de la Unión Europea 2016/1148, por su parte, define seguridad de las redes y sistemas de información, como «la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos» (art. 4 n° 2).

Revista Eletrônica de Direito Processual – REDP. Estrato A2 Qualis.
Rio de Janeiro. Ano 17. Volume 24. Número 3. Setembro a Dezembro de 2023
Periódico Quadrimestral da Pós-Graduação *Stricto Sensu* em Direito Processual da UERJ
Patrono: José Carlos Barbosa Moreira (*in mem.*). ISSN 1982-7636. pp. 316-345
www.redp.uerj.br

Por su parte, la Directiva 2016/1148, del Parlamento Europeo y del Consejo, de 6 de julio de 2016, sobre medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, también refiere expresamente a que los Estados miembros velarán por el cumplimiento de distintas medidas en lo que tiene que ver con la ciberseguridad.[5]

Este velar si bien se puede catalogar como una obligación de medios desde el punto de vista institucional (no directamente garantizar un resultado concreto), es un deber particularmente intenso, puntual y expreso en lo que refiere a la ciberseguridad.[6] No es una expresión genérica, de mero deseo y/o programática, que conlleve asumir una actitud pasiva ante el tema, sino que implica -a mi criterio- ocuparse frontalmente de la ciberseguridad, para que el derecho digital en cuestión (que aquí propongo relaciona con el sistema de justicia) no quede en una mera enunciación lingüística.

Es, en definitiva, un velar que puede ser fuente de responsabilidad de la administración cuando las garantías en materia de ciberseguridad no sean satisfechas, o cuando se produzca el funcionamiento anormal del servicio de justicia.[7] Este piso que

[5] Se pretende que los Estados miembros velen por que los proveedores de servicios digitales adopten medidas para prevenir y reducir al mínimo el impacto de los incidentes que afectan a la seguridad de sus redes y sistemas de información en ciertos servicios que se ofrecen en la Unión, a fin de garantizar la continuidad de dichos servicios. También se busca que los Estados miembros velen por que las autoridades competentes, los Equipos de respuesta a incidentes de seguridad informática (CSIRT), los puntos de contacto únicos dispongan de recursos adecuados para ejercer las funciones que les son asignadas de forma efectiva y eficiente y cumplir así los objetivos previstos en la Directiva (véase, a modo de ejemplo, arts. 9, 10, 14, 15 y 16 de la citada Directiva 2016/1148).

[6] Vale recordar la definición de "Velar" que nos proporciona el *diccionario de la lengua española*, de la Real Academia Española. Una de sus acepciones viene del latín *vigilāre*, y sus significados recuerdan, entre otras cosas a los siguientes significados: «1. tr. Hacer centinela o guardia… (…) 4. tr. Observar atentamente algo. (…) 7. intr. Cuidar solícitamente de algo».

[7] Aunque en la actualidad ya no se acude como antes a la noción de culpa *in vigilando* para determinar la existencia de responsabilidad por el actuar ajeno, es una noción que presenta aristas de interés, para explicar algunas derivaciones del velar o vigilar en relación a la ciberseguridad. En Uruguay, Amézaga (2011, pp. 714-715) afirmó en su tiempo que: «Nadie tiene derecho de tener personas bajo su dependencia y no vigilarlas debidamente para que no causen daño a otras. Si este daño se produce por falta de vigilancia debe ser responsable la persona que ha omitido la diligencia debida en dicha vigilancia (…) la persona responde de la culpa levísima de manera que deberá probar (como ustedes comprenden es una prueba difícil) no haber omitido la más mínima vigilancia, haber procedido con toda la diligencia de un buen padre de familia, tanto en el momento que se ha ejecutado el acto como en todos los momentos que ha estado bajo su dependencia». Otros análisis doctrinarios y jurisprudenciales realizados respecto a otros riesgos, como los laborales, también pueden ser ilustrativos y extrapolables respecto a lo que aquí se quiere transmitir: «La Administración titular del servicio mantiene la obligación de velar por el buen funcionamiento de los

marca la Carta de Derechos Digitales española considero que es un buen comienzo para reflexionar sobre el tema a nivel comparado.

2. LA CIBERSEGURIDAD Y LA INDEPENDENCIA JUDICIAL. EL ECOSISTEMA DIGITAL Y LAS POLÍTICAS PÚBLICAS

Recurrentemente se vislumbra la independencia judicial como un principio, cualidad o característica que, día a día, enfrenta importantes retos. Algunos, muy ilustrativamente, han catalogado el escenario como de constante asedio[8] o de tensión[9].

En el caso, el punto atañe a la independencia digital o tecnológica del Poder Judicial: ¿se verá condicionada la independencia del Poder Judicial a lineamientos, directrices o exigencias tecnológicas exógenas de otros poderes del Estado, agencias de gobierno electrónico u organismos similares o afines?

Como dice Andrés Ibáñez, la independencia externa del Poder Judicial es aquella que lo protege como organización frente a las posibles interferencias invasivas de otros órganos de poder[10].

Al decir de Pereira Campos[11], el sistema judicial debe ser independiente de los demás órganos y poderes del Estado, no pudiendo estos transgredir los límites de su autonomía funcional. Ahora bien, «Esto no excluye la natural tensión existente entre los

medios materiales suministrados para desenvolver su actividad. Si no lo hace así y causa un daño, como ha sucedido en el presente caso, incurrirá en culpa in vigilando, título suficiente para imputar la responsabilidad. La sentencia comentada establece, de forma indirecta, una vinculación entre la imputación del daño a la Administración y la culpa o negligencia de ésta en la infracción de la normativa de prevención de riesgos laborales…» (Ginès i Fabrellas, 2009, pp. 10 y 11).

[8] NIEVA FENOLL, J. y Oteiza, E. (Directores). *La independencia judicial: un constante asedio*. Madrid: Marcial Pons, 2019.

[9] ANDRÉS IBÁÑEZ, P. *Tercero en discordia. Jurisdicción y juez del Estado constitucional*. Madrid: Trotta 2015, pp. 139 y ss.

[10] ANDRÉS IBÁÑEZ, P. *Tercero en discordia. Jurisdicción y juez del Estado constitucional.* Madrid: Trotta 2015, p. 141.

[11] PEREIRA CAMPOS, S. La independencia judicial frente a los otros poderes públicos. Relato general (pp. 505-759). Oteiza, E. y Priori Posada, G. (Coordinadores). *La independencia judicial en el tercer milenio. Relatos generales del XVII Congreso Mundial de Derecho Procesal.* Lima: Palestra, 2023, pp. 546-547.

poderes del Estado en múltiples supuestos y contextos, ni la necesaria interacción entre los poderes en el marco del diseño institucional de cada país».

La independencia externa o institucional se vincula, así, con la separación de poderes. La pone a prueba. Requiere -parafraseando a Andrés Ibáñez[12] - una cultura que le de sustento, que la soporte y le de soporte institucional.

En España encontramos que en el año 2017 se celebró un convenio entre el Centro Criptológico Nacional (CCN), dependiente del Centro Nacional de Inteligencia (CNI), y el Consejo General del Poder Judicial (CGPJ) para impulsar los aspectos de seguridad informática, mediante el intercambio de información, la formación especializada y el desarrollo de proyectos tecnológicos. Como dan cuenta las reseñas de aquel año (CCN-CERT, 2017), el Convenio se articula desde la constatación de que el Consejo General del Poder Judicial debe continuar dotándose de los medios adecuados para la protección y control del acceso a la información de su competencia y ha de regular unos procedimientos eficaces para su almacenamiento, procesamiento y transmisión seguros por medio de sistemas propios. El ámbito de actuación del Centro Criptológico Nacional, en tanto, comprende la seguridad de los sistemas de las tecnologías de la información y comunicaciones de los órganos de la Administración que procesan, almacenan o transmiten información en formato electrónico.

Por su parte, en Uruguay, el art. 76 de la Ley N° 19.355, de 19 de diciembre de 2015, estableció que las entidades públicas -sin hacer en esa disposición ningún tipo de distinción- deberán simplificar sus trámites (en línea), siguiendo los lineamientos de gobierno electrónico, adoptando el procedimiento más sencillo posible para el interesado y exigiéndole únicamente el cumplimiento de los requisitos y etapas que sean indispensables para la obtención del propósito perseguido.

[12] ANDRÉS IBÁÑEZ, P. La independencia judicial frente a los poderes fácticos (pp. 812-834). Oteiza, E. y Priori Posada, G. (Coordinadores). *La independencia judicial en el tercer milenio. Relatos generales del XVII Congreso Mundial de Derecho Procesal.* Lima: Palestra, 2023, p. 824.

Revista Eletrônica de Direito Processual – REDP. Estrato A2 Qualis.
Rio de Janeiro. Ano 17. Volume 24. Número 3. Setembro a Dezembro de 2023
Periódico Quadrimestral da Pós-Graduação *Stricto Sensu* em Direito Processual da UERJ
Patrono: José Carlos Barbosa Moreira (*in mem.*). ISSN 1982-7636. pp. 316-345
www.redp.uerj.br


La referencia a los lineamientos de gobierno electrónico es el *quid* de la cuestión más general que quiero dejar planteada en el presente apartado: o sea, ¿quién fija la agenda digital del Poder Judicial?

Y no nos quedamos en una mera cuestión teórica. El día 19 de octubre de 2022, la Directora de la *Administrative Office of the United States Courts* le remitió una carta al comité que se ocupa de asuntos judiciales en el Congreso de los Estados Unidos, consignándose -en un documento adjunto a la misma (en donde se revisan algunos aspectos de la *Open Courts Act* of 2021)- que:

> […] we are concerned that the current cybersecurity language in S. 2614 may be interpreted to require the Judiciary to comply in detail with all Executive Branch requirements such as Executive Orders **that would otherwise not apply to the Judicial Branch**, into which the Judiciary had no input, and were not crafted with any special characteristics of the Judicial Branch in mind. Moreover, some of those Executive Branch requirements, such as software agents that could be required to run in our environment and network traffic routing requirements, **may infringe separation of powers** (by giving the Executive Branch – often a party to judicial proceedings – inappropriate and potentially unfettered access to Judicial Branch records)) and increase Judiciary implementation costs. The Executive Branch, frequently a party to judicial proceedings, must not have inappropriate and potentially unfettered access to Judicial Branch records. We agree with Congress that strong, modern cybersecurity safeguards are imperative for such a critical system. We believe we can accomplish the spirit of the legislation by making credible risk-based decisions informed by annual security assessments of a modernized case management and public access system, consistent with relevant cybersecurity standards that are practiced by Executive Branch agencies. (el énfasis me pertenece).

Lo que preocupa en ese documento, en lo vinculado a la ciberseguridad, entiendo -siguiendo una traducción no oficial- que es que se le pueda exigir a la rama judicial el cumplimiento exigencias que provienen del Poder Ejecutivo, como las Órdenes Ejecutivas, que de otro modo no se aplicarían a la rama judicial. Órdenes -señala el documento adjunto a la misiva- en las que el poder judicial no ha participado y que no se han elaborado teniendo en cuenta las características especiales del sistema de justicia. Expresamente se añade que algunos de los requisitos del Poder Ejecutivo, como los programas informáticos que podrían requerirse para funcionar en nuestro entorno y los requisitos de enrutamiento del tráfico de red pueden infringir la separación de poderes (al

otorgar al Poder Ejecutivo - a menudo parte de los procedimientos judiciales judicial- un acceso inapropiado y potencialmente sin restricciones a los registros del Poder Judicial) y aumentar los costes de implementación del Poder Judicial. El Poder Ejecutivo, que a menudo es parte en los procedimientos judiciales, no debe tener un acceso inapropiado y potencialmente irrestricto a los registros del Poder Judicial. Se manifiesta estar de acuerdo con el Congreso en que es imperativo contar con fuertes y modernas salvaguardas de ciberseguridad para un sistema tan crítico, y se señala que se puede cumplir el espíritu de la legislación tomando decisiones creíbles basadas en el riesgo, informadas por evaluaciones de seguridad anuales de un sistema de casos y de acceso público, en consonancia con las normas de ciberseguridad pertinentes que que practican los organismos del Poder Ejecutivo.

Bastante claro los términos de la citada nota y su documento adjunto. Ahora, esto no quiere decir, y no se malinterprete, que de por sí esos lineamientos serán injerencias indebidas, lo que sí quiero es problematizar el punto y que se debata pública y racionalmente acerca del tema, y que estemos prevenidos sobre eventuales condicionamientos tecnológicos a los Poderes Judiciales, Tribunales Constitucionales, etc.

Véase el caso de la ciberseguridad que aquí nos convoca:

- ¿quién se establece como encargado o responsable de responder ante los incidentes de ciberseguridad en el sistema de justicia? ¿qué sucede cuando los ataques al sistema de justicia son parte de un ataque más amplio que incluye otras entidades públicas y/o privadas?

- ¿quién aprueba, revisa, supervisa los protocolos frente a eventuales ataques cibernéticos? Estos protocolos pueden llegar a contemplar medidas de prevención, pero también medidas de contención y reacción ante amenazas ya consumadas.

- ¿qué recursos financieros, materiales, humanos se destinan específicamente a la ciberseguridad en justicia?

- ¿a quién deben acudir las y los jueces o cualquier otro sujeto del proceso ante un incidente en esta materia? ¿los mecanismos de consulta y/o respuesta funcionan adecuadamente y son accesibles para los sujetos vinculados al proceso jurisdiccional?

Parece interesante el camino que en su momento se empezó a recorrer por la Cumbre Judicial Iberoamericana en materia de socialización de conocimientos y experiencias para dar respuestas a las amenazas. En la XIX Edición de la Cumbre Judicial Iberoamericana (abril, 2018) se adoptaron algunas recomendaciones sobre ciberseguridad (aunque, *prima facie*, se ven como recomendaciones genéricas)[13].

La seguridad informática, virtual o digital (que como señalaba al comienzo, se agrega a la seguridad jurídica que también es necesaria en el sistema de justicia y en el proceso jurisdiccional), es un tema en permanente cambio, por el surgimiento constante de nuevas prácticas delictivas o nuevas modalidades de ataque a la infraestructura de las instituciones. Es, además, un negocio sin fronteras, un negocio de miles y miles de millones de dólares.

En un ecosistema virtual, la seguridad exige planificación, auditorías constantes para detectar puntos de penetración potenciales, revisión de infraestructuras, actualización y capacitación del conocimiento de los funcionarios (por ejemplo, para configurar alertas tempranas, o para instrumentar bloqueos efectivos en caso de ataques), etc.

[13] Por ejemplo, en Uruguay, el art. 149 de la Ley N° 18.719, de 27 de diciembre de 2010, en la redacción dada por el art. 84 de Ley N° 19.924 de 18 de diciembre de 2020, dispone: «Encomiéndase a la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), a dirigir las políticas, metodologías y mejores prácticas, y regular en materia de seguridad de la información y ciberseguridad a nivel nacional, así como fiscalizar, auditar su cumplimiento y brindar apoyo en las etapas de implementación de las mismas **en todas las entidades públicas**, y además, en las entidades privadas vinculadas a servicios o sectores críticos del país. Dichos cometidos serán ejercidos a través de la Dirección de Seguridad de la Información. La Dirección de Seguridad de la Información albergará al Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy) quien tendrá como cometidos principales centralizar y coordinar la respuesta a incidentes informáticos, y realizar las tareas preventivas que correspondan para la protección de los activos de información críticos de las entidades referidas en el inciso anterior, de acuerdo con los criterios que sugiera el Consejo Asesor Honorario de Seguridad de la Información, creado por el artículo 119 de la Ley N° 18.172, de 31 de agosto de 2007. El Poder Ejecutivo reglamentará lo dispuesto en la presente disposición normativa. (énfasis agregado).»

Considero que se debe trabajar, de modo muy cuidadoso pero decidido, en la articulación y coordinación de políticas con las agencias de gobierno electrónico, con el Poder Ejecutivo, empresas proveedoras de tecnología, en pos de: compartir conocimiento o *know how* (por ejemplo, en el área de la ciberseguridad ya mencionada); lograr una mejora en la infraestructura de datos (potenciando la interconexión e interoperabilidad), digitalizar archivos o registros (y que la información se cargue o deposite electrónicamente una sola vez, compartiéndose luego), etc[14].

Esa coordinación debería, además, propender al desarrollo de políticas concretas de alfabetización digital y educación en el uso de los canales judiciales digitales por parte de las personas (cuando los elijan por sobre los canales judiciales tradicionales, si es que pueden optar). En esa línea, el n° 3 del punto VI de la Carta de Derechos Digitales española prevé que «Los poderes públicos promoverán la sensibilización y formación en materia de ciberseguridad de toda la sociedad e impulsarán mecanismos de certificación».

Toda esa labor de instauración de un modelo de justicia digital o electrónica, es o será gradual, y se ejecutará en etapas o fases como las que propone Bueno de Mata (2021, pp. 57-59), algunas más impetuosas y vertiginosas que otras[15].

Considero que estas fases -sobre las que ha bregado el citado profesor en diferentes oportunidades- son útiles más allá de la realidad española, para ubicarnos en lo que es la inmersión de los sistemas de justicia en el ecosistema digital:

[14] En Uruguay, destaco los arts. 157 a 160 de la Ley N° 18.719, de 27 de diciembre de 2010 (intercambio de información; obligaciones de entidades públicas en materia de intercambio de información; principios de cooperación, integralidad, finalidad, confianza, seguridad, previo consentimiento informado, eficiencia y eficacia, etc.; rol de la AGESIC); y arts. 74 y ss. de la Ley N° 19.355, de 19 de diciembre de 2015, que regulan importantes cuestiones como: derecho de las personas a relacionarse con entidades públicas por medios electrónicos (art. 74); domicilio electrónico de las entidades públicas (art. 75); simplificación de trámites, trámites en línea, solicitud de documentos, certificados, constancias que se pueden proporcionar por sistemas informáticos (art. 76); notificaciones, seguridad en las diligencias (art. 77); copias electrónicas (art. 78); copias electrónicas, de documentos originariamente emitidos en soporte papel (art. 79); copias en soporte papel de documentos electrónicos (art. 80); relacionamiento electrónico (art. 85).

[15] Al decir de Bueno de Mata (2021, p. 226), citando a Gascón Inchausti y reflexionando sobre e-justicia: «…se añade el prefijo "e-" para recalcar que estamos aplicando a una misma realidad un matiz electrónico. De este modo la e-Justicia, se podría definir como la inclusión del uso de las tecnologías del conocimiento e información en la Administración de Justicia y supone el uso de una pluralidad de instrumentos y canales tecnológicos a la hora de impartir justicia».

- *Primera fase:* creación de un patrimonio digital jurídico (recopilación de datos originados en administraciones públicas, digitalización, abandono gradual del expediente en papel, etc.).

- *Segunda fase:* gestión procesal informatizada (expediente judicial electrónico, interoperabilidad entre sistemas informáticos en pos de la agilización de trámites, etc.).

- *Tercera fase:* tecnología interconectada entre ciudadanos y operadores jurídicos (ventanilla judicial única, presentación de escritos, pruebas, y actos de comunicación de manera electrónica, mayor interoperabilidad).

- *Cuarta fase:* aplicación de la inteligencia artificial o -acudiendo a la expresión de Barona Vilar[16], de «algoritmización de la justicia» (utilización de sistemas expertos, debatiendo el alcance de su utilización en el proceso: entre auxilio-asistencia o, en cambio, sustitución en la tarea de decisión, predominando lo primero). Se podría agregar aquí la automatización de ciertos procedimientos vinculada a la inteligencia artificial, tal como lo describe, por ejemplo, Nieva Fenoll[17].

El desarrollo e implementación de cada fase, así como el pasaje o avance a través de las mismas, requerirá de una estrategia firme y en paralelo en materia de ciberseguridad. Quién defina e implemente la agenda en esa materia puede -como se ha dicho- ser todo un desafío para la independencia del Poder Judicial.

3. LA OFICINA DE TECNOLOGÍA DENTRO DE LA ADMINISTRACIÓN DE LA JUSTICIA. ¿UN NUEVO ESTATUTO PARA LAS Y LOS FUNCIONARIOS DE LA JUSTICIA?

Sin perjuicio de lo expresado en el apartado anterior, lo que sí es claro -al menos si apostamos por un procesalismo que no sea ingenuo- es que nuestra disciplina (el Derecho procesal), aisladamente, no es suficiente ni tiene la exclusividad en lo que refiere

[16] BARONA VILAR, S. *Algoritmización del derecho y de la justicia. De la inteligencia artificial a la smart justice.* Valencia: Tirant lo Blanch, 2021.
[17] NIEVA FENOLL, J. y Oteiza, E. (Directores). *La independencia judicial: un constante asedio*. Madrid: Marcial Pons, 2019.

al análisis de los problemas que tiene que afrontar el proceso jurisdiccional, la gestión de la administración de justicia y la inmersión tecnológica.

Así, además de pensar en reformar la legislación o códigos en lo estrictamente procesal, también tenemos que ocuparnos de repensar el diseño de la oficina judicial en estos tiempos y en los que vendrán. Esto requiere -como diré a continuación- de una mirada interdisciplinaria, que exige escuchar y trabajar con los expertos en tecnología (por ejemplo, específicamente en los temas de ciberseguridad).

Una primera advertencia: hay distintas coyunturas en los Poderes judiciales y en las comunidades en las que actúan. Por ello tengamos presente las diferencias de recursos materiales y humanos, el grado de centralismo/descentralización existente, la densidad de órganos jurisdiccionales por cantidad de personas, y otras variables como el desarrollo de la conectividad a internet, el ambiente innovador circundante, etc. (en similar sentido, Pereira Campos, Villadiego Burbano y Chayer, 2011, p. 111). A pesar de lo anterior, sí se pueden hacer algunas referencias genéricas sobre el tema de la oficina judicial, las que luego habría que adaptar a esas situaciones puntuales y concretas[18].

En el plano normativo, entiendo que la regulación se tiene que ocupar de diseñar institucionalmente los nuevos roles (o reperfilar los existentes), así como de repartir las nuevas funciones (por supuesto, excluyendo lo propio de la jurisdicción). Esta normativa orgánica y funcional sería útil que sea pensada a partir de los aportes mancomunados de

[18] La Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC) de Uruguay ha elaborado un *Marco de ciberseguridad* (2020) que distingue distintos niveles en el proceso de gestión de la ciberseguridad, desde el punto de vista técnico y organizacional. Así, se pueden encontrar distintos niveles, que entiendo se podrían tomar como referencia para ubicar lo que hacen las distintas administraciones de justicia respecto del tema ciberseguridad. A saber, Nivel 0: Acciones vinculadas ciberseguridad casi o totalmente inexistentes. Nivel 1: Existen algunas iniciativas sobre ciberseguridad. Enfoques ad-hoc. Alta dependencia del personal. Actitud reactiva ante incidentes de seguridad. Nivel 2: Existen ciertos lineamientos para la ejecución de las tareas. Existe dependencia del personal. Se ha avanzado en el desarrollo de los procesos y documentación de las tareas. Nivel 3: Se caracteriza por la formalización y documentación de políticas y procedimientos. Gobernanza de la ciberseguridad. Métricas de seguimiento. Nivel 4: El Responsable de Seguridad de la Información (RSI) tiene un rol clave en el control y mejora del SGSI. Se realiza control interno. Se trabaja en la mejora continua. La ciberseguridad está alineada con los objetivos y estrategias de la organización. La estrategia uruguaya ha sido destacada a nivel del BID y la OEA, en cuyo reporte de ciberseguridad del 2020 el país alcanza la máxima puntuación en temas referidos a la organización y coordinación de respuesta a incidentes; el desarrollo de la temática en el gobierno y la confianza de las personas en el uso de servicios de gobierno, entre otros.

juristas, ingenieros, expertos en temas de tecnología, así como también por sociólogos expertos en organizaciones, otros profesionales de las relaciones laborales, economistas, etc[19].

Las oficinas de tecnología son y serán cada vez más vitales para la organización de la justicia (aunque, por cierto, ya plantean desafíos palpables que poco tiempo atrás eran impensables[20]). Quien dirija el área informática, dirección de tecnología, o similares, y/o asuma el rol de responsable en el área de la ciberseguridad en la administración de justicia, terminará asumiendo atribuciones, cometidos y responsabilidades muy importantes desde el punto de vista institucional, quizás hasta más relevantes desde el punto de vista sistémico que las que asumen algunos jueces. También posiblemente maneje recursos cuantiosos y vitales, que se irán incrementando año a año para no quedar a merced de amenazas y ataques.

En ese sentido, habrá que pensar muy bien los requisitos, incompatibilidades, prohibiciones que eventualmente se le exijan al personal informático para ser parte de la organización. En el caso uruguayo, para poner un ejemplo, tenemos que en la propia Constitución de la República -arts. 233 y ss.- se establecen algunos de los requisitos que se necesita para ser designado Juez (desde Juez de Paz en adelante), y también incompatibilidades para los cargos de la judicatura, así como prohibiciones a los magistrados y «a todo el personal de empleados pertenecientes a los despachos y oficinas internas de la Suprema Corte, Tribunales y Juzgados». La constitucionalización de parte

[19] En esa línea, Ortells Ramos (2012, p. 414), analizando aspectos generales de las opciones organizativas, señaló: «La mejora de los medios personales y materiales al servicio de la Administración de justicia requiere, para su adecuada gestión, estructuras organizativas que ni han de estar integradas, ni dirigidas, por técnicos jurídicos. No es en este ámbito donde se plantean los mayores problemas. La actividad más abundante, específica y con significación jurídica que se desarrolla en los juzgados y tribunales es la actividad procesal que, además, es inseparable del ejercicio de la potestad jurisdiccional. Los problemas surgen, precisamente, respecto de las diferentes opciones para organizar más racionalmente la realización de esa actividad».

[20] Pienso, por ejemplo, en lo que se titulaba en la siguiente nota periodística: El jefe de Informática del Tribunal Constitucional español renuncia por el «hostigamiento» e «involución» tecnológica del presidente de dicho órgano (*ABC*, 26 de mayo de 2020). Sin conocer los pormenores de esa situación concreta, lo que deja en evidencia la nota es la potencial existencia de problemas funcionales relativos al reparto y ejecución de las responsabilidades en materia tecnológica dentro de órganos de tipo jurisdiccional.

del estatuto tiene sus bondades y fortalezas, pero también -y sin perjuicio de ciertas interpretaciones evolutivas- corre el riesgo de generar anacronismos.

Teniendo en cuenta -por ejemplo- las dificultades que se pueden encontrar desde el ámbito público (concretamente, desde el sistema de justicia) para atraer y mantener personal capacitado e idóneo en el ámbito de la tecnología; así como por los conflictos de interés que pueden existir con proveedores, subcontratistas y la industria en general; o los peligros de fuga de información y otras cuestiones que hacen a la seguridad física y electrónica de la justicia; parece razonable proponer más reflexión acerca de un nuevo estatuto para las y los funcionarios judiciales, distinto al contemplado en la regulación actual, propia del siglo diecinueve o veinte.

4. LA CIBERSEGURIDAD, LOS ATAQUES INFORMÁTICOS Y SU INCIDENCIA EN LOS PROCESOS JURISDICCIONALES CONCRETOS: RESERVA DE LAS ACTUACIONES, PÉRDIDA DE INFORMACIÓN Y PRUEBAS, PLAZOS PROCESALES

El no contar con una estrategia definida en materia de ciberseguridad puede poner en riesgo la tramitación de los procesos jurisdiccionales.

Aquí referiré a algunos ejemplos de ataques a la administración de justicia que se han podido conocer a través de la prensa o de comunicaciones oficiales, pero que no son los únicos. Además se podrían dar «contagios» entre los ataques a la administración de justicia y aquellos dirigidos fiscalías, organizaciones de la sociedad civil, firmas de abogados u otras entidades públicas o privadas. En los últimos años también han existido ataques dirigidos, por ejemplo, a firmas de abogados.

En los casos de las administraciones de justicia, a modo ilustrativo, se puede mencionar lo sucedido en Argentina, donde algunos poderes judiciales provinciales han

Revista Eletrônica de Direito Processual – REDP. Estrato A2 Qualis.
Rio de Janeiro. Ano 17. Volume 24. Número 3. Setembro a Dezembro de 2023
Periódico Quadrimestral da Pós-Graduação *Stricto Sensu* em Direito Processual da UERJ
Patrono: José Carlos Barbosa Moreira (*in mem.*). ISSN 1982-7636. pp. 316-345
www.redp.uerj.br

sufrido de importantes ataques de *ransomware*[21], dejando *offline* el funcionamiento de la justicia por algunos días[22].

En Chile, el sistema informático del Poder Judicial sufrió un ciberataque en septiembre de 2022 en el 1% de los equipos de la red (estimación primaria). Dicho ataque se produjo a través de un *malware* que se expande, bloquea los archivos del ordenador afectado y luego suele pedir una recompensa económica en una moneda virtual para restaurar los datos. La reacción ante este ataque llevó al Poder Judicial a emitir una alerta informática dirigida a los funcionarios para que no abrieran ni leyeran correos electrónicos ni mensajes de dudosa procedencia y fueran escépticos frente ofertas, promociones o premios, etc. El Departamento de Informática de la Corporación Administrativa del Poder Judicial (CAPJ) informó luego que identificó las computadoras comprometidas, tomando medidas de restricción de acceso a la red y cambio de antivirus.

[21] En español sería algo así como secuestro de datos, ya que *ransom* significa rescate en inglés. Este tipo de *malware* restringe el acceso a la información o aplicaciones, exigiendo generalmente dinero para desbloquearla. El *malware* es un concepto más general, que engloba software malicioso (la expresión toma las primeras y últimas letras de estas palabras, y las une: *malicious software*). Para conocer algunas cuestiones básicas acerca de las distintas categorías de *malware* se puede consultar la clasificación expuesta por *Avast Academy* (2022): «El *ransomware* es la versión malware de la nota de rescate de un secuestrador. Suele funcionar bloqueando o denegando el acceso a su dispositivo y sus archivos hasta que pague un rescate al hacker. Cualquier persona o grupo que guarde información esencial en sus dispositivos corre peligro frente a la amenaza del ransomware. (…) El *spyware* recaba información sobre un dispositivo o red para luego enviársela al atacante. Los hackers suelen utilizar spyware para supervisar la actividad en Internet de una persona y recopilar datos personales, incluidas credenciales de inicio de sesión, números de tarjeta de crédito o información financiera, con el propósito de cometer fraude o robo de identidad (…) Los *gusanos* están diseñados con un objetivo en mente: proliferar. Un gusano infecta un equipo y después se replica y se extiende a dispositivos adicionales, permaneciendo activo en todas las máquinas afectadas. Algunos gusanos actúan como mensajeros para instalar malware adicional. Otros están diseñados solo para extenderse y no causan daño intencionadamente a las máquinas anfitrionas, aunque siguen atestando las redes con sus demandas de ancho de banda (…) El trabajo del *adware* es crear ingresos para el desarrollador sometiendo a la víctima a publicidad no deseada. Algunos tipos comunes de adware son los juegos gratuitos y las barras de herramientas para el navegador. Recaban datos personales acerca de la víctima y después los emplean para personalizar los anuncios que muestran. Aunque la mayoría del adware se instala de forma legal, no por ello es menos molesto que otros tipos de malware. *Troyanos.* Los antiguos poetas griegos hablaban de unos guerreros atenienses que se escondieron en un gigantesco caballo de madera para luego salir del interior, una vez que los troyanos lo arrastraron tras las murallas de la ciudad. Por tanto, un caballo de Troya es un vehículo que oculta atacantes. El malware troyano se infiltra en el dispositivo de una víctima presentándose como software legítimo. Una vez instalado, el troyano se activa y, en ocasiones, llega incluso a descargar malware adicional» (cursivas me pertenecen).

[22] Entre otros, Córdoba: caos en la Justicia tras el ataque de ransomware, con expedientes bloqueados y pagos en suspenso (Brodersen, J., 18 de agosto de 2022); El 'antecedente Globant' y las diferentes hipótesis del ciberataque a tribunales (por Romero, M. E., 21 de agosto de 2022).

Este ataque no afectó la Oficina Judicial Virtual. Por la misma fecha se discutía en el parlamento un proyecto de Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información, que crea la Agencia Nacional de Ciberseguridad y del Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional), entre otros servicios para combatir los incidentes en materia de ciberseguridad[23].

En Colombia, un Acuerdo del 13 de septiembre de 2023 del Consejo Superior de la Judicatura da cuenta de fallas originadas en un ataque masivo de *ransomware* contra el proveedor privado que brinda servicios de nube privada para la operación de las soluciones tecnológicas de la Rama Judicial (así como a otras entidades públicas). Se señala que el contratista no puede reestablecer de inmediato el servicio, por lo que suspende los «términos judiciales», salvo acciones de tutela, habeas corpus y control de garantías. El Acuerdo se difundirá a través de todos los medios disponibles (teniendo en cuenta que por ejemplo el sitio web se ha visto afectado), con el fin de lograr el conocimiento de los usuarios y la ciudadanía en general.

En Estados Unidos, por su parte, se ha informado que se ha visto comprometido su sistema electrónico de gestión y archivo de casos.

Esto ha llevado a que la Oficina Administrativa encargada de diversas tareas de gestión respecto de las Cortes federales (*The Administrative Office of the U.S. Courts*) venga trabajando en nuevos procedimientos de seguridad para proteger los registros y sistemas de gestión y archivo[24].

Desde el punto de vista macro o estructural, padecer incidentes vinculados a problemas en la ciberseguridad del sistema de justicia puede generar dificultades importantes en el acceso a la justicia y en la duración razonable de los procesos.

Respecto al acceso a la justicia, el problema se ve amplificado cuando nos encontramos ante sistemas que se han enfocado, o han priorizado, la atención digital de

[23] Un ciberataque pone en alerta al Poder Judicial de Chile (Laborde, A., 27 de septiembre de 2022). *El país.* A octubre de 2022 el Proyecto chileno de Ley Marco sobre Ciberseguridad y del Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional) había sido aprobado en general en el Senado, continuando su tramitación.
[24] U.S. Justice Department probing cyber breach of federal court records system (Lynch, S., y Raymond, N., 29 de julio de 2022). *Reuters.*

las personas. Los riesgos en materia de ciberseguridad serán más relevantes si ese primer acercamiento con la administración de justicia es en el plano digital (*digital first*)[25]. Ello podría generar varios riesgos en el acceso a la justicia de la población en general, y particularmente en sectores vulnerables.

Las personas podrían, en esos casos, tener dificultades para acceder de modo tradicional o presencial al sistema de justicia (problema potenciado por otras inequidades o vulnerabilidades, no sólo tecnológicas): ya sea porque las oficinas judiciales han perdido el «músculo» organizativo que permitía su actuación física, y ni siquiera cuentan con funcionarios que atiendan al público que de modo presencial cuando las personas se aproximan a las mismas (si es que físicamente cuentan con alguna locación o sede), o bien porque esa atención -cuando aún existe- es residual.

Este es un tema que requiere planificación no sólo por casos vinculados a incidentes en materia de ciberseguridad, sino también previendo situaciones más excepcionales y graves, aunque no imposibles, que ya a esta altura no pueden ser considerados una sorpresa (un «cisne negro» tecnológico), como son los eventuales «apagones digitales» con una duración -según los casos- más o menos transitoria (afectando no sólo al sistema de justicia). Todo esto dificultaría el acceso a la justicia o,

[25] En el sumario de la encuesta global sobre gobierno digital (Programa de las Naciones Unidas relativo al Gobierno Digital - encuesta global, 2018, pp. XXIII-XXIV), se señala que existe una correlación -negativa- entre el uso de las herramientas digitales y la exclusión social: «The Survey notes a negative correlation between digital use and social exclusion. Online use, offers an opportunity for e-inclusion but also risks a new digital divide, owing to insufficient access in low-income countries, either because of a lack of devices or of bandwidth and speed. The research also indicates that the greater ease with which information is gathered, stored, analyzed and disseminated and the decreasing cost and coverage of mobile-cellular and mobile broadband subscriptions have improved e-service delivery to vulnerable populations. …Increasingly, United Nations Member States are addressing the needs of marginalized groups through more targeted interventions and services provision. Still, the majority of the world's population remains offline, which increases the risk that vulnerable groups without Internet access will fall further behind in the rapidly progressing digital society. Thus, technology can both aid and impede the overarching goal of leaving no one behind. The digital divides are reviewed, both in terms of access to ICTs and the potentially negative consequences of a "digital first" approach wherein services are primarily offered online, isolating those who do not have online services or do not know how to access or use them. The Survey discusses the implications both of having digital skills and the lack thereof. It concludes that there are many opportunities to enhance social and digital inclusion through e-government and that emerging technologies and innovative multi-stakeholder partnerships can help to expand e-government access for all and provide dedicated services to address traditional problems related to poverty and social exclusion».

en casos de procesos ya iniciados, podría alterar las expectativas de una duración razonable de los mismos.

Por su parte, desde una perspectiva procesal más concreta, destacaré a continuación tres tipos de problemas relacionados con ataques o incidencias informáticas que eventualmente podrían poner en riesgo la seguridad y las garantías procesales.

Un primer tipo de problema se puede vincular con la **reserva de las actuaciones procesales**.

Si bien el principio es la publicidad, tanto interna como externa, no se puede descartar que sea necesario tramitar con carácter reservado ciertas actuaciones procesales. En esos casos, el peligro o directamente el daño se puede verificar cuando un ataque a la seguridad informática provoca filtraciones indebidas, a través de las cuales se permite el acceso a aquello que no se debía conocer por parte de ciertas personas.

Una brecha indebida se puede producir tanto en la reserva interna (respecto de litigantes que no tendrían que tener conocimiento -al menos en un momento determinado- de ciertas actuaciones), como en la externa (por el acceso de terceros ajenos al proceso, quienes en virtud de las filtraciones toman conocimiento de aquello que debía permanecer por fuera del conocimiento público).

También pueden existir ataques vinculados con el proceso de deliberación de los jueces (si dicho proceso se encuentra informatizado). Claro que este tipo de filtraciones, algunas famosas a nivel internacional como la que tuvo lugar en 2022 con el borrador de voto del *Justice* Samuel Alito en la Suprema Corte de los Estados Unidos (en un caso vinculado a la legislación del aborto), no siempre tienen su origen en ataques o problemas con la seguridad informática, sino que se originan en funcionarios infieles, que no mantienen el secreto o la reserva que se espera de los mismos en ciertos casos. El establecer protocolos de acceso, con niveles de seguridad claros, puede ser de gran importancia para prevenir este tipo de filtraciones.

Un segundo elenco de problemas se puede asociar con la **pérdida de la información en sentido amplio** (escritos o memoriales de los litigantes, resoluciones judiciales, evidencias o pruebas, etc.).

Este tipo de pérdida puede llegar a ser también muy dañina si no se cuenta con respaldos adecuados y/o mecanismos de reconstrucción. En ese sentido, la función de registro o archivo de los expedientes procesales debería ser objeto de una regulación *aggiornada*. El caso de Estados Unidos ya comentado, en el cual se afectó el sistema de gestión y archivo a nivel de las Cortes federales, es un ejemplo de esto. Según el Informe anual (2021) elaborado por la Oficina Administrativa que gestiona las Cortes federales, para los documentos altamente confidenciales presentados ante los tribunales federales se aceptó su presentación en papel o a través de un dispositivo electrónico seguro, almacenándose en un sistema informático independiente. Estos documentos ya no se cargaron en el sistema de gestión y archivo general[26].

Lo mismo para los mecanismos de reconstrucción de expedientes que estén pensados originalmente para el expediente papel (a modo de ejemplo, el art. 109 del Código General del Proceso uruguayo prevé la «reconstrucción de expedientes» que se hubieren perdido, destruido, ocultado, sin ninguna alusión puntual al expediente electrónico).

Con relación a esta problemática, entiendo que también podrían ser útiles los acuerdos procesales de las partes (o convenciones procesales) vinculados al archivo de pruebas y/o actuaciones procesales; así como acuerdos para la reserva externa de actuaciones que incluyan pactos vinculados a la ciberseguridad en los procesos jurisdiccionales. A modo de ejemplo, se podría pactar el compartir o archivar documentos en determinada nube, siempre que se den las condiciones para que desde la oficina judicial se pueda acceder a esa documentación. Esto, por supuesto, pensando en sistemas en los cuales no se ha implementado un sitio o plataforma oficial con niveles de seguridad satisfactorios para los usuarios y que por tanto no permitan cumplir en exclusividad y de modo adecuado esta función. Los proveedores que ofrecen almacenamiento en la nube podrían brindar servicios diversos, por ejemplo, en cuanto a encriptado, velocidad, tamaño de archivos, tipos de archivos, costos, etc. Las partes, por tanto, podrían acordar

[26] Administrative Office of the United States Courts. *Information Systems and Cybersecurity – Annual Report 2021*.

la utilización de alguno de estos servicios en particular, por cuestiones vinculadas a la confianza o seguridad informática que les genera un proveedor en particular. En ese sentido, el acuerdo podría incluir cláusulas vinculadas a la ciberseguridad, a la autorización para acceder a ciertos archivos y a la protección o reserva de algunos documentos o actuaciones procesales (ejecutando así materialmente lo que puede ser una resolución judicial que hubiese dispuesto la reserva externa de las actuaciones procesales).

Finalmente, también se pueden llegar a originar inconvenientes con respecto al **cómputo de los plazos procesales**. El inicio, cómputo, vencimiento y término de los plazos procesales es uno de los casos paradigmáticos del Derecho procesal en lo que refiere a la necesidad de previsibilidad y seguridad jurídica. Ahora a ello se suma la seguridad informática y la confianza en la utilización de las herramientas digitales.

La no disponibilidad de los sistemas o plataformas electrónicas puede tener su causa en distintos factores. Los ciberataques o las fallas en la seguridad informática pueden ser uno de ellos.

De ahí que sea necesario contar con alguna previsión en la regulación que opere de manera automática, *ex ante*, y que contemple qué sucede en casos de interrupción planificada y no planificada de los sistemas o plataformas electrónicas que son utilizadas por los litigantes para interactuar con el servicio de justicia. Esto evitaría algunas incertidumbres que se generan cuando se actúa tarde o se actúa *ex post.*

A modo de ejemplo, en España, el art. 135 de la Ley de Enjuiciamiento Civil refiere a la presentación de escritos y el requisito de tiempo de los actos procesales. En ese sentido, entre otras cuestiones, se prevé que se podrán presentar escritos y documentos en formato electrónico todos los días del año durante las veinticuatro horas. Sin embargo, cuando la presentación de escritos perentorios dentro de plazo por los medios telemáticos o electrónicos no sea posible por **interrupción no planificada del servicio de comunicaciones telemáticas o electrónicas** (esto es, fallos que no se han podido prever ni, por tanto, planificar por quienes gestionan el sistema), siempre que sea posible se dispondrán las medidas para que el usuario resulte informado de esta circunstancia, así

como de los efectos de la suspensión, con indicación expresa, en su caso, de la prórroga de los plazos de inminente vencimiento. El remitente podrá proceder, en este caso, a su presentación en la oficina judicial el primer día hábil siguiente acompañando el justificante de dicha interrupción. En los casos de **interrupción planificada** deberá anunciarse con la antelación suficiente, informando de los medios alternativos de presentación que en tal caso procedan. Queda, a su vez, abierta la posibilidad de que si el servicio de comunicaciones telemáticas o electrónicas resultase insuficiente para la presentación de los escritos o documentos, se pueda acudir a presentar en soporte electrónico en la oficina judicial ese día o el día siguiente hábil, junto con el justificante expedido por el servidor de haber intentado la presentación sin éxito.

Es clara la necesidad de contar con información en tiempo real, o de la manera más inmediata posible, así como un sistema que de respuestas, seguridad y transparencia a los litigantes, funcionarios y jueces, para tomar decisiones respecto al cómputo de los plazos procesales.

En el caso del Poder Judicial de Córdoba, se aprobó el Acuerdo Reglamentario 1778 A (15 de agosto 2022) con un Plan de Contingencia ante el ciberataque sufrido en agosto de 2022, suspendiendo la tramitación de expedientes íntegramente electrónicos y declarando día inhábiles (sin que ello signifique la falta de prestación del servicio presencial), habilitándose presentaciones en papel.

Por supuesto que no todo puede preverse *ex ante*, pero sería muy importante para todos los actores del sistema de justicia debatir este tipo de reglas con carácter previo a que tengan lugar los ataques o incidentes informáticos. Se trata de prever, planificar, establecer guías de conducta, buenas prácticas, etc., que permitan a las personas saber cómo comportarse si se diera un incidente. Pueden resultar muy útiles, por ejemplo (sin perjuicio de las normas de rango legal), la aprobación de protocolos o convenios institucionales entre los Poderes Judiciales y los Colegios de Abogados.[27]

[27] Este tipo de protocolos institucionales ha sido caracterizado por do Passo Cabral (2018, pp. 92-94) como un tipo de acuerdo colectivo, celebrado por asociaciones o entidades (que con su actuación vinculan a una categoría o los miembros de un grupo orgánicamente considerado), con la administración de justicia. Sería una forma de consensuar con la administración de justicia ciertos aspectos de índole administrativo -pero

Revista Eletrônica de Direito Processual – REDP. Estrato A2 Qualis.
Rio de Janeiro. Ano 17. Volume 24. Número 3. Setembro a Dezembro de 2023
Periódico Quadrimestral da Pós-Graduação *Stricto Sensu* em Direito Processual da UERJ
Patrono: José Carlos Barbosa Moreira (*in mem.*). ISSN 1982-7636. pp. 316-345
www.redp.uerj.br

Ahora bien, más allá de estas previsiones normativas consagradas para atender *ex ante* los inconvenientes tecnológicos que surjan, también son útiles las disposiciones más generales respecto de la fuerza mayor, la justa causa, etc.

En España, el art. 134 de la Ley de Enjuiciamiento Civil prevé la improrrogabilidad de los plazos los que, no obstante, se podrán interrumpir en caso de fuerza mayor -la que incluso podrá ser apreciada de oficio- que impida cumplirlos, reanudándose su cómputo en el momento en que hubiera cesado la causa determinante de la interrupción o demora. En Uruguay -siguiendo lo previsto en el art. 94 del Código Procesal Civil Modelo para Iberoamérica- el art. 98 del CGP refiere a la suspensión de plazos como «principio general» a quien se vea impedido por justa causa. Se considera justa causa la que provenga de la fuerza mayor o el caso fortuito, colocando al sujeto en la imposibilidad de realizar el acto por sí o por mandatario. No hay, en cambio, por el momento, una regulación específica para casos de impedimentos vinculados puntualmente a lo tecnológico.

CONSIDERACIONES FINALES

Los sistemas de justicia no pueden permanecer omisos en materia de ciberseguridad. Por el contrario, tienen que asumir una actitud activa en un asunto de alta prioridad en la agenda pública y digital [28]. Quienes toman decisiones se tienen que ocupar de entender las necesidades que genera la ciberseguridad desde el punto de vista institucional y velar por la misma, actuando pronta y decididamente.

que indirectamente podrían tener relevancia procesal- y que estarían bajo lo que es su potestad reglamentaria. Pienso que en estos protocolos se podrían establecer mesas de ayuda, mecanismos de consulta para los litigantes preocupados por lo que puedan ser amenazas en lo que hace a la interacción digital con la administración de justicia, canales de capacitación, envió de alertas de amenazas y/o de mensajes en tiempo real que sugieran o indiquen cómo actuar ante ataques que se estén consumando, etc.

[28] Así ha quedado demostrado, por ejemplo, en la Carta enviada al Congreso por la Directora de la *Administrative Office of the United States Courts* (2022), de los Estados Unidos. Allí se consigna, entre otras cosas, que un sistema modernizado mejorará significativamente nuestra postura de ciberseguridad y beneficiará no sólo a los tribunales, sino también a a los litigantes y al público que quiere acceder a los expedientes judiciales.

Los sistemas de justicia no pueden desaprovechar la oportunidad de aprovechar la oportunidad. Se hizo mucho, pero queda mucho por hacer (todo en un marco de permanente cambio, de constante evaluación y diagnóstico, de necesidad de adopción de medidas concretas). Permanecer omisos en materia de ciberseguridad es -y creo que existe unanimidad de pareceres al respecto- extremadamente peligroso […] y puede serlo cada vez más.

La administración de justicia tiene que asumir una actitud activa para prevenir y para saber cómo reaccionar tanto a nivel macro o estructural, como a nivel de los procesos concretos. Se deberá atender incluso detalles más elementales, como los de cómo se comunicará el Poder Judicial con sus usuarios y con la ciudadanía si todos sus canales digitales se han visto atacados.

Las amenazas a la seguridad, desde el punto de vista informático, son un ya un desafío global (no siendo la excepción la administración de justicia, como tampoco las firmas de abogados y abogadas). Es necesario conocer el escenario (hacer diagnósticos, auditorías) y planificar la actuación en materia de ciberseguridad de los próximos años. Probablemente haya mucho por pensar y por construir[29].

Pero esto no es todo, la ciberseguridad será también un tema recurrente en las decisiones jurisdiccionales de los próximos años. Incluso, algunos de estos problemas que se tendrán que enfrentar por las y los jueces en cuestiones de seguridad cibernética puede que sean muy difíciles de imaginar hoy en día (dado el vertiginoso avance de la tecnología, que dentro de unos años cambiará la forma en que hacemos las cosas). El tema estará presente en la agenda de las y los jueces[30]: la ciberseguridad será un gran desafío

[29] Por ejemplo, a nivel de las instituciones y organismos de la Unión Europea relevados para el informe de auditoría elaborado en el 2022 por el Tribunal de Cuentas europeo, se constató que solo el 58 % de las instituciones y organismos considerados (38 de 65) cuenta con una estrategia de seguridad informática o, como mínimo, un plan de seguridad informática aprobado por el consejo o por el equipo de alta dirección.
[30] Así se plantea por Marks, en *Breyer's Supreme Court replacement will face a hefty cyber docket* (nota del 28 de enero de 2022, publicada en el *Washington Post*), en la que se analiza los casos que tendrá que resolver la nueva integración de la Suprema Corte de los Estados Unidos, vinculados a temas de ciberseguridad, responsabilidad empresarial, comercio electrónico y consumidores, protección de datos, etc.

en lo que hace a las discusiones y debates forenses desde el punto de vista fáctico, probatorio y jurídico.

La ciberseguridad ayuda a configurar la base que permite ejercer y hacer efectivos otros derechos en el entorno digital. Sin ciberseguridad, los procesos jurisdiccionales y las oficinas judiciales en línea tendrían grandes dificultades tanto a nivel macro -por la pérdida de legitimidad y confianza en el sistema- como a nivel micro, de cada proceso, por los problemas asociados a filtraciones y brechas en la reserva de las actuaciones, la pérdida de información y el negocio ilícito con los datos obtenidos de actuaciones judiciales, las dificultades en el cómputo de los plazos procesales y las dudas relativas a realización de actos procesales a raíz de interrupciones en los servicios, etc.

REFERENCIAS

AMÉZAGA, J. J. *Obras esenciales. De las nulidades en general. Culpa contractual. Culpa aquiliana* (actualizada por Mariño López, A., Díaz, H., Mirande, S., Nicola, J. L.). Montevideo: La Ley Uruguay, 2011.

ANDRÉS IBÁÑEZ, P. La independencia judicial frente a los poderes fácticos (pp. 812-834). Oteiza, E. y Priori Posada, G. (Coordinadores). *La independencia judicial en el tercer milenio. Relatos generales del XVII Congreso Mundial de Derecho Procesal.* Lima: Palestra, 2023.

_____. *Tercero en discordia. Jurisdicción y juez del Estado constitucional.* Madrid: Trotta, 2015.

BARONA VILAR, S. *Algoritmización del derecho y de la justicia. De la inteligencia artificial a la smart justice.* Valencia: Tirant lo Blanch, 2021.

BUENO DE MATA, F. *Hacia un proceso civil eficiente: transformaciones judiciales en un contexto pandémico.* Valencia: Tirant lo Blanch, 2021.

CABRAL, A. Do Passo. *Convenções processuais* (segunda edición revisada, actualizada y ampliada). Salvador: Ed. JusPodivm, 2018.

GINÈS I FABRELLAS, A. Accidente de trabajo y responsabilidad patrimonial de la administración. Comentario a la STS, 3ª, 3.11.2008 (RJ 2008/5852; MP: Joaquín Huelin Martínez de Velasco). En *Revista InDret*, Barcelona, *2009*(3), pp. 10 y 11.

NIEVA FENOLL, J. Inteligencia artificial y proceso judicial: perspectivas tras un alto tecnológico en el camino. En *Revista General de Derecho Procesal*, 57, Iustel, documento electrónico, 2022, 21 pp. Disponível em: https://www.iustel.com/v2/revistas/detalle_revista.asp?id=9.

NIEVA FENOLL, J. y Oteiza, E. (Directores). *La independencia judicial: un constante asedio*. Madrid: Marcial Pons, 2019.

ORTELLS RAMOS, M. Las funciones procesales del secretario en la nueva oficina judicial: constitucionalidad, efectividad/eficiencia y técnica legislativa. En *Revista Ius et Praxis*, p. 397-424, Talca: Universidad de Talca - Facultad de Ciencias Jurídicas y Sociales, 2012.

PEREIRA CAMPOS, S. La independencia judicial frente a los otros poderes públicos. Relato general (pp. 505-759). Oteiza, E. y Priori Posada, G. (Coordinadores). *La independencia judicial en el tercer milenio. Relatos generales del XVII Congreso Mundial de Derecho Procesal*. Lima: Palestra, 2023.

PEREIRA CAMPOS, S., Villadiego Burbano, C., Chayer, H. M. Bases generales para una reforma a la justicia civil en américa latina y el caribe. En Pereira Campos, S. (Coordinador). *Modernización de la justicia civil* (pp. 17-135). Montevideo: Facultad de Derecho - Universidad de Montevideo, 2011.

ROBLES CARRILLO, M. Análisis de la Normativa sobre Seguridad de Redes y Sistemas de Información: el Real Decreto 43/2021. En Alcaraz, C., Calvo, G., de Castro, N., Fernández-Medina, E., Serrano, M. (2021). *Investigación en Ciberseguridad. Actas de las VI Jornadas Nacionales* (pp. 199-206). Cuenca: Universidad de Castilla-La Mancha, 2021.

SOBA BRACESCO, I. M. La oficina judicial digital y su inserción en el ecosistema de gobierno electrónico (reflexiones sobre independencia judicial y otros tópicos). En

Pérez Daudí, V. (Director) y Mallandrich Miret, N. *¿Cuarentena de la Administración de Justicia?* (pp. 309-330). Barcelona: Atelier, 2021a.

_____. *Estudios de Derecho procesal.* Montevideo: La Ley Uruguay, 2021b.

Legislación / normativa

Argentina. Poder Judicial de Córdoba. Acuerdo Reglamentario 1778 A (15 de agosto 2022). Plan de Contingencia Ciberataque.

- Dirección Nacional de Ciberseguridad – Jefatura de Gabinete de Ministros. Decisión 8/2021, de 10 de noviembre de 2021. https://www.argentina.gob.ar/normativa/nacional/356582/texto#:~:text=Que%20a%20trav%C3%A9s%20de%20la,Ley%20N%C2%B0%2024.156%20de

Unión Europea. Recomendación 2021/1086 de la Comisión de 23 de junio de 2021 sobre la creación de una Unidad Cibernética Conjunta. Recuperado de: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32021H1086

- Reglamento 2019/881, del Parlamento europeo y el Consejo, de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) N° 526/2013 («Reglamento sobre la Ciberseguridad»). Recuperado de: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0881&from=es

- Directiva 2016/1148, del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Recuperado de: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32016L1148

Uruguay. Ley N° 19.355, de 19 de diciembre de 2015, arts. 74 a 80 y 85. Ley de Presupuesto (derecho de las personas a relacionarse con entidades públicas por medios electrónicos, sin exclusión de medios tradicionales, domicilio electrónico, simplificación de trámites, etc.).

- Ley N° 18.719, de 27 de diciembre de 2010, arts. 149 (en redacción dada por Ley N° 19.924, de 18 de diciembre de 2020), sobre el rol del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy), de la Dirección de Seguridad de la Información de AGESIC; arts. 157 a 160 (interoperabilidad, intercambio de información) y 666 (expediente electrónico en el TCA).

Otros recursos / fuentes de internet

Avast Academy (2022). *¿Qué es el malware?* (Belcic, I., 28 de septiembre de 2019, actualizado el 15 de marzo de 2022). Recuperado de: https://www.avast.com/es-es/c-malware

Banco Interamericano de Desarrollo (BID) y Organización de Estados Americanos (OEA). *Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y el Caribe* (2020). Recuperado de: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Chile. Senado. Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información (2022). Recuperado de: https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=14847-06

España. *Carta de Derechos Digitales* (2021). Recuperado de: https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

- CCN-CERT (2017). El CGPJ y el CNI colaborarán en la prevención de las ciberamenazas y los ataques en la Red. Recuperado de: https://www.ccn-cert.cni.es/gl/gestion-de-incidentes/lucia/34-notas-de-prensa/5125-el-cgpj-y-el-cni-colaboraran-en-la-prevencion-de-las-ciberamenazas-y-los-ataques-en-la-red.html

- PwC España. *Digital Trust Survey 2022.* Recuperado de: https://www.pwc.es/es/publicaciones/transformacion-digital/global-digital-trust-insights-2022.html

- Real Academia Española. *Diccionario de la lengua española.* Recuperado de: https://dle.rae.es/

Estados Unidos. Administrative Office of the United States Courts. *Information Systems and Cybersecurity – Annual Report 2021*. Recuperado de: https://www.uscourts.gov/statistics-reports/information-systems-and-cybersecurity-annual-report-2021

- AO Director Updates Congress on Progress in Case Management Technology Modernization (letter - 2022). Recuperado de: https://www.uscourts.gov/news/2022/10/19/ao-director-updates-congress-progress-case-management-technology-modernization; acceso a la carta y documento adjunto: https://www.uscourts.gov/sites/default/files/letter_to_chairman_richard_durbin_october_2022_0.pdf

- Departament of Justice. Cybersecurty Unit. Recuperado de: https://www.justice.gov/criminal-ccips/cybersecurity-unit

Organización de Estados Americanos (OEA). Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE). *Ciberseguridad – Marco NIST. Un abordaje integral de la ciberseguridad* (2019). Recuperado de: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

Unión Europea (UE). Tribunal de Cuentas europeo. *Ciberseguridad de las instituciones, órganos y organismos de la UE: En general, el nivel de preparación no es proporcional a las amenazas.* Informe especial, 2022-5. Recuperado de: https://www.eca.europa.eu/Lists/ECADocuments/SR22_05/SR_cybersecurity-EU-institutions_ES.pdf

Uruguay. Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC). *Marco de ciberseguridad* (2020). https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-ciberseguridad

- Poder Judicial. Acuerdo específico de cooperación interinstitucional en materia de gobierno digital y seguridad de la información entre el poder judicial y la Agencia para el desarrollo del gobierno de gestión electrónica y la sociedad de la información y del conocimiento (2017). Recuperado de: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/convenios/poder-judicial-agesic

Prensa

Breyer's Supreme Court replacement will face a hefty cyber docket (por Marks, J., 28 de enero de 2022). *Washington Post.* Recuperado de: https://www.washingtonpost.com/politics/2022/01/28/breyers-supreme-court-replacement-will-face-hefty-cyber-docket/

Ciberdelincuencia: un jugoso negocio que equivaldría a la tercera economía mundial (por Zamarrón, I., 30 de marzo de 2022). *Forbes - México.* Recuperado de: https://www.forbes.com.mx/ciberdelincuencia-un-jugoso-negocio-que-equivaldria-a-la-tercera-economia-mundial/

Córdoba: caos en la Justicia tras el ataque de ransomware, con expedientes bloqueados y pagos en suspenso (Brodersen, J., 18 de agosto de 2022). *Clarín – Tecnología.* Recuperado de: https://www.clarin.com/tecnologia/caos-justicia-cordoba-ransomware-expedientes-bloqueados-pagos-suspenso_0_7rJdwF0A58.html

El 'antecedente Globant' y las diferentes hipótesis del ciberataque a tribunales (por Romero, M. E., 21 de agosto de 2022). *Perfil.* Recuperado de: https://www.perfil.com/noticias/cordoba/el-antecedente-globant-y-las-diferentes-hipotesis-del-ciberataque-a-tribunales.phtml

El jefe de Informática del Tribunal Constitucional español renuncia por el «hostigamiento» e «involución» tecnológica del presidente de dicho órgano (por Villanueva, N., 26 de mayo de 2020). *ABC.* Recuperado de: https://www.abc.es/espana/abci-jefe-informatica-renuncia-hostigamiento-involucion-tecnologica-presidente-202005260208_noticia.html

Supreme Court's Leak Investigation Is Self-Destructive. (Carter, S., 3 de junio de 2022). *Bloomberg – US edition* Recuperado de: https://www.bloomberg.com/opinion/articles/2022-06-03/supreme-court-s-abortion-leak-investigation-is-tearing-the-court-apart

Un ciberataque pone en alerta al Poder Judicial de Chile. (Laborde, A., 27 de septiembre de 2022). *El país.* Recuperado de: https://elpais.com/chile/2022-09-27/un-ciberataque-pone-en-alerta-al-poder-judicial-de-chile.html

U.S. Justice Department probing cyber breach of federal court records system (Lynch, S., y Raymond, N., 29 de julio de 2022). *Reuters.* Recuperado de: https://www.reuters.com/world/us/us-justice-dept-probing-cyber-breach-federal-court-management-system-2022-07-28/