nº 12 (3er Trimestre 2024)
ISSN: 2792-7962 – ISSNe: 2792-7970

ERTE por fuerza mayor derivado de un "ciberataque". Análisis de la STS 3452/2024[1]

Temporary Employment Regulation File due to force majeure resulting from a"cyberattack". Analysis of the Supreme Court Ruling 3452/2024

Tamara Prieto Pérez *Investigadora Contratada Predoctoral*
Universidad de León
https://orcid.org/0009-0000-5927-1436

Cita Sugerida: PRIETO PÉREZ, T. «ERTE por fuerza mayor derivado de un "ciberataque". Análisis de la STS 3452/2024». *Revista Crítica de Relaciones de Trabajo, Laborum*. nº 12 (2024): 213-230.

Resumen

El objetivo de este estudio jurídico es examinar, a la luz de la jurisprudencia sentada por la sentencia del Tribunal Supremo del 11 de junio de 2024, las circunstancias bajo las cuales un incidente de ciberseguridad que afecte a una entidad corporativa puede ser considerado como un evento constitutivo de fuerza mayor, justificando así la implementación de un Expediente de Regulación Temporal de Empleo (ERTE).

El análisis se propone deconstruir la noción tradicional de fuerza mayor, expandiendo su alcance más allá de los fenómenos de origen natural, tales como desastres geológicos o eventos meteorológicos extremos. En el contexto de una sociedad caracterizada por un alto grado de desarrollo tecnológico, como es el caso de la actual, se argumenta que ciertos eventos "antropogénicos" pueden cumplir con los criterios jurídicos establecidos para la calificación como fuerza mayor.

Palabras clave

Ciberataque, ERTE, fuerza mayor, imposibilidad de la prestación

Abstract

The aim of this legal study is to examine, in light of the jurisprudence established by the Supreme Court's judgment of June 11, 2024, the circumstances under which a cybersecurity incident affecting a corporate entity can be considered an event constituting force majeure, thus justifying the implementation of a Temporary Employment Regulation File (ERTE).

The analysis proposes to deconstruct the traditional notion of force majeure, expanding its scope beyond natural phenomena, such as geological disasters or extreme weather events. In the context of a society characterized by a high degree of technological development, as is the case with the current one, it is argued that certain "anthropogenic" events may meet the legal criteria established for qualification as force majeure.

Keywords

Cyberattack, Temporary Employment Regulation File, Force, Majeure, impossibility of performance

1. ANTECEDENTES DE HECHO

Las incidencias cibernéticas que implican la sustracción o el cifrado no autorizado de datos se han convertido en una amenaza constante en el panorama empresarial actual, constituyendo un obstáculo significativo para el desarrollo normal de las operaciones corporativas. Europol define los ciberataques como "delitos que o pueden perpetrarse mediante el uso de ordenadores, redes informáticas y otras tecnologías de la información y comunicación (TIC)"[2]. Además de esta definición general,

[1] Este trabajo ha sido realizado en el marco del proyecto de investigación "Hacia una transición ecológica justa: los empleos verdes como estrategia frente a la despoblación (TED 2021-1295526B-100), financiado por el Ministerio de Ciencia e Innovación. Nº. Proyecto: UXX12022/00217

[2] Europol accesible en OCTA 2018 https://www.europol.europa.eu/sites/default/files/documents/ iocta2018.pdf

Fecha Recepción:09/09/2024 - Fecha Revisión: 10/09/2024 - Fecha Aceptación: 17/09/2024
Págs. 213-230

existen conceptualizaciones más específicas, como la presentada en el informe "Ciberamenazas y tendencias" del Centro Criptógico Nacional - Computer Emergency Response Team (CCN-CERT), que se centra en las posibles consecuencias de estos ataques: "una operación cibernética, ya sea ofensiva o defensiva, con potencial para causar pérdidas de vidas humanas, lesiones, daños materiales o destrucción de bienes".

Sin necesidad de profundizar en análisis técnicos detallados o revisar exhaustivamente la información actual sobre estos incidentes, es evidente que los ciberataques han alcanzado una prevalencia significativa en nuestra sociedad, extendiéndose más allá del impacto en el ámbito empresarial y afectando igualmente a las administraciones públicas y a los ciudadanos. Además, es innegable la gravedad y las consecuencias de estos ataques, que incluyen efectos económicos adversos, la interrupción de operaciones, el secuestro de datos y su tráfico ilícito, entre otros. En este sentido, los ciberataques pueden considerarse uno de los costos asociados a la digitalización integral de los hábitos y estilos de vida en el siglo XXI. Este fenómeno, caracterizado por su complejidad, innovación constante y creciente sofisticación, presenta una diversidad considerable de formas y efectos.

Recientemente, se ha publicado la resolución de un recurso de casación que podría establecer un precedente jurisprudencial en cuanto a las implicaciones legales de un incidente cibernético de gran magnitud en el ámbito empresarial. La sentencia 908/2024 emitida por la Sala de lo Social del Tribunal Supremo establece que un incidente de seguridad informática puede ser considerado como un caso de fuerza mayor, justificando así la implementación de un Expediente de Regulación Temporal de Empleo (ERTE).

Es pertinente recordar que un ERTE por fuerza mayor es un procedimiento administrativo-laboral que permite a una entidad empresarial suspender temporalmente los contratos laborales de su plantilla ante circunstancias excepcionales que impidan el mantenimiento de sus actividades regulares[3].

Para contextualizar adecuadamente el caso en cuestión, es necesario examinar los antecedentes. El 4 de junio de 2021, la empresa Ilunion Contact Center, con cinco centros de trabajo situados en diferentes provincias, una entidad especializada en servicios de Contact Center y Telemarketing, cuya actividad principal pasaba por proporcionar soporte al cliente y manejar grandes volúmenes de comunicaciones telefónicas para diversas compañías, detectó la presencia de un virus *ransomware*[4] de la familia "Ryuk" en su infraestructura tecnológica, cifrando la información en los sistemas de la empresa y bloqueando el acceso a datos esenciales, lo cual precipitó la necesidad de implementar medidas de suspensión y reducción de jornada laboral, afectando a un total de 1.192 personas empleadas.

Este incidente comprometió de manera crítica sus operaciones, obligando al aislamiento y desconexión de su infraestructura de red. Este malware estaba afectando al funcionamiento normal de su sistema operativo en uno de los servidores centralizados, ubicado en un centro de datos crítico para sus operaciones, comprometiendo el funcionamiento de uno de sus servicios de base de datos,

[3] *Cfr*. Lahera Forteza, J.: «Nuevas perspectivas de suspensión del contrato y reducción de jornada por causas económicas, técnicas, organizativas y de producción», en AAVV: *La reforma laboral de 2012: Nuevas perspectivas del Derecho del Trabajo, La Ley, Madrid,* 2012, pág. 181-183, Sola Monells, X.: "La suspensión por causas empresariales tras la reforma laboral de 2012: problemática aplicativa y valoración crítica" en AAVV: *Balance de la reforma laboral de 2012*, Bomarzo, 2016, págs. 288, 289 y 312.

[4] El ransomware es un código dañino para secuestrar datos, una forma de explotación en la cual el atacante cifra los datos de la víctima y exige un pago por la clave de descifrado.

una parte esencial de su plataforma, ya que almacena y gestiona toda la información de las llamadas y las incidencias registradas[5].

El impacto del *ransomware* fue significativo, ya que interrumpió no solo las operaciones diarias de la empresa, sino también su capacidad para ofrecer un servicio continuo y eficiente a sus clientes.

Para contener la propagación del virus, fue imperativo realizar un apagado completo del Centro de Procesamiento de Datos (CPD) y cortar todas las comunicaciones. Este CPD es crítico, ya que alberga los servidores que manejan y procesan toda la información digital necesaria para la prestación de servicios, incluyendo los procesos administrativos internos y las infraestructuras de comunicación vinculadas. La interrupción implicó la desconexión de todas las redes internas, el cese de operaciones de los sistemas por donde fluye y se procesa información esencial, y la suspensión de los enlaces de comunicación con todas las sucursales donde se llevaban a cabo los servicios de centro de atención telefónica y gestión documental. Estas acciones fueron necesarias para aislar el virus y proteger la integridad de los datos y sistemas operativos involucrados.

Se estimó que el restablecimiento completo de las actividades requeriría un período de 14 semanas. Se constata que Ilunion había previsto la posibilidad de un incidente de ciberseguridad y había implementado medidas de protección acordes con los estándares de la industria. No obstante, estas medidas resultaron insuficientes para prevenir el ataque, lo que condujo a la suspensión de la mayoría de los servicios y a la consecuente paralización de las actividades laborales.

Ante esta situación, la mencionada empresa presentó ante la Dirección de Trabajo una solicitud para declarar fuerza mayor con el fin de activar un ERTE que afectaría a 1.192 personas trabajadoras. sin embargo, la Administración del Estado impugnó el ERTE, argumentando que un incidente de ciberseguridad es previsible dada la naturaleza digital de las operaciones de la entidad. Ante esta decisión, la empresa optó por iniciar un procedimiento judicial para revisar y resolver la situación, buscando amparo legal para proceder con las medidas de ajuste necesarias en respuesta al impacto del ciberataque en sus operaciones y recursos humanos.

Con la sentencia de 11 de junio de 2024[6], el Tribunal Supremo ha confirmado la decisión adoptada por la Audiencia Nacional en sentencia de 14 de marzo de 2022, en el proceso de impugnación de actos administrativos de naturaleza laboral seguido bajo el número 13/2022, a instancia de la empresa Ilunion Contact Center S.A.U, en la que estima la demanda considerando la existencia de silencio administrativo positivo en relación a la solicitud de declaración de fuerza mayor formulada por esta tras sufrir un ciberataque.

El Tribunal Supremo ha dictaminado que un ataque cibernético no puede ser excluido de la categoría de fuerza mayor meramente por su previsibilidad. El factor determinante radica en la inevitabilidad del suceso, a pesar de la implementación de medidas de seguridad pertinentes, argumentando la imposibilidad material de que estas personas trabajadoras desempeñaran sus funciones habituales; así el Tribunal Supremo ha ratificado el recurso presentado ante la Audiencia Nacional, estableciendo que, si bien un ataque cibernético puede ser considerado previsible, también puede clasificarse como "inevitable" cuando supera las medidas de control y prevención razonablemente implementadas por la entidad afectada.

[5] El CCN-CERT ha desarrollado el documento de Buenas prácticas 21 sobre gestión de incidentes de ransomware. Disponible en: https://www.ccn-cert.cni.es/informes/informes-de-buenaspracticas-bp.html Fecha de consulta: 10 de agosto de 2024.

[6] STS 3452/2024 – ECLI:ES:TS:2024:3452

2. POSICIONES DE LAS PARTES

En la sentencia bajo análisis, la empresa fundamenta su argumentación en los resultados del informe emitido por la Unidad Central Operativa (UCO) de la Guardia Civil, relativo a la existencia y efectos del virus sufrido, sosteniendo que dicho ataque constituye una causa que impidió el normal desarrollo de la actividad laboral de los trabajadores, motivo por el cual se solicitó la suspensión de sus contratos. En consecuencia, la empresa considera probada la relación de causalidad entre el virus, el ataque sufrido, y las consecuencias derivadas. De la sentencia se desprende, además, que está pendiente una reclamación patrimonial contra el Estado debido a la denegación del reconocimiento de la fuerza mayor y los daños ocasionados como resultado de ello: los trabajadores no vieron suspendidos sus contratos, se les abonaron los salarios correspondientes y se efectuaron los pagos a la Seguridad Social. Asimismo, se argumenta que el silencio administrativo debería haber tenido efectos favorables en la solicitud de suspensión de los contratos laborales.

Por su parte, la Abogacía del Estado se opone, argumentando que la resolución impugnada fue dictada dentro del plazo legal y que, en todo caso, el silencio administrativo debe interpretarse de manera negativa. En cuanto al fondo del asunto, sostiene que no concurre la causa de fuerza mayor al tratarse de una empresa del sector de las telecomunicaciones, a la cual se le exige un grado especial de diligencia, y que la aparición del virus no determinó el cese de la actividad. El sindicato CGT se opuso a la demanda por las mismas razones, argumentando que el funcionamiento ordinario de la empresa no se vio afectado, que la ocurrencia de un ataque informático era previsible y que la empresa no actuó con la diligencia debida, ya que no contaba con copias de seguridad externas al entorno de red, lo que habría permitido mitigar las consecuencias del ataque.

3. EFECTOS DEL SILENCIO ADMINISTRATIVO

La cuestión nuclear a dirimir en este procedimiento radica en establecer si la solicitud de autorización de ERTE por causa de fuerza mayor presentada por la empresa recurrente se consideró aprobada automáticamente mediante silencio administrativo positivo, dado que la resolución de la Administración demandada fue emitida extemporáneamente, es decir, fuera del plazo legalmente establecido de 5 días. En el supuesto de que no se considere que la Resolución fue aprobada por silencio administrativo positivo y, en consecuencia, se dictamine desfavorable, es preciso evaluar la existencia de una causa justificada de fuerza mayor.

En lo que respecta a los plazos administrativos, la sentencia determina que no procede considerar que la Administración dictó su resolución extemporáneamente, descartando así la estimación por silencio positivo de la solicitud de ERE por fuerza mayor. La ampliación de plazos, regulada en el artículo 32 de la Ley 39/2025 de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, presenta un régimen jurídico diferenciado en función de si deriva o no de un incidente técnico. En el caso de incidencias técnicas, el artículo 32.4 establece requisitos específicos de publicación en la sede electrónica, tanto de la incidencia como de la ampliación concreta del plazo no vencido, manteniéndose la ampliación hasta la resolución del problema técnico. La exhaustividad en el proceso de notificación refleja el compromiso de la organización con la transparencia y la gestión proactiva de las relaciones con los clientes en situaciones de contingencia, así como su adherencia a las mejores prácticas en materia de gestión de incidentes de seguridad de la información.

Tras un análisis exhaustivo de los hechos y evidencias presentados, se corrobora la ocurrencia de un evento exógeno a la entidad, de naturaleza inevitable, que efectivamente obstaculizó el desarrollo normal de las actividades laborales.

En consecuencia, se procede a la estimación parcial del recurso interpuesto, determinando la inexistencia de silencio administrativo positivo en el presente caso.

En lo que respecta al fondo del asunto, se ratifica la resolución inicial que reconoció la concurrencia de circunstancias constitutivas de fuerza mayor. Esta determinación se fundamenta en la evaluación pormenorizada de los elementos fácticos y jurídicos pertinentes, considerando la naturaleza y el impacto del incidente en cuestión sobre las operaciones de la entidad y su capacidad para mantener la continuidad en la prestación de servicios.

La Sala de lo Social de la Audiencia Nacional emitió un fallo favorable a Ilunion, fundamentado en la documentación aportada por la empresa y en el análisis forense realizado por Deloitte, que confirmaron la autenticidad del ciberataque y la subsiguiente recuperación gradual de los sistemas afectados. La presente resolución se emite en consonancia con la normativa aplicable y la jurisprudencia vigente en materia de fuerza mayor en el ámbito laboral, atendiendo a los criterios de excepcionalidad, imprevisibilidad y carácter externo del evento disruptivo.

En el proceso de impugnación de actos administrativos de naturaleza laboral seguido bajo el número 13/2022, a instancia de la empresa, en el que se estima la demanda se consideró la existencia de silencio administrativo positivo en relación a la solicitud de declaración de fuerza mayor formulada por la empresa tras sufrir un ciberataque, ya que aunque pudo ser anticipado, resultó inevitable, insuperable e irresistible, siempre y a su vez la causa que lo generó fue ajena y no dependió de la voluntad de la persona obligada, en este caso la propia empresa, tratándose de un evento externo al ámbito de la misma y totalmente independiente de la voluntad del empresario, cumpliendo por ende, con los criterios establecidos por la jurisprudencia para considerarlo un caso de fuerza mayor.

4. EXPANSIÓN DEL CONCEPTO DE FUERZA MAYOR

El Estatuto de los Trabajadores menciona la fuerza mayor como una de las causas que justifican la suspensión del contrato de trabajo (véase los artículos 45.1.i y 47.3) y también como motivo para su extinción (artículos 49.1.h. y 51.7 ET). No obstante, ninguno de estos artículos define específicamente el concepto de fuerza mayor. Solo se mencionan los requisitos necesarios para aplicar estas medidas laborales: debe tratarse de un evento "temporal" para permitir la suspensión del contrato o la reducción de la jornada laboral mientras que, para justificar la extinción del contrato, debe imposibilitar "definitivamente la prestación de trabajo"[7].

Para comprender el concepto, es necesario recurrir a normas generales, en particular al artículo 1105 del Código Civil. Aunque este artículo no ofrece una lista cerrada de eventos que constituyen fuerza mayor, sí establece los criterios que un evento debe cumplir para ser considerado como tal. El precepto, que regula la responsabilidad derivada del incumplimiento de obligaciones, establece que "nadie será responsable de aquellos eventos que no hubieran podido preverse, o que, previstos, fueran inevitables".

Con base en estos criterios generales, otro pasaje del Código Civil enumera eventos que cumplen con estas características. El segundo párrafo del artículo 1575, por ejemplo, menciona "casos fortuitos extraordinarios" que permiten reducir la obligación de pago de la renta en un contrato de arrendamiento rústico, como incendio, guerra, peste, inundación inusual, plaga de langosta, terremoto u otro evento igualmente inusual y que no hayan podido ser razonablemente previstos por los contratantes.

[7] Solà Monells, X.: "Suspensión del contrato o reducción de jornada" en AA.VV.: *Comentario al Estatuto de los Trabajadores*, Madrid, Ed. La Ley, 2013, págs. 5 y 10.

En otras áreas del ordenamiento jurídico, también existen listas de eventos que constituyen fuerza mayor. Un ejemplo es el artículo 239.2 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, que incluye eventos como incendios causados por electricidad atmosférica, fenómenos naturales catastróficos como maremotos, terremotos, erupciones volcánicas, movimientos del terreno, temporales marítimos, inundaciones, y destrozos causados por guerra, robos tumultuosos o alteraciones graves del orden público.

Por último, una norma histórica en el ámbito laboral, la ya derogada Ley de Contrato de Trabajo, contenía una lista similar en la regla sexta del artículo 76. Aunque derogada, esta norma aún es citada por la jurisprudencia y la doctrina judicial en la resolución de conflictos (por ejemplo, STS de 8 de julio de 2008, rec. 1857/2007). Según esta regla, se consideraba causa de extinción del contrato la "fuerza mayor que imposibilite el trabajo por causas como incendio, inundación, terremoto, explosión, plagas, guerra, tumultos o sediciones, y, en general, cualquier otro evento de carácter extraordinario que los contratantes no hubieran podido prever o que, previsto, no haya podido ser evitado".

A partir de estos fundamentos normativos y la experiencia acumulada en la jurisprudencia, se puede afirmar que el concepto de fuerza mayor es amplio y flexible. Los eventos catastróficos comúnmente enumerados en las disposiciones legales no agotan su definición, ya que es posible incluir otros casos de similar relevancia. Esta flexibilidad se observa claramente en los repertorios jurisprudenciales, que abarcan no solo litigios relacionados con fenómenos naturales, como lluvias intensas (por ejemplo, SSTSJ Castilla-León [Valladolid] cont. 704/2006, de 3 de abril; Extremadura cont. 48/2013, de 22 de enero), nevadas (STS de 23 de mayo de 2006, rec. 78/2005), o incendios (STS cont. 27 de febrero de 2008, rec. 105/2005), sino también circunstancias derivadas de decisiones humanas o de organizaciones. Esto se refiere a la denominada fuerza mayor "impropia", que incluye "hechos imposibilitantes no catastróficos" (como en la STSJ Andalucía (Málaga) 414/2002, de 1 de marzo), los cuales resultan de decisiones adoptadas por un tercero ajeno a la relación laboral[8].

Más que identificar los casos específicos de fuerza mayor, lo fundamental es determinar las características necesarias para que un evento sea considerado como tal[9]. En este sentido, se pueden hacer tres consideraciones clave.

Primero, no es imprescindible que un evento afecte directamente a una empresa para que se considere fuerza mayor. El evento puede impactar en su entorno, generando así la imposibilidad de continuar con sus operaciones[10]. Por ejemplo, aunque la organización no sufra daños directos debido a un desastre natural, es posible que este impida el acceso de los trabajadores o interrumpa el suministro de energía o materias primas esenciales para la producción. En estos casos, también se puede reconocer la existencia de fuerza mayor, como se ha señalado en pronunciamientos judiciales sobre nevadas (STS de 23 de mayo de 2006, rec. 78/2005) o lluvias torrenciales (SSTSJ Castilla-León [Valladolid] cont. 704/2006, de 3 de abril; Extremadura cont. 48/2013, de 22 de enero).

[8] Fernández Domínguez, J. J.: *La fuerza mayor como causa de extinción y suspensión del contrato de trabajo*, Madrid: Civitas, pág. 132.

[9] Blasco Pellicer. Á.: *Los expedientes de regulación de empleo,* Valencia, Tirant lo Blanch, 2009, pág.17.

[10] Esteban Gómez, A.: *Expediente de regulación temporal de empleo: instrumento recurrente ante la COVID-19,* 1ª edic., Albacete, Ed. Bomarzo, 2021.

En segundo lugar, la consideración de un evento como fuerza mayor no se basa únicamente en su existencia. También es crucial que el empresario haya actuado con diligencia en su previsión[11]. Un evento, por extraordinario que sea, no adquiere relevancia si no se han tomado las precauciones razonables para preverlo[12]. Como establece la STS de 8 de julio de 2008, rec. 1857/2007, basándose en la doctrina de la Sala de lo Civil, la fuerza mayor se define como "una fuerza superior a todo control y previsión, ponderándose a efectos de su concurrencia la previsión normal y razonable que las circunstancias exijan en cada caso concreto". Por tanto, no es suficiente que el evento sea externo a la voluntad del empresario; también debe considerarse su carácter previsible y evitable.

El Tribunal Supremo, en su argumentación jurídica, estableció una distinción crítica entre la previsibilidad genérica de los incidentes de ciberseguridad y su inevitabilidad en contextos específicos. El órgano jurisdiccional enfatizó que, no obstante la anticipación teórica de la posibilidad de ciberataques en el paradigma empresarial contemporáneo, la materialización de amenazas cibernéticas específicas puede, bajo determinadas circunstancias, revestir características de inevitabilidad que justifican la aplicación del concepto jurídico de fuerza mayor.

Esta interpretación jurisprudencial reconoce la complejidad y la naturaleza evolutiva de las amenazas cibernéticas, estableciendo un equilibrio entre la expectativa de diligencia preventiva por parte de las entidades empresariales y el reconocimiento de la sofisticación y persistencia de ciertos vectores de ataque que pueden superar incluso las medidas de seguridad más robustas.

El Tribunal subraya que la mera previsibilidad abstracta de un riesgo cibernético no excluye automáticamente la posibilidad de que su materialización constituya un caso de fuerza mayor. Se establece así un criterio que requiere una evaluación casuística de la inevitabilidad del incidente específico, considerando factores como la naturaleza del ataque, la adecuación de las medidas de seguridad implementadas y la capacidad real de la entidad para prevenir o mitigar el impacto del incidente.

Esta postura jurisprudencial refleja una adaptación del concepto tradicional de fuerza mayor a las realidades del entorno digital, reconociendo que ciertos incidentes de ciberseguridad pueden, por su naturaleza y circunstancias, trascender el ámbito de lo prevenible y controlable por parte de una organización, aun cuando esta haya implementado medidas de seguridad acordes con los estándares de la industria.

El órgano jurisdiccional subraya que la conceptualización jurídica de fuerza mayor no se circunscribe de manera exclusiva a fenómenos de origen natural, tales como conflagraciones fortuitas o eventos sísmicos. En el contexto de una sociedad caracterizada por un alto grado de desarrollo tecnológico, se reconoce que ciertos acontecimientos, aun siendo producto de la intervención humana, pueden satisfacer los criterios jurídicos establecidos para la calificación de fuerza mayor.

Esta interpretación expansiva del concepto de fuerza mayor se fundamenta en la evolución del entorno socioeconómico y tecnológico, donde la complejidad de los sistemas y la interconexión digital generan nuevas formas de vulnerabilidad. En consecuencia, el Tribunal adopta una postura que reconoce la posibilidad de que eventos antropogénicos, particularmente aquellos relacionados con la ciberseguridad, puedan cumplir con los requisitos de externalidad, imprevisibilidad e inevitabilidad

[11] Roqueta Buj, R.: *Los Expedientes de Regulación Temporal del Empleo*, 2ª edición, Valencia, Tirant Lo Blanch, 2021, pág. 42.

[12] Molina Navarrete, C.: *La reestructuración empresarial mediante regulación de empleo: Nuevas normas y prácticas sobre ERTE y despidos colectivos*, Madrid, La Ley, 2024.

característicos de la fuerza mayor, pues el artículo 1105 del Código Civil al definir qué se entiende por esta no exige que sea un suceso natural sino que puede ser provocado también por la acción humana.

Esta ampliación del alcance conceptual de la fuerza mayor refleja una adaptación del marco jurídico a las realidades emergentes de la era digital, permitiendo una consideración más comprehensiva de los factores que pueden afectar la operatividad empresarial en un entorno tecnológicamente avanzado. Dejando patente una vez más que el evento causal puede ser de origen antropogénico, tomando en consideración el paradigma tecnológico contemporáneo en el que los incidentes pueden ser el resultado de intervenciones humanas deliberadas o inadvertidas. Este contexto sociotecnológico actual propicia la existencia de vectores de amenaza que emanan de la interacción entre agentes humanos y sistemas informáticos complejos, dando lugar a fenómenos disruptivos que, aunque originados en la esfera de la actividad humana, pueden manifestar características análogas a los eventos de fuerza mayor tradicionalmente reconocidos en el ámbito jurídico.

La conceptualización expandida de fuerza mayor en este escenario tecnológico reconoce la capacidad de las acciones humanas, especialmente en el dominio cibernético, de generar consecuencias que trascienden los límites de previsibilidad y control ordinarios, equiparándose así a los fenómenos naturales en su potencial de crear circunstancias extraordinarias e inevitables desde la perspectiva de la entidad afectada.

El Tribunal Supremo ratifica la resolución de la Audiencia Nacional al reconocer explícitamente la concurrencia de una situación de fuerza mayor, lo que faculta a la empresa para implementar las medidas de suspensión previstas en el artículo 47 del Estatuto de los Trabajadores en relación con los empleados afectados.

5. LA DILIGENCIA EMPRESARIAL FRENTE A LAS AMENAZAS CIBERNETICAS

En el fundamento jurídico sexto, la sentencia se refiere a la evitabilidad o inevitabilidad de un suceso, y, de manera similar a lo que ocurre con los accidentes laborales, no impone la obligación de lograr siempre un resultado exitoso, sino que exige que se hayan adoptado todas las medidas preventivas disponibles para neutralizarlo. En este caso, la prueba presentada demuestra que ILUNION disponía de diversos medios para enfrentar estos ataques, dentro de lo razonablemente posible y de acuerdo con los conocimientos técnicos estandarizados. Específicamente, en el resultado probado noveno, se indica que la empresa tenía implementado un Sistema de Gestión de Seguridad de la Información (SGSI), certificado por la norma ISO/IEC 27001, emitida por AENOR, y renovada anualmente mediante auditorías. Además, la empresa cuenta con una serie de políticas, normas y procedimientos de seguridad que, en caso de un ciberataque, establecen directrices para actuar de manera segura y proteger la información. Entre estas medidas, se incluye una Política de Seguridad (PO01), de la cual derivan normas que cubren todos los aspectos desarrollados en la ISO 27002. Se acreditó la implementación de controles rigurosos que regulan la seguridad operativa de los sistemas de información, los cuales incluyen las siguientes medidas:

— Asignación nominativa de cuentas de usuario, con la exigencia de contraseñas robustas.

— Revisión periódica de los permisos y privilegios asignados a los usuarios.

— Segmentación de redes para la separación de servicios diferenciados.

— Gestión de conexiones remotas a través de métodos seguros.

— Implementación de un programa antivirus actualizado en todos los equipos, con gestión centralizada.

— Realización periódica de copias de seguridad, con almacenamiento en ubicaciones seguras.

Además, la empresa contaba con un servicio de seguridad informática mediante cortafuegos, un manual específico de respuesta técnica frente a ciberataques de tipo *ransomware* y un protocolo para la gestión de incidentes de seguridad informática.

Por lo que adoptó en todo momento medidas proactivas para mitigar el impacto del ataque, además de una póliza con AIG Europe. Dichas medidas ponen de manifiesto que la empresa actuó con rigurosa diligencia para contener y solucionar el incidente acontecido. Todo ello constituye una causa de fuerza mayor que el Tribunal Supremo ha destacado, ya que el ciberataque, a pesar de no ser absolutamente imprevisible, si resultó inevitable pese a las robustas medidas de seguridad ya mencionadas implementadas por la empresa, cumpliendo con todos los estándares de seguridad razonables y legales.

Se ha constatado documentalmente que se procedió a la desactivación integral del CPD y a la subsecuente desconexión de los enlaces de telecomunicaciones con la totalidad de las sedes operativas del Contact Center. Estas medidas se implementaron con el objetivo de mitigar la propagación del software malicioso, en concomitancia con la ejecución de un análisis forense digital exhaustivo del incidente de seguridad detectado.

La implementación de estas medidas de contención y mitigación subraya la criticidad del incidente y la imperativa necesidad de preservar la integridad de la infraestructura tecnológica organizacional. La ejecución de tales protocolos de contingencia corrobora la severidad del impacto operativo y proporciona una justificación técnica para la subsiguiente inactividad laboral, fundamentada en la imposibilidad material de acceso a los sistemas y herramientas esenciales para la ejecución de las funciones laborales habituales.

En consecuencia de las medidas implementadas, se produjo una cesación total del tráfico de datos saliente desde la infraestructura de la organización hacia servicios externos, dado que la red se encontraba en un estado de aislamiento completo. Se procedió a la emisión de notificaciones formales a la cartera de clientes, informándoles sobre el incidente de ciberseguridad acaecido y la subsecuente imposibilidad de mantener la prestación de servicios.

Se constata que se efectuaron un total de 131 comunicaciones oficiales dirigidas a los clientes, detallando la interrupción de los servicios como consecuencia directa del mencionado incidente de ciberseguridad. Estas comunicaciones se llevaron a cabo siguiendo los protocolos establecidos para la gestión de crisis y en cumplimiento de las obligaciones contractuales y legales pertinentes.

El órgano jurisdiccional, en su fundamentación jurídica, estableció una distinción crítica entre la mera disponibilidad laboral del personal y su capacidad operativa efectiva en un contexto de compromiso de la infraestructura tecnológica crítica. En el caso sub judice, la infraestructura de sistemas de información, considerada esencial para la ejecución de las funciones operativas del personal, se vio comprometida de manera sustancial, lo que derivó en una imposibilidad material de facto para la realización de las tareas laborales asignadas.

Esta argumentación jurídica subraya la interdependencia inherente entre la funcionalidad de los sistemas informáticos y la capacidad del personal para desempeñar sus responsabilidades

laborales en un entorno altamente digitalizado. La Sala enfatiza que la mera presencia o disposición del trabajador no constituye per se una condición suficiente para la prestación efectiva de servicios cuando los medios tecnológicos indispensables para dicha prestación se encuentran inoperativos o comprometidos.

La resolución judicial pone de manifiesto la necesidad de considerar la integridad y operatividad de los sistemas de información como un elemento sine qua non para la evaluación de la capacidad real de prestación de servicios en entornos laborales caracterizados por una alta dependencia tecnológica. Este criterio jurisprudencial establece un precedente significativo en la interpretación de las condiciones que configuran una imposibilidad material de ejecución de las obligaciones laborales en el contexto de incidentes de ciberseguridad..

El Tribunal Supremo reconoció que Ilunion actuó con la diligencia debida en las fases previa, concomitante y posterior al incidente de ciberseguridad, implementando de manera exhaustiva las medidas preventivas y correctivas a su disposición. Se enfatizó la ausencia de negligencia por parte de la entidad y se destacó que las acciones adoptadas contribuyeron significativamente a la mitigación de los impactos derivados del incidente.

Por ende, se consideró que la inoperatividad de los sistemas críticos constituye un impedimento sustancial para la prestación de servicios en un entorno altamente dependiente de la tecnología. Esta consideración se fundamenta en la relación causal directa entre la disponibilidad de los sistemas de información y la capacidad operativa del personal en el desempeño de sus funciones laborales específicas.

Asimismo, se valoró positivamente la gestión proactiva del incidente por parte de Ilunion, reconociendo la implementación de medidas de seguridad acordes con los estándares de la industria y la respuesta ágil y efectiva ante la materialización del riesgo cibernético.

La sentencia aborda los argumentos de la representación sindical (CGT), que sostenía que el suceso podría haberse evitado mediante la implementación de una copia de seguridad o un CPD secundario. Sin embargo, la Sala concluye que, según consta probado, el *ransomware* es un software malicioso capaz de infectar equipos o redes, cifrando la información, con métodos de infiltración diversos, siendo el phishing el más común, lo que implica la potencial infección a través de los dispositivos de los propias personas trabajadoras.

6. IMPOSIBILIDAD MATERIAL DE DESEMPEÑAR LAS TAREAS LABORALES EN CONTEXTOS ALTAMENTE TECNIFICADOS

La Sala, en su argumentación jurídica, estableció una distinción crucial entre la mera disponibilidad laboral del personal y la capacidad efectiva de ejecutar las funciones asignadas en un contexto de compromiso de los sistemas críticos. En el caso sub judice, la infraestructura informática esencial para la operatividad del personal se vio comprometida, lo que resultó en una imposibilidad material de llevar a cabo las tareas laborales encomendadas.

El Tribunal Supremo, en su análisis, reconoció la diligencia demostrada por Ilunion en las fases previa, concomitante y posterior al incidente de ciberseguridad, constatando la implementación exhaustiva de medidas preventivas y reactivas acordes con los estándares de seguridad vigentes. Se enfatizó la ausencia de negligencia por parte de la entidad y se valoró positivamente que las acciones adoptadas contribuyeron de manera significativa a la mitigación de los impactos derivados del incidente.

La Sala consideró que la inoperatividad de los sistemas críticos constituye un impedimento sustancial para la prestación de servicios en un entorno altamente dependiente de la tecnología. Esta consideración se fundamenta en la relación causal directa entre la disponibilidad de los sistemas de información y la capacidad operativa del personal en el desempeño de sus funciones laborales específicas.

El órgano jurisdiccional evaluó de manera favorable la gestión proactiva del incidente de ciberseguridad por parte de Ilunion, reconociendo la implementación de un marco de controles de seguridad alineado con los estándares y mejores prácticas reconocidos en la industria. Se destacó particularmente la respuesta ágil y eficaz de la entidad ante la materialización del vector de amenaza cibernética. La actuación diligente de Ilunion en materia de ciberseguridad, tanto en sus aspectos preventivos como reactivos, fue considerada por el Tribunal como un factor mitigante significativo en la evaluación de la responsabilidad corporativa frente al incidente y sus subsecuentes implicaciones en el ámbito laboral, siendo valorada positivamente la adopción de medidas de seguridad que, si bien no lograron prevenir completamente el incidente, demostraron un nivel de preparación y resiliencia organizacional conforme a los estándares de diligencia debida en el contexto de la ciberseguridad empresarial contemporánea.

7. DOCTRINA FIJADA POR EL ALTO TRIBUNAL

Esta valoración jurisprudencial establece un precedente relevante en la consideración de la diligencia empresarial como factor atenuante en casos de fuerza mayor derivados de incidentes de ciberseguridad. Subraya la importancia de la implementación proactiva de medidas de seguridad y de la capacidad de respuesta organizacional como elementos clave en la evaluación de la responsabilidad corporativa en el contexto de amenazas cibernéticas cada vez más sofisticadas y persistentes.

La decisión del Tribunal refleja un enfoque equilibrado que reconoce la complejidad y la naturaleza evolutiva de las amenazas cibernéticas, al tiempo que establece un estándar de diligencia razonable para las entidades empresariales en la protección de sus activos digitales y en la mitigación de los impactos laborales derivados de incidentes de esta naturaleza. La distinción fundamental entre una causa de fuerza mayor y una causa ETOP no radica en la etiología natural de la primera y humana de la segunda, sino en la externalidad y carácter extraordinario de la fuerza mayor, contrapuesta a la naturaleza ordinaria y voluntaria de las causas ETOP.

Se establece que la previsibilidad de un ciberataque en la actividad ordinaria de una empresa no excluye la posibilidad de que ciertos incidentes de esta naturaleza excedan los parámetros contemplados en el desarrollo normal de la actividad empresarial, resultando inevitables. En tales casos, si el evento inevitable supera lo previsto en el curso ordinario de la vida empresarial, se configura un supuesto de fuerza mayor.

La diferenciación jurídica fundamental entre los conceptos de fuerza mayor y causas técnicas reside en sus características intrínsecas y su etiología. La fuerza mayor se distingue por su carácter exógeno y su naturaleza extraordinaria, constituyendo un evento que excede los parámetros de previsibilidad y control ordinarios de la entidad afectada.

La fuerza mayor, en su concepción jurídica, implica una ruptura del nexo causal entre la voluntad del agente y el resultado producido, caracterizándose por su inevitabilidad incluso ante la aplicación de la máxima diligencia exigible. Por el contrario, las causas técnicas se insertan en el espectro de contingencias previsibles y gestionables dentro del marco de la actividad empresarial regular, estando sujetas a un mayor grado de control y previsión por parte de la entidad. En contraposición, las causas

técnicas se enmarcan dentro del ámbito de la gestión interna y operativa habitual de la organización, siendo consideradas de índole endógena y susceptibles de control o mitigación a través de medidas organizativas o tecnológicas implementadas por la propia entidad. El Tribunal Supremo desestima los argumentos esgrimidos por la representación sindical, que propugnaban la calificación del ERTE exclusivamente por causas ETOP, específicamente de índole técnica o productiva, en detrimento de la consideración de fuerza mayor. Esta desestimación se fundamenta en la premisa de que la previsibilidad de un evento no es óbice para su inevitabilidad. En el caso sub judice, se constata que el Ministerio de Trabajo y Economía Social fue el objeto directo del incidente de ciberseguridad en un servicio gestionado por Ilunion Contact Center.

La ponente, la Excma. Sra. Magistrada Dña. María Luz García Paredes, realiza un análisis jurisprudencial exhaustivo, haciendo especial énfasis en la sentencia del propio Tribunal de 22 de septiembre (Recurso de Casación 75/2021), que establece: "Con carácter general, el concepto de fuerza mayor debe ser entendido como un acontecimiento externo al círculo de la empresa y del todo independiente de la voluntad del empresario, que, a su vez, sea imprevisible". Adicionalmente, se hace referencia a la sentencia de 25 de julio de 1989, que subraya: "sobre todo, se trate de un acontecimiento no definitivo o sin vocación de permanencia que conlleve una simple imposibilidad temporal de que la prestación laboral se lleve a cabo".

Con todo ello, la doctrina jurisprudencial consolida la conceptualización de la fuerza mayor como una imposibilidad temporal y sobrevenida de la prestación de servicios, caracterizada por su externalidad respecto al ámbito de control empresarial y por la ausencia de imputabilidad o atribución al empleador. Esta interpretación jurídica refuerza la aplicabilidad del concepto de fuerza mayor en el contexto de incidentes de ciberseguridad que afectan la operatividad empresarial, siempre que se cumplan los criterios de externalidad, imprevisibilidad e inevitabilidad establecidos por la jurisprudencia. La magistrada ponente hace referencia a la jurisprudencia previa del Tribunal Supremo, citando específicamente la sentencia de la Sala de 22 de julio de 2015 (Recurso: 4/2012), que establece los criterios definitorios de fuerza mayor y "situación extraordinaria". Estos se caracterizan por ser acontecimientos exógenos al ámbito empresarial, absolutamente independientes de la voluntad de la entidad, que sean imprevisibles o, aun siendo previsibles, resulten inevitables.

La Sala sintetiza los criterios jurisprudenciales, definiendo la fuerza mayor como aquellos hechos que, aun siendo previsibles, resultan inevitables, insuperables e irresistibles, siempre que su causa sea independiente y ajena a la voluntad del sujeto obligado. Se alude a estos eventos como "sucesos imprevistos e inevitables que rebasan los tenidos en cuenta en el curso normal de la vida y extraños al desenvolvimiento ordinario de un proceso industrial". En el caso sub judice, la ponente evalúa que, en el ámbito de lo inevitable, los hechos probados demuestran que la empresa había previsto la posibilidad de un ciberataque, implementando medidas de seguridad consideradas necesarias y suficientes para su prevención. No obstante, el ataque no pudo ser evitado, como lo corrobora el informe técnico aportado.

Se establece una diferenciación jurídica de carácter fundamental entre la mera disponibilidad laboral y la ejecución efectiva de las obligaciones contractuales. El núcleo del análisis jurisprudencial se focaliza en la imposibilidad material de llevar a cabo las funciones laborales, en contraposición a la mera disposición volitiva de las personas trabajadoras para ejecutarlas. Esta distinción reviste una importancia capital en la conceptualización y calificación jurídica del tiempo de trabajo.

La imposibilidad material de desempeñar las tareas asignadas, aun existiendo voluntad y disponibilidad por parte del trabajador, plantea interrogantes complejos en el ámbito del Derecho Laboral. Estas cuestiones se centran principalmente en la determinación de si dicho período debe ser

considerado como tiempo efectivo de trabajo y, consecuentemente, en las implicaciones retributivas que de ello se derivan.

Es imperativo subrayar que esta problemática es ontológicamente distinta de la evaluación de la capacidad efectiva de trabajo. Mientras que la capacidad efectiva se refiere a la aptitud del trabajador para desempeñar sus funciones en condiciones normales, la situación analizada aborda un escenario en el que, existiendo dicha capacidad, factores exógenos impiden su materialización.

Esta disyuntiva jurídica pone de manifiesto la necesidad de una revisión y posible adaptación de los marcos normativos laborales para abordar adecuadamente las situaciones emergentes en entornos laborales altamente tecnificados. La interpretación de estos casos requiere un equilibrio delicado entre la protección de los derechos de las personas trabajadoras y el reconocimiento de las limitaciones operativas que pueden afectar a las empresas en situaciones de fuerza mayor, como los incidentes de ciberseguridad de gran envergadura.

La resolución de esta cuestión tendrá implicaciones significativas no solo en el ámbito de la remuneración, sino también en la configuración de las políticas de gestión de recursos humanos, la planificación de la continuidad del negocio y la implementación de medidas de contingencia ante disrupciones tecnológicas.

La plantilla total de la empresa comprende 2.158 empleados, cifra que excede considerablemente el total de equipos afectados, que es de 1.200. El número de personas trabajadoras contabilizados por la empresa dentro del ERTE por causa de fuerza mayor fue inferior al de equipos afectados, concretamente 1.192 empleados. Esto implica que la afectación fue parcial y no total, permitiendo que algunas personas trabajadoras continuaran prestando servicios, según consta en el Informe de la Inspección de Trabajo y Seguridad Social (ITSS).

Se puede establecer una categorización dicotómica del personal en función de su operatividad durante el período en cuestión:

1. Personas trabajadoras en situación de disponibilidad laboral sin capacidad efectiva de prestación de servicios.

2. Personas trabajadoras que mantuvieron la continuidad en la prestación de servicios a pesar de las circunstancias adversas.

Esta diferenciación se corrobora mediante las declaraciones obtenidas en el proceso de investigación llevado a cabo por la Inspección de Trabajo y Seguridad Social. Específicamente, dos trabajadoras entrevistadas manifestaron lo siguiente:

De acuerdo con las declaraciones formuladas por los representantes sindicales, se constata que, a pesar de la imposibilidad material de ejecutar las funciones laborales bajo parámetros de normalidad operativa, no se produjo una interrupción absoluta en la prestación de servicios laborales desde una perspectiva formal. El capital humano de la entidad mantuvo un estado de disponibilidad laboral continua hacia la organización empleadora, llevando a cabo el registro telemático de su jornada laboral mediante la utilización de la plataforma de colaboración digital Teams, tanto en el momento de inicio como en el de finalización de la misma.

Esta situación plantea una dicotomía jurídico-laboral entre la disponibilidad formal del personal y la imposibilidad técnica de desempeñar las funciones asignadas de manera efectiva. El mantenimiento

del registro de jornada en estas circunstancias excepcionales suscita cuestiones complejas en torno a la conceptualización del tiempo de trabajo efectivo y la remuneración correspondiente en un contexto de inoperatividad de los sistemas críticos.

La continuidad en el cumplimiento de las obligaciones formales por parte del personal, como el registro de jornada, en un escenario de disrupción operativa, pone de manifiesto la necesidad de una revisión de los protocolos laborales y de las definiciones legales de prestación de servicios en entornos altamente digitalizados. Este fenómeno evidencia la complejidad de las relaciones laborales contemporáneas, donde la presencia virtual y la disponibilidad tecnológica pueden disociarse de la capacidad real de ejecución de las tareas laborales debido a factores exógenos como los incidentes de ciberseguridad.

8. LAGUNAS LEGALES: PROPUESTAS DE REGULACIÓN TRAS LAS ENSEÑANZAS DEL TRIBUNAL SUPREMO

La situación descrita plantea desafíos significativos en la interpretación y aplicación del derecho laboral, requiriendo una adaptación de los marcos normativos para abordar adecuadamente las nuevas realidades del trabajo en la era digital, especialmente en circunstancias excepcionales donde la infraestructura tecnológica se ve comprometida. En una evaluación holística de la situación, no es posible sostener, como postula la Confederación General del Trabajo (CGT), que la totalidad del personal mantuvo una continuidad operativa sin alteraciones. La evidencia empírica sugiere que, si bien un segmento del personal logró mantener su operatividad, la mayoría se encontraba en un estado de disponibilidad para la entidad empleadora. Es pertinente señalar que la cuantía de empleados incluidos en el ERTE fue inferior a la totalidad de los equipos afectados y significativamente menor en relación con el cómputo global de la plantilla de la entidad.

La evidencia factual corrobora que el día 4 de junio de 2021 se produjo una suspensión generalizada de los servicios proporcionados a la cartera de clientes, lo cual derivó en la inoperatividad del personal adscrito a dichas campañas. Esta situación fue consecuencia directa de la imposibilidad de acceder y utilizar las herramientas informáticas fundamentales para el desarrollo de las operaciones, las cuales se vieron específicamente comprometidas por un incidente de ciberseguridad. Dicho incidente tuvo un impacto significativo, afectando a un total de 28 campañas destinadas a una diversidad de clientes.

El incidente de ciberseguridad, caracterizado por su magnitud y complejidad sin precedentes, provocó una disrupción crítica en la continuidad operativa de la entidad, generando un estado de inactividad laboral involuntaria que afectó a un segmento demográficamente relevante del capital humano. Esta coyuntura pone de manifiesto la vulnerabilidad endémica de las infraestructuras de tecnologías de la información y comunicación (TIC), así como su función neurálgica en la orquestación de los procesos empresariales *core* y *non-core*[13].

La paralización de los sistemas informáticos críticos tuvo como consecuencia directa la imposibilidad material de ejecutar las funciones laborales asignadas, evidenciando la simbiosis inextricable entre la operatividad de los sistemas de información y la capacidad productiva del personal. Este evento disruptivo subraya la correlación causal entre la disponibilidad de los activos digitales y la viabilidad de la prestación de servicios en un entorno laboral altamente digitalizado[14].

[13] Calcara, A.; y Marchetti, R., "State-industry relations and cybersecurity governance in Europe", *Review of International Political Economy*, 2021, págs. 1-26.

[14] Fernández Bermejo, D. y Martínez Atienza, G.: *Ciberseguridad, ciberespacio y ciberdelincuencia*, Cizur Menor, Aranzadi Thomson Reuters, 2018.

Las ramificaciones de este incidente en el ámbito laboral son multidimensionales, abarcando aspectos contractuales, organizativos y de productividad. La situación generada plantea interrogantes jurídicos y operativos sobre la conceptualización del tiempo de trabajo efectivo en condiciones de indisponibilidad tecnológica, así como sobre las medidas de contingencia y los protocolos de respuesta ante incidentes que las organizaciones deben implementar para mitigar los impactos laborales derivados de eventos de esta naturaleza.

Este escenario pone de relieve la necesidad imperativa de una reevaluación de los marcos normativos laborales y de ciberseguridad, con el fin de adaptarlos a las realidades emergentes de un ecosistema empresarial caracterizado por una creciente interdependencia tecnológica y una exposición constante a amenazas cibernéticas de complejidad evolutiva[15].

Es evidente que estas transformaciones en el ámbito digital requieren una revisión profunda del ordenamiento jurídico vigente. La rápida evolución de la tecnología y la creciente dependencia de los sistemas digitales exigen que las normativas laborales se actualicen para contemplar nuevas formas de trabajo y los riesgos asociados, como la ciberseguridad, la privacidad de los datos y la flexibilidad laboral[16]. Además, la introducción de reformas legales debe garantizar un equilibrio entre la protección de los derechos de los trabajadores y la capacidad de las empresas para implementar estrategias que aseguren su viabilidad operativa en un entorno digital cada vez más desafiante.

En este contexto, la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2)[17], conocida como Directiva NIS2 (Network and Information Security Directive), adoptada por la Unión Europea, adquiere una relevancia crucial. Esta directiva busca fortalecer la ciberseguridad en los Estados miembros, imponiendo obligaciones más estrictas para la gestión de riesgos cibernéticos y la notificación de incidentes de seguridad. La NIS2 no solo actualiza la normativa para enfrentar las amenazas actuales, sino que también establece un marco más robusto para proteger las infraestructuras críticas y los servicios esenciales contra ciberataques, constituye por ende un avance crucial en la evolución del marco normativo europeo en materia de ciberseguridad. Esta nueva regulación, que reemplaza y expande el alcance de su predecesora, emerge como respuesta a un ecosistema de amenazas cibernéticas en constante evolución y creciente complejidad. NIS2 se erige con el propósito fundamental de robustecer la resiliencia y potenciar las capacidades de respuesta ante incidentes cibernéticos en todo el ámbito de la Unión Europea, estableciendo para ello un conjunto integral de medidas orientadas a garantizar un nivel común elevado de ciberseguridad en sectores críticos y servicios esenciales.

La directiva introduce cambios significativos, entre los que destaca la ampliación de su ámbito de aplicación, abarcando ahora un espectro más amplio de sectores y entidades consideradas críticas para la economía y la sociedad. Además, impone requisitos más estrictos en cuanto a la gestión de riesgos de ciberseguridad y las obligaciones de notificación de incidentes. NIS2 también busca armonizar los regímenes sancionadores entre los Estados miembros, asegurando así una aplicación más coherente y efectiva de la normativa. Asimismo, fomenta activamente la cooperación y el

[15] Gómez de Ágreda, Á.: "Ciberseguridad en un mundo hiperconectado" en *Ciberseguridad. Un nuevo reto para el Estado y los gobiernos locales*, Canals, D. (Ed.), Madrid, Wolters Kluwer, 2021, págs. 29-62.

[16] Aldana Montes, J. F., García Nieto, J. M., Gonzalvez, J. C. y Navas Delgado. I.: *Big data: seguridad y gobernanza,* Madrid, García Maroto Editores, 2018.

[17] Disponible en: https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=es Fecha de consulta: 29 de agosto de 2024.

intercambio de información entre los Estados miembros y las instituciones de la UE, e introduce medidas específicas para mejorar la supervisión y el cumplimiento normativo.

En esencia, la Directiva NIS2 representa un paso decisivo hacia la creación de un ecosistema digital más seguro y resiliente en Europa. Establece un marco común que aspira a elevar el nivel general de ciberseguridad y promueve una cultura de gestión de riesgos más robusta en todos los sectores críticos. Esta iniciativa legislativa refleja el compromiso de la Unión Europea con la adaptación continua a los desafíos cibernéticos emergentes y su determinación de fortalecer la postura de seguridad digital del continente en un contexto global cada vez más interconectado y vulnerable a las amenazas cibernéticas.

La vinculación de la Directiva NIS2 con la doctrina judicial emergente en relación a la ciberseguridad resalta la necesidad de que el ordenamiento jurídico incorpore principios y normas que aborden de manera integral las amenazas digitales. Al integrar los estándares de la NIS2 en las políticas laborales y de seguridad, se podría establecer una base doctrinal que permita a las organizaciones adoptar medidas proactivas y preventivas contra los ciberataques, garantizando tanto la continuidad operativa como la protección de los derechos laborales. Esto también implica que las reformas jurídicas deben alinearse con las disposiciones de la NIS2, promoviendo un entorno de colaboración entre los sectores público y privado para mitigar los riesgos cibernéticos y fortalecer la resiliencia de las infraestructuras críticas.

Por tanto, es fundamental que las reformas propuestas incluyan disposiciones que faciliten la adaptación de los contratos laborales a las dinámicas digitales, sin comprometer los estándares de seguridad laboral ni los derechos adquiridos[18]. Asimismo, se debe promover la formación continua en ciberseguridad y nuevas tecnologías, tanto para empleados como para empleadores, de modo que se minimicen los riesgos y se maximicen las oportunidades que ofrece la digitalización. En definitiva, el ordenamiento jurídico debe evolucionar de manera proactiva, anticipándose a los desafíos futuros y proporcionando un marco normativo que fomente la innovación, la competitividad y la protección integral en el contexto de la economía digital.

9. CONCLUSIONES

Los incidentes de ciberseguridad experimentan un incremento en su frecuencia e impacto, con la capacidad potencial de inducir una interrupción parcial o total de las operaciones de una entidad empresarial. La frecuencia, impacto y virulencia de los ciberataques en las empresas han generado escenarios, como el observado en los casos enjuiciados, que los han hecho previsibles y capaces de obstaculizar la capacidad de trabajar. Estos ataques afectan, por tanto, a los derechos fundamentales relacionados con el desempeño normal de las tareas laborales y la obligación de proporcionar dichas tareas. Esta situación requiere la intervención de la administración, en su rol de mitigación social de las suspensiones de contratos, con el fin de verificar la efectiva existencia de la causa suspensiva en la relación laboral.

El Tribunal Supremo, en la sentencia objeto de análisis, ha establecido un precedente legal significativo al dictaminar que, en circunstancias donde se pueda demostrar fehacientemente una paralización operativa, se considera jurídicamente válida la implementación de un ERTE fundamentado en la causa de fuerza mayor, específicamente cuando dicha paralización es consecuencia directa de un incidente de ciberseguridad. A su vez, ha sentado un precedente jurídico significativo al clasificar los ciberataques dentro de la categoría de eventos de fuerza mayor. Esta calificación está sujeta a la

[18] Terrón Santos, D. (Dir.) Y Domínguez Álvarez. J.L.: *Inteligencia artificial y defensa: nuevos horizontes*, Navarra, Aranzadi Thomson Reuters, 2021.

demostración fehaciente de la inevitabilidad del incidente y su impacto sustancial en la capacidad operativa de la entidad afectada. Es relevante destacar que esta doctrina se aplica con independencia de la previsibilidad del suceso o de su etiología, ya sea antropogénica o de origen natural.

Esta interpretación jurisprudencial reconoce la gravedad y el carácter extraordinario que pueden revestir los ciberataques en el contexto empresarial contemporáneo, equiparándolos a otros eventos tradicionalmente considerados como fuerza mayor. La sentencia del Alto Tribunal subraya la necesidad de evaluar cada caso de forma individual, atendiendo a la magnitud del impacto operativo y a la inevitabilidad del suceso, aun cuando se hayan implementado medidas de seguridad adecuadas.

Esta decisión judicial representa una adaptación del marco legal laboral a las realidades emergentes del entorno digital, reconociendo la vulnerabilidad inherente de las organizaciones ante amenazas cibernéticas sofisticadas y su potencial para generar disrupciones operativas significativas que justifiquen medidas laborales excepcionales. No obstante, es evidente que estas transformaciones en el ámbito digital requieren una revisión profunda del ordenamiento jurídico vigente. La rápida evolución de la tecnología y la creciente dependencia de los sistemas digitales exigen que las normativas laborales se actualicen para contemplar nuevas formas de trabajo y los riesgos asociados, como la ciberseguridad, la privacidad de los datos y la flexibilidad laboral. Además, la introducción de reformas legales debe garantizar un equilibrio entre la protección de los derechos de los trabajadores y la capacidad de las empresas para implementar estrategias que aseguren su viabilidad operativa en un entorno digital cada vez más desafiante.

Por tanto, es fundamental que las reformas propuestas incluyan disposiciones que faciliten la adaptación de los contratos laborales a las dinámicas digitales, sin comprometer los estándares de seguridad laboral ni los derechos adquiridos. Asimismo, se debe promover la formación continua en ciberseguridad y nuevas tecnologías, tanto para empleados como para empleadores, de modo que se minimicen los riesgos y se maximicen las oportunidades que ofrece la digitalización. En definitiva, el ordenamiento jurídico debe evolucionar de manera proactiva, anticipándose a los desafíos futuros y proporcionando un marco normativo que fomente la innovación, la competitividad y la protección integral en el contexto de la economía digital.

Desde mi punto de vista personal, esta decisión jurisprudencial y las propuestas de adaptación del marco legal son pasos fundamentales, pero también plantean desafíos significativos. La equiparación de los ciberataques con eventos de fuerza mayor es un reconocimiento necesario de la realidad digital actual, pero también abre la puerta a posibles abusos por parte de empresas que podrían utilizar esta justificación para implementar medidas laborales desfavorables para los trabajadores.

Considero que es crucial mantener un equilibrio delicado entre la protección de los intereses empresariales y los derechos de los trabajadores. La formación continua en ciberseguridad es esencial, pero debe ir acompañada de una responsabilidad compartida entre empleadores y empleados. Las empresas no deberían poder eludir su responsabilidad en la protección de sus sistemas simplemente alegando la sofisticación de los ataques.

Además, creo que es fundamental que en la elaboración de estas nuevas normativas se incluya la voz de los trabajadores y sus representantes sindicales. La digitalización y la ciberseguridad no pueden ser excusas para precarizar las condiciones laborales o para justificar despidos masivos sin una justificación sólida.

Por último, opino que esta evolución del derecho laboral debe ir acompañada de una reflexión más amplia sobre el impacto de la tecnología en el trabajo y en la sociedad. Debemos preguntarnos

cómo queremos que sea el futuro del trabajo en un mundo cada vez más digitalizado y cómo podemos asegurar que los beneficios de esta transformación se distribuyan de manera justa y equitativa.

En definitiva, mientras aplaudo el reconocimiento legal de las nuevas realidades digitales, insto a una aproximación cautelosa y equilibrada que no pierda de vista la dimensión humana y social del trabajo en nuestra búsqueda de adaptación a la era digital

10. BIBLIOGRAFÍA

Aldana Montes, J. F., García Nieto, J. M., Gonzalvez, J. C. y Navas Delgado. I.: *Big data: seguridad y gobernanza*, Madrid, García Maroto Editores, 2018.

Blasco Pellicer. Á.: Los expedientes de regulación de empleo, Valencia, Tirant lo Blanch, 2009.

Calcara, A. y Marchetti, R.: "State-industry relations and cybersecurity governance in Europe", *Review of International Political Economy*, 2021.

Esteban Gómez, A.: «Expediente de regulación temporal de empleo: instrumento recurrente ante la COVID-19», 1ª edic., Albacete, Ed. Bomarzo, 2021.

Fernández Bermejo, D. y Martínez Atienza, G.: *Ciberseguridad, ciberespacio y ciberdelincuencia*, Cizur Menor, Aranzadi Thomson Reuters, 2018.

Fernández Domínguez, J. J.: *La fuerza mayor como causa de extinción y suspensión del contrato de trabajo*, Madrid, Civitas, 2021.

Gómez de Ágreda, Á.: "Ciberseguridad en un mundo hiperconectado" en *Ciberseguridad. Un nuevo reto para el Estado y los gobiernos locales*, Canals, D. (Ed.), Madrid, Wolters Kluwer, 2021.

Lahera Forteza, J.: «Nuevas perspectivas de suspensión del contrato y reducción de jornada por causas económicas, técnicas, organizativas y de producción», en AAVV: *La reforma laboral de 2012: Nuevas perspectivas del Derecho del Trabajo*, Madrid, La Ley, 2012.

Molina Navarrete, C.: *La reestructuración empresarial mediante regulación de empleo: Nuevas normas y prácticas sobre ERTE y despidos colectivos,* Madrid, Temas La Ley, 2024.

Roqueta Buj, R.: *Los Expedientes de Regulación Temporal del Empleo,* 2ª edición, Valencia, Tirant Lo Blanch, 2021.

Solà Monells, X.: "Suspensión del contrato o reducción de jornada", en AA.VV.: *Comentario al Estatuto de los Trabajadores*, Madrid, La Ley, 2013.

Sola Monells, X.: "La suspensión por causas empresariales tras la reforma laboral de 2012: problemática aplicativa y valoración crítica", en AAVV: *Balance de la reforma laboral de 2012*, Albacete, Bomarzo, 2016.

Terrón Santos, D. (Dir.), y Domínguez Álvarez. J.L.: *Inteligencia artificial y defensa: nuevos horizontes*, Valencia, Aranzadi Thomson Reuters, 2021.