ADMINISTRACION
DE JUSTICIA

A U T O

En Madrid, a 29 de abril de 2025.

ANTECEDENTES DE HECHO

ÚNICO. Sobre las 12,30 horas del día de ayer todo el territorio peninsular sufrió un apagón eléctrico, que comenzó a recuperarse parcialmente a partir de las 16.30 horas. Según ha informado el Gobierno de España pasadas las 12.30 horas "se han perdido" de forma súbita, durante cinco segundos, 15 GW de la energía que se estaba produciendo en ese momento, lo que equivale al 60% de la luz que se estaba consumiendo, siendo "algo que no había ocurrido jamás". Estos hechos, haber afectado a sistemas informáticos que soportan infraestructuras que proporcionan los servicios esenciales a la sociedad, como salud, energía, industria, transporte etc., han supuesto una situación crítica para el bienestar y sentimiento de seguridad de todos los ciudadanos.

FUNDAMENTOS DE DERECHO

ÚNICO. Sobre la posibilidad de un sabotaje informático y afectación a infraestructuras críticas españolas.

Si bien en el momento actual la causa de los referidos hechos resulta descocida, el ciberterrorismo se encuentra entre una de las posibles. Por tanto, resulta necesaria la apertura de una investigación judicial por si tales hechos pudieran ser constitutivos de un delito de terrorismo, previsto y penado en el art. 573.1 y 2 CP, conforme al cual se considerarán delitos de terrorismo los delitos informáticos tipificados en los arts. 197 bis y 197 ter y 264 a 264 quáter cuando los hechos se cometan con alguna de las siguientes finalidades: 1ª Subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, u obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo; 2ª Alterar gravemente la paz pública; 3ª Desestabilizar gravemente el funcionamiento de una organización internacional; y 4ª Provocar un estado de terror en la población o en una parte de ella.

Nuestra sociedad se basa cada vez más de un complejo sistema de infraestructuras en el que se sustentan los sectores productivos, gestión de servicios, sistema financiero y desarrollo de la vida ciudadana en general. Estas infraestructuras son interdependientes entre sí, lo que puede desencadenar problemas de seguridad en cascada a través del propio sistema, con la posibilidad de ocasionar fallos inesperados y graves en servicios básicos para la población, como sucedió en el día de ayer.

Este tipo de infraestructuras son especialmente atractivas para el terrorismo, por los graves daños que pueden ocasionarse para la población. Por ello, ya en el año 2004, el

Consejo de la Unión Europa aprobó el Programa europeo de protección de infraestructuras en infraestructuras críticas, que daría lugar a la Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección. Según el art. 2 de esta Directiva, debe entenderse por infraestructura crítica: "*el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones*".

Es nuestro país, por su parte, esta necesidad fue atendida mediante el Plan Nacional de Protección de las Infraestructuras Críticas, de 07.05.2007 la elaboración de un primer Catálogo Nacional de Infraestructuras Estratégicas y la aprobación en el Consejo de Ministros de 02.11.2007, de un Acuerdo sobre Protección de Infraestructuras Críticas. Resultado de lo anterior, se identifican dieciocho áreas que necesitan del desarrollo de un Plan Estratégico Sectorial, entra las que se encuentra la electricidad.

Además, cumpliendo con la transposición de la Directiva europea de 2008, se aprobó la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, que en su preámbulo insiste en la amenaza del terrorismo expresando que los "*nuevos riesgos, generados, en gran medida, por la globalización, y entre los que se cuentan el terrorismo internacional, la proliferación de armas de destrucción masiva o el crimen organizado, se suman a los ya existentes, de los cuales el terrorismo tradicional venía siendo un exponente*". En este sentido, el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, insiste en el diseño de un planteamiento orientado a prevenir y proteger las denominadas infraestructuras críticas de las amenazas o ac tos intencionados provenientes de figuras delictivas como el terrorismo, potenciados a través de las tecnologías de la comunicación.

El informe sobre Ciberamenazas y tendencias de 2017 del Centro Criptológico Nacional afirmaba que el mayor peligro es el ataque con origen en estados extranjeros. Así ocurrió en el caso de los ciberataques a compañías de electricidad de Ucrania que, en 2016 ocasionaron un apagón, provocando que millones de personas se quedaran sin energía eléctrica.

La Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional, expresa que la cibercriminalidad hace referencia al conjunto de actividades ilícitas cometidas en el ciberespacio que tienen por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, siempre que en su planificación, desarrollo y ejecución resulte determinante la utilización de herramientas tecnológicas; en función de la naturaleza del hecho punible en sí, de la autoría, de su motivación, o de

los daños infligidos, se podrá hablar así de ciberterrorismo, de ciberdelito, o en su caso, de hacktivismo. Los grupos terroristas tratan de aprovechar las vulnerabilidades del ciberespacio para realizar ciberataques. Íntimamente relacionado con ello, se halla la amenaza contra las infraestructuras críticas, con la posibilidad cierta de causar un colapso a través de las redes mediante una caída en cadena de los servicios esenciales

Siguiendo la regulación internacional, los delitos de sabotaje de datos informáticos y de sistemas informáticos propiamente se introdujeron por primera vez en nuestro Código Penal en el año 2010. El legislador, en la Exposición de motivos de la LO 5/2010, de 22 de junio por la que se modifica el Código Penal, justificaba la reforma del art. 264 CP al verse obligado a cumplir "*con lo dispuesto por la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información (…) que en lo relativo a los daños, quedarían incluidas tanto las consistentes en dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos o programas informáticos ajenos, así como obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno*". Bajo esta regulación estos tipos delictivos no presentaron mucho recorrido jurisprudencial, destacando el caso conocido como "virus de la policía" por la dinámica que siguieron los ciberdelincuentes, en el que fueron juzgados varios ciudadanos rusos, que desde 2011 y utilizando la dinámica descrita habrían atacado a usuarios de varios países habiendo más de 300 afectados en España; así como el enjuiciamiento de la cúpula de Anonymous.

En cuanto al delito de terrorismo se refiere, el art. 3 de la Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo de 15.03.2017 relativa a la lucha contra el terrorismo insta a los estados a tipificar con arreglo al Derecho nacional "*actos que, por su naturaleza o contexto pueden perjudicar gravemente a un país o a una organización internacional*", especificando, en su apartado d) las conductas de "*destrucciones masivas de instalaciones estatales o públicas, sistemas de transporte, infraestructuras, sistemas informáticos incluidos*". También en su apartado i) remite al delito de "*interferencia ilegal en los sistemas de información a tenor del artículo 4 de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, en los casos en los que sea de aplicación su artículo 9 (…) apartado 4, letra c*)". Este último apartado es precisamente el que refiere a que esa interferencia ilegal en los sistemas se cometa contra el sistema de información de una infraestructura crítica. Es decir, esta Directiva pone el énfasis precisamente en aquel sabotaje que es capaz de afectar al funcionamiento del sistema informático de una infraestructura crítica, no a cualquiera sistema.

La Decisión marco del Consejo de 13.06.2002 sobre la lucha contra el terrorismo (2002/475/JAI) del Consejo De La Unión Europea, establece en su art. 1 que "*todos los Estados miembros adoptarán las medidas necesarias para que se consideren delitos de terrorismo los actos intencionados a que se refieren las letras a) a i) tipificados como delitos según los respectivos Derechos nacionales que, por su naturaleza o su contexto,*

puedan lesionar gravemente a un país o a una organización internacional cuando su autor los cometa con el fin de: intimidar gravemente a una población, obligar indebidamente a los poderes públicos o a una organización internacional a realizar un acto o a abstenerse de hacerlo, o desestabilizar gravemente o destruir las estructuras fundamentales políticas, constitucionales, económicas o sociales de un país o de una organización internacional". Los instrumentos posteriores no modifican estas finalidades. No lo hace ni la Decisión Marco 2008/919/JAI del Consejo de 28 de noviembre de 2008 por la que se modifica la anterior Decisión Marco 2002/475/JAI sobre la lucha contra el terrorismo, ni tampoco, ni tampoco la Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo de 15 de marzo de 2017 relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/ JAI del Consejo.

La Ley Orgánica 1/2015, de 30 de marzo, añade una serie de agravantes en relación con los delitos de sabotajes informáticos, recogidas en el apartado 2 de los art. 264 y 264 bis CP cuando el sabotaje "*se hubiera cometido en el marco de una organización criminal, o bien haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos, o que hubieran perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad*"; así como en el punto 4, que refiere la afección del "*sistema informático de una infraestructura crítica o la creación de una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea*". A estos efectos, en el mismo párrafo se define infraestructura crítica como "*un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones*".

Esta especial consideración a la protección de estas infraestructuras frente a ataques terroristas llevó el legislador español a introducir en el CP este fenómeno dentro de los delitos de terrorismo, mediante Ley Orgánica 2/2015, de 30 de marzo concretamente en el art. 573.2 CP, en el que inicialmente, conforme a lo ya expresado, podrían tener cabida los hechos objeto de investigación en el caso de que su origen hubiera estado auspiciado en la forma y con alguna de las finalidades descritas en dicho tipo penal.

Por consiguiente, procede acordar la práctica de las siguientes diligencias de investigación a fin de determinar si los hechos sucedidos ayer en la red electiva tuvieron su causa en algún acción delictiva:

- Requerir al Centro Criptológico Nacional la emisión de un informe sobre los hechos que en el día de ayer motivaron el cese de suministro eléctrico en el territorio peninsular, y concretamente, sobre la causa o causa que motivaron la

pérdida súbita, durante cinco segundos, 15 GW de la energía que se estaba produciendo en ese momento.

- Requerir a Red Eléctrica Corporación SA la emisión de un informe sobre los hechos que en el día de ayer motivaron el cese de suministro eléctrico en el territorio peninsular, y concretamente, sobre la causa o causa que motivaron la pérdida súbita, durante cinco segundos, 15 GW de la energía que se estaba produciendo en ese momento.
- Encomendar a la Comisaría General de Información de Policía Nacional la investigación de los hechos objeto de la presente causa, con presentación de un informe preliminar en el plazo de diez días.
- Todos los informes acordados deberán emitirse, aun cuando sea con carácter preliminar, en el improrrogable plazo de diez días.

Vistos los arts. citados y demás de general y pertinente aplicación,

PARTE DISPOSITIVA

Se acuerda la incoación de Diligencias Previas, previo registro en los libros informáticos de su razón, dándose parte de incoación a la Fiscalía de la Audiencia Nacional.

Líbrese oficio al Centro Criptológico Nacional a fin de que en el plazo improrrogable de 10 días, expida y remita a este órgano judicial un informe sobre los hechos que en el día de ayer motivaron el cese de suministro eléctrico en el territorio peninsular, y concretamente, sobre la causa o causa que motivaron la pérdida súbita, durante cinco segundos, 15 GW de la energía que se estaba produciendo en ese momento.

Líbrese oficio a Red Eléctrica Corporación SA a fin de que en el plazo improrrogable de 10 días, expida y remita a este órgano judicial un informe sobre los hechos que en el día de ayer motivaron el cese de suministro eléctrico en el territorio peninsular, y concretamente, sobre la causa o causa que motivaron la pérdida súbita, durante cinco segundos, 15 GW de la energía que se estaba produciendo en ese momento.

Se acuerda encomendar a la Comisaría General de Información de Policía Nacional la investigación de los hechos objeto de la presente causa, con presentación de un informe preliminar en el plazo improrrogable de diez días.

Contra la presente resolución podrán formularse, ante este Juzgado, recurso de reforma en el plazo de tres días y apelación en el plazo de cinco días. El recurso de apelación podrá interponerse subsidiariamente con el de reforma o por separado, sin que sea necesario interponer previamente el de reforma para presentar la apelación.

Así lo acuerda, manda y firma el Ilmo. Sr. D. José Luis Calama Teixeira Magistrado-Juez del Juzgado Central de Instrucción núm. 4 en funciones de Juzgado de Guardia. Doy fe.

EL MAGISTRADO-JUEZ **EL LETRADO DE LA ADMINISTRACIÓN DE JUSTICIA**

DILIGENCIA. Seguidamente se cumple lo acordado. Doy fe.