V CONGRESO PENITENCIARIO

PONENCIA

"SEGURIDAD NACIONAL Y CIBERSEGURIDAD".

Gorgonio Martínez Atienza

A SEGURIDAD NACIONAL

La Seguridad Nacional se entiende como la acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en cumplimiento de los compromisos asumidos. La seguridad es actualmente responsabilidad de todos, y, es una tarea compleja en un mundo interdependiente y en transformación.

La Política de Seguridad Nacional es una política pública en la que bajo la dirección del Presidente del Gobierno y la responsabilidad del Gobierno, participan todas las Administraciones Públicas, de acuerdo con sus respectivas competencias, y la sociedad en general, para responder a las necesidades de la Seguridad Nacional. Los principios básicos que orientarán la política de Seguridad Nacional son la unidad de acción, anticipación, prevención, eficiencia, sostenibilidad en el uso de los recursos, capacidad de resistencia y recuperación, coordinación y colaboración.

Afrontamos amenazas y riesgos transversales, interconectados y transnacionales (muchos intereses globales que defender y amenazas y riesgos transnacionales que afrontar surgirán en el exterior).

Preservar la seguridad requiere coordinación interna e internacional, y, la contribución de la sociedad en su conjunto.

Sólo un enfoque integral que conciba la seguridad de manera amplia e interdisciplinar, a nivel nacional, europeo e internacional, puede responder a los complejos retos a los que nos enfrentamos (los límites entre la seguridad interior y la seguridad exterior se han difuminado, y, las políticas nacionales en los ámbitos tradicionales de la seguridad ya no son suficientes para salvaguardarla en el siglo XXI).

Son factores transnacionales que pueden potenciar los efectos de las amenazas y riesgos e incluso cambiar su naturaleza, la globalización, los

desequilibrios demográficos, la pobreza y la desigualdad, el cambio climático, los peligros tecnológicos y las ideologías radicales y no democráticas.

Las amenazas y riesgos más importantes para la seguridad de nuestro país, que es necesario anticipar y prevenir, pueden tener lugar en los ámbitos terrestre, marítimo, aéreo, espacial y ciberespacio. Son amenazas toda circunstancia o agente que ponga en peligro la seguridad o estabilidad de España, y, riesgos toda contingencia o probabilidad de que una amenaza se materialice produciendo un daño.

La realidad demuestra que los desafíos para la Seguridad Nacional que afectan a la sociedad revisten en ocasiones una elevada complejidad, que desborda las fronteras de categorías tradicionales, como el ciberespacio; y la dimensión que adquieren ciertos riesgos y amenazas, su acusada transversalidad, o la combinación de estos rasgos con su naturaleza abierta e incierta, son factores que indican claramente que toda respuesta se verá reforzada y resultará más eficiente si se realiza de forma coordinada.

Se considerarán ámbitos de especial interés de la Seguridad Nacional aquellos que requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales (la ciberseguridad es uno de ellos).

B CIBERSEGURIDAD Y SEGURIDAD HUMANA

1º.- Aspectos generales.

Uno de los principales ámbitos de especial interés de la seguridad nacional es la ciberseguridad, que es uno de los objetivos y líneas de acción estratégicas para los ámbitos de la Seguridad Nacional, la cual se encarga de la seguridad en el medio informático o telemático; y siendo el ciberespacio un dominio común, global y dinámico que hace partícipes a sus usuarios de una globalización e internacionalización sin precedentes, es considerado como el quinto dominio después de la tierra, el mar, el aire y el espacio (derecho de todos al desenvolvimiento normal de sus vidas en paz, sosiego, bienestar y tranquilidad en el ciberespacio). El ciberespacio como dominio global y dinámico hace partícipes a sus usuarios de una globalización e internacionalización sin precedentes, y, es considerado como el quinto dominio después de la tierra, el mar, el aire y el espacio.

Los avances tecnológicos en la información y comunicación han supuesto la entrada de nuevos valores y bienes susceptibles de protección jurídica, que determinan la necesidad de una mayor cooperación internacional; y de una regulación normativa específica nacional, comunitaria e internacional.

Existe una tendencia colaboradora para abordar la ciberseguridad de forma conjunta, pues la participación de los Estados en las diversas iniciativas internacionales que contribuyen a compartir la información sobre los riesgos y amenazas y que proporcionan los medios con los que alcanzar un mayor grado de ciberseguridad es creciente, aunque aumenta el interés de las países por contar con herramientas propias para salvaguardar la independencia y la seguridad.

Desarrollar estrategias de ciberseguridad supranacionales y fortalecer la cibercooperación internacional deberían ser prioridades de las agendas estatales para proteger a sus ciudadanos y lograr progreso a través de las Técnicas de la Información y la Comunicación.

Con la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional de 2000, la comunidad internacional demostró la voluntad política de abordar un problema mundial con una reacción mundial. Si la delincuencia atraviesa las fronteras, lo mismo ha de hacer la acción de la ley. Si el imperio de la ley se ve socavado no sólo en un país, sino en muchos países, quienes lo defienden no se pueden limitar a emplear únicamente medios y arbitrios nacionales. la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional constituirá un instrumento eficaz y el marco jurídico necesario para la cooperación internacional para prevenir y combatir más eficazmente la delincuencia organizada transnacional, esto es, actividades delictivas como el blanqueo de dinero, la corrupción, el tráfico ilícito de especies de flora y fauna silvestres en peligro de extinción, los delitos contra el patrimonio cultural y los crecientes vínculos entre la delincuencia organizada transnacional y los delitos de terrorismo.

Uno de los últimos objetivos de esta práctica internacional es la necesidad de la cooperación internacional en la modulación jurídica de la compleja realidad que supone el ciberespacio, dentro del cual se circunscribe la lucha contra la cibercriminalidad, así como los aspectos de la seguridad cibernética, incluidos los actos de agresión y las políticas de proliferación de armas informáticas o tecnológicas conexas que pongan en peligro la paz y la seguridad internacionales. La aparición de las Tecnologías de la Información y la Comunicación ha supuesto un avance

decisivo en las relaciones internacionales, constituyendo uno de los principales aspectos de la globalización.

La Resolución de la Asamblea General de las Naciones Unidas 57/239 (2002) para la creación de una cultura global de ciberseguridad, exhorta a crear la citada cultura teniendo en cuenta los principios de conciencia, responsabilidad, respuesta ética, democracia, evaluación de riesgos, diseño y puesta en práctica de la seguridad, gestión de la seguridad y reevaluación.

2º.- Derecho humanitario y seguridad humana.

1.- Derecho humanitario: Comenzamos aludiendo al Convenio de Viena sobre el Derecho de los Tratados de 23 de mayo de 1969, al que se adhiere España por Instrumento de 2 de mayo de 1972, que es de aplicación a los Tratados entre Estados. Para los efectos de la presente Convención: Se entiende por "tratado" un acuerdo internacional celebrado por escrito entre Estados y regido por el derecho internacional, ya conste en un instrumento único o en dos o más instrumentos conexos y cualquiera que sea su denominación particular; y se entiende por "ratificación", "aceptación", "aprobación" y "adhesión", según el caso, el acto internacional así denominado por el cual un Estado hace constar en el ámbito internacional su consentimiento en obligarse por un tratado. Se entiende por "Estado contratante" un Estado que ha consentido en obligarse por el tratado, haya o no entrado en vigor el tratado; y se entiende por "parte" un Estado que ha consentido en obligarse por el tratado y con respecto al cual el tratado está en vigor.

La Carta de las Naciones Unidas que se firmó el día 26 de junio de 1945 en San Francisco, al terminar la Conferencia de las Naciones Unidas sobre Organización Internacional, y que entró en vigor el día 24 de octubre de 1945, proclama el desarrollo y estímulo del respeto a los Derechos Humanos y a las Libertades Fundamentales de todos; habiendo aumentado las normas de Derecho Internacional Público que persiguen esa finalidad. Es Derecho Internacional Humanitario a tener en consideración, la Declaración Universal de Derechos Humanos de 10 de diciembre de 1948, el Pacto Internacional de Derechos Civiles y Políticos de 19 de abril de 1966 y el Convenio Europeo para la protección de los Derechos Humanos y las Libertades Fundamentales de 4 de noviembre de 1950. Y en relación con los Derechos del Niño se ha de tener en cuenta la Declaración de 20 de noviembre de 1959 que tiene como base la Declaración de Ginebra de 1924, y, la Convención de 20 de noviembre de 1989 (establece los derechos civiles, políticos, sociales, económicos y culturales de los niños).

La Política de Estado para la Seguridad Nacional se basa, entre otros aspectos, en el estricto respeto al Derecho Internacional y en el fiel cumplimiento de los Tratados Internacionales, además de en el respeto a los derechos humanos que tienen su fundamento en la dignidad humana -configurada como un valor supremo que escapa a los límites del derecho y que fundamenta la totalidad de los derechos reconocidos a la persona por el hecho de serlo-, reconocida constitucionalmente en el art. 10.1 CE como valor esencial, fuente de derechos iguales, inalienables e inherentes a cada persona que vienen a identificarse con los derechos fundamentales (para el Tribunal Constitucional la dignidad de la persona se presenta como un valor supremo que escapa a los límites del Derecho y que informa y fundamenta la totalidad de derechos reconocidos a la persona por el hecho de serlo, cuya tutela parece concretarse a través de la protección de los derechos fundamentales) y el reconocimiento expreso del respeto debido a la dignidad humana absorbe la totalidad de los derechos fundamentales, cuya individualización dependerá de la concreta conducta lesiva. La dignidad humana se configura por el TC como un valor espiritual y moral inherente a la persona según la STC 53/1985, de 11 de abril, que constituye un mínimum invulnerable que todo estatuto jurídico debe asegurar, de modo que, sean unas u otras las limitaciones que se impongan en el disfrute de los derechos individuales, no conlleven menosprecio para la estima que, en cuanto ser humano, merece la persona, según la STC 120/1990, de 27 de junio; la ausencia de una definición concreta de la misma obliga a la doctrina cuanto menos a la realización de una labor de la determinación de sus elementos característicos, señalando J. Ruiz-Jiménez Cortes que el concepto de dignidad humana responde a una realidad ontológica y ético-social a través de la cual ésta viene a referirse a la autonomía de la persona, la libertad del ser humano, la racionalidad y su fin en sí mismo considerado. Se atribuye a la dignidad la consideración de valor esencial, valor absoluto, valor universal o superioridad; señalando a este respecto De Esteban, J. y González Trevijano, P. J. que la supremacía del ser humano en el mundo significa que todos los hombres, por ser personas, tienen que ser iguales en dignidad, y apuntando Garrido Falla, F. que ni siquiera un comportamiento indigno priva, sin más, a la persona de algunos derechos que le son inherentes en cuanto tal.

Los derechos fundamentales y los derechos humanos son categorías afines, que precisan de la determinación de una distinción entre los mismos. Los derechos fundamentales aparecen consagrados en la CE, y, se consideran como tales en su acepción amplia, los derechos básicos y necesarios para el desarrollo de una vida basada en la libertad y en la dignidad; y en su acepción estricta, son fundamentales los derechos que el ordenamiento jurídico considera como tales. Los derechos fundamentales

son derechos subjetivos que no son absolutos, y, tanto los derechos individuales como sus limitaciones son considerados por el art. 10.1 CE como fundamento del orden político y de la paz social; y la norma contenida en el art. 10.1 CE impone un derecho penal respetuoso del principio de culpabilidad por el hecho concretamente cometido y no puede servir de base a una pretensión autónoma de amparo, según la STS, Sala 2ª, de 6 de abril de 1990; y STC 64/1986, de 21 de mayo.

La expresión derechos humanos debe ser utilizada para referirse a los derechos básicos del ser humano, reconocidos por el orden internacional, que traducen desde el punto de vista normativo, determinados valores de dignidad, libertad, igualdad y solidaridad; los derechos humanos se concretan en aquellos atributos inherentes a todo ser humano, derivados de su propia naturaleza y de la necesidad de tener una existencia digna, son intrínsecos a nuestra naturaleza por incluir a toda persona por el simple hecho de su condición humana y aparecen en los Pactos Internacionales y sus Protocolos que obligan jurídicamente a los Estados que los suscriben.

3.- Seguridad humana: La justicia y la paz en el mundo tienen como fundamento el reconocimiento y el respeto de los derechos humanos; y con base en los mismos aparece en los años 90 el concepto de seguridad humana, como resultado de los cambios operados en la sociedad internacional tras el final de la Guerra Fría, en los planos de la seguridad (propicia un cambio esencial en el clima global de la seguridad internacional), de las ideas (auge del liberalismo y sus valores) y de la política internacional. La seguridad humana presupone el derecho a tener derechos, siendo la democracia el sistema político que potencia el ejercicio de los derechos de las personas y facilita la resolución de los conflictos y las diferencias de intereses de forma pacífica e institucionalizada (la aparición del concepto de seguridad humana responde, fundamentalmente, a que la seguridad debe centrarse en las personas, esto es, la seguridad humana erige a la persona y no al Estado en sujeto de seguridad -se pone el acento en la protección de las personas-; con el objetivo de la seguridad humana, que trae causa de los conflictos de carácter internacional y de la complejidad de los problemas mundiales, han proliferado las ``intervenciones humanitarias´´, que tienen una naturaleza militar y se justifican por razones humanitarias).

El concepto de seguridad humana se difundió a partir de ser tratado por el Programa de las Naciones Unidas para el Desarrollo en su Informe sobre Desarrollo Humano de 1994 (la seguridad humana es una preocupación universal y sus componentes son interdependientes). De hecho, la seguridad humana está estrechamente vinculada al concepto de

desarrollo humano, que consiste en un proceso de ampliación de la gama de opciones y capacidades de las personas; la seguridad humana consiste en que las personas puedan ejercer tales opciones de forma libre y segura, esto es, la seguridad de las personas en sus vidas cotidianas se alcanza mediante el desarrollo humano y no mediante las armas y los ejércitos. Una mejora de la seguridad humana repercute favorablemente en el desarrollo.

Frente a esa visión defensiva y estrecha, el nuevo concepto de seguridad humana tiene un carácter ``integrador y globalizador´´, por cuanto no se basa en la fuerza de los ejércitos sino en la satisfacción de las necesidades universales básicas mediante la participación solidaria de todos en los beneficios del desarrollo, esto es, el nuevo escenario de seguridad requiere respuestas cooperativas. En definitiva, el eje ha basculado de la seguridad del territorio hacia la de las personas, y de buscarla mediante las armas a hacerlo buscando el desarrollo humano sostenible. En consecuencia, frente a la visión tradicional centrada en la disuasión y el conflicto, se revaloriza la cooperación para el desarrollo internacional como vía para alcanzar la seguridad. La seguridad humana es una preocupación universal, que es aplicable a todas las personas en todo el mundo, que se centra en la protección de la persona y de las comunidades.

Del mismo modo que para la seguridad convencional se han armado ejércitos y se han constituido sistemas defensivos, para aplicar el enfoque de la seguridad humana sería necesario implementar políticas nacionales e internacionales que garantizaran a todas las personas la capacidad de tomar parte en el desarrollo. Hablar de seguridad humana, por tanto, plantea exigencias, objetivos y medios diferentes a los que se derivan meramente del concepto tradicional de seguridad. En suma, se trata de una visión innovadora que, como la noción de desarrollo humano, puede contribuir al cambio social.

La seguridad humana es complementaria de la seguridad estatal (según la definición de la Comisión de la Seguridad Humana, la seguridad humana significa la creación de sistemas políticos y militares que brinden al ser humano las piedras angulares de la supervivencia, los medios de vida y la dignidad), y, reafirma y potencia la aplicación del Derecho Humanitario; significa proteger las libertades fundamentales que constituyen la esencia de la vida (en el mundo actual existe una brecha entre las capacidades de seguridad actualmente disponibles, consistentes, sobre todo, en fuerzas militares, y las necesidades de seguridad reales). En el ámbito de la UE se ha resaltado que se debe construir una política de seguridad que aborde simultáneamente la seguridad estatal y la seguridad humana; los aspectos humanos en la Política Común de Seguridad y

Defensa en la UE imponen una actuación multidisciplinar, estableciendo la Estrategia Europea de Seguridad que ``el mejor medio para consolidar el orden internacional es difundir el buen gobierno, apoyar las reformas políticas y sociales, combatir la corrupción y el abuso de poder, instaurar la supremacía de la ley y proteger los derechos humanos´´.

Se pone de manifiesto por la Comisión de la Seguridad Humana que, "la seguridad humana complementa la ``seguridad del Estado´´ en los aspectos siguientes: Se preocupa por la persona y de la comunidad más bien que del Estado; las amenazas para la seguridad de la persona incluyen amenazas y condiciones que no siempre se han clasificado como amenazas a la seguridad del Estado; la gama de agentes no se circunscribe al propio Estado; y la consecución de la seguridad humana no incluye solamente la protección de la persona, sino que también le brinda los medios de valerse por sí misma.

El respeto a los Derechos Humanos constituye la base y fundamento de la paz y estabilidad internacional, y, la primacía de los derechos humanos es lo que distingue el enfoque de la seguridad humana de los enfoques tradicionales basados en el Estado.

4º.- Ciberseguridad.

La ciberseguridad que es un aspecto técnico de la seguridad y un eje fundamental de nuestra sociedad, no ha sido definida todavía en una legislación específica y completa, aunque si existe a nivel nacional una legislación distribuida en distintos ámbitos ministeriales (no se ha desarrollado todavía una política común que refleje su ámbito nacional y estratégico) y unas disposiciones normativas comunitarias destacando la Directiva sobre seguridad de las redes y sistemas de información a la que ya hemos hecho referencia.

La ciberseguridad, seguridad informática o seguridad de las Tecnologías de la Información y la Comunicación sólo se encarga de la seguridad en el medio informático o telemático, diseñando las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable; y se encuentra enfocada esencialmente en la información que se encuentra en formato digital y los sistemas interconectados que la procesan, transmiten o almacena, por lo que tienen una mayor cercanía a la seguridad informática o seguridad de las tecnologías de la información y la comunicación. Con los avances tecnológicos que se incorporan cada vez más a nuestras vidas cotidianas, la

dependencia de la tecnología se incrementa, y como consecuencia se genera la necesidad de su aplicación.

La ciberseguridad se concreta en un conjunto de actuaciones orientadas a asegurar los sistemas que constituyen el ciberespacio, preservando la confidencialidad, disponibilidad e integridad de la información; y es una actividad por la que la información contenida en los sistemas de información, está protegida contra su uso no autorizado. En la Recomendación de la Unión Internacional de Telecomunicaciones-T X.1205 (04/2008) es definida como, "el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno (incluye a usuarios, redes, dispositivos, todo el software, procesos, información almacenada o que circula, aplicaciones, servicios y sistemas que están conectados directa o indirectamente a las redes)".

Se puede entender por ciberseguridad, "la protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena o transporta mediante los sistemas de información interconectados".

En la ciberseguridad se comprenden actuaciones orientadas a asegurar las redes y sistemas de la información y la comunicación que dan vida al ciberespacio, mediante la detección y enfrentamiento a intrusiones e incidentes, preservando la confidencialidad, disponibilidad e integridad de la información.

5º.- Ciberdelitos, cibercrímenes o delitos informáticos.

Las amenazas en el espacio digital adquieren una dimensión global que va más allá de la tecnología. El ciberespacio es un escenario con características propias marcadas por su componente tecnológico, fácil accesibilidad, anonimidad, alta conexión y dinamismo. En los últimos tiempos, las acciones negativas en el ámbito de la ciberseguridad han aumentado notablemente en número, alcance y sofisticación. Tales acciones adquieren creciente relevancia para España, un país altamente interconectado y que ocupa una posición de liderazgo en Europa en materia de implantación de redes digitales. Desde un punto de vista tecnológico, ha de destacarse la transformación digital de la Administración. Este factor agudiza la dependencia de las tecnologías de la información, extiende la posible superficie de ataque y, en consecuencia, los beneficios potenciales

derivados para los atacantes, en un entorno donde el derecho a la protección de datos de carácter personal es un requisito esencial en la relación del ciudadano con la Administración por medios electrónicos. En lo relativo a las ciberamenazas, es creciente la actividad tanto por parte de Estados, que persiguen la expansión de sus intereses geopolíticos a través de acciones de carácter ofensivo y subversivo, como de organizaciones terroristas, grupos de crimen organizado y actores individuales. Estos grupos aprovechan el carácter anónimo que el ciberespacio ofrece para conseguir sus fines a un mínimo coste y asumiendo un riesgo menor dada la dificultad de atribución. El robo de datos e información, los ataques ransomware y de denegación de servicios, el hackeo de dispositivos móviles y sistemas industriales y los ciberataques contra las infraestructuras críticas son ejemplos de ciberamenazas. La utilización del ciberespacio como medio para la realización de actividades ilícitas, acciones de desinformación, propaganda o financiación terrorista y actividades de crimen organizado, entre otras, impacta en la Seguridad Nacional, amplificando la complejidad y la incertidumbre, y también pone en riesgo la propia privacidad de los ciudadanos.

El ciberdelito, cibercrimen o delito informático es un concepto que manejamos socialmente para referirnos a un conjunto de conductas que vulneran los derechos de terceros y se producen en un escenario o medio tecnológico, provocando un rechazo social y sobre las que media el Derecho Penal.

Con la expresión delito informático, cibercrimen o ciberdelito se define a todo ilícito penal llevado a cabo a través de medios informáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las Tecnologías de la Información y la Comunicación o que tiene como fin estos bienes (se caracteriza por ser un delito permanente al precisar de la repetición y el automatismo del hecho; su extensa y elevada lesividad; sus dificultades de averiguación y comprobación; su alto volumen de cifra negra; su mayor frecuencia, diversidad y peligrosidad; su distanciamiento espacio-temporal; y su transnacionadad). Las nuevas Tecnologías de la Información y la Comunicación han obligado a que en el seno del Derecho Penal Sustantivo se haya procedido a una mayor precisión en la tipificación de los delitos informáticos, que avanzan al mismo tiempo que aquellas y de los que pueden ser responsables criminalmente también las personas jurídicas.