



**XIII
JORNADAS
STIC
CCN-CERT**

ccn-cert
centro criptológico nacional

**Ciberespaña: un modelo
de criptored para la
seguridad y la
gobernanza de la
soberanía nacional en el
ciberespacio**

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCCNCERT



⁻¹
concepto
Fundación Concepto López Mosteiro

Andrés Montero

Fundación Concepto

amg@theconcept.foundation

Índice

- 1. El ciberespacio como territorio pre(¿anti?)-democrático**
- 2. El ciberespacio como territorio de soberanía popular**
- 3. Topografía de CiberEspaña**
- 4. Anomalías de un ciberespacio a-democrático**
- 5. Conceptualizando la soberanía en el ciberespacio**
- 6. Esquemática de un modelo de criptored para la gobernanza**
- 7. ¿CiberEspaña sin CiberEuropa?; ¿Sin CiberMundo?**

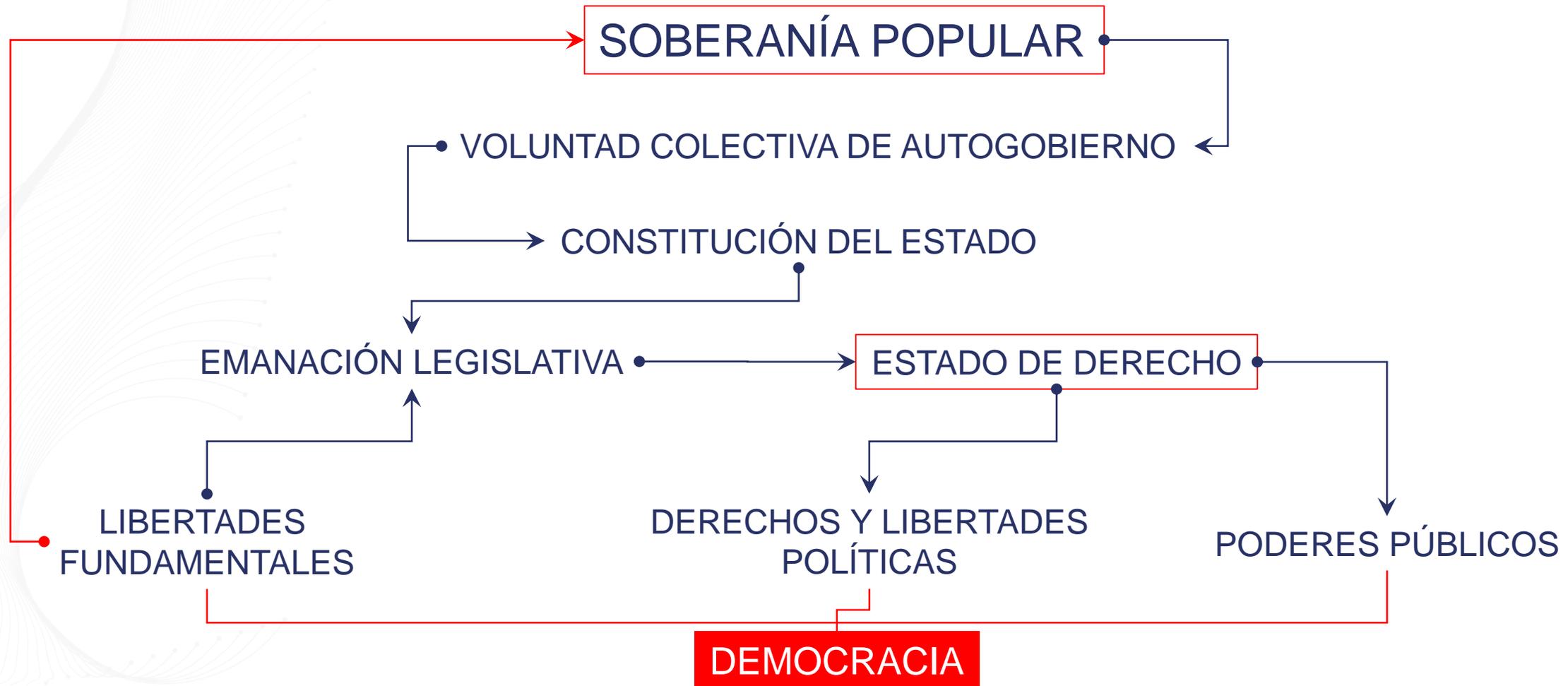
El ciberespacio como territorio pre(¿anti?)-democrático

Sin soberanía no hay Estado de Derecho; sin derecho no hay democracia

- Algunas obviedades:
 - La Democracia es el gobierno del pueblo.
 - El pueblo, por tanto, determina el modo en que quiere gobernarse, puesto que es soberano respecto de su destino. El pueblo es el **sujeto político colectivo del sujeto político individual que es el ciudadano**. La soberanía reside en el pueblo (*no en el ciudadano*), del que emanan los poderes del Estado (Art. 1 CE).
 - Queda entendido, por tanto, que el Estado es el artefacto colectivo a través del cual el pueblo se dota de una estructura de autogobierno. El pueblo se gobierna a sí mismo a través de un “Estado”, que como instrumento de gobierno es un **estructura política**.
 - Dentro de esas formas de gobierno, la democracia adopta diversas formas a través del Estado, basadas en la expresión de la soberanía popular.
 - Todas las formas de gobierno democráticas tienen en común la regulación de la convivencia a través de leyes que emanan de la soberanía popular y definen los derechos y libertades del ciudadano. Por tanto, ese artefacto político que es un Estado se define a través de una realidad jurídica. El Estado se constituye a través de la ley y, por tanto, la **soberanía popular se expresa a través del Estado de Derecho**.
 - Queda deducido, pues, que la democracia es Estado de Derecho, y el Estado de Derecho es la expresión de la soberanía popular en un ejercicio de autogobierno.

El ciberespacio como territorio pre(¿anti?)-democrático

Sin soberanía no hay Estado de Derecho; sin derecho no hay democracia



El ciberespacio como territorio pre(¿anti?)-democrático

La soberanía reside en el pueblo; ¿hay pueblo en el ciberespacio?

- El Estado es un agrupamiento jurídico de ciudadanos que se autogobiernan.
- Tradicionalmente, el Estado, además de asentarse en el Derecho, se ha vinculado a unas coordenadas espaciales (y por tanto espacio-temporales) donde son de aplicación las leyes del Derecho emanado de la soberanía popular y que se constituye, por tanto, en el **espacio donde se ejerce esa soberanía**. Ese conjunto de coordenadas espacio-temporales es un **territorio**, que por lo general es la dimensión física que abarca la jurisdicción del Estado.
- El concepto territorio, a pesar de su raíz semántica, no representa únicamente a la tierra, sino a todo el conjunto de límites espacio-temporales donde, en virtud de la intersección entre Estados de Derecho en el mundo, alcanza la jurisdicción de un conjunto de ciudadanos agrupados en un pueblo soberano.
- El territorio del Estado, donde se aplican las leyes emanadas de la soberanía popular, está compuesto por el **espacio terrestre**, el **espacio aéreo**, el **marítimo**.
- Quedan, como áreas no jurisdiccionales, el espacio ultraterreste (espacio exterior al planeta Tierra, cosmos) y el ciberespacio.

El ciberespacio como territorio pre(¿anti?)-democrático

La soberanía reside en el pueblo; ¿hay pueblo en el ciberespacio?

- La Constitución Española, carta jurídica que define al Estado emanado de la soberanía del pueblo español, no menciona al ciberespacio; aunque tampoco explícitamente a los otros territorios de soberanía: están repartidos irregularmente como “áreas de control” por diversos artículos constitucionales. Sí se definen la “indisoluble unidad de la Nación española” (art. 2) y la “integridad territorial de España” (art.8).

Artículo 132

2. Son bienes de dominio público estatal los que determine la ley y, en todo caso, la zona marítimo-terrestre, las playas, el mar territorial y los recursos naturales de la zona económica y la plataforma continental.

Artículo 149

1. El Estado tiene competencia exclusiva sobre las siguientes materias:

20.ª Marina mercante y abanderamiento de buques; iluminación de costas y señales marítimas; puertos de interés general; aeropuertos de interés general; control del espacio aéreo, tránsito y transporte aéreo, servicio meteorológico y matriculación de aeronaves.

El ciberespacio como territorio pre(¿anti?)-democrático

La soberanía reside en el pueblo; ¿hay pueblo en el ciberespacio?

ESTRATEGIA DE **SEGURIDAD NACIONAL**

2017



El ciberespacio, el espacio marítimo y el espacio aéreo y ultraterrestre son espacios comunes globales. Conectan el mundo y permiten el libre flujo de personas, bienes, información, servicios e ideas. Son espacios abiertos a todos los Estados, también a los particulares, a nadie se le puede excluir de su disfrute. Se caracterizan por **no tener fronteras físicas, la ausencia general de soberanía y jurisdicción por parte de los Estados, la difícil atribución de acciones delictivas y su débil regulación.**



PRINCIPALES CARACTERÍSTICAS

Apertura geográfica y funcional

Ausencia de soberanía y jurisdicción por parte de los Estados

Facilidad de acceso

Dificultad de atribución de las acciones que en ellos tienen lugar

El ciberespacio como territorio pre(¿anti?)-democrático

La soberanía reside en el pueblo; ¿hay pueblo en el ciberespacio?

- Por tanto, de las leyes que regulan la convivencia en el Estado de Derecho que emana de la soberanía popular, se deduce que:
 - El pueblo está representado en una Nación indisoluble asociada a un territorio dotado de integridad, es decir, de contornos y límites territoriales.
 - La integridad territorial abarca al espacio terrestre, al marítimo y al aéreo.
 - Deja fuera al espacio ultraterrestre
 - Deja fuera al ciberespacio.

que, por definición, no son pues espacios soberanos

Si no son espacios soberanos, ¿son espacios democráticos?

Si no son espacios soberanos, ¿son espacios donde se ejerzan los derechos y libertades públicas, que ya hemos visto quedan definidas por el Estado de Derecho, que a su vez emana de la soberanía popular?

El ciberespacio como territorio pre(¿anti?)-democrático

Huevo/Gallina: ¿Es la libertad pre-existente al Estado de Derecho?

- En las democracias reguladas por Estados de Derecho, la libertad es una cuestión de derechos y de obligaciones:
 - Hay derechos que son innatos e inalienables, que no se conceden jurídicamente, aunque tengan trasposición jurídica: los derechos fundamentales.
 - Hay derechos que quedan definidos y expresados por las leyes, que emanan de la soberanía popular: derechos civiles y políticos.
 - Hay obligaciones que determinan la contribución del ciudadano al espacio de convivencia regido por las leyes democráticas.
 - La **combinación entre derechos fundamentales, civiles y políticos, y obligaciones legales, define la libertad entendida democráticamente**, más allá de cualquiera otra acepción filosófica.
 - Por tanto, el ser humano es ontológicamente libre en sus derechos inalienables (la 'potencia' aristotélica), pero para que esa libertad tenga expresión democrática (el 'acto' aristotélico) tiene que estar definida por el Derecho. La **libertad democrática tiene contorno y límite**: en la libertad del otro.

El ciberespacio como territorio pre(¿anti?)-democrático

El ciberespacio como espacio político

- De lo anterior se infiere que un espacio de convivencia sin presencia del Estado de Derecho será un espacio, y podrá haber convivencia, pero no será democrático, puesto que
 - no estará gobernado;
 - y ni no está gobernado, no es expresión de soberanía;
 - y si no se expresa la soberanía, el pueblo no es sujeto político;
 - y si el pueblo no es sujeto político, no hay ciudadanía;
 - y si no hay ciudadanía, no hay sujetos políticos individuales.
- Siguiendo, pues, a la Estrategia de Seguridad de España 2017, el ciberespacio es un espacio de convivencia **a-democrático**, puesto que no es un espacio jurisdiccional donde se exprese el Derecho de ningún sujeto de soberanía.
 - Si no es un espacio jurisdiccional, no tiene regulación.
 - Si no tiene regulación, no tiene libertad democrática.

El ciberespacio como territorio pre(¿anti?)-democrático

El ciberespacio como espacio político

- La alternativa a la a-democracia del ciberespacio sería que se le considerara un territorio poblado por **identidades (digitales)** que conforman un **pueblo (digital)** como sujeto político de soberanía, que expresa su **Derecho como autorregulación**.
 - La regulación no lo haría automáticamente democrático, pues para ello a los derechos fundamentales habría que añadirle derechos civiles y políticos, que por definición habría que regular: ¿alguna forma no-normativa de autorregularlo?
 - Además, para ser democrático, el ejercicio de las libertades públicas en un espacio autorregulado debería emanar de la soberanía popular de tal forma que por sí sólo (autorregulación) generara los límites de derechos y obligaciones que definen a la libertad: ¿algún ejemplo en la historia de un sistema autorregulado que no genere abusos de unas partes sobre otras?
- Tal vez el error de concepto es definir la <<**libertad del ciberespacio**>> como la ausencia de regulación.
 - Podría ser esa libertad un tipo de libertad, pero no será una libertad democrática.
 - Al ser autorregulada, los límites se establecerán por colisión interpares, y entonces no operarán parámetros de igualdad o de fraternidad, sino de fuerza para desplazar el límite a una posición más favorable para el sujeto capaz de ejercerlas.

El Ciberespacio como territorio de soberanía popular

Regular para democratizar. La libertad desde el Estado de Derecho

- De lo analizado deducimos:
 - La autorregulación sin mecanismos que garanticen la libertad conduce al abuso de la fuerza, fuerza expresable de diversas formas, intensidades, y vectores.
 - Esos mecanismos de regulación a introducir sobre una hipotética autorregulación implicarían el ejercicio de una determinada voluntad, que sería expresión del pueblo, y por tanto soberana.
 - Al introducir esos mecanismos, ya se estaría regulando, y por tanto encaminando al ciberespacio hacia una gobernanza, pero
 - ¿es posible la gobernanza del ciberespacio por un pueblo soberano global que establece un nuevo **Estado de Derecho del Ciberespacio** a partir de un sentimiento compartido de **Nación Digital Global**, traducido entonces a través del ejercicio de la soberanía?
 - ¿o en cambio, si reconocemos que la democratización del ciberespacio pasa por su **gobernanza a través del Estado de Derecho**, es más sencillo y viable considerar al ciberespacio como **un territorio más de las soberanías nacionales**?

a-regulación vs. regulación

autorregulación => regulación

Nacional Digital Global vs. Estados Nacionales Digitales

El Ciberespacio como territorio de soberanía popular

Regular para democratizar. La libertad desde el Estado de Derecho

- La **Gobernanza Democrática del Ciberespacio** requiere, por tanto, el desarrollo de un Estado de Derecho del ciberespacio.
 - Y el Estado de Derecho es una expresión de Soberanía
 - Por tanto la Gobernanza Democrática del Ciberespacio requiere un **sujeto político de soberanía popular**.
- A efectos didácticos, supongamos que una hipotética Nacional Digital Global que desarrolle un Estado de Derecho Universal del Ciberespacio Global es incapaz de fructificar en las condiciones actuales de gobernanza internacional basadas en Estados-Nación y en organismos de cooperación y/o integración supranacional de estos Estados-Nación (p.ej. ONU, UE).
 - O supongamos, a los mismos efectos, que si existieran unos Poderes Públicos Universales que tradujeran la voluntad popular de hipotético sujeto político universal de la Nación Digital Global en términos de gobernanza democrática, actuarían sobre el Ciberespacio Global desarrollándolo hacia un Estado de Derecho Universal.
 - En cualquiera de los dos supuestos, cualquiera de las dos gobernanzas (la universal o la nacional) deberían ser capaces de definir un **ciberespacio como territorio de ejercicio de la soberanía digital popular**, ya fuera universal o nacional.

Topografía de CiberEspaña

¿Cómo definimos un ciberespacio para su gobernanza democrática?

- En primera instancia, definamos ciberespacio como un **territorio donde dispositivos electrónicos están conectados en redes transmitiendo información digital**. Es una definición generalista, pero operativa.
 - En unos casos esos dispositivos operarán automáticamente sin intervención de usuarios humanos y en otros su comportamiento se derivará de comandos introducidos por la acción de usuarios humanos.
 - En unos casos las conexiones serán entre dispositivos y para dispositivos (máquina-a-máquina) y en otra los dispositivos serán una interface para conectar humanos-a-humanos o humanos-a-máquina, por ejemplo en el contexto de servicios digitales.

Topografía de CiberEspaña

¿Cómo definimos un ciberespacio para su gobernanza democrática?

- Comencemos por lo sencillo: en tanto territorio de soberanía popular, el ciberespacio debería ser un espacio coordinado. ¿De qué dispone España actualmente para satisfacer ese requisito?
 - **INFRAESTRUCTURA DE CIBERESPAÑA** (algunos ejemplos sin ánimo de exhaustividad):
 - Cableado de transmisión de rango de señal eléctrica, radioeléctrica, óptica... dedicado a la transmisión de información digital.
 - Espectro radioeléctrico español.
 - IP en España asignados para IPv4 e IPv6 por la IANA (Internet Assigned Numbers Authority).
 - Redes backbone.
 - Instancias de servidores raíz DNS.
 - **DISPOSITIVOS:**
 - Todas las interfaces mediante las cuales las personas se conectan a redes de información digital a través de la infraestructura de CiberEspaña
 - Todos los dispositivos conectados a redes de información digital a través de la infraestructura de CiberEspaña que realicen operaciones máquina o máquina-a-máquina.
 - **PERSONAS:** Todas las personas con personalidad jurídica reconocida para desarrollar actividades en CiberEspaña, unas con nacionalidad, otras con residencia, otras con estancia.

Anomalías de un ciberespacio a-democrático

Cuando la RGPD no es suficiente

- ¿Por qué el ciberespacio debería ser un espacio social donde se ejerza soberanía?
 - Porque allí se están desarrollando numerosas (y cada vez más) de las conductas sociales que implican interacción entre el ejercicio de las libertades públicas individuales, y al configurar un espacio social de convivencia ese ejercicio, en las democracias está regulado por la ley.
- No basta con introducir regulaciones puntuales (como el RGPD)
 - En el ciberespacio las personas no interactúan actualmente como sujetos políticos, y por tanto como tenedores y receptores de derechos y libertades.
 - No hay un correlato biunívoco entre persona física o jurídica y persona digital: el concepto de persona digital no está jurídicamente definido.
 - Salvo en los casos específicos de servicios digitales o de conexiones que incorporan mecanismos de verificación de identidad (p.ej banca electrónica), una persona física puede operar en el ciberespacio a través de varias interfaces con varias identidades digitales ¿Nos imaginamos personas físicas en el espacio terrestre conduciendo un coche sin DNI ni permiso de conducir, sin matrícula ni permiso de circulación en el vehículo; o pilotando un avión sin licencia de piloto en una aeronave sin matrícula ni certificado de aeronavegabilidad?
 - El Reglamento General de Protección de Datos es una extensión del Estado de Derecho de los espacios de soberanía regulada debido a que tiene capacidad de establecer una conexión entre personalidad jurídica de la persona física/jurídica y actos llevados a cabo por medios digitales.

Anomalías de un ciberespacio a-democrático

Cuando la RGPD no es suficiente

- No basta con introducir regulaciones puntuales (como el RGPD o la LSSICE)
 - Al contrario de la opinión más general extendida el elemento principal respecto de la falla de gobernanza democrática del ciberespacio **no es el anonimato**, sino la ausencia de garantía jurídica en la biyección entre persona física/jurídica y persona digital o, dicho de otra manera, que la persona digital no tiene personalidad jurídica y, por tanto, no es sujeto de derechos y obligaciones; y, de suyo, no participa del sujeto de soberanía que es pueblo.
 - El problema no es el anonimato: en otros territorios de soberanía (terrestre, marítimo, aéreo) una persona física puede circular anónimamente pero su trazabilidad identitaria está garantizada en su personalidad jurídica, de manera que tanto en el ejercicio de derechos como de obligaciones puede actuar como sujeto político.
 - A falta de una **personalidad jurídica para la persona digital**, los servicios digitales realizan “simulacros” contractuales sobre los que no hay capacidad de cumplimiento (de *enforcement*), puesto que podrían no estar tratando con la extensión digital biyectiva de una persona física/jurídica: los términos y condiciones de servicio que son equivalentes a un contrato, pueden ser suscritos por un alias operando a través de una interface (dispositivo) que tenga su IP enmascarada. ¿Aceptamos que en el espacio terrestre, o el aéreo, una persona viaje con documentación falsificada y no seamos capaces (ni siquiera bajo la protección de garantías de un procedimiento judicial) de hacer trazabilidad de su origen o personalidad jurídica aunque descubramos que ha falseado?

Conceptualizando la soberanía en CiberEspaña

¿Cuál es el propósito?

- Establecer el ciberespacio español como un territorio más de ejercicio de la soberanía popular.
- Por tanto crear un territorio de derechos y libertades públicas dotando de un Estado de Derecho del Ciberespacio a ese nuevo territorio.
- Posibilitar el ejercicio de derechos, obligaciones y libertades públicas a sujetos con personalidad jurídica: las **Personas Digitales**.
- Con un Estado de Derecho del Ciberespacio donde Personas Digitales realizan conductas que interaccionan con las de otras Personas Digitales, garantizar los mecanismos para una gobernanza democrática a través de la acción de los poderes públicos, que son una expresión de la soberanía popular: garantías administrativas, garantías legales (seguridad jurídica), garantías judiciales, ciberseguridad, ciberdefensa...
- Al igual que ocurre en los distintos territorios de soberanía, el Estado de Derecho no proporciona espacios libres de incertidumbre, ni de criminalidad, pero arbitra mecanismos mínimos (no ideales) para ejercer la libertad en convivencia colectiva.
- Y ¿quién sabe?, un ciberespacio democrático puede llevar a mayor democracia.

Conceptualizando la soberanía en CiberEspaña

¿Cómo lo hacemos?

- Para avanzar hacia CiberEspaña nada mejor que recurrir a la **Constitución Española de 1978**, que no establece la soberanía en términos de territorio sino en términos de un pueblo (art.1) constituido en un constructo de expresión de la soberanía popular que es la Nación (art.2).
- La idea es, por tanto, que cada personalidad jurídica española, además de su forma analógica (persona física o persona jurídica) tenga correlato jurídico en una persona digital que esté indubitadamente identificada, tanto ella como sus interfaces,
- No se trata de vulnerar la privacidad ni la libre circulación: ambos son derechos fundamentales (por tanto, ni siquiera tienen que ser concedidos, sino reconocidos, garantizados y protegidos por el ordenamiento jurídico – arts. 18 y 139 CE) que formando parte del Estado de Derecho en los territorios de soberanía no pueden por menos que aplicarse al ciberespacio como (nuevo) territorio soberano.
 - Al contrario de muchas de las narrativas circulando, la privacidad no implica “carencia de identidad verificable” u “operar socialmente con un alias o un identidad falsa”: la privacidad es la protección de la intimidad personal, que no puede ser quebrada salvo por mandato judicial motivado ante la presunta vulneración de la ley.

Conceptualizando la soberanía en CiberEspaña

¿Cómo lo hacemos?

- Tampoco se trata de implantar en Internet (que es la arquitectura base del ciberespacio) un sistema de control ni de censura, sino de garantías:
 - No implica el control del contenido circulando por Internet, ni su seguimiento o fiscalización.
 - Aducir que regular la presencia de personas digitales en el ciberespacio es equivalente a controlar lo que dicen o piensan, a fiscalizar qué tipo de contenidos comparten esas personas, o que actividades digitales realizan, es tan peregrino como afirmar que el hecho de que un periódico esté constituido en una persona jurídica con un CIF, formada a su vez por personas física asociadas, que operan en el tráfico social a través de una serie de regulaciones, implica que el sistema administrativo o de gobernanza implantado está “controlando las noticias” que el periódico publica.
 - La directriz de diseño de CiberEspaña no estaría basada en introducir controles, sino garantía, seguridad jurídica, que son la piedra angular del Estado de Derecho, la que permitirá la residencia en el ciberespacio de personas digitales en un espacio de convivencia democrático.

Esquemática de un modelo de criptored para la gobernanza

La dificultad no es tecnológica, sino conceptual

- Por más que la tecnología para desarrollar e implantar CiberEspaña pueda llevar complicaciones, el **obstáculo más marcado es conceptual**: tener claro un modelo interpretativo específico basado en el Estado de Derecho y en la Constitución Española en un ecosistema narrativo que, en relación con Internet, está dominado por visiones ideológicas (o interesadas) que consideran que debería existir una “excepcionalidad jurídica” en el ciberespacio, excepcionalidad básicamente reducida a
 - equiparar “libertad” con ausencia de regulación
 - equiparar “privacidad” con “anonimato”.

Esquemática de un modelo de criptored para la gobernanza

Elementos de diseño

- Un Documento Nacional de Identidad Digital. ¡Enhorabuena!, ¡ya lo tenemos!
 - Que permite que todas las personas físicas (y través de un NIFe, también las jurídicas) tengan un correlato identificativo, de naturaleza criptográfica, para su Persona Digital.
- La vinculación del DNle a todos los dispositivos que se utilicen como interface para acceder al ciberespacio.
 - No es más complicado que los certificados digitales criptográficos ampliamente en uso.
- Un procedimiento que asegure que la identificación de la Persona Digital se produce en el punto más bajo (más proximal al primer eslabón de la secuencia de conducta digital de la persona) de acceso al ciberespacio.
 - No sirve que la persona se autentique en servicios digitales, como ya se hace.
 - No sirve que la persona se autentique para conectarse a Internet, como se hacía en los noventa del s.XX con los modems que funcionaban por marcación por tono.
 - Tiene que ser un mecanismo anclado al “operador de infraestructura” y además automático, sin interacción del usuario una vez haya sido configurado: que “autentique” y mantenga “logada” mientras dure la presencia de la persona digital en CiberEspaña.
- Dispositivos máquina dotados de identificador criptográfico.
- Un mecanismo de seguridad jurídica, que garantice que ningún derecho es violentado (ni la privacidad, ni la libre circulación, entre otros), ni por parte de proveedor ni por parte de administración pública, salvo actuación judicial motivada.

Esquemática de un modelo de criptored para la gobernanza

La criptored de CiberEspaña

- Personas Digitales identificadas mediante tecnología criptográfica, relacionadas con dispositivos igualmente dotados de identificador criptográfico, en un ecosistema de máquinas con ID criptográfico, en donde todas ellas están llevando a cabo acciones muchas de las cuales requieren unos reconocimiento e identificación mutuos automáticos, se parece demasiado a una criptored desarrollada a través de un **modelo blockchain**.
- Por tanto, CiberEspaña requiere de la habilitación de una criptored basada en blockchain donde los nodos sean:
 - Principales: Códigos criptográficos derivados de la Firma Digital del DNle o el CIFE. Es el equivalente digital al DNI o pasaporte.
 - (Probablemente) Supernodos: proveedores de infraestructuras de red y administraciones públicas.
 - Secundarios (o tal vez alternativamente, conexiones tokenizadas fuera de la blockchain): Códigos criptográficos de interfaces máquina derivados de DNle o CIFE: inicialmente todas las máquinas estarán operando por cuenta de una persona física o jurídica. Este planteamiento es válido así mismo para todas las máquinas de la infraestructura de red. Es el equivalente digital a la matrícula de un coche, avión o barco.

Esquemática de un modelo de criptored para la gobernanza

La criptored de CiberEspaña

- En la blockchain de CiberEspaña los nodos ejecutarían operaciones sobre la infraestructura de red (p.ej. una conexión de un smartphone con un router inalámbrico es una operación sobre la infraestructura de red).
 - La IP puede continuar estando asignada a un dispositivo que se conecta a red a través de un router: hoy en día se desconoce la identidad de la persona física que realiza la conexión (sólo que está asociada a un número de teléfono). En el modelo de CiberEspaña, cada conexión es una transacción cifrada donde el dispositivo es un nodo de la cadena de bloques provisto de un identificador criptográfico finalmente asociado a un DNle o CIFE.
- Al contrario de lo que habitualmente ocurre con infraestructuras blockchain asociadas a criptomonedas como Bitcoin, que son cadenas de bloques públicas, CiberEspaña sería una **cadena de bloques privada**, que mantiene protegida una base de datos distribuida de nodos y transacciones basada en la total inter-confiabilidad de los nodos principales (en nuestro modelo, personas físicas y jurídicas) pero que puede operar en un ecosistema, como la Internet global, no sometido a las mismas reglas de confiabilidad.

Esquemática de un modelo de criptored para la gobernanza

La criptored de CiberEspaña

- En ese modelo de criptored para CiberEspaña quien quisiera podría:
 - Seguir navegando anónimamente, incluso utilizar Tor, VPNs o cualquier otro anonimizador.
 - Abrirse 'n' perfiles con 'z' alias en redes sociales para ocultar su identidad administrativa real.
 - Cifrar cualquiera de sus comunicaciones con encriptado fuerte (incluso con encriptado militar).
 - Las diferencias entre todas estas acciones en la actualidad y en el modelo de CiberEspaña radicarían en que:
 - Todas las personas digitales podrían ejercer su libertad (derechos y obligaciones) sin que otros pudieran vulnerarlas con impunidad: el sistema sería trazable en términos de **rendición de cuentas**.
 - Aplicaría la misma protección de privacidad que proporciona el RGPD o cualquier otra legislación similar.
 - Tendría la misma protección de derechos individuales que cualquier otro territorio de soberanía.
 - Habilitaría a las autoridades judiciales para el "**levantamiento del velo**" en caso de vulneración del ordenamiento jurídico.

¿CiberEspaña sin CiberEuropa? ¿Sin CiberMundo?

- Inicialmente no hay problema tecnológico en hacer convivir una arquitectura de internet basada en blockchain en el seno de una arquitectura de internet global basada en otros modelos: de hecho, el blockchain de Bitcoin, entre otros muchos, convive en Internet.
- En el modelo de CiberEspaña, ¿que ocurriría con cualquier persona o máquina sin credenciales digitales expedidas en CiberEspaña que realice conexiones con el ciberespacio español?
 - Algo así como una proyección de lo que ya sucede con la entrada y circulación de personas, mercancías o capitales en el resto de territorios de soberanía: una firma digital válida que les permitiera conectar, entrar y permanecer (cualquiera de los procedimientos actuales de autenticación criptográfica serviría).
 - ¿Sería ideal que todos los países tuvieran un ciberespacio soberano con Personas Digitales y dispositivos asociados, de manera que sus conexiones en otros ciberespacios soberanos fuera trazable y permitiera la rendición de cuentas? Eso implicaría una CiberFrancia, CiberItalia, CiberEuropa... y una infraestructura global compartida de CyberWorld.
 - Otra cuestión sería que articular e implantar CiberEspaña no sería un asunto totalmente nacional: probablemente requería convergencia comunitaria con la Unión Europea.

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

**XIII
JORNADAS
STIC
CCN-CERT**

CCN-cert
centro criptológico nacional