Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

ESTRATEGIA NACIONAL FRANCESA

PARA LA SEGURIDAD DEL ÁMBITO DIGITAL

Francia está plenamente comprometida en la transición digital. Con una gran población ampliamente conectada y una economía digital en sostenido crecimiento, Francia dispone de talentos y ventajas a la vanguardia de la innovación europea y mundial.

El mundo digital es también un espacio de competición y enfrentamiento. Competencia desleal y espionaje, desinformación y propaganda, terrorismo y criminalidad encuentran en el ciberespacio un nuevo ámbito de expresión.

La «República digital en hechos», voluntad del Gobierno, ha de promover nuestros valores, nuestra economía y ha de proteger a los ciudadanos. Trabajar para la seguridad digital, es favorecer el desarrollo de un ciberespacio yacimiento de crecimiento y lugar de oportunidades para las empresas francesas; es afirmar nuestros valores democráticos; es por fin preservar la vida digital y los datos personales de los franceses.

Mi aspiración en este ámbito es máxima. La estrategia nacional francesa para la seguridad del ámbito digital debe apoyarse en particular sobre la formación y sobre la cooperación internacional, y debe ser respaldada por el conjunto de la comunidad nacional: el Gobierno, las administraciones, las colectividades territoriales, las empresas y más ampliamente sobre todo nuestros compatriotas. Es asunto de todos.

Responder a los retos en torno a la seguridad del mundo digital es un factor clave del éxito colectivo. Quisiera que esta estrategia nacional francesa para la seguridad del ámbito digital desencadene un proceso dinámico a la vez protector y liberador de energías.

Manuel Valls
Primer ministro

Traducción de cortesía del prólogo de Manuel Valls, Primer Ministro de Francia, a la estrategia nacional para la seguridad del ámbito digital

ESTRATEGIA NACIONAL FRANCESA PARA LA SEGURIDAD DEL ÁMBITO DIGITAL

La digitalización de la sociedad francesa se acelera: el rol digital en los servicios, los objetos, los trabajos no deja de incrementarse y se ha convertido en una cuestión nacional fundamental. Esta transición digital crea un entorno propicio para la innovación y el crecimiento, pero también conlleva riesgos para el Estado, los actores económicos y los ciudadanos. Cibercriminalidad, espionaje, propaganda, sabotaje o explotación excesiva de datos personales representan una amenaza para la confianza y la seguridad en el ámbito digital y exigen una respuesta colectiva y coordinada en torno a cinco objetivos estratégicos.

 # Intereses fundamentales, defensa y seguridad de los sistemas de información del Estado y de las infraestructuras críticas, crisis informática mayor.

Al desarrollar un pensamiento estratégico autónomo, respaldado por un conocimiento técnico de primer rango, Francia creará un dispositivo para defender sus intereses fundamentales en el ciberespacio del futuro. Paralelamente, continuará reforzando la seguridad de sus redes críticas y su capacidad de resistencia en caso de ataque grave mediante el desarrollo de cooperaciones tanto a escala nacional con actores privados como a escala internacional.

 # Confianza digital, vida privada, datos personales, ciberataques.

Para que el ciberespacio permanezca un espacio de confianza para todo tipo de empresas y para los particulares, se adoptarán medidas de protección y de reacción. La protección implicará una mayor vigilancia de los poderes públicos en el uso de los datos personales y el desarrollo de una oferta de productos de seguridad digital adaptada al público en general. La reacción se articulará en torno a un dispositivo de asistencia a las víctimas de ciberataques que brindará una respuesta técnica y judicial a tales actos.

 # Sensibilización, formaciones iniciales, formaciones continuas.

La concienciación individual frente a los riesgos ligados a la digitalización de la sociedad sigue siendo insuficiente. Ante este hecho, se reforzará la sensibilización de los colegiales y estudiantes. Además, con el fin de dar respuesta a la creciente demanda de empresas y administraciones en materia de ciberseguridad, se desarrollará la formación de expertos en este ámbito.

 # Entorno de las empresas del sector digital, política industrial, exportación e internacionalización.

El crecimiento de los mercados del sector digital a escala mundial y el consiguiente aumento de las exigencias de seguridad constituyen una oportunidad de diferenciación para los productos y servicios franceses que dispongan de un nivel de seguridad digital adaptada a los usos. A través del apoyo a la inversión, a la innovación y a la exportación, pero también a través de la contratación pública, el Estado desarrollará un entorno propicio a las empresas francesas del sector digital que propondrá una oferta de productos y servicios seguros.

 # Europa, soberanía digital, estabilidad del ciberespacio.

La regulación de las relaciones en el ciberespacio se ha convertido en un tema de suma importancia en las relaciones internacionales. Francia promoverá, junto con los Estados miembros que así lo deseen, una hoja de ruta para la soberanía digital de Europa. Reforzará asimismo su influencia en las instancias internacionales y respaldará a los países voluntarios menos protegidos en la implementación de dispositivos de ciberseguridad con el fin de contribuir a la seguridad global del ciberespacio.

La seguridad del sector digital consolida el proyecto de República digital. El Estado desempeña un papel fundamental al elaborar esta estrategia y al lanzar una dinámica que de ahora en adelante deberá contar con el apoyo de los profesionales del sector digital, los responsables públicos y privados y los ciudadanos.

RESUMEN

INTRODUCCIÓN

La transición digital de Francia está en marcha. Las redes están omnipresentes en el funcionamiento del Estado, en la actividad económica y en la vida cotidiana de los ciudadanos.

Como vehículo de nuevos usos, nuevos productos y nuevos servicios, el ámbito digital es un factor de innovación. Engendra una mutación de la mayoría de las profesiones. Transforma los sectores de actividad y las empresas para aportarles más flexibilidad y competitividad. Beneficiados por un lado, estos sectores se encuentran también simultáneamente más expuestos a las amenazas propias del ámbito digital.

Privarse del entorno digital o no poder acceder al mismo conduce a una forma de exclusión económica y social. Asimismo, un Estado que no dispusiera de la autonomía necesaria en el sector digital vería su soberanía amenazada.

Para que el ámbito digital siga siendo un espacio de libertad, intercambios y crecimiento, es necesario que la confianza y la seguridad estén establecidas y que sean defendidas. Solo un esfuerzo colectivo y coordinado puede permitir alcanzar este objetivo.

* *
*

A comienzos de 2010 se elaboró una primera estrategia de ciberseguridad de Francia y se publicó a principios de 2011, poco después de que se descubriera un ataque informático con fines de espionaje contra los ministerios de economía y finanzas. Presentes desde hacía varios meses, los atacantes habían tomado el control del centro de una de las redes del ministerio y recopilaban regularmente información de índole política, económica y financiera.

Este tipo de ataque informático apunta a numerosas empresas francesas, de todos los tamaños, y en todos los sectores de actividad. Asimismo, las empresas son el blanco de estafas de todo tipo, como por ejemplo la infección de un software malévolo que deja inservibles los archivos de la empresa hasta que se paga un rescate por medios difícilmente rastreables.

En paralelo, se multiplican las intrusiones informáticas que pretenden sustraer información personal (identidad, datos de identificación a sitios comerciales, datos bancarios). Se trata, por lo general, para estos delincuentes de cometer delitos idénticos a los conocidos en el mundo material —robos, estafas, chantaje— solo que de forma más industrializada, con algo menos de riesgo de ser identificado y juzgado. El crimen organizado ha aprovechado la ventaja de las redes de comunicaciones electrónicas. Sus capacidades técnicas son cada vez mayores hasta el punto de estar en posición de llevar a cabo, para sí mismos o como contratistas por hibridación, actos de sabotaje o de secuestro de herramientas de producción.

Se desarrollan campañas de acoso en las redes sociales, como casos de estafas a la buena voluntad que llevan víctimas crédulas a transferir dinero al extranjero.

Las numerosas desfiguraciones de sitios web, como las de los entidades territoriales, tras los atentados de enero de 2015 o, unas semanas más tarde, el cibera-

taque contra un medio de comunicación francés de proyección internacional, pusieron de manifiesto la voluntad y la capacidad de grupos organizados de dejar fuera de servicio recursos informáticos que sustentan nuestra vida cotidiana.

La llamada «situación de la amenaza» definida en 2010 ha resultado ser acertada. La amenaza se ve hoy acentuada por el aumento de las capacidades de los atacantes, la proliferación de las técnicas de ataque y el desarrollo en el ciberespacio de la criminalidad organizada.

Pero una amenaza de otra naturaleza se extiende. La de la captación de riquezas digitales por parte de un oligopolio de empresas que utilizan su posición dominante para obstaculizar la llegada de nuevos protagonistas y captar el valor añadido de esta economía naciente, que explotará los datos para inventar nuevos servicios, mejorar nuestro día a día o volver más accesibles los servicios públicos. Entre esos datos figuran a la cabeza nuestros datos personales, incluidos los de nuestra vida privada. El control de estas masas de datos abre la puerta a la desestabilización económica y a sofisticadas formas de propaganda o de orientación de las convicciones y des los hábitos. En este sentido, esta amenaza incumbe, por su amplitud nacional y sus aspectos estratégicos, a la defensa y a la seguridad nacional.

* *
*

Frente a estos riesgos lamentablemente confirmados, ya se han logrado significativos avances.

Como anunciado en el libro blanco sobre la Defensa y la Seguridad Nacional de 2008, se creó en 2009 una agencia nacional para tratar los ataques informáticos y proteger los sistemas de información del Estado y de las infraestructuras críticas.

Una política industrial a favor de la industria nacional de ciberseguridad se inscribe, por ejemplo, en el programa de inversiones de porvenir y en el marco del plan «Industria del futuro».

El Parlamento francés aprobó en 2013 las medidas propuestas por el Gobierno con vistas a reforzar la seguridad informática de los operadores de importancia vital y de los que participan en sus sistemas de información más críticos.

La postura de Francia está respaldada en todas las instancias internacionales, y especialmente en la Organización de las Naciones Unidas (ONU) que reconoció en 2013 la aplicación al ciberespacio del derecho internacional. Por otro lado, los servicios del Estado han establecido relaciones bilaterales operativas con varios países.

Los ministerios han tomado conciencia del impacto político y técnico de las tecnologías de la información en sus misiones y en la actividad de su administración, y se dotan de coordinadores encargados de los temas relacionados con lo digital y su seguridad. Se ha elaborado una política de seguridad de los sistemas de información del Estado y se está aplicando progresivamente.

Los años venideros deben permitir cosechar los beneficios de las acciones emprendidas y ampliar el perímetro de la acción pública y de los actores implicados. Es hora de comprobar y de compartir esta comprobación: la defensa y la seguridad del ámbito digital incumben a la comunidad nacional y no solamente a la acción del Estado.

* *
*

Hasta estos últimos años, nuestra defensa y nuestra seguridad nacional dependían de los conocimientos, del comportamiento y de las decisiones de los hombres y mujeres que tenían acceso a las instalaciones, a los equipos los más sofisticados, los más protegidos y los más secretos. Cuando está emergiendo una sociedad masivamente conectada, parte de esta responsabilidad recae sobre todos los franceses. Un objeto conectado o un servicio que no ha sido asegurado lo suficiente por sus desarrolladores, la negligencia de un responsable en cuestión de seguridad de los sistemas de información, el comportamiento descuidado de un proveedor o el de

un empleado que mezcla sin precaución alguna vida privada y vida profesional pueden acarrear pérdidas de disponibilidad, de confidencialidad o de integridad de información esenciales, interrupciones de actividad y pérdidas económicas, accidentes industriales y pérdidas de vidas humanas o catástrofes ecológicas y perturbaciones del orden público, susceptibles de repercutir sobre la vida de la nación.

En efecto, nunca antes la estabilidad de nuestro porvenir, impulsado por el ámbito digital, había sido tan dependiente de la responsabilidad individual de los ciudadanos y de la responsabilidad colectiva de tres comunidades de actores.

Una primera comunidad tiene la responsabilidad de proponer y de implementar tecnologías, productos y servicios dotados del nivel de seguridad adaptado a los usos y capaces de contrarrestar los riesgos identificados. Los principales actores de esta comunidad son los investigadores, los inventores de productos y servicios y los integradores, las empresas del sector de la ciberseguridad, los operadores de redes de comunicaciones electrónicas, los proveedores de acceso a Internet o los proveedores de servicios informáticos remotos.

La segunda comunidad tiene la responsabilidad de proteger a la nación de los depredadores del ámbito digital. Además de la elaboración de políticas de ciberseguridad, se trata de llevar a cabo de forma voluntarista una política de desarrollo de las competencias técnicas necesarias y de crear un ecosistema de confianza que acompañe la transformación digital de la sociedad, defendiendo a los ciudadanos, nuestros valores y nuestros intereses en el ciberespacio. Quien tiene esta responsabilidad está obligado a expresar su postura a favor de soluciones de seguridad cualificadas y a promover la industria nacional, incluidas las exportaciones. Esta comunidad está constituida por los que detienen un mandato electoral, el Gobierno, las administraciones centrales y territoriales y los sindicatos.

La tercera comunidad tiene la responsabilidad de utilizar de manera acertada los servicios y las tecnologías disponibles, de tomar decisiones razonadas y de evitar las conductas de riesgo en los actos de la vida digital. Esta comunidad está integrada por todos los usuarios, empresarios actores de la sociedad civil y ciudadanos.

Los compromisos sinalagmáticos asumidos por cada uno de los actores permitirán que Francia se beneficie plenamente de las aportaciones del ámbito digital, transforme en ventaja competitiva nacional las decisiones relativas a la seguridad digital, percibidas hoy en día como una restricción económica, la exigencia de métodos de trabajo rigurosos , y promueva nuestros valores, nuestros productos y nuestros servicios.

En el ciberespacio, el Estado asume la función de garantía de la libertad de expresión y de acción de Francia, así como garantiza la seguridad de sus infraestructuras críticas en caso de ataque informático mayor (objetivo 1), protege la vida digital de los ciudadanos y de las empresas, lucha contra la cibercriminalidad (objetivo 2), asegura la sensibilización y la formación necesarias para la seguridad digital (objetivo 3), favorece el desarrollo de un ecosistema favorable a la confianza en el ámbito digital (objetivo 4) y fomenta la cooperación entre los Estados miembros de la Unión Europea en un sentido que impulse la emergencia de una soberanía digital europea, garante a largo plazo de un ciberespacio más seguro y respetuoso con nuestros valores (objetivo 5).

CINCO
OBJETIVOS
ESTRATÉGICOS

1

#INTERESES FUNDAMENTALES, DEFENSA Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DEL ESTADO Y DE LAS INFRAESTRUCTURAS CRÍTICAS, CRISIS INFORMÁTICA MAYOR

CUESTIONES FUNDAMENTALES

Francia es el blanco de ataques informáticos que socavan sus intereses fundamentales.

En la actualidad, cuando el blanco es el Estado, los operadores de importancia vital o empresas estratégicas, el agresor pretende instalarse de forma duradera en el sistema de información para sustraer datos confidenciales (políticos, diplomáticos, militares, tecnológicos, económicos, financieros o comerciales). Mañana, un atacante podría tomar el control de objetos conectados, interrumpir a distancia una actividad industrial o destruir su meta. Desde 2011, las administraciones y los proveedores de servicio competentes han tratado un centenar de ataques informáticos importantes, casi siempre de manera totalmente confidencial.

En paralelo, algunos ataques informáticos destinados a impactar la opinión pública acompañan las posiciones adoptadas por Francia a nivel internacional, sus operaciones militares o ciertos debates públicos. A título ilustrativo, las desfiguraciones de sitios web que siguieron los atentados dirigidos contra Francia a comienzos de 2015 tuvieron escaso impacto técnico pero sí un alcance simbólico deseado por los atacantes. En el mismo orden de ideas, el ciberataque contra un medio francés de comunicación internacional y que interrumpió el servicio también pretendía impactar las conciencias y favorecer la radicalización que conduce a actos terroristas. Además, este ataque puso de manifiesto la capacidad de atacantes determinados para perturbar el funcionamiento de una infraestructura de alto valor simbólico.

Desde hace unos años, varios Estados han movilizado su voluntad política y medios humanos, técnicos y financieros considerables a fin de llevar a cabo, contra nosotros, operaciones informáticas a gran escala en el ciberespacio.

Tanto si son conocidas por documentos públicamente revelados o puestas de manifiesto por ataques informáticos, los excesos de tales prácticas

« los excesos de tales prácticas afectan la credibilidad de algunos de estos Estados en el plano internacional y minan la confianza que sería natural atribuir a los productos y servicios digitales de sus empresas. »

afectan la credibilidad de algunos de estos Estados en el plano internacional y minan la confianza que sería natural atribuir a los productos y servicios digitales de sus empresas.

Por lo tanto, el riesgo cibernético, en tercera posición de las mayores amenazas para Francia en el Libro Blanco sobre la Defensa y la Seguridad Nacional de 2013, se ha reforzado y constituye un enorme desafío para el país.

OBJETIVO

Francia se dotará de los medios necesarios para defender sus intereses fundamentales en el ciberespacio. Consolidará la seguridad digital de sus infraestructuras críticas y la seguridad de sus operadores esenciales para la economía.

ORIENTACIONES

> **Estar en posesión de las capacidades científicas, técnicas e industriales necesarias para la protección de la información de soberanía, para la ciberseguridad y para el desarrollo de una economía digital de confianza.**

Se creará un grupo de expertos para la confianza digital, bajo la dirección de la Secretaría de Estado para la Economía Digital y de la autoridad nacional de seguridad de los sistemas de información.

Un grupo de expertos para la confianza digital reunirá con bastante frecuencia las administraciones competentes del Primer Ministro, de los ministerios de Educación Nacional, de Enseñanza Superior y de Inves-

tigación, de Defensa, de Justicia, de Asuntos Sociales, de Sanidad y de Derechos de las Mujeres, del Interior, de Economía, Ministerio de Industria y del Ámbito Digital, la Comisaría General de la Inversión, la Agencia Nacional de Investigación y los organismos de investigación pertinentes. El grupo podrá asociar a sus actividades a protagonistas del sector privado y a personalidades cualificadas.

La misión de este grupo será, entre otras cosas, identificar las tecnologías clave cuyo dominio es necesario para los sectores de la ciberseguridad y, en términos más generales, para el desarrollo de un entorno digital de confianza. Evaluará las necesidades de formaciones iniciales y continuas en ciencias, participará a la mejora del asesoramiento de los jóvenes doctores, prestara particular atención a los trabajos de investigación y a su valorización. Contribuirá, en el campo de las tecnologías digitales, a la definición de los ejes estratégicos de los dispositivos de financiación y de asesoramiento de los trabajos de investigación y de desarrollo industrial. Estos trabajos observaran la coherencia con los trabajos de las estructuras ya establecidas como el Comité del Sector de las Industrias de Seguridad (CoFIS).

En términos más generales, la elección de protagonistas privados destacados en materia de modelo económico, de tecnología, a veces sin marco normativo, o sencillamente ciertas innovaciones en los usos en el ámbito digital pueden consolidar la confianza o suscitar recelo. El grupo de expertos para la confianza digital organizará la vigilancia tecnológica y económica que permitirá prever los cambios en el ámbito digital. Cuando sea necesario, se propondrán medidas adaptadas para acompañar o ajustar esos cambios. Tales medidas podrán, por ejemplo, referirse a la protección del potencial científico y técnico de la Nación o al control de las inversiones extranjeras en empresas nacionales críticas.

Una comisión del grupo de expertos reunirá a los coordinadores ministeriales para asuntos relativos al ciberespacio alrededor del secretario general de defensa y de seguridad nacional para los asuntos que sean de su competencia.

Este grupo de expertos rendirá cuentas de sus actividades anualmente al Primer Ministro.

> Encargarse en beneficio del Estado, de las empresas y de los ciudadanos de una anticipación activa en materia de seguridad de las tecnologías y de los usos.

En la perspectiva de cambios tecnológicos muy importantes, como las telecomunicaciones móviles de 5.a generación o las «redes definidas por el software», Francia permanecerá alerta a la naturaleza y a las capacidades del hardware y software instalados en el centro de sus redes de comunicaciones electrónicas, para proteger el secreto de las correspondencias, la vida privada de sus ciudadanos y la resistencia de estas infraestructuras, y tratará de adaptar su marco normativo a las nuevas tecnologías emergentes.

La autoridad nacional de seguridad de los sistemas de información informará con regularidad a los ministerios, las empresas, las entidades territoriales y los ciudadanos, utilizando medios adaptados al destinatario, sobre los elementos propensos a presentar un peligro en su uso del ámbito digital. Cuando proceda, esta información se habrá consolidado previamente con las administraciones competentes.

> Acelerar el refuerzo de la seguridad de los sistemas de información del Estado.

Desde 2010, se han acometido varias acciones destinadas a elevar el nivel de seguridad de los sistemas de información del Estado. Se ha elaborado una política de seguridad de los sistemas de información del Estado (PSSIE), se está desarrollando una red interministerial de comunicaciones electrónicas, se ha iniciado el despliegue de terminales móviles seguros. Estas acciones, como las encaminadas a la producción de equipos de seguridad destinados a proteger la información y la soberanía, movilizan recursos humanos y presupuestarios. Continuarán a fin de ofrecer al Gobierno y a nuestras fuerzas militares el nivel de seguridad adecuado para la preservación a largo plazo de la autonomía de decisión y de acción de Francia.

La aplicación de la política de seguridad de los sistemas de información del Estado y la eficacia de las medidas adoptadas se evaluarán anualmente. El Primer Ministro recibirá un balance anual confidencial y el Par-

lamento se mantendrá informado mediante indicadores.

Con el mismo propósito de informar al Parlamento, los proyectos de ley incluirán en su estudio de impacto a partir de 2016 un apartado dedicado al ámbito digital y, dentro de este apartado, uno dedicado a la ciberseguridad establecido bajo la égida de altos funcionarios a cargo de la calidad de la reglamentación. Más ampliamente, los altos funcionarios a cargo de la calidad de la reglamentación tendrán especialmente en cuenta las cuestiones relativas al refuerzo de la seguridad de los sistemas de información del Estado en el marco del pilotaje de la actividad normativa.

> Preparar a Francia y a las organizaciones multilaterales de las que es miembro a enfrentarse a una crisis informática grave.

Anunciado en el Libro Blanco sobre la Defensa y la Seguridad Nacional de 2013, el refuerzo de la seguridad de los sistemas de información más sensibles de los operadores de importancia vital ha sido objeto de medidas legislativas (artículos 21 y 22 de la ley n.° 2013-1168 del 18 de diciembre de 2013). Los trabajos iniciados con estos operadores continuarán de forma duradera, entre otras cosas, a través la actualización de los textos normativos. Estos trabajos se ampliarán progresivamente, tal como lo estipula la ley, a los operadores públicos o privados que participan en estos sistemas de información sensibles.

Esta elección efectuada por Francia le habrá permitido participar activamente en la elaboración de las orientaciones de la Directiva europea relativa a la seguridad europea de los sistemas de información en el interior de la Unión Europea y anticipar su transposición. En su momento, Francia definirá sus operadores esenciales para la economía conforme a las orientaciones de la directiva y participará en las iniciativas europeas destinadas a reforzar su seguridad digital.

Los ejercicios de gestión de crisis cibernética realizados a nivel nacional se llevarán a cabo, gradualmente, en todo el territorio y en todos los sectores de actividad de importancia vital. El Ministerio de Defensa, en coordinación con la autoridad nacional de seguridad de los sistemas de información, continuará el desarrollo de une reserva de ciberdefensa de vocación operativa destinada a enfrentarse a una crisis informática grave.

En paralelo, Francia seguirá participando en la emergencia de un marco de cooperación voluntaria de gestión de crisis cibernética a escala europea, contribuyendo especialmente a las labores de la agencia europea ENISA.

Corresponde al CERT-EU de la Unión Europea (UE) y al NCIRC en el seno de la Organización del Tratado del Atlántico del Norte (OTAN) garantizar la ciberdefensa de sus instituciones respectivas. Activa durante los ejercicios de gestión de crisis cibernéticas organizadas por estas organizaciones y fuertemente representada en las instancias que orientan las decisiones de la UE y de la OTAN en materia de tecnologías digitales seguras, Francia seguirá colaborando con estas instituciones y con sus Estados miembros respetando las competencias de cada uno.

Francia contribuirá asimismo a reforzar la ciberseguridad de otras organizaciones internacionales de las que es miembro, a nivel político y técnico, especialmente las que se alojan en el territorio nacional que se aprovechan del ecosistema técnico nacional.

> Desarrollar un pensamiento autónomo y conforme a nuestros valores.

Las decisiones estratégicas tomadas por Francia tras la Segunda Guerra Mundial llevaron a la emergencia de un pensamiento estratégico autónomo y a la elaboración de una doctrina que otorgó a Francia un lugar singular en el plano internacional que impregna, hasta nuestros días, su diplomacia y los conceptos de empleo de sus fuerzas armadas.

El ámbito digital modifica profundamente nuestras sociedades, pero falta por medir su impacto en otras realidades, como la soberanía, el territorio nacional, la moneda o los intereses fundamentales de la nación, así como replantearse la organización y los medios de la acción pública para aplicarles la ley o para garantizar su protección. Se llevará a cabo una reflexión bajo la coordinación del secretario general de defensa y de seguridad nacional para elaborar un corpus intelectual relativo al ciberespacio.

2

#CONFIANZA DIGITAL, VIDA PRIVADA, DATOS PERSONALES, CIBERATAQUES

CUESTIONES FUNDAMENTALES

Aunque de forma general los franceses confían en el ámbito digital, muestran cierto recelo en cuanto a su impacto en su vida cotidiana, especialmente personal. A pesar de que en general se preocupan por el uso y la conservación de sus datos personales, los ceden a plataformas cuyas condiciones de uso son leoninas en detrimento de los usuarios.

El modus operandi observado de ciertos ataques informáticos contra empresas o administraciones revela asimismo una verdadera dificultad para disociar la vida privada de la profesional en el uso de los equipos así como de los servicios.

Los ataques informáticos que afectan a los particulares pretenden, por lo general, obtener alguna ganancia económica. A través de la toma de control del equipo personal utilizado —ordenador, tableta, Smartphone— la usurpación de la identidad y el robo de identificadores de acceso a cuentas bancarias o a sitios comerciales, mediante el inicio de una relación afectiva virtual que desemboca en una petición de envío de dinero, a través del cifrado de datos sin

el conocimiento del usuario que lleva al pago de un rescate, el chantaje es practicado hoy en día a gran escala por delincuentes que se han organizado y han aumentado su eficacia.

Aunque no recurra a una técnica de ataque particular, el acoso, facilitado y amplificado por las redes de comunicaciones electrónicas, es una agresión informática contra las personas cuyo desenlace es, en ocasiones, dramático.

Si la Agencia Nacional de Seguridad de los Sistemas de Información (ANSSI) es el interlocutor estatal identificado en caso de incidente informático grave que afecta a las administraciones y a los operadores de importancia vital, la oferta pública es netamente menos evidente en cuestión de asistencia a las víctimas de ciberataques para los demás actores, ya sean pymes, profesiones liberales, entes territoriales o particulares.

Se anima a las víctimas de ciberataques a poner una denuncia en los servicios pertinentes de policía o de gendarmería que se han adaptado al tratamiento de este tipo de contencioso. Sin embargo, la respuesta que se les da en este marco se centra en la identificación de los presuntos autores del ciberataque y, eventualmente, en el procesamiento de los autores. Las víctimas deben poder ser orientadas hacia un servicio de asistencia al tratamiento del incidente informático a menudo causa del ciberataque.

De manera insidiosa, las plataformas digitales y particularmente las redes sociales moldean la opinión y son vectores de valores que no siempre son los de la República francesa. Se pueden instrumentalizar con fines de desinformación y de propaganda dirigida a los ciudadanos franceses y en especial los más jóvenes. En algunos casos, las opiniones difundidas son contrarias a los intereses fundamentales de Francia y se inscriben entonces en una vulneración de la defensa o de la seguridad nacional sancionada por la ley.

En un registro diferente, los desarrollos recientes y simultáneos de nuevos usos y de nuevas técnicas de almacenamiento y de tratamiento de datos favorecen la emergencia de riesgos de desequilibrio económico y de vulneración de la seguridad individual de las personas así como la de las naciones. El deseo de ver instaurarse, por ejemplo, a través de los tratados comerciales, la libre circulación de datos, incluidos los personales recopilados mediante objetos conectados, a duras penas oculta la volun-

« De manera insidiosa, las plataformas digitales y particularmente las redes sociales moldean la opinión y son vectores de valores que no siempre son los de la República francesa »

« El desarrollo digital no puede ser duradero en un ciberespacio en el que los Estados no respetan las buenas prácticas necesarias para una transición digital equilibrada y provechosa para todas las naciones »

tad de captación de estos datos por oligopolios cuyos valores y prácticas no corresponden ni a la concepción de la vida privada francesa o europea ni a su marco jurídico. La captación masiva e ilícita de ciertos tipos de datos personales, como los de salud, pueden acarrear la vulneración de la seguridad individual y colectiva, o sencillamente la explotación comercial abusiva (reventa a compañías de seguros, por ejemplo).

El desarrollo digital no puede ser duradero en un ciberespacio en el que los Estados no respetan las buenas prácticas necesarias para una transición digital equilibrada y provechosa para todas las naciones y en el que algunos actores económicos acaparan la riqueza que constituyen los datos digitales, especialmente los personales, verdaderos recursos de las generaciones futuras.

OBJETIVO

Francia desarrollará un uso del ciberespacio conforme a sus valores y en el que protegerá la vida digital de sus ciudadanos. Incrementará su lucha contra la ciberdelincuencia y la asistencia a las víctimas de ciberataques.

ORIENTACIONES

> Promover y defender nuestros valores en las redes de comunicaciones electrónicas y en los foros internacionales.

Los derechos de las personas se aplican de la misma manera «en línea» y «fuera de línea». El ciberespacio debe, por tanto, seguir siendo un lugar de libre expresión para todos los ciudadanos, donde los abusos solo se pueden prevenir en el marco fijado por la ley y la conformidad con nuestros compromisos internacionales. Francia promueve este enfoque encaminado a preservar un ciberespacio libre y abierto en los foros internacionales.

Corresponde al Estado informar a los ciudadanos sobre los riesgos de manipulación y las técnicas de propaganda utilizadas por actores malévolas en Internet. Tras los atentados perpetrados contra Francia en enero de 2015, el Gobierno instauró una plataforma de información sobre los riesgos relacionados con la radicalización islamista a través de las redes de comunicaciones electrónicas. « Stop-djihadisme.gouv.fr ». Este enfoque se podría extender para responder a otros fenómenos de propaganda o de desestabilización. Corresponde a los servicios competentes en materia de defensa y de seguridad detectar estos fenómenos y proponer al Gobierno la creación de estos medios.

> Brindar una asistencia de cercanía a las víctimas de ciberataques.

Bajo la dirección del Ministerio del Interior y la Agencia Nacional de Seguridad de los Sistemas de Información (ANSSI), con el apoyo de los ministerios de Justicia, de Finanzas y de las Cuentas Públicas, de Defensa, de Economía, de Industria y del Ámbito Digital, se creará un dispositivo nacional en 2016 para brindar asistencia a las víctimas de ciberataques.

Este dispositivo tendrá asimismo una misión de sensibilización sobre las cuestiones de protección de la vida privada digital y de prevención que se apoyará localmente sobre la acción de los prefectos y de los servicios del Estado. La red territorial de la ANSSI, los delegados regionales para la inteligencia económica y los servicios del Ministerio del Interior competentes en materia de seguridad económica, la red «transición digital», la del Banco de Francia —que podría integrar con el tiempo en su cotización de las empresas un criterio vinculado al riesgo cibernético—, participarán en esta misión. Las cámaras de comercio y de industria, las cámaras profesionales serán contactadas y de forma más amplia todas

las agrupaciones profesionales.

El dispositivo adoptará una forma jurídica y una organización que le permita beneficiarse de los aportes de los actores económicos del sector de la ciberseguridad como editores de software, plataformas digitales, proveedores de soluciones. Gracias a las tecnologías utilizadas, el dispositivo tendrá que ofrecer a las víctimas soluciones técnicas a través de los actores de proximidad y facilitar los trámites administrativos, sobre todo para favorecer la presentación de denuncia.

> Medir la cibercriminalidad.

Los trabajos interministeriales realizados a iniciativa del Ministerio del Interior desde 2013 pusieron de manifiesto que no existen hoy estadísticas fiables relativas específicamente a la delincuencia o a la criminalidad informática, la mayoría de las infracciones de este tipo se registran con una denominación que no indica esta dimensión, en la actualidad ausente de los referenciales utilizados.

La falta de tales estadísticas, perjudica la elaboración por los poderes públicos de políticas constantemente revalorizadas e impide la puesta en marcha de los medios adaptados. Por eso, el Ministerio del Interior creará nuevos instrumentos de seguimiento de la evolución de la ciberdelincuencia a fin de orientar la acción pública. El Observatorio Nacional de la Delincuencia y de las Respuestas Penales también colaborará dedicando una parte de sus trabajos al estudio estadístico de la ciberdelincuencia. Este componente, concebido en coordinación con la agencia nacional de seguridad de los sistemas de información y el dispositivo de asistencia a las víctimas de ciberataques, integrará los datos de que dispongan.

> Proteger la vida digital, la vida privada y los datos personales de los franceses.

Junto con el Reglamento europeo sobre tarjeta de identidad electrónica (eIDAS), Francia se dotará de una hoja de ruta clara sobre identidad digital emitida por el Estado. Esta hoja de ruta se elaborará antes de finales de 2015 bajo los auspicios del Ministerio del Interior y de ciertas secretarías del Estado encargadas del ámbito digital y de la reforma del Estado, con la asistencia de los servicios del Primer Ministro, y tendrá que incluir un capítulo que definirá un marco de referencia para el

uso de la identidad digital en beneficio de las entidades territoriales.

Esta hoja de ruta tendrá en cuenta la estrategia digital del Gobierno que prevé el despliegue de dispositivos de federación de identidad que permita utilizar una misma identidad digital para autenticarse en diferentes servicios. Gracias a estos dispositivos, las identidades digitales pueden haber sido emitidas por entidades diferentes siempre que el tercero que gestiona la federación de la identidad sea capaz de determinar el nivel de confianza asociado a la identidad.

Bajo reserva de respetar exigencias de seguridad adaptadas a los usos y a las amenazas, estos dispositivos son de naturaleza a reforzar la confianza de los usuarios en su vida digital, a favorecer su fluidez a la vez que limitan el riesgo de una explotación no deseada de sus datos personales. Para los usos más sensibles, como los referentes a la vida democrática o a los intercambios internacionales relativos a la justicia, se emplearán sistemáticamente niveles de confianza elevados en los dispositivos y servicios. Estos niveles elevados de confianza se basarán en el tejido industrial nacional y el esquema de certificación de seguridad establecido.

Francia protegerá la vida privada y los datos personales de sus nacionales. Los derechos a la vida privada y al control individual y colectivo de los datos personales se reafirmarán cada vez que sea necesario y en particular con ocasión de las negociaciones comerciales entre Estados, ya sean bilaterales o multilaterales.

Para informar a los franceses sobre el uso hecho de sus datos confiados a los servicios digitales, en 2016 se creará una señalización adaptada y compartida con los Estados voluntarios y en coherencia con los trabajos europeos sobre protección de datos personales. Esta señalización permitirá visualizar las características esenciales de las condiciones de uso de las plataformas y de los servicios digitales o de los medios de pago utilizados.

> Proponer soluciones técnicas encaminadas a asegura la vida digital, accesibles para todas las empresas y el público en general.

Los servicios del Estado concederán sellos a soluciones de seguridad de los terminales personales. Una señalización coherente con la descrita anteriormente permitirá a los usuarios estar informados de eventuales transmisiones de datos a un tercero en el marco de esta protección. Una vez creado, el sistema de asistencia a las víctimas de ciberataques ya mencionado, a título de su misión de prevención, difundirá estos dispositivos entre los destinatarios pertinentes.

Por otro lado, y tal como se pudo establecer en el programa de inversiones de futuro, se apoyará la oferta de soluciones accesibles y adaptadas encaminadas a hacer segura la vida digital de las pymes.

Se brindará apoyo al desarrollo de soluciones francesas, así como a las comunidades de software libre que desarrollan soluciones de seguridad.

> Reforzar los mecanismos operativos de cooperación judicial internacional y universalizar los principios del Convenio de Budapest sobre la lucha contra la ciberdelincuencia.

Adoptado en 2001 en el marco del Consejo de Europa, el Convenio de Budapest se ha convertido en un instrumento de referencia que permite la cooperación en la lucha contra la ciberdelincuencia entre Estados de los cinco continentes. Ratificado por 46 Estados, de los cuales 7 no son miembros del Consejo de Europa, este instrumento reúne ya a 125 Estados en diferentes grados (firmantes, Estados invitados a adherirse, Estados que reciben asistencia técnica con vistas a una futura adhesión, Estados que han aprobado una ley interna siguiendo el modelo del Convenio).

En la actualidad es esencial universalizar y consolidar tanto la base normativa como la herramienta de cooperación que este texto representa.

Por otro lado, Francia promoverá en el seno de la Unión Europea la definición de un dispositivo de cooperación judicial simplificada entre Estados miembros a fin de acelerar la transmisión de los datos y de poner fin a las actividades ilegales.

3

#SENSIBILIZACIÓN, FORMACIONES INICIALES, FORMACIONES CONTINUAS

CUESTIONES FUNDAMENTALES

Francia lleva retraso respecto a sus socios en materia de sensibilización de su población ante los riesgos asociados a los usos del ámbito digital y de formación en ciberseguridad.

Los franceses descuidan de forma general las buenas prácticas en el uso de las redes de comunicaciones electrónicas.

En el uso privado de las redes de comunicaciones electrónicas, los niños y adolescentes, confrontados a contenidos inadecuados, expuestos al acoso o a los depredadores, son las primeras víctimas. A fin de romper el silencio y de permitir los procesamientos, se debería iniciar a los más jóvenes en la conducta a seguir cuando son víctimas de ataques cibernéticos.

La sensibilización de todos es un requisito para que los cargos electos, los dirigentes de administraciones o de empresas puedan tener en cuenta el «riesgo cibernético» en su justa medida y decidir las medidas susceptibles de proteger a los ciudadanos a los que representan o a los organismos que dirigen frente a amenazas de robo de datos o de propiedad intelectual, de vulneración de los datos personales, o incluso las interrupciones de actividad, accidentes de producción, con repercusiones tecnológicas o medioambientales a las que están potencialmente expuestos.

Además de sensibilizar a los más jóvenes, formase profesionalmente al mundo digital debe permitir a los futuros profesionales de este campo disponer de una enseñanza avanzada en seguridad de los sistemas de información. En la actualidad esta enseñanza sigue ausente de numerosas formaciones superiores.

Por otro lado, el contenido y el número de formaciones iniciales y superiores en las profesiones de la ciberseguridad no permiten satisfacer la demanda de las empresas y de las administraciones.

OBJETIVO

Francia promoverá desde la escuela la sensibilización sobre la seguridad digital y los comportamientos responsables en el ciberespacio. Las formaciones iniciales superiores y continuas incorporarán un componente dedicado a la seguridad digital adaptado al sector correspondiente.

ORIENTACIONES

> **Sensibilizar a todos los franceses.**

Hay que impulsar un programa ambicioso de sensibilización de todos los franceses

Bajo la dirección del Ministerio de Educación Nacional, de la Enseñanza Superior y de Investigación y de la Secretaría de Estado para la Economía Digital, con el apoyo del servicio de información del Gobierno y de la agencia nacional de seguridad de los sistemas de información, se hará un llamamiento a la manifestación de interés para la realización de contenidos de sensibilización del público en general.

El Ministerio del Interior continuará la operación «Permiso de Internet» iniciada en 2014 por la gendarmería nacional en asociación con una fundación privada, y secundada desde comienzos de 2015 por la Policía Nacional. Esta operación permite sensibilizar sobre los riesgos y asesorar a más de 300 000 alumnos de CM2 [de 9 a 11 años] cada año para protegerlos en su navegación por Internet.

La visibilidad del Portal "Una educación digital para todos "de la Comisión para la informática y las libertades (CNIL) se reforzará.

Se invitará a las asociaciones a elaborar proyectos de campañas de comunicación con vistas a reforzar la confianza en el ámbito digital susceptibles de inscribirse en el marco de una «gran causa nacional».

> Integrar la sensibilización sobre ciberseguridad en cualquier formación superior y en las formaciones continuas.

El Ministerio de Educación Nacional, de la Enseñanza Superior y de Investigación, con la ayuda de la Conferencia de rectores de universidad, de la Conferencia de las grandes escuelas y de las administraciones competentes, fomentará, a partir de la vuelta a clase de 2016, acciones de sensibilización sobre la ciberseguridad correspondiente a la rama de formación en cualquier formación inicial superior.

El Ministerio de Trabajo, del Empleo, de la Formación Profesional y del Diálogo Social, en colaboración con las administraciones del Estado competentes en materia de ciberseguridad, iniciará las consultas necesarias para que, a partir de 2016, los organismos que ofrecen formaciones continuas incorporen en los diferentes planes de estudios la sensibilización sobre las cuestiones de ciberseguridad adecuada a la formación.

Por último, bajo la coordinación de la Secretaría de Estado para la Economía Digital, con los ministerios pertinentes y el apoyo de la ANSSI, se iniciará la sensibilización de categorías profesionales para las cuales es especialmente necesaria una sólida asimilación de los temas de ciberseguridad en razón de sus responsabilidades sociales. El comité estratégico para la confianza digital precisará estas categorías.

> Integrar la formación sobre ciberseguridad en cualquier formación superior que tenga una parte de informática.

La iniciativa «Cyber-Edu» lanzada en 2013 permitió confirmar el interés de los docentes que intervienen en los planes de estudios de formaciones superiores de las ramas informáticas por los temas de seguridad de los sistemas de información. Hay que consolidar esta iniciativa.

El Ministerio de Educación Nacional, de la Enseñanza Superior y de Investigación, con la ayuda de la Conferencia de rectores de universidad, de la Conferencia de las grandes escuelas y de las administraciones, se encargará de que a partir de la vuelta a clase de 2016, se imparta una formación sobre seguridad de los sistemas de información adaptada a la rama en cualquier formación inicial superior y en la que se incluirán temas sobre el ámbito digital. Se deberá procurar integrar de forma prioritaria estos elementos de seguridad en los cursos existentes y de forma permanente en el contexto más amplio de cada especialidad enseñada. Estas acciones podrán basarse útilmente en los contenidos pedagógicos en curso de elaboración, en estrecha colaboración con la comunidad docente, en el marco del proyecto Cyber-Édu.

El Ministerio de Descentralización y de la Función Pública velará por que las formaciones para los puestos de responsabilidad de la administración pública incluyan elementos de sensibilización sobre ciberseguridad. En coordinación con el Ministerio del Interior, velará por que el concurso para la contratación en el Cuerpo de ingenieros de los sistemas de información y de comunicación previsto por el decreto n.° 2015-576 del 27 de mayo 2015 así como las formaciones que se impartirán a sus miembros incluyan un componente de ciberseguridad.

Frente a una creciente demanda de nuestros socios, convendrá, en la medida de lo posible, adaptar una parte de la oferta de formación y de sensibilización a un público internacional, ofreciendo por ejemplo programas en inglés.

> Recopilar y anticipar las necesidades de formaciones iniciales y continuas.

Bajo los auspicios del Grupo de expertos para la confianza digital, las necesidades de formaciones iniciales a corto, medio y largo plazo se definirán en coordinación con todos los actores implicados de la administración y del sector privado.

Se consultará a los sindicatos profesionales para la elaboración y la organización de formaciones continuas adaptadas a las necesidades de los empleados y de las empresas.

4

#ENTORNO DE LAS EMPRESAS DEL SECTOR DIGITAL, POLÍTICA INDUSTRIAL, EXPORTACIÓN E INTERNACIONALIZACIÓN

CUESTIONES FUNDAMENTALES

La construcción del ciberespacio es rápida. Cada hora se conectan a Internet 100 000 nuevos objetos. La presencia de numerosas empresas francesas en los salones internacionales como el éxito de la iniciativa «French Tech» pone de manifiesto un verdadero dinamismo de la innovación francesa en materia de productos y servicios digitales. Esta realidad, sin embargo, no debe ocultar cierta pérdida de control y una auténtica dependencia tecnológicas.

Los grandes equipos con los que funcionan las redes de comunicaciones electrónicas cuyas infraestructuras se ubican en Francia, con frecuencia se diseñan, desarrollan y administran desde centros situados fuera de Europa. Lo mismo ocurre con la mayor parte de los equipos de comunicaciones y de seguridad informática de nuestros operadores de importancia vital. El funcionamiento de un creciente número de empresas se basa en el uso de aplicaciones y el tratamiento de datos alojados en espacios virtuales no controlados, en infraestructuras físicas situadas fuera del territorio nacional y no sujeto al derecho europeo.

Las evoluciones tanto a nivel de tecnologías como a nivel de los modelos económicos con, por ejemplo, la multiplicación de los objetos conectados o la concentración de las plataformas de servicio en línea entre las manos de solo unos pocos actores, son de naturaleza a amplificar esta pérdida de control del ciberespacio nacional. En caso de crisis internacional, podrían negarnos el acceso a segmentos enteros del ciberespacio.

La respuesta a esta cuestión de soberanía requiere en primer lugar mantener una industria nacional y europea fuerte y competitiva en el campo especializado de los productos y servicios de ciberseguridad. Con carácter más general, pasa por el desarrollo, en Francia y en Europa, de una oferta de equipos y de servicios digitales que aporten a sus clientes las garantías de seguridad y de confianza adecuada para los retos y los usos.

« El desarrollo, por las empresas nacionales del sector digital, de una oferta de productos y de servicios seguros debe asimismo considerarse como un factor fundamental de competitividad para estas empresas. »

Los usuarios no están en condiciones de asegurarse ellos mismos del nivel de seguridad de los objetos y servicios digitales. La promoción de la seguridad en el discurso comercial de los proveedores se generaliza aunque no permite una evaluación objetiva del nivel de seguridad realmente alcanzado. El desarrollo de una mayor transparencia en el plano de la seguridad de la oferta digital, basada en elementos objetivos y verificables por un tercero, constituye un reto mayor para asegurar la confianza en la economía digital.

El desarrollo, por las empresas nacionales del sector digital, de una oferta de productos y de servicios seguros debe asimismo considerarse como un factor fundamental de competitividad para estas empresas. El control de los medios de pago (tarjetas con chip, terminales de pago, etc.) es el arquetipo de un sector económico en el que un nivel de seguridad adecuado para la amenaza y verificable por un tercero constituye un argumento comercial de primer orden. Varias empresas nacionales cuentan en este sector con una posición competitiva a nivel mundial que le debe mucho a la excelencia que supieron desarrollar y demostrar en cuestión de seguridad.

La multiplicación de las amenazas cibernéticas y la concienciación cada vez más extendida de estas amenazas conducirán dentro de unos años a que la seguridad sea un criterio de compra esencial en muchos otros sectores. Actuar ahora para mejorar la seguridad y la transparencia de la oferta nacional de soluciones digitales, también es preparar su competitividad futura.

En 2015, la parte de empresas francesas y especialmente de las pymes que recurren de forma intensiva al ámbito digital solo está en la media de

los países europeos. Para recuperar este retraso, hay que lograr una mayor seguridad de la vida digital de las empresas y en primer lugar una mayor seguridad de sus sistemas de información. De ello depende nuestra competitividad y, por tanto, nuestros empleos.

El reto al que se enfrentan las empresas francesas es conciliar investigación de productividad, de ahorro, de rentabilidad y uso o desarrollo de productos y servicios digitales que no pongan en peligro su seguridad, la de sus socios o la de sus clientes.

La mayoría de los equipos, objetos y servicios digitales disponibles en la actualidad en el mercado no tienen el nivel de seguridad informática que les permita evitar un incidente —filtración de datos, funcionamiento incorrecto o interrupción de servicio. Para las empresas francesas, la ergonomía, la protección de los datos personales, el nivel de seguridad de los productos y servicios digitales que desarrollan y producen, deben convertirse a corto plazo en un elemento diferenciador, una ventaja competitiva para estas empresas y a cambio para el país.

Por otro lado, aunque la falsificación no depende directamente a la seguridad de los sistemas de información, los productos de seguridad informática falsificados pueden poner en peligro la actividad de las organizaciones que los adquieren.

« Para las empresas francesas, la ergonomía, la protección de los datos personales, el nivel de seguridad de los productos y servicios digitales que desarrollan y producen, deben convertirse a corto plazo en un elemento diferenciador, una ventaja competitiva para estas empresas y a cambio para el país. »

En cuestión de internacionalización de las empresas y de exportación, frente a una competencia internacional exacerbada en la que nuestros socios conceden un apoyo basado y estructurado a su industria, los servicios del Estado deben organizarse de forma perenne para apoyar a las empresas francesas de la ciberseguridad.

La movilización y la coordinación de todos los recursos públicos y privados disponibles son esenciales para aumentar la visibilidad y la competitividad de la oferta francesa a nivel internacional, compartir los conocimientos, las experiencias y así favorecer que se comparta la información entre les diferentes actores del sector.

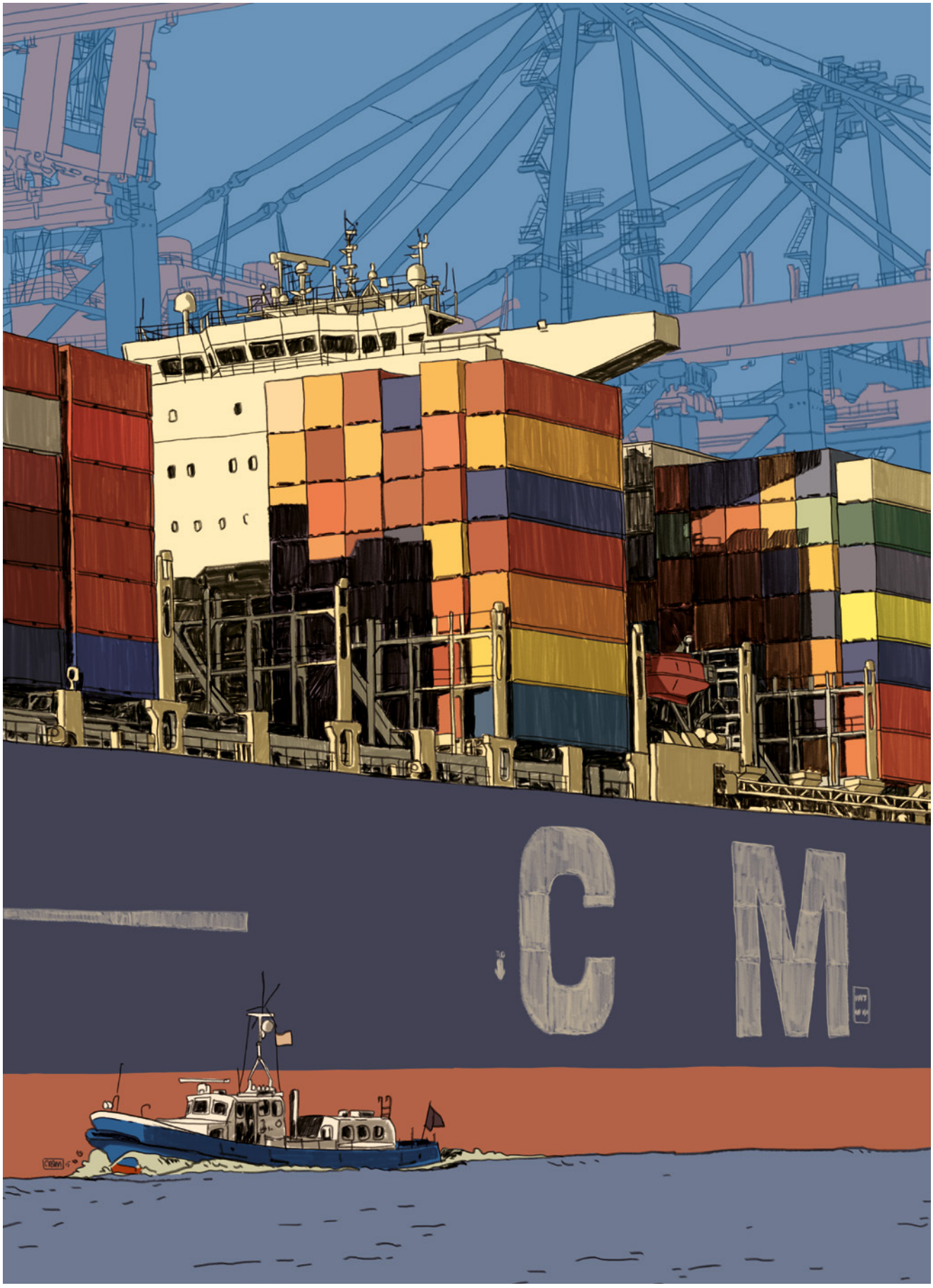
OBJETIVO

Francia desarrollará un ecosistema favorable a la investigación y a la innovación y hará de la seguridad digital un factor de competitividad. Fomentará el desarrollo de la economía y la promoción internacional de sus productos y servicios digitales. Se asegurará de la disponibilidad, para sus ciudadanos, sus empresas y sus administraciones, de productos y servicios digitales que presenten niveles de ergonomía, de confianza y de seguridad adecuados para los usos y las ciberamenazas.

ORIENTACIONES

> **Desarrollar y valorizar la oferta nacional y europea de productos y de servicios de seguridad.**

En coordinación con las administraciones competentes del Ministerio de Economía, de Industria y del Ámbito Digital y del Ministerio de Defensa, la agencia nacional de seguridad de los sistemas de información inició en 2012 una política industrial encaminada a impulsar el tejido nacional de las empresas que desarrollan productos y servicios de seguridad informática.


C
M

El lanzamiento en 2013 del plan «Ciberseguridad» de la Nueva Francia Industrial, ahora integrado en la solución «Confianza digital» con el respaldo de la Comisaría General para la Inversión y de BpiFrance han permitido organizar el sector y poner en marcha convocatorias de proyectos encaminados a crear una oferta de equipos de confianza para la detección de ataques informáticos, esencialmente dirigidos a los operadores de importancia vital, y de productos de movilidad segura para todas las empresas.

Los servicios del Estado intensificarán sus esfuerzos en materia de calificación y de seguimiento de productos y servicios de seguridad informática, así como en su apoyo al desarrollo de nuevos productos de seguridad que respondan a la evolución de los usos. Respaldarán asimismo la valorización y la continuidad de estas ofertas a través de la contratación pública que dará preferencia a los productos y servicios de seguridad calificados con el nivel adecuado, así como mediante acciones de comunicación y de sensibilización dirigidas al sector privado.

Por otro lado, los servicios del Estado difundirán los resultados de los trabajos de investigación y desarrollo que financian para equipos de alto nivel de seguridad con el fin de elevar la de los productos dirigidos a las empresas y al público en general.

Por último, Francia se preocupará por sacar todo el partido a los dinamizadores ofrecidos por la Unión Europea a fin de apoyar, promover y defender las competencias científicas, tecnológicas e industriales francesas en el campo de la ciberseguridad. Animará, además, a la UE a no limitarse a un papel de consumidor, sino a imponerse como un actor global imprescindible de la oferta de este sector.

> Transferir los conocimientos adquiridos al sector privado para llevarlo a hacerse cargo de su seguridad informática.

Francia se ha dotado en los últimos cinco años de una capacidad de detección y de tratamiento de los ataques informáticos, como anunciaba el libro blanco sobre la defensa y la seguridad nacional de 2008. Aunque hay que seguir en esta línea, especialmente por parte de la ANSSI, corresponde al sector privado ocuparse de su propia seguridad en el ámbito informático igual que en los otros ámbitos, solo en caso de crisis grave deben intervenir los servicios del Estado.

Gracias a la transferencia de los conocimientos adquiridos por las administraciones hacia el sector privado, la certificación de proveedores competentes y de confianza debería permitir detectar y tratar el inevitable incremento del número de ataques informáticos que las empresas soportan.

> Preparar un mundo digital más seguro a través una mejor anticipación de los usos, una asistencia adecuada y una información de los protagonistas.

Para los próximos cinco años, la prioridad de las administraciones competentes en materia de seguridad de los sistemas de información debe ser la anticipación y la prevención.

Se tratará de lograr que los productos y servicios digitales o que integran un elemento digital, diseñados, desarrollados y producidos en Francia, estén entre los más seguros del mundo. Para alcanzar este objetivo las administraciones competentes tendrán que orientar sus esfuerzos de comunicación hacia la comunidad científica, pública y privada, y hacia los lugares de innovación (polos de competitividad, institutos de investigación tecnológicos, viveros empresariales, «fab labs») asignando, en caso necesario, medios específicos, como es el caso en el Ministerio de Defensa y, más recientemente en el Ministerio del Interior.

Cuando los productos y servicios digitales alojen datos personales o estén destinados a los sectores de actividad de importancia vital, los servicios del Estado aportarán los elementos de análisis de los riesgos o los consejos necesarios para la obtención del nivel de seguridad correspondiente al uso del producto o del servicio en curso de diseño o de desarrollo. Contribuirán asimismo, para los usos que lo justifiquen, a crear los dispositivos que permitan evaluar de manera independiente el nivel de seguridad y de confianza de estos productos y servicios, y a ofrecer a los potenciales usuarios las garantías adecuadas a través de una certificación.

En paralelo, habrá que anticipar el entorno jurídi-

co que regirá los nuevos productos y servicios. A título ilustrativo, la próxima llegada de vehículos autónomos debe incitar al regulador a preparar las condiciones que garanticen la seguridad de su circulación. La ciberseguridad se debe tener en cuenta en los grupos de trabajo internacionales que definen el referencial y los procedimientos técnicos de control.

Para otros tipos de productos y servicios, una señalización adaptada deberá informar al consumidor de sus características digitales fundamentales y, en particular, del tratamiento que se da a los datos recopilados. Para ciertos sectores, como el de la sanidad, se estudiará una señalización sistemática de los productos y servicios digitales.

Francia tratará de que otros Estados miembros de la Unión Europea se unan a la implantación de estas prácticas con el fin de crear una zona de confianza y de seguridad digitales. Los trabajos iniciados con Alemania en materia de informática en nube o de mensajerías seguras van en este sentido.

> Integrar la exigencia de ciberseguridad en las ayudas y la contratación públicas.

Para la protección de su soberanía y especialmente la protección de sus datos que se inscriben en el secreto de defensa nacional, Francia conservará su capacidad financiera e industrial para desarrollar soluciones que alcancen los más altos niveles de seguridad.

Con carácter más general, el conjunto de la administración tendrá que mostrar ejemplaridad en el marco de la contratación pública, integrando criterios de seguridad al justo nivel en la elección de los productos y servicios digitales.

Por último, a partir de 2016, cualquier producto o servicio que incluya o se base en un sistema de información y que desee presentarse a una licitación, a un concurso de proyecto público, o acceder a fondos públicos, se beneficiará de un factor de bonificación si va acompañado de un análisis de riesgos en materia de ciberseguridad que corresponda al uso previsto del producto o servicio y de la respuesta técnica aportada.

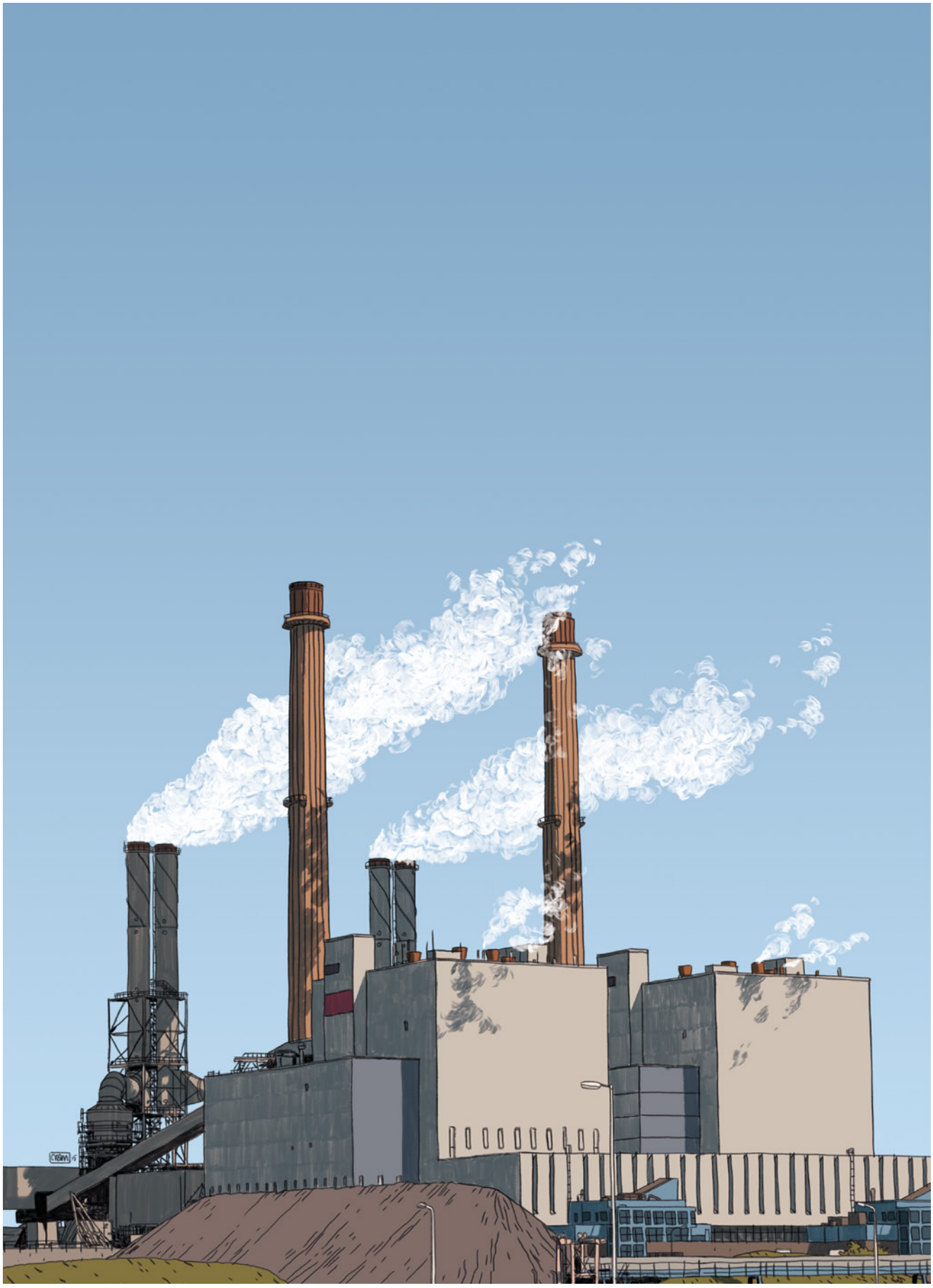
> Apoyar las exportaciones y la internacionalización de las empresas del sector.

A fin de apoyar el desarrollo económico del sector industrial de ciberseguridad, Francia velará por reforzar la visibilidad y la competitividad de la oferta francesa a escala internacional y por facilitar el acceso de las pymes y de las start-ups en particular en los mercados internacionales.

La coordinación interministerial se estructurará y reforzará. Se creará una organización adaptada en apoyo de las empresas francesas más allá de las acciones puntuales y con frecuencia aisladas llevadas a cabo en la actualidad por los diferentes ministerios y entidades estatales.

Además de la posible creación de dispositivos de apoyo específicos para los actores del sector de la ciberseguridad, las condiciones de acceso a los dispositivos de apoyo existentes, así como sus modalidades de implementación se esclarecerán y optimizarán. Los procedimientos de control de las exportaciones de soluciones de ciberseguridad se esclarecerán y optimizarán.

Por otro lado, al igual que en las acciones de «French tech», se respaldarán las iniciativas de colaboración procedentes del sector privado y encaminadas a favorecer el apoyo a las pymes y a las start-ups a nivel internacional.



5

#EUROPA, SOBERANÍA DIGITAL, ESTABILIDAD DEL CIBERESPACIO

CUESTIONES FUNDAMENTALES

El ciberespacio se ha convertido en un tema capital en el seno de las organizaciones internacionales cuyos trabajos se refieren a todo el ámbito digital.

En 2013, los Estados reconocieron que, lejos de ser un espacio sin normas, el ciberespacio se rige por el derecho internacional existente. Sin embargo, el marco jurídico internacional todavía es objeto de debate, lo cual, en ausencia de avances en las negociaciones, podría perjudicar la preservación de un ciberespacio estable y seguro, respetuoso con los derechos fundamentales y propicio al desarrollo de una economía próspera y de confianza en la era digital.

Aunque un creciente número de países declara dotarse de capacidades ofensivas, la conflictividad entre Estados se expresa cada vez más en el ciberespacio. Por otro lado, las revelaciones de prácticas masivas y de técnicas de espionaje llevadas a cabo por grandes Estados o alianzas de Estados contra otros —en ocasiones aliados—, personas y empresas, han aumentado la desconfianza política contra los países autores de estas prácticas y el recelo técnico respecto de sus productos y servicios. Estas revelaciones favorecen también la proliferación de medios técnicos similares.

Paralelamente, algunos grupos de individuos con motivos y apoyos diversos, mercenarios contratados mundialmente y asociados según las circunstancias, recurren regularmente a ataques informáticos en el ciberespacio para tratar de desestabilizar las autoridades gubernamentales de numerosos países o a las empresas que los encarnan de forma simbólica. Además, algunas organizaciones terroristas se aprovechan de la gran audiencia de las redes sociales para difundir una propaganda encaminada a captar voluntarios y aterrorizar a la población. Estos diferentes grupos disfrutan de impacto mediático constante.

En el plano económico, la tendencia de comienzos de la década se confirma. Un número reducido de empresas, impulsadas por los Estados que han facilitado su desarrollo, utilizan su ventaja tecnológica, su dominio del mercado y su capacidad financiera para controlar la innovación digital. Esta privatización del ciberespacio en beneficio de algunos monopolios condena a los demás actores del ámbito digital a la dependencia y capta una parte demasiado importante del valor añadido del sector digital para que esta situación sea soportable para la economía de los demás países.

« Aunque contribuye al crecimiento en el mundo, el ciberespacio se ha convertido en un lugar de competencia a menudo desleal y de conflictos »

Aunque contribuye al crecimiento en el mundo, el ciberespacio se ha convertido en un lugar de competencia a menudo desleal y de conflictos, hasta ahora de baja intensidad informática, de desestabilización política y de hegemonía económica.

Europa ha sabido identificar estas cuestiones fundamentales y trata de aportar, mediante el discurso y la regulación, ideas y soluciones más respetuosas con el desarrollo digital duradero, tanto en materia de gobernancia de Internet como de protección de los datos personales o de seguridad informática de los operadores esenciales para la economía. A Europa, que en 2013 aprobó una estrategia de ciberseguridad, le cuesta sin embargo optar firmemente por una soberanía digital y dotarse de las herramientas necesarias para devolver el equilibrio al ciberespacio en su favor, a pesar de que este tema figura en el orden del día de numerosos foros de discusión y de negociaciones europeas.

Porque comparte valores comunes con otros Estados miembros de la Unión Europea, Francia debe desempeñar un papel activo en el ámbito digital.

Francia desea participar en la transformación digital de Europa a través de alianzas. Europa se construyó ayer gracias a una alianza en torno a las materias primas. La Europa digital se construirá sobre alianzas, confianza y el control de los datos, materia prima de las próximas décadas.

OBJETIVO

Francia será, junto con los Estados miembros voluntarios, el motor de una soberanía digital europea. Desempeñará un papel activo en la promoción de un ciberespacio seguro, estable y abierto.

ORIENTACIONES

> **Establecer con los Estados miembros voluntarios una hoja de ruta para la soberanía digital de Europa.**

Abierta a los Estados miembros de la Unión Europea, esta hoja de ruta determinará los factores clave del éxito de la implantación a corto plazo de las políticas propicias a la emergencia de una soberanía digital europea, en particular en materia de reglamentación, de normalización y de certificación, de investigación y desarrollo, de confianza en el ámbito digital, de defensa y de seguridad de los sistemas de información —dentro de los límites del respeto de la soberanía de los Estados— de protección de la vida privada y de los datos personales entendidos como un bien de interés público.

Del mismo modo, Francia velará por que los tratados internacionales negociados en nombre de Europa no conduzcan a la dependencia tecnológica o económica de los actores europeos y no alienen los datos personales de sus ciudadanos o los datos sensibles de sus administraciones.

Se tratará de convertir a Europa en el territorio digital más respetuoso de los derechos fundamentales e individuales y de crear, yendo en el sentido de los trabajos precursores entre Francia y Alemania sobre la informática en nube (CLOUD) o al intercambio cifrado de mensajes de correo electrónico entre los dos países, una zona de confianza y de prosperidad económica.

> **Reforzar la presencia y la influencia francesa en las discusiones internacionales sobre ciberseguridad.**

Con el fin de reforzar la confianza a escala internacional y explorar nuevos mecanismos de regulación encaminados a prevenir los conflictos en el ciberespacio, Francia reforzará sus contactos con todas las partes interesadas dispuestas a dialogar sobre las cuestiones fundamentales de ciberseguridad.

La participación en las negociaciones multilaterales sobre ciberseguridad (ONU, OSCE) se intensificará a fin de consolidar una base global de compromisos de buena conducta para los Estados en el ciberespacio, de conformidad con el derecho internacional.

Los contactos bilaterales se reforzarán, sobre todo en el marco de las conversaciones diplomáticas con vocación interministerial sobre las cuestiones fundamentales del ciberespacio, bajo la dirección del Ministerio de Asuntos Exteriores y del Desarrollo Internacional.

Por último, en una lógica de influencia, Francia invertirá más en los foros internacionales más informales en los que las comunidades técnicas y académicas y los responsables políticos reflexionan juntos sobre los equilibrios futuros.

> **Contribuir a la estabilidad global del ciberespacio apoyando a los países voluntarios en la creación de capacidades de ciberseguridad.**

La transición digital, que brinda oportunidades políticas, sociales y económicas, está lejos de estar bajo control de forma homogénea en todos los países. Esto perjudica la seguridad y el desarrollo de los Estados menos protegidos, y fragiliza todo el ecosistema digital a escala internacional.

Con el fin de contribuir a un despliegue fiable y sostenible de las tecnologías digitales en todos los países, y en particular de los países en vía de desarrollo, Francia debe contribuir al refuerzo de las capacidades de los países que desean aumentar la resistencia y la seguridad de sus sistemas de información, especialmente en materia de protección de las infraestructuras críticas y la lucha contra la ciberdelincuencia.

A fin de garantizar la sostenibilidad y la durabilidad de los proyectos de refuerzo de las capacidades, Francia enmarcará su acción, preferiblemente, en asociaciones de confianza a largo plazo. Esta acción también deberá permitir que Francia refuerce su propia ciberseguridad.