Contribution citoyenne

Proposition de Code de la sécurité dans le Cyberespace

Souveraineté, attractivité et protection des citoyens

David Pauillac

avril 2026

Le Cyberespace, un espace juridique désordonné

Le constat de départ est simple.

Le corpus normatif applicable à la cybersécurité, à la protection des données et à l'économie numérique est aujourd'hui dispersé entre une quarantaine de textes de niveaux hétérogènes — codes, lois, ordonnances, règlements et directives européens transposés — sans architecture d'ensemble.

Cette fragmentation produit trois effets : une charge de conformité disproportionnée pour les opérateurs, une illisibilité totale pour les citoyens et leur sécurité, et des zones de friction institutionnelles entre autorités compétentes qui obèrent la réactivité de l'État face aux cybermenaces.

La proposition

La création d'un Code de la sécurité dans le cyberespace, structuré autour de quatre axes :

1. **Simplification** : un guichet unique de notification d'incident opéré par une autorité technique cyber unique, avec redistribution automatique aux autorités sectorielles compétentes — fin des cinq obligations de notification parallèles aux délais et destinataires divergents

2. **Compétitivité** : un audit cyber unique opposable — le « *Pass Cyber* » — dont les conclusions, produites par un prestataire qualifié, sont reconnues par l'ensemble des régulateurs sectoriels pour la durée de leur validité

3. **Souveraineté** : un titre dédié à l'attribution souveraine des cyberattaques, définissant les acteurs habilités, le régime de classification des conclusions et les effets juridiques de l'attribution publique, notamment les droits à réparation des victimes

4. **Citoyenneté** : un protocole de résilience identitaire post-fuite de données — révocation automatique des documents d'identité compromis, remplacement gratuit aux frais de l'entité responsable, recours obligatoire à France Identité dans les contextes à risque élevé, protection renforcée des mineurs.

Le moment est opportun

L'ordonnance de transposition NIS2 est en vigueur depuis janvier 2025. Le règlement DORA est applicable depuis le 17 janvier 2025. Le CRA et l'AI Act montent en charge jusqu'en 2027. Ces textes créent des obligations nouvelles sans résoudre les incohérences du droit national existant. La fenêtre de codification est ouverte — elle ne le restera pas indéfiniment.

Les constats concrètement

La Pluralité des Régimes de Notification d'incident : un fardeau de conformité insoutenable

L'analyse des textes révèle l'existence d'au moins cinq régimes de notification d'incident distincts, aux délais, formats, destinataires et seuils de déclenchement hétérogènes : RGPD (72h/CNIL), NIS2 (24h+72h/ANSSI), DORA (4h+72h/ACPR ou AMF), HDS (délai propre/ANS), Code de la défense OIV (délai classifié/ANSSI). Pour une entité bancaire gérant des données de santé et classée EE au titre de NIS2, **une seule et même cyberattaque peut théoriquement déclencher cinq obligations de notification simultanées et non coordonnées**.

L'intégration du COMCYBER-MI : une rationalisation prometteuse mais dont la consolidation juridique reste inachevée

La création du Commandement du ministère de l'Intérieur pour le cyberespace (COMCYBER-MI), placé sous l'autorité directe du ministre de l'Intérieur et chargé du pilotage unifié des capacités cyber de la Police Nationale (OFAC) et de la Gendarmerie Nationale (UN Cyber), a substantiellement résorbé le doublon opérationnel PN/GN identifié comme structurellement inefficace sous le régime antérieur. L'unité de commandement ainsi instaurée permet une orientation cohérente des enquêtes, une mutualisation des ressources techniques et une interlocution rationalisée avec les partenaires institutionnels (ANSSI, parquets spécialisés, Europol).

L'Absence de Cadre Juridique pour l'Attribution des Cyberattaques : un vide légistique stratégique

L'attribution publique d'une cyberattaque à un acteur étatique étranger est un acte politique majeur qui engage simultanément la DGSI (renseignement intérieur), la DGSE (renseignement extérieur), l'ANSSI (analyse technique), le SGDSN (coordination stratégique) et le Quai d'Orsay (dimension diplomatique). Or, aucun texte législatif ou réglementaire public ne régit ce processus : ni les modalités de partage inter-services de l'analyse technique, ni les conditions de la décision d'attribution publique, ni ses effets juridiques (mesures de rétorsion, contre-mesures cyber). Le Code de la défense effleure la LIO sans en traiter le versant attribution.

La coexistence de trois strates normatives sur les contenus numériques : l'abrogation de la LCEN s'impose

La régulation des contenus et de la responsabilité des acteurs numériques est aujourd'hui régie par **trois corpus superposés** : la LCEN de 2004[1], la loi SREN de 2024[2] et le DSA de 2022[3]. Ces trois textes traitent du même objet — responsabilité des intermédiaires, retrait des contenus illicites, signalement — avec des définitions, des seuils et des autorités compétentes divergents. La LCEN, qui n'a pas été abrogée, continue de générer un contentieux nourri sur des fondements devenus obsolètes depuis l'entrée en vigueur du DSA.

L'absence d'alignement terminologique OIV / EE-EI : le chantier de codification central

Le corpus normatif fait coexister deux nomenclatures d'opérateurs critiques sans équivalence formelle : les OIV du Code de la défense (régime classifié, arrêtés sectoriels, environ 300 entités) et les EE et EI de NIS2 (régime public, registre ANSSI, environ 15 000 entités). Un même opérateur peut être simultanément OIV et EE, soumis à des obligations partiellement redondantes issues de textes de nature et de niveau différents. Cette dualité, produit de l'histoire normative française, est incompatible avec un Code lisible et opposable aux citoyens comme aux opérateurs.

L'absence de textes et règles claires pour la protection des individus

Les délits fréquemment rencontrés dans le cyberespace (*Swatting*, harcèlement, usurpation d'identité numérique…) sont aujourd'hui dispersés voire absents des textes. Cet état engendre un flou aussi bien juridique qu'au niveau de la déposition : aucun acteur ne peut actuellement qualifier clairement un acte délictuel commis dans le Cyberespace ayant des répercussions directes dans le réel. Par

1. Droit national primaire, obsolète
2. Droit national récent
3. Règlement européen d'applicabilité directe

exemple l'usurpation d'identité numérique conduisant à la souscription d'un crédit ou l'arrêt d'un service essentiel, la fausse alerte conduisant à l'intervention des forces de l'ordre chez la victime (swatting), le cumul de tous ces exemples…

> **C**ette analyse préliminaire sur les acteurs étatiques et les différents textes traitant du Cyberespace met en lumière que le problème n'est pas le manque de lois, mais leur sédimentation. Le futur Code ne doit pas seulement « compiler », il doit abroger et simplifier pour supprimer ces zones de friction et de flou.

Quatre recommandations

Forts des constats énoncés supra, j'ai structuré trois scénarios autour de quatre recommandations transverses, présentes dans chaque scénario avec une intensité normative croissante :

- **R1** : Guichet unique de notification avec l'ANSSI/ANSC comme pivot redistribuant aux autorités sectorielles
- **R2** : Sanctuarisation du COMCYBER-MI via une codification dans le Code et une précision de l'articulation judiciaire et défense
- **R3** : Attribution souveraine des cyberattaques à travers un processus formalisé et une inscription des effets juridiques pour les victimes
- **R4** : Protection des individus et, plus particulièrement, des mineurs via un dispositif de résilience identitaire post-fuite, augmentation du périmètre de France Identité et une protection accrue des mineurs dans le Cyberespace.

Synthèse des 3 scénarios

Critère	Scénario 1	Scénario 2	Scénario 3
Recommandation	Applicable immédiatement — socle minimum non négociable	**Scénario de référence recommandé** — réalisable 24-36 mois	Horizon cible à 5 ans — à atteindre par étapes depuis le scénario 2
Niveau de transformation	Minimal (codification + coordination)	Modéré (concentration technique ANSSI + rationalisation des régulateurs + protection identitaire)	Ambitieux (refonte architecturale complète + résilience identitaire comme droit opposable)
Textes nécessaires	Loi de codification + ordonnances sectorielles + modification ANTS [Réf. à confirmer]	Loi ordinaire (Code) + modifications CMF / CSP / Loi I&L + décret abrogation CIAN + modification statut ANTS	Loi ordinaire + loi organique (PNC) + modification décret CDSN + décret abrogation CIAN + modification statut ANTS
Délai de mise en œuvre	12-18 mois	24-36 mois	36-60 mois
Statut de l'autorité technique cyber	ANSSI — service du Premier ministre (inchangé)	ANSSI — service du PM à compétences élargies	**ANSC — AAI** (précédent ASN/ASNR 2024)

Critère	Scénario 1	Scénario 2	Scénario 3
Unicité de l'autorité technique cyber (R1 — R2)	Non prévu — chaque régulateur conserve ses capacités techniques	Mandat légale d'expertise unique (ANSSI), pivot et guichet unique de redistribition de rapport contradictoire	Mandat légale d'expertise unique (ANSC AAI) — **valeur probatoire renforcée devant le PNC** et légitimité renforcée vis-à-vis des régulateurs de même rang
Sort de la LCEN (R1 — R2)	Partiellement absorbée — subsiste comme texte résiduel	Abrogée dans ses dispositions absorbées — résiduel codifié dans le Code et chez l'ARCOM	**Abrogation totale** comme texte autonome
Instance de coordination stratégique (R3)	SGDSN (rôle informel formalisé) + CIAN maintenu comme entité séparée	CNCyb — deux formations + coordination inter-institutionnelle + rapport annuel Parlement — missions du CIAN absorbées par formation plénière CNCyb (décret PM)	CSC (formation CDSN) — légitimité constitutionnelle + pilotage stratégique + rapport annuel Parlement
Chaîne judiciaire cyber (R4)	Concurrence OFAC/UNCYBER arbitrée par COMCYBER-MI sanctuarisé par le Code	COMCYBER-MI unifié + PHAROS intégré + magistrat de liaison permanent (JUNALCO/PNAT) + pôle usurpation identité	COMCYBER-MI unifié + **PNC** (modèle PNF) — interlocuteur judiciaire exclusif + **pôle protection mineurs dédié**
Accompagnement cybervictimes (R4)	ANTS — procédure créée par le Code — délai 72h révocation / 5j remplacement — gratuité pour la victime	ANTS + CRI dédiée — délais codifiés renforcés — créance de recouvrement coordonnée avec sanction CNIL + **solidarité sous-traitants**	ANTS + CRI proactive (surveillance darkweb, alerte préventive établissements financiers) + carte d'identité numérique provisoire
France Identité obligatoire (R4)	Périmètre restreint : services post-fuite + ouverture compte bancaire en ligne	Périmètre étendu : banque, crédit, assurance, EE/EI NIS2, santé numérique, vérification d'âge SREN	**Périmètre maximal** : tout renouvellement de titre + services publics sensibles + crypto-actifs + ensemble du périmètre scénario 2 + **mode mineur protégé France Identité**
Fonds de résilience identitaire - FRI (R4)	Création minimale — alimenté par sanctions CNIL + contributions EE/EI	FRI géré par ANTS — **conseil de surveillance** — dimension préventive (surveillance identité 5 ans)	FRI géré par ANTS — **gouvernance société civile** — surveillance proactive + programmes éducation identité numérique + États généraux triennaux

Critère	Scénario 1	Scénario 2	Scénario 3
Compatibilité NIS2 et eIDAS2	Partielle avec France Identité dans périmètre restreint	Complète + améliorée avec France Identité étendu	**Optimale** — ANSC AAI répond pleinement à l'art. 8 §1 NIS2 et France Identité comme implémentation nationale de référence eIDAS2
Compatibilité RGPD / DORA / DSA	Sous réserve validation EDPB guichet	Sous réserve avis EDPB mandatement ANSSI (art. 57 RGPD)	Optimale — avis EDPB requis sur mandatement + **validation CNIL sur France Identité obligatoire**
Lisibilité citoyenne	Moyenne — architecture existante sans simplification visible	Bonne — chaîne claire ANSSI (technique) → régulateur (juridique) → ANTS (identité) → citoyen (droits)	**Excellente** — ANSC identifiable, PNC comme juridiction dédiée, France Identité comme bouclier d'identité numérique
Risque juridique principal	Compatibilité guichet / art. 33 RGPD + [Réf. ANTS à confirmer pour révocation]	Compatibilité mandatement ANSSI / art. 57 RGPD + tension vie privée / France Identité étendu	Architecture bicéphale ANSC + **acceptabilité sociale France Identité obligatoire élargi** — validation CNIL préalable obligatoire
Risque institutionnel principal	Insuffisance structurelle — frictions normatives de fond non résolues	Résistance régulateurs sectoriels à cession expertise technique + résistance ANTS à nouvelle mission CRI	Résistance SGDSN (perte tutelle ANSC) + résistance MI sur périmètre France Identité maximal

Scénario 1

> Principe conducteur : *Le droit positif est globalement suffisant. Les frictions identifiées relèvent de lacunes de coordination, non d'une défaillance architecturale. Le Code codifie, clarifie et crée les mécanismes de liaison manquants sans modifier les équilibres institutionnels existants.*

Synthèse du scénario

Le scénario 1 repose sur le principe que le problème est **procédural, non structurel**. Les acteurs existants sont compétents et légitimes ; ce sont les mécanismes de liaison qui font défaut. L'ANSSI devient guichet unique de notification sans acquérir de nouveaux pouvoirs de sanction, préservant ainsi les équilibres entre autorités indépendantes. Le COMCYBER-MI est sanctuarisé dans le CSI, ce qui constitue l'innovation institutionnelle principale. Le processus d'attribution souveraine est codifié pour la première fois, créant des droits pour les victimes. La protection des individus dans le cyberespace est intégrée de façon pragmatique et opérationnelle : le protocole de résilience identitaire repose sur la chaîne ANSSI(détection/qualification) $\rightarrow$ ANTS (révocation/remplacement) $\rightarrow$ CNIL (sanction) $\rightarrow$ COMCYBER-MI (répression). L'innovation principale est la révocation administrative automatique des documents compromis, qui transforme une procédure individuelle et laborieuse en mécanisme de protection collective déclenché par la fuite elle-même. France Identité est rendu obligatoire dans un périmètre restreint — l'extension relève des scénarios 2 et 3. La protection des mineurs est renforcée à travers l'ARCOM et le référent mineur obligatoire. Le Fonds de résilience identitaire est créé dans sa forme minimale.

Le risque principal est l'insuffisance : les frictions entre NIS2 et DORA sur les délais de notification ne disparaissent pas — elles sont seulement gérées par le guichet. La qualification par l'ANSSI des données d'identité compromises dans le délai de 48 h exige un renforcement substantiel de ses effectifs ce type d'analyse.

Ce scénario est le plus rapidement réalisable (ordonnance de codification $+$ loi de ratification) mais **ne résout pas les incohérences normatives de fond**.

Tableau synoptique du scénario

Acteur Statut	**Mission principale**	**Reprise de compétences**	**Doublons supprimés**
ANSSI SCA renforcé	Cybersécurité nationale ; guichet unique R1 ; déclencheur du protocole R4 sur les fuites d'identité	Réception unifiée notifications ; notification ANTS en cas de fuite d'identité	Suppression des flux directs CNIL/ACPR/AMF/ANS pour la notification initiale
CNIL AAI (inchangée)	Protection DCP ; qualification violations ; sanctions RGPD ; garant du respect de R4 pour les mineurs	Reçoit notifications via ANSSI ; instruit les violations DCP incluant données de mineurs	Fin de la double saisine directe ANSSI $+$ CNIL

Acteur Statut	**Mission principale**	**Reprise de compétences**	**Doublons supprimés**
ARCOM AAI (inchangée)	Régulation plateformes (DSA/SREN) ; contenus illicites ; supervision des obligations R4 envers les mineurs	Contrôle du référent mineur obligatoire au sein des plateformes EE/EI	Fin du canal parallèle LCEN résiduelle
ANTS / France Identité (rôle formalisé — R4) Opérateur d'État	Gestion des titres d'identité ; révocation/remplacement automatique post-fuite (R4) ; déploiement France Identité (R4)	Reçoit les notifications de l'ANSSI ; déclenche la révocation et la procédure de remplacement ; gère le FRI en phase initiale	Fin de la procédure individuelle de déclaration de perte/vol pour les cas de fuite massive
COMCYBER-MI (sanctuarisé R2) Commandement ministériel codifié CSI	Pilotage PN/GN cyber ; PHAROS intégré ; magistrat de liaison ; enquêtes sur usurpations d'identité post-fuite	Compétence exclusive sur les infractions d'usurpation d'identité numérique aggravées (art. 226-4-1 CP étendu)	Fin de la concurrence OFAC/UNCYBER non arbitrée
SGDSN (pilote R3) Service du PM (inchangé)	Coordination interministérielle ; attribution souveraine R3 ; coordination interministérielle R4 (ANSSI/ANTS/CNIL/MI)	Pilotage du Collège d'attribution souveraine ; arbitrage R4 entre ANSSI, ANTS et CNIL	Formalisation d'une mission existante de facto
Autorités sectorielles (ACPR, AMF, ART, ANS) Statuts inchangés	Supervision sectorielle cyber (DORA, HDS, télécoms) ; réception des redistributions ANSSI	Suppression du reporting direct concurrent à l'ANSSI	Suppression du reporting direct concurrent à l'ANSSI

Scénario 2

Principe conducteur : *Les frictions actuelles ne relèvent pas seulement de lacunes procédurales — elles traduisent une fragmentation structurelle incompatible avec un Code lisible. Une rationalisation ciblée des compétences est nécessaire, sans fusion des grandes autorités indépendantes. L'ANSSI monte en puissance comme autorité de régulation cyber à part entière. Le COMCYBER-MI intègre une dimension de coordination judiciaire renforcée afin de diffuser la vision de la protection des individus (dont les mineurs) dans le cyberespace. La CNIL reprend sa place de garant des libertés dans le cyberespace en laissant la sécurité à l'ANSSI.*

Synthèse du scénario

Le scénario 2 opère une **rationalisation ciblée** : l'ANSSI monte en puissance sans devenir une super-autorité, la CNIL se spécialise sans perdre son indépendance, la LCEN est absorbée, PHAROS est intégré au COMCYBER-MI. La création du CNCyb, et l'absorbtion du CIAN est l'élément le plus novateur — elle répond au besoin d'un arbitre interministériel identifié.

La protection des individus dans le cyberespace devient un enjeu national avec la création de la Cellule de résilience identitaire au sein de l'ANTS et le renforcement du rôle de France Identité sont les innovations les plus visibles pour les citoyens. L'extension de France Identité comme solution obligatoire dans les contextes à risque constitue un changement de paradigme dans la gestion de l'identité numérique en France — cohérent avec eIDAS2 mais nécessite une campagne d'appropriation sociale importante. Le CNCyb en formation plénière assure que cette transition est accompagnée d'un dialogue avec la société civile.

Deux risques principaux :

— La résistance institutionnelle des autorités sectorielles (CNIL, AMF, ACPR) au transfert partiel de compétences de supervision cyber. Ce scénario nécessite plusieurs textes de niveau législatif (modification CMF, CSP, LCEN, loi SREN) mais reste dans le périmètre d'une loi ordinaire de codification,

— L'acceptabilité sociale de la révocation automatique des documents — les victimes pourraient vivre cette révocation comme une double peine ; le Code doit impérativement garantir la fluidité et la rapidité du remplacement.

Il est le scénario de référence recommandé pour l'avant-projet de Code.

Tableau synoptique du scénario

Acteur Statut	**Mission principale**	**Reprise de compétences**	**Doublons supprimés**
ANSSI SCA renforcé	Cybersécurité nationale ; guichet unique (R1) ; déclencheur du protocole (R4) sur les fuites d'identité	Réception unifiée notifications ; notification ANTS en cas de fuite d'identité	Suppression des flux directs CNIL/ACPR/AMF/ANS pour la notification initiale

Acteur Statut	**Mission principale**	**Reprise de compétences**	**Doublons supprimés**
CNIL (recentrée libertés/DCP) AAI (inchangée, périmètre redéfini)	Garant des libertés et DCP ; qualification juridique ; sanctions RGPD ; garant des droits des mineurs (R4) ; doctrine IA	Reçoit conclusions ANSSI ; instruit violations DCP incluant données mineurs ; émet les sanctions à l'encontre des entités (R4)	Fin de la double capacité technique CNIL/ANSSI
ARCOM (régulateur contenus consolidé) AAI	Régulation plateformes DSA/SREN ; absorption LCEN ; supervision renforcée protection mineurs (R4)	contrôle référent mineur obligatoire ; France Identité comme solution de conformité vérification d'âge	Suppression strate LCEN autonome
ANTS / France Identité (acteur clé R4) Opérateur d'État (renforcé par le Code)	Gestion des titres ; révocation/remplacement automatique (R4) ; France Identité obligatoire étendu (R4) ; gestion du FRI	Reçoit notifications qualifiées ANSSI ; gère le FRI ; recouvre les coûts auprès des entités responsables via procédure codifiée ; création de la Cellule de Résilience Identitaire	Fin de la procédure individuelle de déclaration de perte/vol pour les fuites massives
COMCYBER-MI (sanctuarisé R2 + R4) Commandement ministériel codifié CSI	Pilotage PN/GN cyber ; PHAROS intégré ; magistrat liaison permanent ; pôle usurpation d'identité numérique (R4)	Compétence exclusive usurpations d'identité post-fuite ; coordination ANTS pour suspensions d'urgence	Fin dualité PHAROS/OFAC/C3N non articulés
CNCyb (Conseil national pour le cyberespace) Instance coordination (décret PM) — deux formations	Coordination stratégique cyber ; attribution souveraine (R3) ; arbitrage conflits ; missions CIAN absorbées ; coordination interinstitutionnelle (R4)	Pilote le comité de suivi annuel (R4) ; arbitre les conflits ANSSI/ANTS/CNIL sur les procédures de résilience identitaire	Suppression CIAN comme entité séparée
Autorités sectorielles (ACPR/AMF/ANS) Statuts inchangés	Supervision sectorielle résiduelle (DORA, HDS) après guichet ANSSI ; pouvoirs de sanction intacts	Reçoivent la redistribution ANSSI ; conservent l'instruction sectorielle	Suppression du triple flux direct concurrent

Scénario 3

Principe conducteur : *Les frictions actuelles sont le symptôme d'une fragmentation institutionnelle irréductible par la seule coordination. Un Code véritablement lisible requiert une architecture institutionnelle unifiée autour d'un pôle de régulation cyber clairement identifiable par les citoyens et les opérateurs. Ce scénario crée une Autorité nationale de la sécurité dans le cyberespace (ANSC) fusionnant les missions régulatoires de l'ANSSI et intégrant un pôle protection des citoyens. Les AAI (CNIL, ARCOM) conservent leur indépendance mais voient leur périmètre rationalisé.*

Synthèse du scénario

Le scénario 3 repose sur un pari institutionnel fort : **l'ANSSI doit devenir une Autorité Administrative Indépendante (AAI)** pour être crédible comme régulateur cyber indépendant au sens du droit de l'Union Européenne et donner aux rapports techniques une valeur probatoire directement utilisable devant le PNC — la cohérence entre la régulation technique et la justice civile est ainsi garantie sans déperdition d'information. Le précédent ASN/ASNR (2024) le rend juridiquement plausible.

Ce scénario pousse la protection des citoyens dans le cyberespace à son terme logique : **la résilience identitaire des individus devient un droit opposable**, garanti par une chaîne institutionnelle complète allant de la détection (ANSC [4],ex-ANSSI) à la réparation judiciaire (PNC chambre civile) en passant par la protection administrative (ANTS) et la répression pénale (COMCYBER-MI).

La création du Parquet National Cyber (PNC) rationalise la chaîne judiciaire sur le modèle éprouvé du Parquet National Financier (PNF). Le Conseil de Sécurité du Cyberespace (CSC) donne enfin un cadre légal à l'attribution souveraine tout en offrant aux victimes un guichet judiciaire unique — fin de l'éparpillement juridictionnel.

France Identité, rendu obligatoire dans un périmètre maximal et activé automatiquement lors de l'émission de tout nouveau titre, devient le **pilier de l'identité numérique régalienne**.

Les risques sont élevés :

- La transformation de l'ANSSI en AAI rompt son lien avec le SGDSN et crée une tension sur la composante défense (la LID et la contribution à la LIO ne sont pas compatibles avec le statut d'AAI — **une scission ANSSI régulatrice / ANSSI défense** devra être envisagée)
- **L'acceptabilité sociale de France Identité obligatoire** et la tension avec le droit au respect de la vie privée — le Code doit impérativement prévoir des garanties fortes (minimisation, pseudonymisation, droit à l'opt-out dans les cas non critiques) validées par la CNIL avant l'entrée en vigueur.

Ce scénario est le plus cohérent sur le long terme mais le plus long à mettre en œuvre (3 à 5 ans) et implique des arbitrages politiques de premier ordre. Il est recommandé comme **horizon cible du Code**, à atteindre par étapes à partir du scénario 2.

Tableau synoptique du scénario

4. Autorité Nationale de Sécurité dans le Cyberespace

Acteur Statut	**Mission principale**	**Reprise de compétences**	**Doublons supprimés**
ANSC(ex-ANSSI) AAI créée par le Code	Régulation cyber unifiée : NIS2, certification, guichet (R1), injonction, sanction administrative cyber ; qualification technique des fuites d'identité (R4) avec valeur probatoire renforcée	Toutes missions ANSSI + supervision cyber ART + mandat technique CNIL/AMF/ACPR/ANS + qualification pour ANTS (R4)	Suppression de tous les doublons de supervision cyber sectorielle
CNIL (recentrée libertés/DCP) AAI (inchangée)	Garant libertés et DCP ; autorité de référence pour les droits des mineurs (R4) ; sanctions RGPD ; doctrine IA/données	Reçoit conclusions ANSC (AAI de même rang — indépendance renforcée) ; autorité de sanction principale (R4)	Fin tension subordination : CNIL reçoit conclusions d'une AAI de même rang
ARCOM (régulateur unifié contenus) AAI (inchangée)	Régulation plateformes DSA/SREN ; supervision renforcée protection mineurs (R4) ; LCEN abrogée intégralement	Contrôle référent mineur ; France Identité comme solution de conformité exclusive pour vérification d'âge	Abrogation totale LCEN comme texte autonome
ANTS / France Identité (acteur stratégique R4) Opérateur d'État — compétences étendues par le Code	Gestion des titres ; France Identité obligatoire élargi (R4) ; gestion autonome du FRI ; alerte proactive victimes	Reçoit rapports qualifiés ANSC (AAI) ; gère le FRI de façon autonome ; recouvrement via PNC (chambre civile)	Fin de la procédure individuelle ; guichet unique identitaire national
PNC (Parquet National Cyber) Juridiction spécialisée (loi organique)	Juridiction 1^er degré cyber ; chambre civile spécialisée (R4) — recouvrement des coûts de remplacement et réparation des victimes ; pilotage enquêtes COMCYBER-MI	Reprend le contentieux civil (R4) recouvrement ANTS, réparation victimes usurpation d'identité, actions en responsabilité contre entités responsables	Fin de la dispersion entre TGI locaux et juridictions commerciales pour ces litiges
COMCYBER-MI (sanctuarisé, liaison PNC exclusive) Commandement ministériel codifié CSI	Pilotage PN/GN cyber ; PHAROS intégré ; liaison PNC exclusive ; pôle usurpation d'identité et protection des mineurs (R4)	Compétence exclusive usurpations d'identité post-fuite + infractions pénales contre mineurs dans le cyberespace	Fin multiplicité interlocuteurs judiciaires
CSC (Conseil de Sécurité du Cyberespace) Formation CDSN — deux formations	Attribution souveraine (R3) ; arbitrage ANSC/CNIL/ARCOM ; pilotage stratégique (R4) ; missions CIAN absorbées en formation plénière	Absorbe totalement le CIAN ; pilote le comité stratégique (R4) ; rapport annuel Parlement	Suppression CIAN comme entité séparée

Liste des réglementations

AI Act Artificial Intelligence Act, règlement (UE) 2024/1689 du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle.. 1, 27

CMF Code Monétaire et Financier. 3, 8, 15, 18, 22

CP Code Pénal. 7

CRA Cyber Resilience Act, règlement (UE) 2024/2847 du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques.. 1, 26

CSI Code de la Sécurité Intérieure. 6, 7, 9, 11, 16–18, 23, 28

CSP Code de la Santé Publique. 3, 8, 22

DORA Digital Operationnal Resilience Act, règlement (UE) 2022/2554 du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier.. 1, 5–7, 9, 14, 15, 26

DSA Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques.. 2, 5, 7, 9, 11, 16, 21

LCEN Loi pour la Confiance dans l'Économie Numérique 2004-575. 2, 4, 7–9, 11, 16, 21

Loi I&L Loi Informatique et Liberté 1978 modifiée. 3

LOPMI Loi d'Orientation et de Programmation du Ministère de l'Intérieur 2023-22. 18

SREN La loi visant à Sécuriser et Réguler l'Espace Numérique (SREN)2024-449. 2, 4, 7, 9, 11, 15, 16, 21, 22

NIS2 Network and Information Security, directive (UE) 2022/2555 du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union.. 1, 2, 4–6, 11, 14, 17, 20, 22, 24, 26

eIDAS2 Règlement (UE) 2024/1183 du 11 avril 2024 relatif à une identité numérique. 5, 8, 15, 16

RGPD Règlement Général sur la Protection des Données, règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.. 1, 5, 9, 11, 14, 15, 17, 26–28

Liste des entités existantes

ACPR Autorité de Contrôle Prudentiel et de Résolution. 1, 6–9, 11, 18

AMF Autorité des Marchés Financiers. 1, 6–9, 11, 18

ANSSI Agence Nationale de la Sécurité des Systèmes d'Information. 1–11, 14, 15, 17–26

ANS Agence du Numérique en Santé. 1, 6–9, 11, 18

ANTS Agence Nationale des Titres Sécurisés. 3–11, 14–18, 20–22, 24, 27–29

ARCOM Autorité de régulation de la communication audiovisuelle et numérique. 4, 6, 7, 9–11, 15, 16, 21, 23, 24, 29

ART Autorité de régulation des transports. 7, 11, 18, 20

CDSN Conseil de Défense et de Sécurité Nationale. 3, 4, 11

CIAN Conseil de l'Intelligence Artificielle et du Numérique. 3, 4, 8, 9, 11

CNIL Commission Nationale de l'Informatique et des Libertés. 1, 5–11, 14–17, 20, 22–24, 27–29

COMCYBER-MI COMmandement dans le CYBERespace du Ministère de l'Intérieur. 2–4, 6–11, 14–18, 20, 21, 23, 24, 27–29

EDPB Comité européen de la protection des données ou European Data Protection Board. 5

DGSE Direction Générale de la Sécurité Extérieure. 2, 19, 29

DGSI Direction Générale de la Sécurité Intérieure. 2, 19, 29

OFAC OFfice Anti-Cybercriminalité. 2, 4, 7, 17

SGDSN Secrétariat Général de la Défense et de la Sécurité Nationale. 2, 4, 5, 10, 14, 18–20, 24, 26, 27, 29

Liste des entités issues de la proposition

ANSC Autorité Nationale de Sécurité dans le Cyberespace. 3–5, 10, 11, 26–29

CNCyb Conseil National pour le Cyberespace. 4, 8, 9, 20, 22–24

CRI Cellule de Résilience Identitaire. 4, 5, 9, 21

CSC Conseil de Sécurité du Cyberespace. 10, 11, 29, 30

PNC Parquet National Cyber. 3–5, 10, 11, 26–29

Liste des acronymes

AAI Autorité Administrative Indépendante. 3–7, 9–11, 16, 18, 20–22, 24, 26, 27

DCP Données à Caractère Personnel. 9, 11, 20, 22, 27

EE Entité Essentielle. 1, 2, 4, 7, 19, 20, 26, 29

EI Entité Importante. 2, 4, 7, 19, 20, 26, 29

FRI Fonds de Résilience Identitaire. 4, 9, 11, 15, 27–29

HDS Hébergement de Données de Santé. 1, 7, 9, 18, 26

LID Lutte Informatique Défensive, l'ensemble des mesures garantissant la disponibilité, la confidentialité et l'intégrité des systèmes d'information de défense. 10

LIO Lutte Informatique Offensive, opérations conduites pour perturber, altérer ou neutraliser les capacités numériques adverses. 2, 10

OIV Organisme d'Importance Vitale. 1, 2, 26

Annexes

Éléments détaillés du scénario 1

Agence Nationale de la Sécurité des Systèmes d'Information - ANSSI

Statut juridique

Service à compétence nationale rattaché au SGDSN, Premier ministre.
Statut inchangé — renforcement par voie législative dans le Code.
Tutelle : Premier ministre via SGDSN.

Compétences principales dans le scénario

- Autorité nationale compétente unique NIS2 (déjà consacrée par l'ordonnance 2024-821)
- Guichet unique de notification : réception de toute notification d'incident significatif quelle que soit la base légale déclencheuse (NIS2, DORA, RGPD, HDS, Code de la défense OIV), redistribution automatisée aux autorités sectorielles dans un délai normé (proposition : 4h pour les notifications urgentes)
- Certification, qualification des produits et prestataires (CSPN)
- Coordination du CERT-FR et du réseau des CSIRT sectoriels
- Contribution technique au processus d'attribution souverain

Évolution par rapport à l'existant

Le rôle de guichet unique est nouveau en droit mais prolonge naturellement la mission d'autorité compétente prévue par NIS2. Il nécessite une modification législative du Code monétaire et financier (art. L. 612-1), du Code de la santé publique (art. L. 1111-24) et de la loi Informatique et Liberté pour substituer l'ANSSI comme point de réception primaire unique. Les autorités sectorielles conservent intégralement leurs pouvoirs d'instruction et de sanction.

Déclencheur du protocole de résilience identitaire : Lorsque le guichet unique reçoit une notification d'incident dont l'analyse révèle la compromission de données d'identité régaliennes, l'ANSSI est tenue par le Code de :

1. Qualifier la nature et le volume des données d'identité compromises dans un délai de 48h à compter de la notification
2. Notifier automatiquement l'ANTS avec la liste des catégories de documents compromis et le volume estimé de victimes
3. Notifier la CNIL pour le volet violations de données personnelles (R1)
4. Notifier le COMCYBER-MI pour l'ouverture d'une enquête sur l'exploitation potentielle des données volées (usurpation d'identité, fraude documentaire)
5. Produire une fiche d'information publique sur la fuite (nature, données concernées, démarches conseillées) diffusée via cybermalveillance.gouv.fr

Justification juridique et opérationnelle

Le modèle s'inspire du mécanisme de coopération RGPD (art. 60 RGPD — autorité chef de file). Il est compatible avec DORA : le règlement prévoit lui-même (art. 19 §5) des dispositions de coordination avec les autorités NIS2. L'obstacle principal est d'ordre *infralégislatif* : les formats de notification

DORA (ABE/AEAPP/ESMA) sont européens et ne peuvent être fusionnés par le seul législateur national — le Code devra prévoir une clause de compatibilité européenne et un formulaire national servant de base à la redistribution. L'ANSSI est le seul acteur disposant des capacités techniques pour qualifier rapidement la nature des données compromises. Le déclenchement automatique du protocole de résilience (R4) ne requiert pas de décision administrative individuelle — il s'agit d'une procédure d'urgence codifiée dont le déclencheur est technique, non discrétionnaire.

ANTS / France Identité

Statut juridique

Agence nationale des titres sécurisés — établissement public administratif placé sous la tutelle du ministère de l'Intérieur. France Identité est un service opéré par l'ANTS, fondé sur le règlement eIDAS2.
Tutelle : Ministère de l'Intérieur.

Compétences principales dans le scénario

Révocation et remplacement des documents compromis Sur notification de l'ANSSI, l'ANTS déclenche dans un délai de 72 h :

- La révocation administrative des documents d'identité compromis (inscription au fichier des titres invalidés — FTI [Référence à confirmer])
- L'envoi d'un courrier recommandé et d'un message électronique à chaque victime identifiable, l'informant de la révocation et de la procédure de remplacement
- L'ouverture d'un guichet prioritaire de remplacement (délai accéléré de 5 jours ouvrés vs délai normal)
- La gratuité totale de la procédure pour la victime — les frais sont consignés en vue du recouvrement auprès de l'entité responsable.

Mécanisme de recouvrement des coûts L'ANTS émet une créance administrative à l'encontre de l'entité responsable de la fuite, notifiée simultanément à la CNIL (procédure de sanction RGPD) et au COMCYBER-MI (procédure pénale éventuelle). En cas de contestation, le contentieux relève du tribunal administratif. En cas d'insolvabilité ou d'impossibilité d'identification de l'entité responsable, le Fonds de résilience identitaire (FRI) prend en charge les coûts — le Code prévoit une action subrogatoire du FRI contre le responsable.

France Identité obligatoire dans les cas à risque Le Code définit les cas d'usage obligatoire dans le scénario 1 de façon restreinte (périmètre minimal) :

- Services ayant subi une fuite de données dans les 24 mois précédents : obligation temporaire de recourir à France Identité pour toute nouvelle création de compte
- Ouverture de compte bancaire en ligne (via modification du CMF par voie d'ordonnance de codification).

Protection des mineurs — rôle de l'ANTS France Identité intègre un mécanisme de vérification de l'âge mineur opposable aux plateformes — alternative à la vérification d'âge ARCOM/SREN, plus robuste car fondée sur l'identité régalienne. Les plateformes soumises à l'obligation de vérification d'âge (loi SREN) peuvent utiliser France Identité comme solution de conformité.

Justification juridique

La révocation administrative des titres d'identité n'est pas explicitement prévue dans ce cas de figure par le droit positif — le Code crée cette compétence par voie législative, en complétant les procédures ANTS. Le règlement eIDAS2 fournit la base européenne pour l'obligation d'acceptation de France Identité par les services en ligne.

Autorité de régulation de la communication audiovisuelle et numérique - ARCOM

Statut juridique

Autorité administrative indépendante (AAI) — loi n° 2021-1382 du 25 octobre 2021. Statut inchangé.
Tutelle : Indépendante (AAI).

Compétences principales dans le scénario

- Coordinateur des services numériques (CSN) au titre du DSA
- Retrait des contenus illicites (terrorisme, pédopornographie, manipulation de l'information)
- Supervision des VLOP (Very Large Online Platforms)
- Articulation clarifiée avec PHAROS : le Code établit que PHAROS oriente vers la voie pénale (COMCYBER-MI) et l'ARCOM vers la voie administrative/régulatoire — critère de bifurcation défini dans le Code

- Contrôle du référent mineur obligatoire au sein des plateformes et VLOP — l'ARCOM peut mettre en demeure et sanctionner les plateformes ne désignant pas ce référent
- Supervision des mécanismes de vérification d'âge (loi SREN étendue par le Code) — France Identité reconnu comme solution de conformité de référence
- Pouvoir d'injonction de suspension de service à l'encontre des plateformes exposant délibérément des mineurs à des contenus préjudiciables, en coordination avec le COMCYBER-MI pour la dimension pénale.

Évolution par rapport à l'existant

Introduction d'un protocole d'articulation codifié ARCOM/COMCYBER-MI/PHAROS pour les signalements à double dimension (administrative et pénale) et renforcement de la protection des mineurs dans le cyberespace. La LCEN résiduelle est partiellement abrogée dans ses dispositions absorbées par le DSA et codifiées dans le futur Code.

Justification juridique et opérationnelle

Aucune modification du statut d'AAI n'est requise. La clarification procède par voie d'articles de coordination dans le Code (analogie avec les articles de coordination entre CSI et CPP).

Commission Nationale de l'Informatique et des Libertés - CNIL

Statut juridique

Autorité administrative indépendante — statut inchangé (loi n° 78-17 modifiée).
Tutelle : Indépendante.

Compétences principales dans le scénario

- Contrôle de la licéité des traitements de données personnelles (RGPD, loi I&L)
- Instruction des violations de données redistribuées par l'ANSSI
- Pouvoir de sanction administrative (art. 83 RGPD)
- Avis sur les textes réglementaires
- Autorité chef de file dans le mécanisme européen (EDPB).

Évolution par rapport à l'existant

La CNIL perd le flux direct de notification initiale pour les entités soumises à NIS2 — elle reçoit de l'ANSSI les notifications comportant des données personnelles dans le délai réglementaire (72h RGPD préservé). Elle conserve l'intégralité de ses pouvoirs d'instruction et de sanction. Le Code précise explicitement que la redistribution par l'ANSSI vaut notification au sens de l'art. 33 RGPD, ce qui requiert une vérification de compatibilité avec le RGPD (règlement d'applicabilité directe — [interprétation à valider avec le EDPB]).

Justification juridique et opérationnelle

L'art. 33 §1 RGPD oblige à notifier « à l'autorité de contrôle compétente » — une loi nationale ne peut modifier ce flux. La solution retenue est donc un mandat légal confié à l'ANSSI d'agir comme mandataire de transmission, la notification CNIL restant juridiquement distincte mais techniquement fusionnée. Ce mécanisme est juridiquement défendable sous réserve de validation par le EDPB.

Commandement du ministère de l'Intérieur pour le cyberespace - COMCYBER-MI

Statut juridique

Commandement ministériel. Sanctuarisé par le Code dans le CSI (nouveau Livre dédié).
Tutelle : Ministre de l'Intérieur.

Compétences principales dans le scénario

- Pilotage unifié des capacités cyber de la PN (OFAC) et de la GN (UNCyber) — règle de compétence primaire inscrite dans le Code
- Règles de dessaisissement entre OFAC et UN Cyber : critère fonctionnel (nature de l'infraction, montant, secteur victime) codifié dans le CPP par renvoi
- Articulation judiciaire : protocole légal de liaison avec les parquets spécialisés (JUNALCO, PNAT) — saisine formalisée
- Coordination avec l'ANSSI : procédure codifiée pour les incidents à double dimension technique et pénale (incident NIS2 donnant lieu à des poursuites) — clause de transmission mutuelle d'information dans le Code
- Interface COMCYBER des Armées : clause de compétence codifiée pour le basculement vers le COMCYBER/MinArm en cas de menace étatique caractérisée — critères objectifs définis dans le Code
- Compétence primaire et exclusive (codifiée) pour les enquêtes relatives aux usurpations d'identité numériques consécutives à une fuite de données (art. 226-4-1 CP étendu par le Code)
- Réception des signalements ANTS sur les cas d'utilisation frauduleuse de documents compromis
- Procédure d'urgence codifiée : en cas d'usurpation avérée causant un préjudice immédiat (ouverture de crédit frauduleux, accès à des services de santé, fraude aux prestations sociales),

le COMCYBER-MI peut requérir en urgence la suspension du document usurpé auprès de l'ANTS sans attendre l'issue de l'enquête.

Évolution par rapport à l'existant

Passage d'une existence de fait (organisation administrative interne) à une existence de droit dans le CSI. C'est l'évolution majeure de ce scénario.

Justification juridique et opérationnelle

LOPMI 2023 a amorcé cette consécration. Le Code la parachève en lui conférant une base législative opposable définissant le périmètre, les règles de liaison et les critères de compétence. Aucune révision constitutionnelle n'est nécessaire — le COMCYBER-MI reste un commandement ministériel, non une autorité indépendante.

Autorités sectorielles (ACPR, AMF, ART, ANS)

Statut juridique

Statuts inchangés (AAI pour AMF, ACPR adossée à la Banque de France, ART AAI, ANS GIP).
Tutelles : Inchangées.

Compétences principales dans le scénario

- Réception des notifications redistribuées par l'ANSSI dans leur périmètre sectoriel
- Instruction et contrôle sectoriels (DORA pour ACPR/AMF, L. 33-14 CPCE pour ART, HDS pour ANS)
- Pouvoir de sanction sectoriel inchangé.

Évolution par rapport à l'existant

Le flux entrant de notification est réorganisé — les autorités sectorielles ne reçoivent plus directement la notification initiale des entités mais instruisent sur dossier redistribué. Leurs pouvoirs d'instruction et de sanction sont intégralement préservés.

Justification juridique et opérationnelle

Nécessite une modification des textes sectoriels (CMF, CSP) pour prévoir la clause de réception via ANSSI — modifications de faible intensité normative, techniquement réalisables par ordonnance de codification.

SGDSN - Pilote du processus d'attribution souveraine

Statut juridique

Service du Premier ministre — inchangé. Le Code lui confie explicitement le secrétariat du Collège d'attribution souveraine.
Tutelle : Premier ministre.

Compétences principales dans le scénario

- Coordination interministérielle cyber (inchangée)
- Nouveau : pilotage du processus d'attribution souveraine codifié dans un Titre dédié du Code :
  - Acteurs habilités : ANSSI (analyse technique), DGSI (renseignement intérieur), DGSE (renseignement extérieur), SGDSN (synthèse), MEAE (dimension diplomatique) — liste limitative dans le Code
  - Régime de classification : les conclusions techniques sont classifiées ; la décision d'attribution publique appartient au Premier ministre sur avis du SGDSN
  - Effets juridiques : l'attribution publique ouvre un droit à indemnisation administrative des victimes (personnes morales et physiques EE/EI) et autorise des mesures de gel d'avoirs ou d'interdiction d'accès au marché à l'encontre des entités liées à l'acteur désigné — sur le modèle du régime de sanctions cyber de l'UE (règlement 2019/796)

Évolution par rapport à l'existant

Formalisation législative d'un processus existant de facto mais non codifié. L'essentiel tient dans la création des effets juridiques de l'attribution au profit des victimes — innovation normative majeure mais juridiquement plausible par analogie avec les régimes d'indemnisation des victimes du terrorisme.

Éléments détaillés du scénario 2

ANSSI — Autorité nationale de cybersécurité à compétences élargies

Statut juridique

Service à compétence nationale — statut inchangé mais compétences matérielles élargies par le Code (modification de l'ordonnance 2024-821 et du décret 2009-834).
Tutelle : Premier ministre / SGDSN.

Compétences principales dans le scénario

- Guichet unique de notification — identique au scénario 1 mais formalisé dans un article de loi autonome du Code (non par renvoi)
- Nouveau pouvoir d'injonction directe aux EE et EI pour remédier à des manquements constatés (analogie avec les pouvoirs de l'ARCEP sur les opérateurs télécoms au titre du L. 33-14 CPCE) — sans attendre la procédure de sanction administrative
- Absorption de la supervision cyber des opérateurs de communications électroniques (art. L. 33-14 CPCE) : l'ART conserve la régulation économique des télécoms mais transfère la supervision de sécurité des réseaux à l'ANSSI — alignement avec NIS2 qui désigne l'ANSSI comme ANC pour ce secteur
- Homologation des SI des autorités administratives (inchangée)
- Contribution technique au CNCyb pour l'attribution souveraine

Évolution par rapport à l'existant

L'ANSSI franchit un seuil institutionnel : elle cesse d'être un service d'assistance et de conseil pour devenir une autorité de régulation cyber à part entière, dotée de pouvoirs d'injonction. Cette évolution est juridiquement plausible sans révision constitutionnelle (l'ANSSI n'est pas dotée de la personnalité morale mais ses pouvoirs d'injonction peuvent être conférés par la loi, comme pour d'autres services à compétence nationale). l'ANSSI ne se contente pas de qualifier l'incident — elle qualifie la nature et la sensibilité des données compromises, notamment leur caractère d'identité régalienne, et produit à destination de l'ANTS un rapport technique d'identification des victimes (volume, catégories de documents, entité responsable, niveau de certitude de la compromission). Ce rapport ANTS est distinct du rapport CNIL (violation de DCP) et du rapport COMCYBER-MI (dimension pénale) — la triple diffusion est automatique et simultanée, orchestrée par le guichet unique. Délais codifiés dans le scénario 2 :

- 24h : alerte initiale (incident significatif avec possible composante identitaire)
- 48h : qualification technique confirmée des données d'identité compromises
- 72h : rapport complet transmis à ANTS, CNIL, COMCYBER-MI simultanément
- 7 jours : rapport détaillé sur les victimes identifiables transmis à l'ANTS pour déclenchement individuel des procédures de remplacement.

Justification juridique et opérationnelle

Le modèle de référence est l'ARPA (Agence de la Biomédecine) ou l'ASN (Autorité de Sûreté Nucléaire) — services ou autorités sectorielles dotés de pouvoirs contraignants sans être des AAI au sens strict. Le transfert de la supervision cyber des télécoms de l'ART vers l'ANSSI répond à la logique NIS2 (l'ANSSI est déjà l'ANC — avoir deux superviseurs cyber pour les mêmes opérateurs est une anomalie structurelle).

ARCOM — Intégration des dispositions LCEN

Statut juridique

AAI inchangée.
Tutelle : Indépendante.

Compétences principales dans le scénario

- Régulation des plateformes (DSA/SREN — inchangée)
- Absorption des dispositions résiduelles de la LCEN relatives à la responsabilité des hébergeurs (non couvertes par le DSA) et au régime de signalement des contenus
- La cryptologie commerciale (déclaration/autorisation — art. 29 à 36 LCEN) est transférée à l'ANSSI, compétente en matière de produits de sécurité
- PHAROS devient une unité du COMCYBER-MI (voir fiche infra)

Évolution par rapport à l'existant

L'ARCOM devient le réceptacle de la codification des obligations des intermédiaires en ligne, mettant fin à la coexistence LCEN/DSA/SREN. La LCEN est abrogée dans ses dispositions absorbées.

Justification juridique et opérationnelle

La loi SREN de 2024 a déjà opéré une intégration partielle. Le Code parachève ce mouvement. L'abrogation de la LCEN résiduelle est une mesure de codification classique (analogie avec l'abrogation des lois codifiées lors de l'adoption d'un code).

ANTS / France Identité

Statut juridique

Établissement public administratif
Tutelle : Ministère de l'Intérieur.

Évolution par rapport à l'existant

L'ANTS devient un acteur de premier plan de la chaîne de protection post-fuite, avec des obligations de résultat codifiées. Le Code crée au sein de l'ANTS une Cellule de Résilience Identitaire (CRI) — unité dédiée au traitement des fuites massives de données d'identité, dotée d'effectifs et de moyens propres, opérationnelle 24h/24.
La procédure codifiée est la suivante :

1. Réception du rapport ANSSI $\rightarrow$ activation de la CRI dans les 4h
2. Croisement avec les bases de gestion des titres $\rightarrow$ identification des victimes dans les 48h
3. Révocation des documents compromis $\rightarrow$ inscription au FTI dans les 72h
4. Notification individuelle des victimes (courrier recommandé $+$ notification France Identité si compte actif $+$ SMS) dans les 5 jours
5. Ouverture du guichet de remplacement prioritaire (5 jours ouvrés) $\rightarrow$ gratuité totale
6. Émission de la créance de recouvrement à l'encontre de l'entité responsable dans les 10 jours

Mécanisme de recouvrement renforcé dans le scénario 2 Le Code crée une solidarité de responsabilité entre l'entité responsable directe et ses sous-traitants ayant contribué à la fuite (en cohérence avec l'art. 28 RGPD sur les sous-traitants). La CNIL coordonne ses sanctions RGPD avec la créance ANTS pour éviter le cumul disproportionné — le Code prévoit un mécanisme d'imputation coordonnée (la sanction CNIL intègre le remboursement ANTS).
Le Code étend l'obligation à :

- Ouverture de compte bancaire ou de paiement en ligne (CMF modifié)
- Souscription à un crédit ou une assurance en ligne (CMF modifié)
- Création de compte sur toute plateforme EE/EI soumise à NIS2 (ordonnance 2024-821 étendue)
- Accès aux services de santé numériques (CSP modifié)
- Tout service ayant subi une fuite de données dans les 24 mois (obligation temporaire renforcée)
- Vérification d'âge pour les plateformes soumises à la loi SREN (France Identité comme solution de conformité de référence)

France Identité intègre un mode mineur protégé Lorsque le porteur est mineur, le service génère une attestation d'âge sans révéler la date de naissance exacte ni l'identité complète (conformément au principe de minimisation — art. 5 RGPD). Les plateformes utilisant France Identité pour la vérification d'âge reçoivent uniquement un certificat booléen (majeur/mineur) — protection de la vie privée des mineurs par conception.
Le Code crée un Fonds de résilience identitaire (FRI) ; L'ANTS est désignée gestionnaire du FRI dans le scénario 2. Le FRI est alimenté par :

- Les sanctions RGPD affectées par décision de la CNIL (fraction définie dans le Code)
- Une contribution obligatoire des EE/EI traitant des données d'identité à grande échelle (barème défini par décret en fonction du volume et de la sensibilité des données traitées)
- Les recouvrements effectués auprès des entités responsables

Le FRI finance la prise en charge immédiate des victimes dans l'attente du recouvrement et couvre les cas d'irrecouvrabilité.

CNIL — Pôle cyber dédié

Statut juridique

AAI inchangée — création d'une formation spécialisée interne (analogie avec la formation restreinte existante, sur le modèle des chambres spécialisées du Conseil d'État).
Tutelle : Indépendante.

Compétences principales dans le scénario

- Instruction des violations de données dans le cyberespace via le flux ANSSI et coordination de sa sanction avec la créance ANTS (mécanisme d'imputation coordonnée décrit supra)
- Pôle cyber : formation collégiale dédiée aux affaires à dimension cyber (violations massives, profilage par IA, dark patterns)
- Nouveau : compétence exclusive sur le profilage commercial illicite (retrait de la DGCCRF qui conserve les pratiques commerciales déloyales non liées au traitement de données)
- Participation au CNCyb pour les sujets à dimension DCP
- Compétence exclusive de sanction pour les manquements aux obligations de protection des données de mineurs (profilage interdit, droit à l'effacement renforcé, référent mineur obligatoire).

Évolution par rapport à l'existant

La CNIL ne change pas de statut mais se spécialise dans le cyber. La répartition avec la DGCCRF est clarifiée par le Code : le critère de compétence est la présence ou non d'un traitement de données personnelles dans la pratique contestée. La coordination avec l'ARCOM pour les plateformes — la CNIL contrôle le volet données personnelles des mineurs, l'ARCOM contrôle le volet exposition aux contenus.

Justification juridique et opérationnelle

La CNIL dispose déjà d'une formation restreinte pour les sanctions. La création d'une formation spécialisée est une mesure d'organisation interne ne nécessitant qu'une modification du règlement intérieur de la CNIL, approuvé par décret. Le transfert partiel de compétences DGCCRF nécessite un article de coordination dans le Code.

COMCYBER-MI — Commandement avec magistrat de liaison permanent

Statut juridique

Commandement ministériel sanctuarisé dans le CSI (Nouveau Livre).
Innovation du scénario 2 : intégration de PHAROS et désignation d'un magistrat de liaison permanent détaché du parquet spécialisé.
Tutelle : Ministre de l'Intérieur, avec liaison fonctionnelle avec le garde des Sceaux pour la composante judiciaire.

Compétences principales dans le scénario

- Pilotage unifié PN/GN cyber (identique au scénario 1)
- PHAROS intégré : la plateforme de signalement devient une unité organique du COMCYBER-MI, mettant fin à l'autonomie non structurée de PHAROS
- Magistrat de liaison permanent : un magistrat du parquet (JUNALCO ou PNAT selon spécialité) est détaché à titre permanent auprès du COMCYBER-MI — modèle des magistrats de liaison internationaux, prévu par accord entre la Chancellerie et le Ministère de l'Intérieur
- Coordination avec l'ANSSI : procédure codifiée dans le CSI pour les incidents à double dimension (seuil de déclenchement défini, délai de partage d'information, désignation d'un officier de liaison ANSSI-COMCYBER-MI permanent)
- Interface COMCYBER Armées : critères légaux de basculement définis dans le Code (niveau de la menace, caractérisation étatique par le CNCyb).

Évolution par rapport à l'existant

L'intégration de PHAROS est la principale évolution — elle simplifie la chaîne de traitement des signalements et clarifie la bifurcation pénal/administratif. Le magistrat de liaison permanent est une innovation procédurale sans équivalent exact en droit français (à confirmer).

Justification juridique et opérationnelle

L'intégration de PHAROS dans le COMCYBER-MI est une mesure d'organisation administrative interne au Ministère de l'Intérieur, ne nécessitant qu'un décret de réorganisation. La désignation du magistrat de liaison requiert un accord entre le Garde des Sceaux et le Ministre de l'Intérieur formalisé par arrêté conjoint.

Conseil National de Cybersécurité (CNCyb) — Instance nouvelle

Statut juridique

Instance de coordination interministérielle créée par décret du Premier ministre (analogie avec le Conseil national du numérique ou le SGDSN lui-même dans sa dimension de coordination).
Pas d'AAI — pas de personnalité morale propre.
Tutelle : Premier ministre / SGDSN (secrétariat assuré par le SGDSN).

Compétences principales dans le scénario

- Coordination stratégique des acteurs du Code (ANSSI, CNIL, ARCOM, COMCYBER-MI, autorités sectorielles) — réunions périodiques et réunions de crise
- Arbitrage des conflits de compétence entre acteurs du Code — décision du Premier ministre sur proposition du CNCyb
- Secrétariat du processus d'attribution souveraine :
  - Réunit les acteurs habilités (ANSSI, DGSI, DGSE, MEAE, SGDSN)
  - Produit une analyse consolidée transmise au Premier ministre
  - Gère le régime de classification des conclusions
  - Notifie les effets juridiques aux victimes après décision d'attribution publique
- Coordinateur de la protection des citoyens dans le cyberespace :
  - Arbitrage des conflits de compétence ANSSI/ANTS/CNIL/COMCYBER-MI lors des crises de fuite massive (ex : fuite touchant plusieurs millions de victimes)
  - Décision de déclenchement du FRI en urgence
  - Consultation citoyenne périodique sur l'extension du périmètre de France Identité obligatoire
  - Recommandations sur l'éducation numérique des mineurs — articulation avec l'Éducation Nationale et les associations de protection de l'enfance.

Évolution par rapport à l'existant

Le CNCyb formalise et structure une coordination interministérielle qui existe de façon ad hoc au sein du SGDSN. Il n'a pas de pouvoir décisionnel propre — il prépare les décisions du Premier ministre. Sa création par décret est suffisante ; le Code peut simplement y faire référence. Le CNCyb est un acteur central de la protection des citoyens dans le cyberespace et produit un rapport annuel au Parlement comportant un volet dédié à la protection des individus et des mineurs dans le cyberespace

Justification juridique et opérationnelle

La création d'une instance de coordination sans personnalité juridique propre est une technique classique du droit administratif français (Comité interministériel, Conseil national…). Le risque de bureaucratisation est réel — le Code doit définir un rythme de réunion contraint et des obligations de résultat (délai d'arbitrage, délai de traitement de l'attribution).

Autorités sectorielles consolidées

Statut juridique

Inchangé — mais le Code crée un mécanisme formel de délégation d'instruction de l'ANSSI vers les autorités sectorielles pour les incidents NIS2 à dimension sectorielle forte.

Évolution par rapport à l'existant

Passage d'une réception directe concurrente à une instruction déléguée formalisée dans le Code, avec délais et obligations de retour vers l'ANSSI.

Éléments détaillés du scénario 3

ANSC — Autorité Nationale de Sécurité dans le Cyberespace

Statut juridique

Autorité administrative indépendante créée par la loi portant Code de la sécurité dans le cyberespace. Dotée de la personnalité morale, d'un budget propre, d'un collège délibérant et de pouvoirs de sanction administrative.
Tutelle : Indépendante — analogie avec l'ANSSI devenant AAI sur le modèle de l'ASN devenue ASNR (Autorité de sûreté nucléaire et de radioprotection) par la loi n° 2024-364 du 22 avril 2024 qui constitue un précédent immédiatement transposable.

Compétences principales dans le scénario

- Guichet unique de notification : réception de toute notification d'incident (NIS2, DORA, RGPD, HDS, OIV) — redistribution aux autorités sectorielles compétentes
- Supervision unifiée des entités NIS2 (EE et EI) et des OIV à composante non militaire (selon nomenclature unifiée du Code)
- Pouvoir d'injonction et de sanction administrative (jusqu'à 2% du CA mondial pour les EI, 4% pour les EE — alignement NIS2)
- Certification et qualification des produits et prestataires (CSPN, PRIS)
- Surveillance du marché CRA (Cyber Resilience Act) — autorité de surveillance nationale au sens du règlement 2024/2847 (compétence actuellement non attribuée)
- Coordination du réseau des CSIRT sectoriels
- Contribution technique au Conseil de sécurité du cyberespace
- Qualification des fuites de données avec valeur probatoire directe devant le PNC (chambre civile)
- Publication d'un registre public des fuites d'identité (anonymisé sur les victimes, nominatif sur les entités responsables) — transparence renforcée, pression réputationnelle sur les entités défaillantes.

Évolution par rapport à l'existant

L'ANSC est la transformation de l'ANSSI en AAI — mouvement institutionnel majeur mais techniquement possible : cf. la transformation de l'ASN en ASNR en 2024. Les agents de l'ANSSI sont transférés à l'ANSC. Le rattachement au SGDSN est rompu — l'ANSC devient indépendante du pouvoir exécutif pour ses décisions régulatoires, ce qui renforce sa légitimité européenne (NIS2 exige une autorité compétente « fonctionnellement indépendante »). La direction défense à régime classifié de l'ANSC traite les fuites d'identité affectant des données régaliennes sensibles (membres des forces de sécurité, personnel de renseignement, agents protégés) avec un protocole distinct et classifié — la révocation et le remplacement des documents de ces personnes est opérée par voie spéciale non publique.

Justification juridique et opérationnelle

NIS2 (art. 8 §1) exige que les autorités compétentes soient « fonctionnellement indépendante des entités qu'elles supervisent ». L'ANSSI actuelle, service du Premier ministre, est dans une position structurellement ambiguë pour superviser les SI gouvernementaux. La transformation en AAI résout cette tension. Le précédent ASN/ASNR est juridiquement solide.

La principale résistance viendra du SGDSN et des services de l'État qui perdent leur tutelle sur l'agence.

CNIL — Recentrage sur la protection des données personnelles

Statut juridique

AAI inchangée — périmètre redéfini par le Code.

Compétences principales dans le scénario

- Protection des données personnelles stricto sensu (RGPD, loi I&L)
- Reçoit de l'ANSC les notifications comportant des DCP dans le délai réglementaire RGPD
- Cède à l'ANSC la compétence d'instruction des incidents techniques mixtes (cyber + DCP) pour la phase d'urgence — la CNIL reprend l'instruction dans sa sphère dès la phase de stabilisation
- Conserve l'intégralité de son pouvoir de sanction RGPD
- Recentrage sur les droits des personnes, la conformité des traitements, l'AI Act.

Évolution par rapport à l'existant

La CNIL perd la primo-réception des incidents cyber — elle reste l'autorité compétente au sens du RGPD mais délègue la gestion de crise initiale à l'ANSC. Cette évolution requiert une validation par le EDPB[5] (art. 33 RGPD ne prévoit pas de délégation formelle — [mécanisme à expertiser avec le EDPB]).

ANTS / France Identité

Statut juridique

Établissement public administratif
Tutelle : Ministère de l'Intérieur.

Compétences principales dans le scénario

- Surveillance active des marchés illicites (darkweb, forums de revente de données) pour détecter les documents compromis même en l'absence de notification formelle — en coordination avec le COMCYBER-MI
- Alerte préventive aux établissements financiers, organismes sociaux et services de santé référencés dans les données compromises — pour bloquer préventivement toute tentative d'usurpation avant même que la victime n'ait été notifiée
- Carte d'identité d'urgence numérique : en attendant le remplacement physique du document, l'ANTS délivre via France Identité une attestation numérique provisoire valable 30 jours, permettant à la victime d'accéder aux services essentiels
- France Identité obligatoire dans des périmètres élargis (renouvellement de tout titre d'identité, fiscalité, prestations sociales, justice, plateformes de financement et d'investissement) — France Identité comme seule modalité d'authentification forte
- Conseil de surveillance du FRI comprenant des représentants de la société civile (associations de victimes, associations de protection des consommateurs), un représentant de la CNIL et un représentant du PNC

5. European Data Protection Board

— Recouvrement via le PNC, cette chambre civile spécialisée offre aux victimes un accès simplifié à la justice — une seule juridiction pour l'ensemble du contentieux civil lié à la fuite, évitant l'actuel éparpillement entre tribunaux judiciaires locaux. (cf. infra).

Évolution par rapport à l'existant

L'ANTS voit son rôle élevé au rang d'acteur stratégique de l'identité numérique, avec une autonomie renforcée dans la gestion du FRI et une articulation directe avec le PNC pour le recouvrement.

Parquet National Cyber (PNC) — Nouvelle juridiction spécialisée

Statut juridique

Juridiction spécialisée créée par la loi portant Code — modification du Code de l'organisation judiciaire. Modèle : Parquet National Financier (PNF) ou JUNALCO. Siège à Paris, compétence nationale.
Tutelle : Ministère de la Justice (mais indépendance juridictionnelle garantie).

Compétences principales dans le scénario

— Compétence de premier degré pour les infractions cyber d'une certaine gravité (seuil défini dans le Code — montant du préjudice, caractère organisé, dimension internationale)
— Pilotage des enquêtes menées par le COMCYBER-MI (OFAC et C3N) — saisine directe
— Magistrat de liaison permanent avec l'ANSC pour les incidents à double dimension régulatoire et pénale
— Chambre civile spécialisée pour les litiges relatifs aux actifs numériques, vol de crypto-actifs, swatting (volet réparation), fuite de données d'identité et protection des mineurs
— Coordination internationale (Europol EC3, INTERPOL IGCI).

Évolution par rapport à l'existant

Le PNC rationalise la dispersion actuelle entre JUNALCO (fraude informatique), PNAT (cyberterrorisme) et parquets cyber locaux. Il ne supprime pas ces structures mais fixe un chef de file clair pour les affaires complexes. Les décisions de sanction administrative de la CNIL (RGPD) et les injonctions de l'ANSC constituent des éléments de preuve recevables devant la chambre civile du PNC — le Code prévoit leur valeur probatoire et les modalités de leur production en justice.
La création nécessite une loi organique pour la partie organisation judiciaire et une loi ordinaire pour les règles de compétence.

Justification juridique et opérationnelle

Le précédent du PNF (Parquet National Financier) — créé par la loi n° 2013-1117 du 6 décembre 2013 — est directement transposable. La cybercriminalité a atteint un niveau de sophistication et de volume (rançongiciels, cryptofraudes, attaques étatiques) qui justifie le même traitement institutionnel que la corruption et la fraude fiscale.

COMCYBER-MI — Pleine sanctuarisation et liaison PNC

Statut juridique

Commandement ministériel sanctuarisé dans le CSI (Livre VI nouveau). Dans ce scénario, le COMCYBER-MI est l'interlocuteur exclusif du PNC pour les enquêtes cyber judiciaires — unicité de la chaîne de commandement opérationnelle.
Tutelle : Ministère de l'Intérieur.

Compétences principales dans le scénario

- Pôle usurpation d'identité numérique : Unité spécialisée au sein du COMCYBER-MI, dédiée aux infractions consécutives aux fuites d'identité, coordination en temps réel avec la CRI de l'ANTS pour les cas d'usurpation active
- Pôle protection des mineurs dans le cyberespace : Unité dédiée aux infractions pénales commises contre des mineurs dans le cyberespace (harcèlement, grooming[6], exposition à des contenus préjudiciables, exploitation d'images), articulation avec l'ARCOM (signalements PHAROS → ARCOM pour la dimension régulatoire → COMCYBER-MI pour la dimension pénale), procédure d'urgence codifiée pour les mineurs en danger immédiat : déclenchement dans les 2h d'une procédure de protection en coordination avec les services sociaux et le parquet du PNC.

Justification juridique et opérationnelle

L'interlocuteur judiciaire unique est le PNC (non plus plusieurs parquets spécialisés), ce qui clarifie définitivement la chaîne de commandement. PHAROS est intégré comme unité organique. Le critère de basculement vers le COMCYBER des Armées est défini par référence aux décisions du Conseil de sécurité du cyberespace (voir infra). La création de deux pôles dédiés aux usurpations d'identité numérique et à la protection des mineurs complète le dispositif du COMCYBER-MI.

Conseil de Sécurité du Cyberespace (CSC) — Instance stratégique de haut niveau

Statut juridique

Formation spécialisée du Conseil de Défense et de Sécurité Nationale (CDSN), créée par modification du décret n°2009-1657. Pas de révision constitutionnelle nécessaire — le CDSN est une instance constitutionnelle (art. 15 C) mais ses formations spécialisées sont créées par décret.
Tutelle : Présidence de la République / Premier ministre (coprésidence).

Compétences principales dans le scénario

- Pilotage stratégique de la politique nationale de cybersécurité
- Attribution souveraine des cyberattaques :
  - Acteurs habilités : ANSC (analyse technique), DGSI, DGSE, SGDSN, MEAE — liste limitative dans le Code
  - Conclusions classifiées — décision d'attribution publique par le Premier ministre après délibération du CSC
  - Effets juridiques de l'attribution : ouverture du droit à indemnisation des victimes (EE/EI et personnes physiques) par un fonds dédié (modèle FGTI) ; possibilité de mesures de gel d'avoirs et d'interdiction d'accès au marché à l'encontre des entités désignées (sur le modèle du règlement UE 2019/796 sur les sanctions cyber)
  - Arbitrage en cas de crise de fuite massive d'identité (millions de victimes) et décision de déclenchement du FRI en urgence et de mesures exceptionnelles (révocation collective, déploiement renforcé de France Identité)
- Arbitrage des conflits de compétence entre ANSC, CNIL, ARCOM
- Décision de basculement COMCYBER-MI → COMCYBER Armées
- Rapport annuel au Parlement comportant un chapitre dédié à la protection des individus et des mineurs — rendu public, présenté devant les commissions compétentes

6. Processus par lequel une personne, généralement un adulte, utilise pour se faire passer pour un ami afin d'établir une relation de confiance avec un enfant, dans l'objectif ultime de l'exploiter sexuellement

— Organisation d'États généraux de l'identité numérique tous les trois ans — bilan de France Identité, perspective d'extension, évaluation de l'acceptabilité sociale
— Recommandations sur l'éducation à la sécurité identitaire — programmes scolaires, formation continue, sensibilisation des publics vulnérables.

Justification juridique et opérationnelle

Le CDSN dispose déjà de formations spécialisées (cyberdéfense notamment). La formalisation en CSC dans le Code donne une base législative à ces délibérations, sans révision constitutionnelle. L'essentiel de l'innovation porte sur les effets juridiques de l'attribution (droits des victimes, sanctions contre entités tierces) — c'est la création d'un régime d'indemnisation spécifique qui constitue la nouveauté normative majeure.