



Numérisation, sécurité et résilience nationale

Protection des données, continuité des services essentiels
et responsabilités publiques et privées

Dossier public consolidé V1.1 • 13 octobre 2026

Analyse documentaire consolidée — ouvert à la contradiction et à l'expertise externe

Ni technophobie, ni confiance aveugle : vérifier ce que protège réellement la numérisation, ce qu'elle expose et qui répond de ses défaillances.

Périmètre : France et Union européenne, avec comparaisons internationales pertinentes. Sources vérifiées jusqu'au 13 octobre 2026. Le document ne comporte aucune proposition de loi finalisée.

Statut éditorial : version publique consolidée, contradictoire et évolutive. Les constats factuels sont dissociés des hypothèses et pistes encore à instruire. Les pièces manquantes et les besoins de relecture externe sont explicités dans les annexes.

Sommaire

Résumé exécutif et conclusions provisoires

1. Mission, périmètre et méthode Diploval
2. Concepts : données, cybersécurité, sûreté et résilience
3. État documenté des risques en France et en Europe
4. Études de cas comparatives
5. Facturation électronique et numérisation imposée
6. Droit existant et régime des responsabilités
7. Défaillances en cascade et sécurité nationale
8. Dimension démocratique, humaine et sociale
9. Objections, bénéfices et alternatives
10. Évaluation économique et réalités de terrain
11. Épreuve contradictoire de robustesse Diploval
12. Hypothèses d'amélioration — sans préjuger du droit nouveau
13. Plan de vérification et dispositif de contribution citoyenne

Annexes A à K — Grilles, questions, glossaire, sources, enquêtes, preuves manquantes et protocole de contribution

Mode de lecture : les renvois [S01] à [S34] désignent les sources détaillées dans les bibliographies et les compléments. « Établi », « partiellement établi », « plausible », « contesté » et « à instruire » sont des niveaux de preuve, non des jugements sur les acteurs.

Résumé exécutif et conclusions provisoires

La France et l'Union européenne poursuivent une numérisation profonde de leurs activités administratives, économiques et industrielles. Le numérique offre des bénéfices réels — accessibilité à distance, traçabilité, traitement plus rapide, coopération, détection d'anomalies — mais accroît aussi certaines dépendances techniques, les besoins de maintenance et les conséquences potentielles d'une indisponibilité ou d'une compromission.

Ce dossier examine conjointement quatre phénomènes souvent confondus : (a) attaque intentionnelle, (b) panne accidentelle, (c) erreur organisationnelle ou humaine, (d) propagation d'une défaillance par interdépendance. Il confronte ces mécanismes aux obligations réglementaires et aux capacités d'exécution des administrations, grandes entreprises, TPE/PME, sous-traitants et usagers.

Les faits déjà établis sont significatifs. L'ANSSI a recensé 1 366 incidents en 2025 parmi les événements portés à sa connaissance [S01]. France Travail a fait l'objet d'une sanction en janvier 2026 pour des insuffisances de sécurité, puis d'une clôture de l'injonction après mise en conformité en septembre 2026 [S02-S03]. Les opérateurs Free et Free Mobile ont aussi été sanctionnés en 2026 à

la suite d'une fuite survenue en 2024 [S04]. Parallèlement, les crises CrowdStrike et les blackouts européens montrent que des défaillances non criminelles peuvent avoir une portée systémique [S10-S12].

La facturation électronique interentreprises a commencé à s'appliquer au 1er septembre 2026 ; elle repose sur des plateformes agréées et des obligations techniques déjà définies. L'agrément n'équivaut pas à une invulnérabilité, mais il serait inexact de prétendre qu'aucun régime de sécurité n'existe [S13-S14].

Constat provisoire : la présence d'incidents ne démontre pas, en elle-même, une lacune législative. L'enquête doit établir si la difficulté relève des règles, de leur application, des moyens, de la conception des systèmes, de leur contrôle, ou d'un risque résiduel non supprimable.

Ce que le dossier établit et ce qu'il n'établit pas

- Établi : de grandes fuites de données françaises et des interruptions majeures de services ont été documentées par des autorités ou des sources primaires.
- Établi : la réglementation européenne traite déjà l'analyse de risque, les fournisseurs, la continuité et la réparation, à des degrés et pour des périmètres différents.
- Établi : une certification ou une simulation apporte des éléments de confiance, mais ne garantit jamais une sécurité absolue.
- Non établi : une dégradation générale de la cybersécurité du fait de la seule obligation de numériser ; aucune démonstration causale globale n'est disponible ici.
- À instruire : l'efficacité comparative des protections, les coûts complets, la fréquence réelle des pannes et l'accessibilité des réparations.
- À instruire : l'opportunité d'un dispositif de responsabilité ou d'indemnisation renforcée pour les usages numériques imposés.

1. Mission, périmètre et méthode Diploval

1.1 Objet

Question directrice : « La numérisation des activités publiques et privées progresse-t-elle avec des garanties de sécurité, de continuité, d'accessibilité et de responsabilité adaptées aux risques qu'elle crée ou transforme ? » Cette question ne préjuge ni de l'existence d'une faute ni de la nécessité d'une réforme.

1.2 Périmètre

- Secteurs : administration, fiscalité et facturation, prestations sociales, santé, télécommunications, commerce alimentaire, énergie, transports, eau et chaînes industrielles stratégiques.
- Événements : accès non autorisé, rançongiciel, altération, perte de données, panne logicielle, dysfonctionnement industriel, blackout et interruption de prestataire.
- Acteurs : État, collectivités, opérateurs privés, plateformes agréées, éditeurs, sous-traitants, organismes de contrôle, salariés, usagers, citoyens.

- Effets : vie privée, sécurité des patients, continuité d'activité, coûts, droit d'accès au service, souveraineté et confiance institutionnelle.

1.3 Méthode de vérification

1. Identifier le fait exact, sa date, l'organisation et le périmètre concerné ; ne jamais déduire une cause de la seule ampleur des conséquences.
2. Classer les sources : document officiel ou décision, rapport primaire, communiqué d'organisation, enquête de presse, témoignage, déclaration ou revendication non corroborée.
3. Distinguer provenance, authenticité et intégrité du document ; consigner ses versions et mises à jour.
4. Séparer les chiffres de personnes, comptes, contrats, systèmes ou établissements ; rechercher les doubles comptes.
5. Comparer les obligations en vigueur au moment des faits avec les règles introduites ultérieurement.
6. Chercher activement des contre-exemples, des correctifs mis en œuvre et des raisons alternatives.
7. Publier les limites, les questions non tranchées et un registre de corrections.

1.4 Échelle des preuves

Statut	Définition	Règle de rédaction
Établi	Source primaire concordante ou décision officielle suffisamment précise	Affirmer en citant date et portée.
Partiellement établi	Fait principal confirmé, portée ou mécanisme incomplet	Indiquer ce qui manque.
Plausible	Hypothèse cohérente mais sans preuve causale suffisante	Formuler au conditionnel.
Contesté	Sources crédibles divergentes ou procédure non achevée	Présenter les versions et leur niveau d'appui.
Non vérifié	Aucune source fiable suffisante identifiée	Ne pas présenter comme un fait.

Le dossier est documentaire. Il ne constitue pas un audit technique de systèmes réels, une enquête judiciaire ou une expertise économique chiffrée exhaustive. Les projets législatifs et les alertes peuvent évoluer rapidement après sa date de clôture.

2. Concepts : données, cybersécurité, sûreté et résilience

2.1 Les trois propriétés des données

La confidentialité protège contre l'accès non autorisé ; l'intégrité contre l'altération non maîtrisée ; la disponibilité contre l'indisponibilité. Dans les services essentiels, la modification discrète d'un résultat médical ou d'une facture peut être aussi problématique qu'un vol massif de fichiers.

2.2 Trois familles d'événements à ne pas confondre

Famille	Exemple	Ce qu'il faut mesurer
Acte malveillant	Rançongiciel, espionnage, sabotage, fraude	Intention établie, chemin d'attaque documenté, dommage réel.
Défaillance non malveillante	Mise à jour défectueuse, erreur de paramétrage, panne matérielle	Cause technique et responsabilités opérationnelles, sans présumer un pirate.
Propagation systémique	Perte de prestataire, tension sur un réseau électrique, interruption en chaîne	Dépendances, capacité d'isolement, modes de secours, temps de rétablissement.

2.3 Interconnexion : risque et ressource

L'interconnexion peut accélérer la propagation d'un incident, mais aussi permettre la mutualisation des secours et une reprise plus rapide. La relation entre complexité et vulnérabilité n'est donc pas mécanique : la redondance indépendante peut augmenter la complexité tout en améliorant la sécurité. L'objet de l'enquête est la complexité mal gouvernée, la dépendance non cartographiée et l'absence de repli éprouvé.

2.4 Résilience

La résilience correspond ici à la capacité de prévenir, absorber, contenir, réagir, poursuivre des fonctions minimales et rétablir l'activité après un incident. Les directives européennes NIS2 et CER comportent déjà des exigences explicites de continuité, de gestion des crises et de chaîne d'approvisionnement pour les entités concernées [S15-S16].

3. État documenté des risques en France et en Europe

3.1 Panorama français

Le Panorama de la cybermenace 2025 publié par l'ANSSI le 11 mars 2026 recense 3 586 événements de sécurité traités, dont 1 366 incidents et 2 209 signalements. Les secteurs les plus présents parmi ces incidents sont l'éducation et la recherche (34 %), les ministères et collectivités (24 %), la santé (10 %) et les télécommunications (9 %) [S01].

Ces chiffres décrivent les cas parvenus à l'agence, pas l'intégralité de la cybercriminalité en France. Les taux de signalement, la taille des secteurs et la qualification des faits peuvent évoluer. Une baisse du nombre de déclarations ne prouverait donc pas, seule, une amélioration de la sécurité.

3.2 Typologie des motivations

Les cyberattaques peuvent rechercher le profit, l'exfiltration d'informations, l'espionnage, la désorganisation, la visibilité médiatique ou une cause militante revendiquée. La motivation déclarée par l'attaquant n'équivaut pas à une motivation démontrée. Dans certains cas, des revendications sont trompeuses. Les signalements responsables de vulnérabilités, réalisés dans un cadre autorisé, ne doivent pas être confondus avec des intrusions dommageables.

3.3 Un risque qui dépasse la donnée personnelle

Les données bancaires, sociales et médicales constituent un enjeu majeur, mais un système compromis peut aussi provoquer une interruption des soins, une perte de denrées, la suspension d'un service de paiement, l'arrêt de chaînes de fabrication ou la perturbation d'un réseau. L'impact doit être évalué en fonction des personnes exposées, de la durée et de la gravité des dommages, et non du seul volume de fichiers.

3.4 La menace n'est pas toujours cybercriminelle

Une panne d'électricité, une erreur logicielle, un défaut de maintenance ou une dépendance commune peuvent causer une crise de grande échelle. Les études de cas CrowdStrike et ENTSO-E permettent de vérifier cette distinction [S10-S12].

4. Études de cas comparatives

La sélection ci-dessous n'est ni un palmarès de gravité ni un échantillon statistiquement représentatif. Elle vise à faire varier la cause, le secteur, le type d'atteinte et le régime de responsabilité. La date des conclusions est celle de la source citée.

4.1 France Travail — fuite de données et mise en conformité

Au premier trimestre 2024, des attaquants ont utilisé des comptes de conseillers Cap emploi détournés après des techniques d'ingénierie sociale pour accéder à des données de personnes inscrites à France Travail au cours des vingt années précédentes. La CNIL a infligé une amende de 5 millions d'euros en janvier 2026 pour insuffisance de mesures de sécurité [S02].

Le 8 octobre 2026, la CNIL a annoncé avoir clos son injonction, estimant les mesures attendues mises en conformité, sans liquidation de l'astreinte [S03]. Ce second fait est aussi important que la sanction : toute évaluation honnête doit examiner non seulement la défaillance, mais les corrections et leurs effets vérifiables.

Questions ouvertes : quelles défaillances relevaient de politiques d'accès, de contrôle des prestataires ou de moyens ? Les personnes exposées ont-elles reçu une information suffisante ? Quels bénéfices préventifs les mesures correctrices produiront-elles dans la durée ?

4.2 Viamedis et Almerys — intermédiaires du tiers payant

En février 2024, la CNIL a annoncé une fuite concernant plus de 33 millions de personnes chez deux opérateurs de tiers payant. Des données d'état civil, de sécurité sociale et de couverture santé figuraient dans le périmètre communiqué [S05]. Le volume illustre l'exposition créée par des intermédiaires communs à plusieurs organismes. Il n'autorise pas à affirmer que tous les dossiers médicaux ont été compromis.

Question centrale : qui choisit et supervise les prestataires, qui informe les personnes concernées et comment prouver la correction des défaillances ?

4.3 Free et Free Mobile — responsabilité privée, données conservées

Une intrusion en octobre 2024 a exposé des informations liées à 24 millions de contrats d'abonnés, avec des IBAN pour une partie des clients. En janvier 2026, la CNIL a prononcé des amendes de 27 et 15 millions d'euros, évoquant des mesures de sécurité inadaptées et, pour certains fichiers, une conservation excessive de données [S04]. Les 24 millions correspondent à des contrats, pas nécessairement à des individus distincts.

Question centrale : la durée de conservation et la qualité des accès sont-elles contrôlées indépendamment de l'agrément ou de la taille de l'opérateur ?

4.4 Synnovis / NHS — lorsque les soins sont perturbés

Le 3 juin 2024, une attaque par rançongiciel contre le prestataire britannique de laboratoires Synnovis a fortement réduit certaines capacités de biologie médicale et provoqué le report de plus de 11 000 rendez-vous ou interventions, selon la synthèse publiée par NHS England [S06]. Cet épisode illustre une dépendance de la continuité des soins à un prestataire extérieur.

L'enjeu ne se limite pas à savoir si des données ont été dérobées : il porte sur la capacité de soins minimale, les résultats disponibles et les délais de rétablissement. Le présent dossier ne chiffre pas les dommages sanitaires individuels faute d'expertise clinique dédiée.

4.5 Réfrigération commerciale en France — octobre 2026

Le CERT-FR a publié une alerte le 12 octobre 2026, actualisée le 13, sur de nombreuses compromissions de contrôleurs de réfrigération à distance de plusieurs gammes (Danfoss, Copeland, Dixell). Il souligne les risques liés à l'exposition d'interfaces d'administration sur Internet et aux équipements en fin de vie [S07]. Des médias ont rapporté plusieurs centaines de magasins touchés et des pertes alimentaires ; ces bilans évoluaient encore au 13 octobre [S08].

Ce cas est une porte d'entrée pour les systèmes industriels connectés : les conséquences physiques peuvent survenir sans compromission préalable des bases de données clients. Le CERT-FR ne permet pas, à cette date, de conclure à la motivation des attaquants, à la responsabilité individuelle des exploitants ni à l'utilisation d'une vulnérabilité unique.

4.6 CrowdStrike — juillet 2024, panne non criminelle

Une mise à jour défectueuse d'un produit de sécurité a touché environ 8,5 millions de terminaux Windows, selon l'estimation publiée par Microsoft le 20 juillet 2024 [S10]. Le nombre ne représente pas tous les utilisateurs affectés indirectement. L'événement montre qu'une dépendance commune à un logiciel fortement déployé peut provoquer une désorganisation mondiale, sans cyberattaque.

Enseignements à examiner : contrôles de déploiement, segmentation, possibilité de retour arrière, plans de continuité et vulnérabilité aux fournisseurs dominants.

4.7 Balkans — 21 juin 2024, panne électrique en cascade

Le rapport final ENTSO-E du 25 février 2025 lie le blackout de plusieurs pays des Balkans à deux courts-circuits causés par de la végétation, à une visibilité insuffisante de la situation régionale et à

des moyens insuffisants pour éviter un effondrement de tension [S11]. Il ne s'agit pas d'une cyberattaque établie.

Intérêt méthodologique : la maintenance de routine, la coordination et la protection des réseaux peuvent être aussi déterminantes que la sophistication informatique.

4.8 Espagne-Portugal — 28 avril 2025, régulations et propagation

Le rapport final ENTSO-E du 20 mars 2026 identifie des facteurs conjoints : oscillations, lacunes de contrôle tension/puissance réactive, différences de pratiques de régulation, réductions de production, déconnexions successives et capacités de stabilisation inégales [S12]. Le blackout ne doit pas être présenté comme une cyberattaque prouvée.

Il rappelle que l'interconnexion permet aussi des secours entre réseaux. Les conséquences d'une panne doivent être examinées avec les dispositifs ayant limité la propagation et facilité le rétablissement, sans généraliser à tous les systèmes numériques.

4.9 Compléments d'étude à documenter

Les incidents concernant les collectivités, les données des allocataires du RSA, la santé française, France Titres et les fichiers fiscaux pourront faire l'objet de fiches annexes, après réunion de pièces publiques primaires et d'éventuels retours d'organismes concernés. Les exemples militaires ou industriels nominativement identifiés ne seront retenus que sur preuves publiques vérifiables ; aucune vulnérabilité de site particulier ne sera inférée à partir de la seule nature de son activité.

Cas	Nature principale	Donnée / service	Ce qui est certain au 13/10/2026
France Travail	Intrusion et sanction	Données administratives	Sanction + clôture d'injonction [S02-S03]
Viamedis/Almerys	Fuite de données	Tiers payant	Plus de 33 M de personnes [S05]
Free	Intrusion et sanction	Contrats et coordonnées	24 M de contrats ; sanctions [S04]
Synnovis	Rançongiciel	Continuité des soins	>11 000 reports [S06]
Réfrigération 2026	Compromissions industrielles	Conservation alimentaire	Alerte CERT-FR actualisée [S07]
CrowdStrike	Mise à jour défectueuse	Services multiples	~8,5 M appareils Windows [S10]
Balkans / Ibérie	Défaillances électriques	Réseaux interconnectés	Rapports finaux ENTSO-E [S11-S12]

5. Facturation électronique et numérisation imposée

5.1 Portée exacte de l'obligation

Depuis le 1er septembre 2026, les entreprises françaises concernées doivent pouvoir recevoir des factures électroniques ; les grandes entreprises et ETI doivent aussi émettre les factures relevant du

dispositif. L'émission pour les PME et microentreprises entre en application le 1er septembre 2027. La réforme cible des échanges et transmissions dans le périmètre prévu par les textes fiscaux ; elle n'impose pas la création de devis électroniques de manière générale [S13-S14].

Une entreprise doit recourir à une plateforme agréée, directement ou via un outil compatible. Les exigences incluent certification ISO 27001, mécanismes d'authentification et contrôles ; certaines exigences d'hébergement renforcé sont applicables selon les cas [S13-S14].

5.2 Les limites réelles de l'agrément

L'agrément prouve qu'une procédure et des exigences réglementaires ont été suivies : il ne démontre pas une sécurité à 100 %, ni la bonne configuration de chaque entreprise cliente, ni la conformité de toutes les réutilisations des données. Une certification est une garantie procédurale et organisationnelle, pas une promesse d'absence future de faille. La CNIL souligne que les mesures standard peuvent devoir être complétées selon les traitements concernés [S13].

5.3 Chaîne de responsabilité et flux de données

À étudier : l'émetteur, son éditeur de logiciel, sa plateforme agréée, la plateforme du client, les hébergeurs, les prestataires de support et l'administration recevant les seules données exigées. La CNIL précise que la plateforme est généralement sous-traitante pour les données personnelles traitées pour ses clients, mais peut devenir responsable du traitement lorsqu'elle réutilise des données pour son propre compte sous les conditions applicables [S13].

Les factures relatives exclusivement à des personnes morales n'entrent pas nécessairement dans le champ du RGPD. Les informations identifiant des entrepreneurs individuels ou des salariés y entrent fréquemment ; les données commerciales non personnelles relèvent d'autres protections (contrats, secret des affaires, sécurité opérationnelle). Il serait donc inexact d'affirmer que chaque facture relève intégralement du RGPD [S13].

5.4 Scénarios de risque à tester, sans les présenter comme des incidents observés

8. Indisponibilité prolongée d'une plateforme un jour de forte activité : délais, factures en attente, obligations fiscales, trésorerie.
9. Usurpation ou falsification de coordonnées de paiement : séparation des canaux de validation et intégrité des pièces.
10. Intrusion chez un prestataire commun : exposition simultanée d'informations de plusieurs entreprises.
11. Changement forcé de prestataire : portabilité des données, délais, export, preuves de traitement.
12. Conflit entre sécurité et accessibilité : authentification trop complexe, perte d'accès ou insuffisance de support humain.
13. Panne généralisée et fonctionnement de secours : règles applicables à la régularisation et à la preuve des opérations.

5.5 Question ouverte sur la responsabilité publique

Quand l'autorité publique rend un outil numérique indispensable, quelles garanties de secours et de réparation doit-elle assurer sans effacer la responsabilité propre des exploitants et prestataires ?

Il s'agit d'une question de répartition du risque, non d'une règle actuelle d'indemnisation automatique. Une analyse juridique spécifique devra étudier la faute, la responsabilité sans faute, le lien causal, la preuve du dommage et les ressources de financement.

6. Droit existant et régime des responsabilités

6.1 Tableau des principaux cadres

Texte / cadre	Obligations ou protections pertinentes	Limite de l'analyse
RGPD (UE 2016/679)	Sécurité proportionnée (art. 32), notification, droits et réparation (art. 82).	Concerne les données personnelles ; réparation soumise à conditions.
NIS2 (UE 2022/2555)	Gestion des risques, incidents, fournisseurs, continuité, contrôle pour entités concernées.	Transposition française et périmètre à vérifier au cas par cas [S15].
CER (UE 2022/2557)	Résilience « tous risques » des entités critiques désignées.	Ne couvre pas indistinctement toutes les entreprises [S16].
DORA (UE 2022/2554)	Résilience opérationnelle numérique dans la finance, depuis 2025.	Champ sectoriel ; exigences déjà détaillées.
Cyber Resilience Act (UE 2024/2847)	Sécurité des produits numériques ; signalements dès septembre 2026, dispositif général décembre 2027.	Effets sur parc ancien et obligations transitoires [S17].
Code de la défense L1332-6-1	Règles de sécurité de certains opérateurs d'importance vitale et acteurs participant à leurs SI.	Désignations et détails parfois confidentiels [S18].
Conseil d'État, 3 juin 2022	Garanties d'accès aux téléservices obligatoires de titres de séjour.	Ne crée pas une alternative générale inconditionnelle [S19].
Projet de loi français 2024-2026	Résilience des infrastructures critiques et renforcement cybersécurité.	En cours de procédure au 13 octobre 2026 [S20].

6.2 Responsabilité RGPD et préjudice

La CNIL rappelle le 2 octobre 2026 qu'une indemnisation peut être demandée devant le juge lorsqu'une violation du RGPD a causé un dommage matériel ou moral et qu'existe le lien de causalité requis. Une simple violation de données n'entraîne pas automatiquement une somme versée à toute personne concernée ; inversement, un préjudice moral ne suppose pas nécessairement qu'une fraude financière ait déjà été commise [S21].

Il faut distinguer l'indemnisation, la sanction administrative d'un organisme, l'action de la justice pénale contre les attaquants et les recours contractuels entre prestataires. Une amende infligée par la CNIL n'est pas en elle-même une indemnité payée aux victimes.

6.3 Pourquoi la responsabilité de l'État ne peut être décrétée automatique

L'État législateur ou régulateur, l'organisme public exploitant, la collectivité, le responsable du traitement et le fournisseur peuvent constituer des personnes juridiques distinctes. Le fait d'imposer une démarche et celui de stocker les données ne coïncident pas toujours. Identifier les compétences est indispensable avant toute analyse d'une faute, d'une obligation de garantie ou d'une indemnisation sans faute.

Hypothèse d'étude : prévoir, dans certains cas de dispositifs numériques obligatoires, une garantie subsidiaire ou un guichet de réparation rapide, sans exonérer le responsable du traitement ni le prestataire. Objections prévisibles : coût collectif, risque d'aléa moral, critères de réparation, compatibilité européenne et difficultés de preuve.

6.4 Périmètre des activités stratégiques

Les systèmes d'information de certains opérateurs d'importance vitale sont déjà soumis à des prescriptions renforcées du Code de la défense [S18]. Le secteur de la défense ne peut être examiné comme une entreprise ordinaire, pas plus que chaque entreprise industrielle ne peut être présumée « d'importance vitale ». Le dossier ne publie aucune information technique sensible ou localisation de faiblesse exploitable.

7. Défaillances en cascade et sécurité nationale

7.1 Une approche « tous risques »

Nous proposons de tester les dépendances communes à l'électricité, aux télécommunications, à l'hébergement, aux systèmes d'identité, aux maintenances externalisées, aux paiements et aux fournisseurs. Une interruption peut se propager sans qu'un attaquant ait pénétré chacun des systèmes concernés. Les directives NIS2 et CER contiennent des obligations sur la continuité ou les chaînes d'approvisionnement, ce qui invite à contrôler leur application avant de suggérer de nouveaux textes [S15-S16].

7.2 Fonctions minimales et isolement

Une analyse de résilience doit identifier les fonctions absolument nécessaires à préserver, le délai maximal d'interruption tolérable, la possibilité d'isoler un segment compromis, et l'indépendance effective du dispositif de secours. Un secours qui dépend du même hébergeur, du même identifiant ou du même accès réseau n'est pas nécessairement une redondance indépendante.

7.3 Exercices et limites de la simulation

L'exercice national REMPAR25 organisé le 18 septembre 2025 a réuni, selon l'ANSSI, près de 5 680 professionnels de 1 263 organisations et simulé une crise cyber systémique [S22]. Sa valeur est

pédagogique et opérationnelle ; il ne démontre pas qu'une crise réelle serait maîtrisée. Les exercices sont à comparer selon scénarios, fréquence, résultats, corrections et contre-tests ultérieurs. Les données non publiées ne sauraient être présumées inexistantes.

7.4 Indicateurs de robustesse

- Temps maximal d'interruption des fonctions essentielles et temps réel de restauration.
- Existence et qualité des procédures dégradées, secours hors ligne, moyens humains de relais.
- Taux de correctifs critiques appliqués sur le parc concerné, sans exposition d'informations sensibles.
- Diversité réelle des prestataires et risque de point commun de défaillance.
- Part des retours d'expérience donnant lieu à une correction et taux de correction vérifié.
- Capacité d'entraide entre réseaux et territoires sans compromettre l'isolation en crise.

8. Dimension démocratique, humaine et sociale

8.1 Accès réel aux droits

L'enquête du Défenseur des droits, portant sur la relation aux services publics, montre que 61 % des personnes interrogées évoquent des difficultés administratives ponctuelles ou régulières en 2024 et que 23 % déclarent avoir renoncé à un droit au cours des cinq années précédentes. Ces difficultés ne sont pas toutes attribuables au numérique [S23]. Les conditions de contact humain et de correction d'un dossier doivent être évaluées au même titre que la vitesse du service.

8.2 Trois moments de participation

14. Avant le déploiement : étude d'impact et consultation adaptée aux usagers concernés, y compris ceux sans maîtrise numérique.
15. Pendant le déploiement : signalements, accès à une assistance compétente, correction d'erreurs, mesures transitoires et information compréhensible.
16. Après le déploiement : bilan public des coûts, délais, incidents, corrections et révisions de modalités, y compris lorsque cela conduit à revenir sur un choix.

8.3 Le contact humain n'est pas seulement un guichet

Un échange humain n'apporte pas grand-chose si l'interlocuteur ne peut ni expliquer les motifs d'une décision, ni corriger une donnée erronée, ni orienter vers un recours effectif. Il faut distinguer présence d'une assistance, accessibilité réelle et pouvoir concret de résolution. Les alternatives ne sont pas nécessairement exclusivement papier : elles peuvent être une assistance qualifiée, un canal téléphonique, un mandataire ou une procédure de secours.

8.4 Charge administrative transférée

La numérisation peut réduire le traitement interne tout en déplaçant le temps de saisie, le matériel nécessaire ou les risques d'erreur vers les usagers, les aidants et les petites entreprises. Le bilan

économique devra compter ces charges, et pas seulement les économies budgétaires des administrations. Ce transfert constitue une hypothèse mesurable, non une conclusion universelle.

8.5 Protections à préserver lors de la consultation

Les témoignages citoyens ne devront pas divulguer de données personnelles de tiers, d'identifiants, de détails permettant l'exploitation d'un système ou d'éléments couverts par la confidentialité professionnelle. Les contributions spontanées ne constitueront pas un sondage représentatif. Une modération motivée, des durées de conservation explicites et une procédure de correction seront prévues.

9. Objections, bénéfices et alternatives

Le protocole Diploval exige de rechercher les arguments susceptibles d'infirmes nos intuitions initiales. Ceux-ci ne sont pas de simples concessions : ils conditionnent la validité des recommandations futures.

Argument contraire / objection	Réponse méthodologique
La numérisation facilite l'accès à distance et réduit certaines erreurs.	Comparer délais, taux d'erreur et publics réellement bénéficiaires.
Les systèmes papier ont aussi des pertes, fuites et fraudes.	Analyser le contrefactuel non numérique plutôt que l'idéaliser.
Un incident isolé ne prouve pas une défaillance générale.	Raisonnement en taux, périmètres et séries comparables ; signaler le biais de sélection.
Sécuriser à 100 % est impossible.	Mesurer sécurité proportionnée, réduction d'impact et qualité du secours.
Les règles RGPD/NIS2/CER existent déjà.	Démontrer la lacune réelle avant toute proposition de loi.
Les exigences coûtent trop cher aux petites structures.	Évaluer coûts, aides, délais et risques différenciés.
Un fonds d'indemnisation déresponsabiliserait les prestataires.	Tester recours contre responsables, franchises, contributions et critères.
La transparence expose des infrastructures critiques.	Publier résultats agrégés sans configuration technique sensible.
Les services publics disposent déjà d'exercices non publiés.	Ne pas inférer l'absence de contrôle depuis une absence de publicité.
Les interconnexions rendent aussi les secours possibles.	Évaluer bénéfices et risques de chaque dépendance.

10. Évaluation économique et réalités de terrain

10.1 Modèle de coût complet

Coût total de la numérisation = acquisition et abonnement + intégration + migration + formation + supervision + maintien en sécurité + support + audits + sauvegardes + continuité + gestion des incidents + temps des usagers et salariés + coûts de sortie du fournisseur. Toute estimation devra préciser l'horizon temporel, la taille de l'organisme et le scénario de référence.

Les coûts évités doivent être comptés au même titre : déplacement, impression, ressaisie, délais postaux, traitements manuels, fraude éventuellement réduite, besoins d'archivage et pertes de productivité. Aucun chiffrage générique non sourcé ne sera présenté comme le coût national de la réforme.

10.2 Variabilité des capacités

Une commune rurale, une pharmacie, une microentreprise, un hôpital et un équipementier stratégique ne disposent ni des mêmes budgets ni des mêmes équipes, ni des mêmes niveaux d'exposition. La proportionnalité des obligations ne doit pas conduire à ignorer le risque pour les personnes vulnérables, mais elle doit tenir compte de la capacité réelle de mise en conformité.

10.3 Indicateurs demandés aux acteurs

Dimension	Indicateurs quantitatifs recherchés
Sécurité	Incidents détectés, gravité, temps de remédiation, taux de correction vérifiée.
Continuité	Disponibilité observée, délai de reprise, taux de tests de repli réussis.
Droits	Taux de dossiers bloqués, recours aboutis, délais de réponse, renoncements.
Économie	Coûts d'équipement/formation/maintenance et heures usager ; économies vérifiées.
Données	Périmètre de collecte, duplication, accès, purges, réutilisations autorisées.
Responsabilités	Délai d'alerte, procédure d'indemnisation, litiges et issue documentée.

10.4 Stratégie de collecte

Les questionnaires devront combiner questions fermées descriptives et espaces d'observation libre, éviter les formulations orientées et distinguer répondants affectés de répondants non affectés. Les entretiens professionnels devront documenter des exemples contrastés : déploiement réussi, défaillance corrigée, coût excessif et obstacle insoluble. Le consentement et la confidentialité des personnes seront organisés avant collecte.

11. Épreuve contradictoire de robustesse Diploval

Cette déclinaison applique les épreuves transversales déjà utilisées dans les dossiers Diploval ; elle n'instaure pas un protocole distinct. Chaque proposition future devra passer les treize examens ci-dessous, puis une épreuve intégrale de cohérence.

11.1 Treize épreuves sectorielles

1. Factualité

Les faits et chiffres ont-ils une source primaire datée, et les causes sont-elles distinguées des conséquences ?

2. Définitions

Les termes « obligatoire », « agréé », « sensible », « critique » et « faute » sont-ils juridiquement et techniquement définis ?

3. Droit existant

Une mesure comparable existe-t-elle déjà, dans quel texte et pour quels acteurs ?

4. Application

Quelles preuves établissent la mise en œuvre réelle des obligations ?

5. Proportionnalité

La règle s'adapte-t-elle au risque, au secteur et à la taille de l'acteur ?

6. Faisabilité

Les compétences, délais, dispositifs de contrôle et financements existent-ils ?

7. Effets indirects

La mesure crée-t-elle de nouvelles dépendances ou transfère-t-elle les coûts aux usagers ?

8. Conséquences humaines

Les effets sur les droits, les personnes vulnérables et les salariés sont-ils mesurés ?

9. Réciprocité

Une règle imposée à une entreprise serait-elle défendable si elle concernait une administration ?

10. Alternance / institutions

La proposition reste-t-elle protectrice quel que soit le décideur politique ou l'organisme chargé de l'appliquer ?

11. Confrontation externe

Des juristes, techniciens, professionnels et usagers opposés à l'hypothèse ont-ils pu la critiquer ?

12. Corrigibilité

Comment seront mesurés les résultats, révisés les paramètres et reconnus les échecs ?

13. Préservation des libertés

La mesure respecte-t-elle vie privée, secret professionnel, sûreté des personnes et droit d'accès ?

Épreuve intégrale Ω

Exiger qu'une hypothèse d'amélioration reste cohérente simultanément avec les exigences de sécurité, de liberté, de souveraineté, de justice, de proportionnalité, de continuité et de coût. La

contradiction qui ne peut être résolue doit être publiée, avec arbitrages possibles et impacts différenciés. Aucune proposition ne sera validée sur le seul fondement de sa popularité.

12. Hypothèses d'amélioration — sans préjuger du droit nouveau

Les pistes ci-dessous ne constituent ni un programme législatif arrêté ni des articles de loi. Chacune comporte une condition préalable de validation et peut conduire à l'absence de réforme. Elles seront comparées aux obligations déjà prévues.

Piste	Objet	Condition de validation
A — Preuve d'application avant nouvelle obligation	Auditer les contrôles, sanctions, moyens et remédiations dans les régimes existants.	Comparer normes existantes et audits publics ; absence de contrôle démontrée ou non.
B — Continuité de la démarche obligatoire	Clarifier la reprise d'activité et la protection des délais administratifs ou fiscaux en cas de panne démontrée.	Vérifier dérogations et mécanismes actuels ; coûts de gestion des exceptions.
C — Portabilité, sortie et secours	Évaluer des garanties adaptées de récupération de données et de changement de fournisseur.	Vérifier obligations contractuelles et normes déjà applicables.
D — Sécurité des équipements anciens	Examiner maintenance, fin de vie, accès distant et dispositifs industriels à conséquences physiques.	Caractériser le parc, les coûts et les obligations déjà applicables.
E — Transparence des corrections	Améliorer les bilans agrégés sur les incidents, recommandations mises en œuvre et résultats des exercices.	Ne pas exposer des vulnérabilités ou informations stratégiques.
F — Assistance humaine effective	Mesurer le pouvoir de résolution des services d'assistance et les alternatives disponibles.	Vérifier jurisprudence, moyens et droits déjà ouverts.
G — Réparation accessible	Comparer responsabilité classique, guichet simplifié, garantie subsidiaire et mécanismes mutualisés.	Démontrer lacunes d'indemnisation, coûts et compatibilité avec le droit UE.
H — Consultation et évaluation ex post	Étudier des consultations adaptées et la publication d'évaluations après les grandes obligations numériques.	Éviter procédures purement formelles ; mesurer charge administrative et efficacité.

Les cinq issues possibles de notre enquête

17. Le droit actuel paraît suffisant ; aucune nouvelle mesure législative justifiée.
18. Le droit est pertinent mais son application, ses contrôles ou ses financements sont insuffisants.
19. Une adaptation réglementaire, contractuelle ou organisationnelle est adéquate.
20. Une lacune législative précise et démontrée appelle une rédaction ciblée et évaluable.
21. Les preuves sont insuffisantes ; toute conclusion est suspendue et les pièces manquantes sont publiées.

13. Plan de vérification et contribution citoyenne

13.1 Pièces à rechercher avant publication définitive

- 22. Dispositions françaises et européennes consolidées, dates exactes d'entrée en vigueur et état de la transposition des directives.
- 23. Rapports complets et bilans de mise en conformité des organismes étudiés ; contrôles publics disponibles.
- 24. Informations de terrain sur les incidents, leurs coûts, la réparation et l'accompagnement humain.
- 25. Contrats-types de plateformes et procédures opérationnelles de secours, dans leurs versions publiques.
- 26. Avis contradictoires d'autorités, représentants de TPE/PME, DPO, juristes, ingénieurs industriels, associations et usagers.
- 27. Comparaisons des effets positifs et négatifs de la dématérialisation sur des services similaires.

13.2 Organisation prévue pour la rubrique « Propositions & contributions »

La page publique présentera : problème documenté ; droit et pratique actuels ; hypothèses contradictoires ; questions ouvertes ; données manquantes ; version du dossier ; calendrier de réception des contributions ; synthèse motivée après instruction. Une contribution favorable ne bénéficie d'aucune présomption de pertinence face à une contribution critique.

Les contributions seront structurées par thème (sécurité, continuité, expérience, coût, alternatives, responsabilité, droits) plutôt que sous forme de commentaires libres. Le formulaire recueillera uniquement les éléments nécessaires. Les informations de contact seront traitées selon une notice de confidentialité explicite ; aucune donnée de santé, identité de tiers ni donnée technique exploitable ne devra être publiée.

13.3 Exemples de questions ouvertes

- 28. Quelle démarche numérique a facilité votre accès à un droit ou votre activité ? Quel gain précis avez-vous constaté ?
- 29. Avez-vous rencontré une panne, une fraude, une difficulté d'authentification ou une procédure inaccessible ? Sur quels éléments vérifiables fondez-vous votre récit ?
- 30. Avez-vous obtenu une réponse humaine dotée d'un pouvoir de résolution ? Dans quel délai ?
- 31. Quels coûts d'abonnement, de formation, de migration et d'assistance sont réellement supportés par votre structure ?
- 32. En cas de défaillance d'un système obligatoire, quel recours ou secours était disponible ?
- 33. Quelles obligations ou solutions existantes fonctionnent et mériteraient d'être conservées ?
- 34. Quelle proposition améliore un résultat mesurable sans ajouter une contrainte disproportionnée ?

13.4 Gouvernance de version

Chaque mise à jour conservera date, auteur ou équipe, nouvelles sources, passages corrigés, argument contradictoire reçu et motif de décision. Les erreurs factuelles seront corrigées

publiquement lorsque la version a été diffusée. Les données personnelles collectées pour la consultation ne seront pas utilisées pour d'autres objectifs sans base juridique appropriée.

Conclusion générale provisoire

La numérisation n'est ni un danger intrinsèque ni une garantie intrinsèque de progrès. Les incidents étudiés démontrent que les failles peuvent tenir aux accès, aux traitements de données, à la maintenance, aux dépendances communes et parfois à des mécanismes techniques sans aucune intention criminelle. Les régulations européennes couvrent déjà une part notable de ces enjeux ; la démonstration d'une lacune de droit exige donc un examen exigeant de leur application et de leurs limites.

L'autorité qui rend une technologie obligatoire doit pouvoir expliquer les risques retenus, les garanties exigées, le fonctionnement en cas de panne et les possibilités de recours. Cela relève d'une responsabilité institutionnelle à discuter ; la responsabilité juridique et l'indemnisation dépendent aujourd'hui de cadres plus spécifiques. L'étude examine la possibilité de garanties supplémentaires sans supposer que le seul caractère obligatoire suffit à établir une faute ou un droit automatique à compensation.

Principe de travail : une modernisation réussie ne se mesure pas uniquement à ce qu'elle permet quand tout fonctionne, mais aussi à ce qu'elle protège lorsque quelque chose échoue — et à la capacité de corriger ses propres choix.

Statut de cette V1.0 : base documentaire globale, structurée et sourcée ; ouverte à vérifications contradictoires. Aucun amendement n'est proposé pour dépôt à ce stade. Le dossier est apte à nourrir le futur espace citoyen de Diploval, mais l'édition publique finale devra intégrer les relectures juridique, technique, économique et accessibilité.

Annexe A — Fiche type de chaque incident

Champ	Information à renseigner
Identification	Date, lieu/périmètre, acteur, catégorie du fait.
Sources	Références primaires, version, provenance, authenticité, intégrité.
Preuves	Faits confirmés, hypothèses, contradictions, éléments manquants.
Population	Personnes vs contrats vs comptes ; pas d'addition non contrôlée.
Conséquences	Confidentialité, intégrité, disponibilité, santé, environnement, économie.
Droit applicable	Textes et obligations effectifs au jour de l'incident.
Responsables	Rôles juridiques distincts ; aucune faute présumée.
Correctifs	Mesures annoncées, réalisées, vérifiées, efficacité observée.
Suites	Enquête, procédures judiciaires, sanctions, réparations, limites.

Champ	Information à renseigner
État	Établi / partiellement établi / plausible / contesté / non vérifié.

Annexe B — Guide bref d'entretien contradictoire

Usagers et citoyens

Décrire une démarche précise, le canal utilisé, le temps nécessaire, les difficultés ou avantages, le moyen humain de recours et l'issue. Ne recueillir ni numéros de dossier, ni identifiants ni documents personnels non nécessaires.

TPE, PME, commerçants et professionnels indépendants

Préciser les obligations réellement applicables, les fournisseurs choisis, la formation, les coûts annuels, les pannes, les sauvegardes, les démarches de changement de prestataire et les marges de manœuvre en cas d'incident.

Professionnels de la sécurité, du soin et de l'industrie

Distinguer contraintes connues, sécurité conçue et sécurité constatée ; vérifier l'existence de procédures dégradées, de tests de reprise et de responsabilités claires. Ne demander aucun paramètre technique permettant de compromettre des équipements.

Juristes, contrôleurs et décideurs

Identifier précisément le texte actuel, son champ, les sanctions disponibles, les jurisprudences, les difficultés de contrôle, les besoins budgétaires, les alternatives à une nouvelle loi et les effets pervers d'une réforme proposée.

Annexe C — Glossaire minimal

Terme	Sens retenu dans le dossier
Cyberattaque	Action malveillante dirigée contre un système numérique ; sa cause et sa portée doivent être documentées.
Incident cyber	Événement compromettant ou menaçant la sécurité ; ne prouve pas toujours une intention criminelle.
Panne systémique	Perturbation qui affecte plusieurs acteurs à cause de dépendances ou mécanismes de propagation.
OIV	Opérateur d'importance vitale, catégorie juridique soumise à des obligations spécifiques.
PCA / PRA	Plan de continuité d'activité / plan de reprise d'activité.
RGPD	Règlement général sur la protection des données personnelles.
Agrément	Reconnaissance administrative de la conformité à des

Terme	Sens retenu dans le dossier
	conditions déterminées ; pas une garantie absolue.
Résilience	Capacité de prévenir, absorber, contenir, continuer et se rétablir.
Donnée personnelle	Information se rapportant à une personne physique identifiée ou identifiable.
Risque résiduel	Risque restant malgré des mesures adaptées et effectivement mises en œuvre.

Annexe D — Bibliographie et traçabilité des sources

Date de clôture des recherches : 13 octobre 2026. Les sources officielles et primaires ont été privilégiées. Les liens servent à vérifier les faits ; toute actualisation future devra dater la consultation et contrôler les versions des pages.

[S01] ANSSI, **Panorama de la cybermenace 2025**, 11 mars 2026. <https://cyber.gouv.fr/actualites/panorama-de-la-cybermenace-2025/>

[S02] CNIL, **Sanction de France Travail**, 29 janvier 2026. <https://www.cnil.fr/fr/violation-de-donnees-sanction-5millions-france-travail>

[S03] CNIL, **Clôture de l'injonction France Travail**, 8 octobre 2026. <https://www.cnil.fr/fr/cloture-injonction-france-travail>

[S04] CNIL, **Sanctions Free / Free Mobile**, 14 janvier 2026. <https://www.cnil.fr/fr/sanction-free-2026>

[S05] CNIL, **Viamedis et Almerys**, 7 février 2024. <https://www.cnil.fr/fr/violation-de-donnees-de-deux-operateurs-de-tiers-payant-la-cnil-ouvre-une-enquete-et-rappelle-aux>

[S06] NHS England, **Synnovis cyber incident**, mise à jour 10 novembre 2025. <https://www.england.nhs.uk/synnovis-cyber-incident/>

[S07] CERT-FR, **Alerte CERTFR-2026-ALE-012**, mises à jour 12-13 octobre 2026. <https://www.cert.ssi.gouv.fr/alerte/CERTFR-2026-ALE-012>

[S08] Reuters, **France : incidents sur les systèmes frigorifiques**, 13 octobre 2026. <https://www.reuters.com/legal/litigation/investigators-hunt-french-supermarket-fridge-hackers-no-claim-responsibility-2026-10-13/>

[S09] Union européenne, **Règlement (UE) 2016/679 (RGPD), texte consolidé**. <https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=fr>

[S10] Microsoft, **Incident CrowdStrike**, 20 juillet 2024. <https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/>

[S11] ENTSO-E, **Rapport final incident Europe du Sud-Est 2024**, 25 février 2025. <https://www.entsoe.eu/news/2025/02/25/entso-e-publishes-the-final-report-on-the-grid-incident-in-south-east-europe/>

[S12] ENTSO-E, **Rapport final blackout ibérique**, 20 mars 2026. <https://www.entsoe.eu/news/2026/03/20/entso-e-publishes-expert-panel-final-report-on-28-april-2025-blackout-in-spain-and-portugal/>

[S13] CNIL, **Facturation électronique : enjeux de protection des données**, 10 septembre 2026. <https://www.cnil.fr/fr/facturation-electronique-quels-enjeux>

[S14] DGFIP, **Facturation électronique et plateformes agréées**, page de référence. <https://www.impots.gouv.fr/facturation-electronique-et-plateformes-agreees>

[S15] Directive (UE) 2022/2555, NIS2, **article 21 et annexes**. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=fr>

[S16] Directive (UE) 2022/2557, CER, article 13. <https://eur-lex.europa.eu/eli/dir/2022/2557/oj?locale=fr>

[S17] Règlement (UE) 2024/2847, Cyber Resilience Act. <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32024R2847>

[S18] Code de la défense, article L1332-6-1. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000030949364

[S19] Conseil d'État, décision n°452798, 3 juin 2022. <https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2022-06-03/452798>

[S20] Assemblée nationale, dossier de loi sur résilience et cybersécurité. <https://www.assemblee-nationale.fr/dyn/17/dossiers/DLR5L17N50731>

[S21] CNIL, Indemnisation pour violation de données, 2 octobre 2026. <https://www.cnil.fr/fr/violations-de-donnees-personnelles-cas-indemnite>

[S22] ANSSI, Retour d'expérience de l'exercice REMPLAR25. <https://cyber.gouv.fr/securisation/gestion-de-crise/entrainement-crise/rempar/rempar25/>

[S23] Défenseur des droits, Enquête 2025 sur les relations aux services publics. <https://www.defenseurdesdroits.fr/enquete-sur-laces-aux-droits-sur-les-relations-des-usagers-avec-les-services-publics-que-retenir>

[S24] Service Public, généralisation de la facturation électronique (calendrier). <https://entreprendre.service-public.fr/actualites/A17450>

Les sources officielles sont privilégiées. L'index renvoie à des documents publiés à des dates différentes ; certaines évaluations évolueront et devront être réexaminées.

Annexe E — Registre des réserves et corrections futures

Sujet	Limite actuelle	Action de révision
Facturation 2026	Déploiement récent ; recul empirique limité.	Actualiser incidents et fonctionnement après plusieurs mois.
Réfrigération oct. 2026	Événement en évolution, périmètre encore variable selon les sources.	Privilégier versions datées du CERT-FR et décisions d'enquête.
NIS2 / CER en France	Parcours législatif susceptible d'évoluer.	Vérifier les textes définitivement promulgués avant publication.
Cas locaux RSA / collectivités	Pièces primaires et suites parfois incomplètes.	Recueillir déclarations, décisions et contradictions.
Coûts de la dématérialisation	Pas d'étude économique chiffrée exhaustive.	Collecter budgets, coûts évités et charges transférées.
Préjudices indemnisés	Fuite ne signifie pas indemnisation automatique.	Documenter décisions de justice et recours.
Dimension militaire	Données stratégiques et contrôles en partie non publics.	S'en tenir aux constats publics, sans extrapolation.

Annexe F — Enquêtes et indicateurs d'opinion : chiffres contextualisés

Cette annexe complète les chapitres 3 et 8 sans se substituer aux données d'incidents. Elle rassemble des enquêtes dont les populations, périodes et questions diffèrent. Aucune moyenne générale n'est calculée entre ces indicateurs.

F.1. Accès aux droits et difficultés administratives : Défenseur des droits

Enquête menée par Ipsos entre octobre 2024 et janvier 2025, auprès de 5 030 personnes âgées de 18 à 79 ans vivant en France métropolitaine, par téléphone ; publication le 13 octobre 2025. [S23, S25]

Indicateur	Résultat	Périmètre et interprétation
Difficultés administratives	61 % en 2024 ; 39 % en 2016	Difficultés ponctuelles ou régulières dans les démarches administratives ; ne mesure pas uniquement le numérique.
Démarches en ligne avec aide ponctuelle	36 %	Déclarent avoir besoin d'une aide ponctuelle pour leurs démarches en ligne.
Démarches en ligne impossibles seul	8 %	Déclarent ne pas y arriver seuls ; catégorie distincte des personnes évitant les démarches.
Évitement des démarches en ligne	7 %	Déclarent éviter les démarches en ligne ; ne pas additionner automatiquement avec d'autres catégories.
Renoncement à un droit	23 %	Ont déjà renoncé à demander un droit dans les cinq années précédentes ; toutes causes possibles.
Problème avec un service public	42 %	Déclarent avoir rencontré un problème avec un ou plusieurs services publics dans les cinq dernières années.
Difficulté à joindre quelqu'un	72 %	Parmi les personnes ayant rapporté un problème : obstacle cité pour obtenir information ou rendez-vous.

Précaution méthodologique : les 61 % ne sont pas des « opposants au numérique » ; les 23 % ne sont pas uniquement des victimes de dématérialisation. Les 72 % sont conditionnels au sous-groupe ayant déclaré un problème.

F.2. Baromètre du numérique, édition 2026 : pratiques, aide et perceptions

Enquête réalisée en juin 2025, publiée début 2026, sous l'égide de l'Arcep, du CGE, de l'Arcom et de l'ANCT, avec le CREDOC ; 4 145 personnes interrogées à travers plusieurs sous-échantillons et modes de recueil. [S26]

Indicateur	Résultat	Précaution
Aide apportée à l'entourage pour les outils numériques	57 %	Ont déjà aidé une personne de leur entourage ; ne signifie pas que l'aide était obligatoire.
Aide à un membre de la famille pour une démarche en ligne	50 %	Expérience déjà vécue ; pas un indicateur de panne de service.
Numérique ne facilite pas le quotidien	36 %	Perception déclarée ; ne signifie pas rejet complet des outils numériques.
Freins aux usages du numérique	40 %	Déclarent des freins ; le manque de maîtrise des outils figure parmi les facteurs évoqués.

F.3. Union européenne : fréquentation et compétences numériques

Source et population	Chiffre	Lecture
Eurostat 2025, résidents de l'UE de 16 à 74 ans	71,9 %	Ont utilisé des sites ou applications des pouvoirs publics durant les 12 mois précédents. [S27]
Eurostat, édition 2026, compétences en 2025	40 %	Personnes dans l'UE ne disposant pas de compétences numériques au moins élémentaires, selon l'indicateur publié. [S28]

Ces statistiques renseignent l'exposition au numérique et les capacités déclarées ou mesurées ; elles ne démontrent ni la sécurité technique des services ni leur défaillance.

F.4. Indicateurs absents et prudence sur les « sondages Diploval »

- À rechercher : enquêtes représentatives sur le niveau de confiance dans les plateformes de facturation, différenciées selon taille d'entreprise et connaissance effective de la réforme.
- À rechercher : données comparables sur l'usage des alternatives non numériques, avec mesure des résultats (dossiers résolus, délais, coûts, satisfaction).
- À rechercher : études fiables reliant incidents ou indisponibilités à des dommages indemnisés, sans confondre personnes concernées et dommages constatés.
- Les contributions volontaires sur Diploval.fr ne constitueront pas un sondage représentatif. Publier systématiquement le nombre de réponses, le mode de recrutement, la formulation des questions, les exclusions et les limites.

Annexe G — Registre probatoire des pièces à obtenir

Cette annexe transforme les questions de la section 13.1 en actions vérifiables. « À obtenir » signifie que le document ou son contenu complet n'a pas été évalué dans cette version ; cela ne présume pas qu'il n'existe pas.

Pièce / donnée recherchée	Acteur ou source à consulter	État au 13/10/2026	Impact sur la conclusion
Bilans publics de contrôle et mise en conformité après les cyberattaques	CNIL, responsables de traitement, décisions publiées	Partiel	Évaluer les corrections réelles, pas seulement les fautes initiales.
Nombre de personnes victimes d'un préjudice démontré et indemnisations	Décisions de justice, associations de victimes, organismes	À documenter	Évaluer le préjudice réel et l'effectivité du recours.
Incidents : durée, services suspendus et coûts comparables	ANSSI, opérateurs, autorités sectorielles, rapports d'activité	À consolider	Comparer l'ampleur et la gravité sans additionner les cas.
Exigences, audits et disponibilité des plateformes de facturation	DGFIP, CNIL, plateformes, certificateurs	Cadre identifié ; audits non collectés	Distinguer conformité déclarée, contrôle et performance réelle.
Protocoles publics de gestion de panne et migration de plateforme	DGFIP, plateformes, éditeurs, TPE/PME	À obtenir	Vérifier la continuité et les coûts de bascule.
Conditions contractuelles, limitation de responsabilité et sous-traitance	Contrats-types publics, représentants TPE/PME, juristes	À obtenir	Évaluer répartition du risque et information des clients.
Coûts complets pour TPE/PME, collectivités et usagers	Études d'impact, enquêtes terrain, chambres consulaires	À mesurer	Tester faisabilité et effets redistributifs.
Tests de secours / retour d'expérience d'exercices multisectoriels	ANSSI, régulateurs, collectivités, opérateurs	Partiel ; détails parfois non publics	Éviter de confondre exercice avec résistance garantie.
Résultats des consultations avant et après dématérialisation	Ministères, Défenseur des droits, associations	À documenter	Évaluer l'inclusion démocratique et la corrigibilité.
État précis des textes français et européens à la date de publication	Légifrance, EUR-Lex, Assemblée, Sénat	À recontrôler avant nouvelle édition	Éviter de proposer une obligation déjà en vigueur.

G.1. Demandes d'informations prioritaires et restrictions de publication

- Saisir les autorités et organismes concernés de demandes sur les dispositifs et leurs résultats, en se limitant aux informations communicables au public.
- Ne pas publier d'identifiants, configurations sensibles, failles non corrigées, lieux techniques de défense ou éléments permettant une intrusion.

- Documenter tout refus ou impossibilité d'accès, son motif (secret, absence de donnée, coût, réponse différée) et la conséquence sur le niveau de preuve.
- Pour chaque réponse obtenue : date, version, émetteur, vérification croisée, correction éventuelle du dossier et traçabilité de la publication.

Annexe H — Arbitrages à ne pas préjuger : droit, technique et finances

H.1. Cinq chemins de décision à conserver ouverts

Constat démontré	Réponse possible	Condition avant préconisation
Le cadre juridique existe et est effectivement appliqué	Aucune réforme nouvelle	Évaluer les incidents résiduels, proportionnellement aux risques.
Obligation pertinente, défaut de moyens ou de contrôle	Financement, contrôle, compétence et organisation	Établir le lien entre le défaut et la conséquence observée.
Règle lacunaire mais domaine déjà réglementé	Adaptation réglementaire ou contractuelle	Vérifier compétence nationale et droit UE.
Lacune législative explicite et mesurable	Amendement ou avant-projet ciblé	Étude d'impact, proportionnalité et avis contradictoires.
Informations insuffisantes ou incompatibles	Suspension des conclusions	Publier les questions et pièces manquantes.

H.2. Hypothèse centrale sur la responsabilité de la numérisation imposée

Une autorité qui organise une obligation numérique n'est pas automatiquement garante d'une sécurité absolue ni juridiquement responsable de tout incident. En revanche, Diploval étudie s'il faut renforcer les garanties de continuité, l'information sur les risques, les contrôles et l'effectivité de la réparation pour les personnes n'ayant pas choisi le dispositif. [S29, S30]

La question doit être examinée au regard des articles 32 et 82 du RGPD, de la responsabilité des prestataires et responsables de traitement, du droit des contrats, du droit administratif, des règles fiscales et des mécanismes d'action de groupe. Une garantie publique subsidiaire ne saurait être recommandée sans chiffrage et examen de ses effets sur les comportements.

H.3. Coûts à quantifier pour chaque scénario

- Prévention : matériels, logiciels, authentification, maintenance, audits, formation et renouvellement des équipements.
- Incident : indisponibilité, commandes ou soins reportés, reconstruction, restauration, assistance, notification, fraude et pertes indirectes.
- Continuité : secours indépendant, tests, stocks, effectifs, conventions de substitution et redondances.
- Coûts supportés par l'utilisateur : équipement, connexion, temps, déplacement, aide familiale, non-recours et retards.

- Bénéfices documentés : fiabilité, rapidité, traçabilité, accessibilité à distance, gains administratifs et diminution de certaines fraudes.

Le dossier ne retient aucune somme globale de « coût de la cybercriminalité pour la France » sans préciser définition, périmètre, méthode d'estimation et incertitude. La somme des montants déclarés dans des médias ne serait pas une estimation nationale valide.

Annexe I — Protocole de participation et de traitement des contributions

I.1. Deux ressources publiques, deux fonctions

Ressource A : le présent dossier est la base documentaire et juridique. Ressource B : un cahier citoyen distinct présente les questions ouvertes, une notice claire et les modalités de retour. Aucun formulaire public ne doit être ouvert en prétendant qu'une proposition de loi est déjà arrêtée.

I.2. De la contribution à la décision motivée

Étape	Action proposée	Trace publique
Information	Mettre à disposition résumé, version, sources et limites	Date, liens et version des documents.
Recueil	Formulaire structuré ; contributions favorables, contraires ou alternatives	Nombre de contributions reçues, règles de modération.
Vérification	Qualifier faits, témoignages, avis ; écarter les données personnelles non nécessaires	Méthodologie et classes de preuve.
Contradiction	Confronter avec les sources, l'expérience de terrain et les obligations existantes	Table des objections et des réponses motivées.
Décision	Retenir, modifier, ajourner ou écarter une piste, ou constater l'absence de réforme	Bilan public des motifs, pas simple compteur de votes.
Suivi	Mettre à jour dossiers, corrections et sources	Journal des versions et date de réexamen.

I.3. Confidentialité, sécurité et accessibilité de l'outil citoyen

- Limiter les champs au strict nécessaire ; éviter l'envoi de documents d'identité, d'informations de santé ou de données sur des tiers.
- Ne pas publier automatiquement les contributions ; demander une autorisation spécifique si des extraits anonymisés sont rendus publics.
- Informer sur la finalité du traitement, les destinataires, la durée de conservation des contacts jusqu'à clôture de la consultation, les droits et les moyens de contact ; vérifier le cadre RGPD avant lancement.

- Prévoir un mécanisme anti-spam proportionné, un accusé de réception et, si possible, un canal alternatif pour les personnes empêchées par le formulaire.
- Publier un bilan qualitatif : les volumes de contributions ne sont pas un vote ni un sondage représentatif.

Annexe J — Fiche de publication sur le site : articulation des contenus

Proposition éditoriale pour Diploval.fr : une page centrale d'analyse et une page de participation reliées entre elles, chacune pouvant être mise à jour sans écraser les versions archivées.

Sur le site	Contenu recommandé	Précaution
Page « Dossier d'analyse »	Résumé exécutif ; enjeux ; chiffres sourcés ; PDF de référence ; méthode ; historique de version.	Afficher la date de vérification et les réserves, sans annoncer une loi prête.
Page « Propositions & contributions »	Questions ouvertes ; arguments et contradictions ; formulaire ; calendrier ; règlement de participation.	Ne pas faire croire à un référendum, ni à un mécanisme institutionnel de vote.
Page « Résultats et suites »	Rapport de traitement ; arguments retenus/écartés ; besoins d'expertise ; textes futurs éventuels.	Protection des personnes, versions datées et rectifications visibles.

J.1. Métriques de suivi à publier

Nombre de contributions reçues et recevables, thèmes abordés, proportion de contributions comportant un exemple ou une source, délais de traitement, corrections apportées, arguments contradictoires ayant fait évoluer le dossier et nombre de demandes d'information sans réponse. Ces indicateurs mesurent le fonctionnement de la consultation, non l'opinion générale des Français.

J.2. Critères de passage vers une rédaction juridique

- Insuffisance précisément identifiée au regard d'un article de droit actuel ; correction non réalisable uniquement par organisation ou contrôle.
- Objectif évaluable, population concernée, coûts et conséquences indésirables documentés.
- Avis contradictoires et compatibilité avec le droit européen analysés.
- Publication préalable d'une synthèse des contributions favorables et défavorables.
- Texte présenté comme avant-projet citoyen, distinct d'une proposition de loi déposée au Parlement.

Annexe K — Sources nouvelles et registre de publication V1.1

[S25] Défenseur des droits, « Enquête sur les relations des usagers avec les services publics », 13 octobre 2025.
<https://www.defenseurdesdroits.fr/enquete-sur-lacces-aux-droits-sur-les-relations-des-usagers-avec-les-services-publics-que-retenir>

[S26] Arcep / ANCT / CREDOC, Baromètre du numérique, édition 2026 (enquête de juin 2025), février-avril 2026.
<https://anct.gouv.fr/ressources/publications/publication-barometre-du-numerique-edition-2026>

[S27] Eurostat, « E-government services used by 72% of people in the EU », données 2025, 12 mars 2026.
<https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20260312-1>

[S28] Eurostat, Digitalisation in Europe, édition 2026 : compétences numériques en 2025.
<https://ec.europa.eu/eurostat/en/web/interactive-publications/digitalisation-2026>

[S29] CNIL, « Facturation électronique : quels enjeux pour la protection des données personnelles ? », 10 septembre 2026. <https://www.cnil.fr/fr/facturation-electronique-quels-enjeux>

[S30] CNIL, « Violations de données personnelles : dans quels cas peut-on être indemnisé ? », 2 octobre 2026.
<https://www.cnil.fr/fr/violations-de-donnees-personnelles-cas-indemnite>

[S31] CNIL, « Clôture de l'injonction prononcée à l'encontre de France Travail », 8 octobre 2026.
<https://www.cnil.fr/fr/cloture-injonction-france-travail>

[S32] CNIL, « Violation de données : sanction de 42 millions d'euros contre Free Mobile et Free », 14 janvier 2026.
<https://www.cnil.fr/fr/sanction-free-2026>

[S33] DGFIP, « Facturation électronique et plateformes agréées », page de référence.
<https://www.impots.gouv.fr/facturation-electronique-et-plateformes-agreees>

[S34] Conseil d'État, décision n° 452798 du 3 juin 2022, téléservice titres de séjour.
<https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2022-06-03/452798>

K.1. Historique de version

V1.0 — 13/10/2026 : socle documentaire ; treize chapitres et cinq annexes, dont épreuve contradictoire intégrale Ω.

V1.1 — 13/10/2026 : maintien du socle V1.0 ; insertion graphique du logo sur la couverture ; ajout des annexes F à K (sondages contextualisés, registre probatoire, arbitrages, protocole de contribution, architecture du site, sources). Aucune proposition de loi n'est finalisée.

K.2. Limites éditoriales et corrections

Ce document peut être diffusé comme dossier de référence public à date, à condition de conserver ses réserves. Une expertise externe contradictoire et certaines pièces probatoires restent attendues. Une correction future mentionnera le point changé, l'ancienne formulation, la nouvelle formulation, les références et la date.