Facturation électronique : données, infrastructures et possibilités d'interconnexion

Ce dépôt documente, à partir de sources officielles, les données et infrastructures mises en place autour de la réforme française de la facturation électronique.

L'objectif est de distinguer clairement :

- **AVÉRÉ** : explicitement établi par une source officielle ;
- **DÉDUCTIBLE TECHNIQUEMENT** : rendu possible par l'architecture documentée, sans usage correspondant officiellement établi ;
- **HYPOTHÈSE** : scénario nécessitant des éléments supplémentaires ;
- **À ÉTABLIR** : question identifiée pour laquelle les sources étudiées ne permettent pas encore de tirer une conclusion suffisamment solide.

Documentation

Chapitre 1 — Données de facturation

Données de facturation, de transaction et de paiement transmises à l'administration, ainsi que leur granularité.

→ Lire le Chapitre 1

Chapitre 2 — Conservation, accès et finalités

Conservation des factures et des données, acteurs intervenant dans leur traitement et leur transmission, objectifs officiels de la réforme et éléments restant à établir concernant l'accès, les traitements et les possibilités de réutilisation.

→ Lire le Chapitre 2

Chapitre 3 — Données environnementales

Passeport numérique de produit, identification des produits, données environnementales structurées, empreinte carbone, interopérabilité et possibilités techniques de rapprochement avec les données de transaction.

→ Lire le Chapitre 3

Chapitre 4 — Euro numérique et infrastructures de paiement

Architecture de l'euro numérique, données de paiement, programmabilité et garanties prévues.

→ Lire le Chapitre 4

Chapitre 5 — Interconnexions

Recherche d'interconnexions existantes, prévues, expérimentées ou techniquement possibles entre les différentes infrastructures.

→ Lire le Chapitre 5

Chapitre 6 — Garanties juridiques

RGPD, finalité et croisement des données, profilage, proportionnalité, droits des personnes, CNIL, garanties propres aux infrastructures étudiées, évolution du cadre juridique et limites des interconnexions.

→ Lire le Chapitre 6

Chapitre 7 — Synthèse

Synthèse des faits établis, des capacités techniques, des interconnexions documentées, des garanties juridiques et des éléments qui restent non établis.

→ Lire le Chapitre 7

Sources

Registre des sources officielles utilisées dans l'enquête.

→ Consulter les sources

Chapitre 1 — Données de facturation transmises à l'administration

> **Navigation :** ← Retour au sommaire

Ce premier chapitre documente les données de facturation, de transaction et de paiement transmises à l'administration dans le cadre de la réforme française de la facturation électronique.

Ce dépôt a pour objectif de documenter, à partir de sources officielles, les données collectées, transmises et traitées dans le cadre de la réforme française de la facturation électronique.

L'objectif n'est pas de présenter comme établis des usages futurs qui ne le sont pas.

La méthode consiste à documenter séparément chaque composant du dispositif, puis à étudier les possibilités techniques et juridiques de croisement ou d'évolution de ces infrastructures.

Chaque élément est classé selon quatre niveaux :

- **AVÉRÉ** : explicitement établi par une source officielle.
- **DÉDUCTIBLE TECHNIQUEMENT** : rendu possible par l'architecture ou les données disponibles, sans usage correspondant officiellement établi.
- **HYPOTHÈSE** : scénario potentiel nécessitant des éléments supplémentaires pour être démontré.

- **À ÉTABLIR** : question identifiée pour laquelle les sources étudiées ne permettent pas encore de tirer une conclusion suffisamment solide.

Sommaire

- 1.1 — Le principe de transmission
- 1.2 — Rôle du Portail Public de Facturation
- 1.3 — Données B2B domestiques
- 1.4 — E-reporting B2B international
- 1.5 — Cas particulier du B2C
- 1.6 — Données de paiement
- 1.7 — Architecture de transmission
- 1.8 — Conclusion du premier chapitre

---

1. Transmission des données de facturation à l'administration

1.1 Le principe de transmission est officiellement établi

Statut : AVÉRÉ

La réforme française de la facturation électronique ne consiste pas uniquement à remplacer les factures papier ou PDF par des documents électroniques.

Elle organise également la transmission de données à l'administration fiscale.

La DGFiP distingue trois mécanismes :

1. la facturation électronique entre entreprises concernées ;
2. la transmission électronique des données de transaction ;
3. la transmission électronique des données de paiement ou d'encaissement.

Dans le cadre de la facturation électronique, les plateformes agréées extraient de la facture les données réglementaires destinées à l'administration S1.

Pour les opérations relevant du e-reporting, des données de transaction ou de paiement sont également transmises à l'administration S2-S3.

1.2 Rôle du Portail Public de Facturation

Statut : AVÉRÉ

À la suite du recentrage du Portail Public de Facturation (PPF), celui-ci conserve notamment une fonction de concentrateur pour la transmission à l'administration fiscale des données de facturation et de transaction S4.

L'architecture peut donc être représentée, de manière simplifiée, ainsi :

```
Entreprise
   ↓
Plateforme agréée
   ↓
Extraction / transmission des données réglementaires
   ↓
Portail Public de Facturation
   ↓
Administration fiscale
```

Le PPF n'est donc pas uniquement un annuaire permettant le routage des factures.

Il constitue également un point de concentration des données destinées à l'administration S4.

1.3 Données de facturation B2B domestique transmises à l'administration

Statut : AVÉRÉ

La DGFiP publie un tableau récapitulatif des données de facture devant être transmises à l'administration pour les opérations domestiques réalisées entre deux entreprises assujetties à la TVA établies en France S1.

Ces données sont introduites progressivement en deux étapes.

À compter du 1er septembre 2026

Donnée	Granularité
SIREN du fournisseur	Facture
Pays d'établissement du fournisseur	Facture
SIREN du client	Facture
Pays d'établissement du client	Facture
Catégorie de l'opération : biens, services ou les deux	Facture
Date d'émission	Facture
Numéro unique de facture	Facture
Montant HT par taux de TVA	Facture
Montant de TVA par taux	Facture
Taux de TVA applicable	Facture
Montant HT total	Facture
Montant total de TVA	Facture
Devise	Facture

Selon l'opération, d'autres informations doivent également être transmises :

- numéro de TVA intracommunautaire du fournisseur ;
- numéro de TVA intracommunautaire du client ;
- identification d'un éventuel représentant fiscal ;
- référence de la facture initiale en cas de rectification ;
- option pour le paiement de la TVA sur les débits ;
- motif d'exonération de TVA ;
- autofacturation ;
- régime particulier de TVA ;
- autoliquidation ;
- appartenance à un assujetti unique ;
- date effective de livraison du bien ou de réalisation de la prestation ;
- date de versement d'un acompte dans les situations prévues.

À compter du 1er septembre 2027

La granularité des données transmises augmente.

Deviennent notamment obligatoires :

Donnée	**Granularité**
Dénomination précise du bien livré ou du service rendu	Ligne de facture
Quantité de biens ou services	Ligne de facture
Prix unitaire HT	Ligne de facture
Rabais, remises, ristournes et réductions	Ligne ou document selon le cas
Frais et charges, par exemple frais de transport	Ligne ou document selon le cas
Adresse de livraison lorsqu'elle diffère de celle du client	Ligne ou document selon le cas
Date de la facture rectifiée	Facture
Mention d'escompte	Facture
Éco-participation	Ligne ou document selon le cas

À partir du 1er septembre 2027, l'administration ne reçoit donc plus uniquement des totaux comptables et fiscaux pour les factures B2B domestiques.

La transmission réglementaire comprend également des informations permettant d'identifier la nature précise du bien ou du service facturé, sa quantité et son prix unitaire hors taxe S1.

1.4 E-reporting B2B international

Statut : AVÉRÉ

Les transactions réalisées avec une entreprise assujettie à la TVA non établie en France sont également concernées par une transmission de données à l'administration S2.

À compter du 1er septembre 2026, les informations transmises comprennent notamment :

- l'identification de l'entreprise française ;
- l'identification de l'entreprise étrangère, notamment par son numéro de TVA intracommunautaire ou un identifiant étranger lorsqu'il existe ;
- le pays du fournisseur ;
- le pays du client ;
- la catégorie de l'opération ;
- la date de facture ;
- le numéro de facture ;
- le montant HT par taux de TVA ;
- le montant de TVA par taux ;
- les taux de TVA ;
- le montant HT total ;
- le montant total de TVA ;
- la devise.

Selon l'opération, d'autres données fiscales ou relatives à la transaction sont également transmises.

À compter du 1er septembre 2027, sont notamment ajoutés :

- la dénomination précise du bien ou du service ;
- la quantité ;
- le prix unitaire HT ;
- les réductions de prix ;
- les frais et charges ;
- l'adresse de livraison dans les cas prévus ;
- certaines informations relatives aux factures rectificatives ;
- l'éco-participation.

La granularité ligne par ligne prévue pour certaines données en 2027 concerne donc également les opérations B2B internationales entrant dans le champ du e-reporting.

1.5 Cas particulier du B2C

Statut : AVÉRÉ

Le traitement des transactions réalisées avec des personnes non assujetties, notamment les particuliers, doit être distingué du B2B.

Pour ces opérations, la DGFiP prévoit actuellement une transmission agrégée par jour.

Pour chaque catégorie de transactions concernée sont notamment transmis :

- la date du jour ;
- la base d'imposition totale HT des opérations de la journée ;
- le montant de TVA correspondant ;
- une ventilation par taux de TVA lorsqu'il existe plusieurs taux.

Le dispositif réglementaire documenté ne permet donc pas d'affirmer que l'administration reçoit, dans le cadre général du e-reporting B2C, le détail individuel de chaque produit acheté par chaque particulier.

Cette distinction est essentielle :

B2B : données pouvant atteindre la ligne de facture à compter de 2027.

B2C : données de transaction actuellement prévues sous forme agrégée par jour S2.

Cette différence devra être conservée dans toute analyse ultérieure.

1.6 Données de paiement

Statut : AVÉRÉ

La réforme comprend également un e-reporting des paiements pour les opérations dont la TVA est exigible à l'encaissement, notamment certaines prestations de services S3.

Les données transmises comprennent :

- la date d'encaissement effectif ;
- le montant encaissé ;
- la ventilation du montant par taux de TVA lorsque nécessaire.

Lorsqu'une facture électronique existe, la transmission peut être rattachée à celle-ci par son statut « encaissée ».

Les informations comprennent alors notamment :

- le numéro de facture ;
- la date de paiement ;
- le montant encaissé par taux de TVA.

Pour certaines opérations B2B internationales sans dépôt de facture électronique, les données de paiement sont également transmises par facture.

Pour le B2C, les données de paiement suivent la logique du e-reporting de transaction : elles sont agrégées par jour.

1.7 Architecture de transmission

Statut : AVÉRÉ

Les spécifications externes version 3.2 décrivent le Portail Public de Facturation comme un concentrateur S4.

Son rôle comprend la concentration :

- des données de facturation ;
- des données de transaction ;
- des données de paiement ;
- de certaines informations relatives au cycle de vie des factures.

Ces données sont ensuite transmises à l'administration fiscale.

L'architecture peut donc être représentée de manière simplifiée ainsi :

```
Entreprise
   ↓
Plateforme agréée
   ↓
Données réglementaires
   ↓
Portail Public de Facturation
   ↓
Administration fiscale
```

La facture complète et les données réglementaires transmises à l'administration ne doivent pas être confondues.

L'administration reçoit les données prévues par les textes et les spécifications applicables.

1.8 Ce que ce premier chapitre permet d'établir

Statut : AVÉRÉ

À ce stade, les documents officiels permettent d'établir que la réforme met en place une infrastructure nationale permettant la collecte et la transmission automatisées de données économiques structurées à l'administration fiscale.

Ces données permettent notamment d'identifier :

- les entreprises participant à une transaction ;
- la date et le numéro de la facture ;
- la nature générale de l'opération ;
- les montants HT ;
- les taux et montants de TVA ;
- certaines informations relatives à la livraison ;
- certaines informations relatives au paiement.

À compter du 1er septembre 2027, pour les opérations B2B concernées, cette granularité comprend également :

- la dénomination précise du bien ou du service ;
- sa quantité ;
- son prix unitaire HT.

Il est donc établi que l'infrastructure permet, pour les transactions B2B concernées, de transmettre à l'administration des données structurées décrivant précisément le contenu économique de certaines lignes de facture.

En revanche, les documents étudiés à ce stade ne permettent pas d'établir :

- que chaque achat effectué par un particulier est individuellement transmis à l'administration ;
- qu'un profil de consommation individuel est constitué ;
- que ces données sont actuellement utilisées pour calculer une empreinte carbone individuelle ;
- qu'elles sont croisées avec des données environnementales ;
- qu'elles sont liées à un système de paiement ou à une monnaie numérique ;
- qu'un mécanisme de restriction individuelle des achats est prévu.

Ces questions constituent les chapitres suivants de l'analyse.

Chapitre 2 — Conservation, accès et finalités des données

Navigation : ← Retour au sommaire

Ce chapitre examine ce qu'il advient des données après leur transmission dans le cadre de la réforme française de la facturation électronique.

Trois questions sont étudiées séparément :

1. combien de temps les factures et données doivent ou peuvent être conservées ;
2. quels acteurs peuvent accéder aux informations ;
3. pour quelles finalités ces données peuvent être utilisées.

Une distinction essentielle doit être faite entre :

- la conservation obligatoire des factures et documents par les assujettis ;
- la conservation ou le traitement effectué par les plateformes agréées ;
- la conservation des données transmises à l'administration fiscale.

Ces trois mécanismes ne doivent pas être confondus.

Sommaire

- 2.1 — Conservation des factures et documents fiscaux
- 2.2 — Conservation et traitement par les plateformes agréées
- 2.3 — Conservation des données par l'administration
- 2.4 — Accès aux données
- 2.5 — Finalités officielles de la réforme
- 2.6 — Contrôle fiscal et lutte contre la fraude
- 2.7 — Connaissance de l'activité économique
- 2.8 — Limites et éléments restant à établir
- 2.9 — Ce que ce chapitre permet d'établir

2.1 Conservation des factures et documents fiscaux

Statut : AVÉRÉ

La transmission de données à l'administration ne supprime pas les obligations de conservation applicables aux entreprises.

Au 1er septembre 2026, l'article L. 102 B du Livre des procédures fiscales prévoit que les livres, registres, documents et pièces sur lesquels peuvent s'exercer les droits de communication, d'enquête et de contrôle de l'administration doivent être conservés pendant six ans S8.

Lorsqu'ils sont établis ou reçus sous forme informatique, ils doivent être conservés sous cette forme pendant la période prévue.

Cette obligation concerne notamment les pièces justificatives permettant l'exercice du contrôle fiscal.

Évolution à compter du 1er janvier 2027

La législation prévoit une modification importante à compter du 1er janvier 2027.

Le délai général prévu par l'article L. 102 B passe alors de six à dix ans S8.

Les livres, registres, documents ou pièces sur lesquels peuvent s'exercer les droits de communication, d'enquête et de contrôle de l'administration devront être conservés pendant dix ans à compter de la dernière opération mentionnée ou de la date à laquelle le document a été établi.

Lorsqu'ils sont établis ou reçus sur support informatique, ils devront être conservés sous cette forme pendant cette période.

Un nouvel article L. 102 B bis précise également que la conservation des factures doit garantir, depuis leur émission jusqu'à l'expiration de leur période de conservation, l'authenticité de leur origine, l'intégrité de leur contenu et leur lisibilité S9.

Conclusion intermédiaire

À compter du 1er janvier 2027, l'environnement réglementaire français prévoit donc une conservation pouvant atteindre dix ans pour les documents et pièces entrant dans le champ de l'article L. 102 B.

Cette obligation de conservation concerne les assujettis et les documents soumis au contrôle de l'administration.

Elle ne permet pas, à elle seule, d'affirmer que l'administration fiscale conserve pendant dix ans une copie de l'ensemble des données qui lui sont transmises dans le cadre de la facturation électronique.

Cette question doit être étudiée séparément.

2.2 Conservation et traitement par les plateformes agréées

Statut : AVÉRÉ

Les plateformes agréées ne constituent pas de simples relais techniques instantanés.

Le Code général des impôts et ses textes d'application leur imposent plusieurs obligations relatives au traitement, à la transmission, à la sécurité et, dans certains cas, à la conservation d'informations S10.

Les plateformes doivent notamment assurer la transmission des factures électroniques dans des conditions garantissant :

- l'authenticité de leur origine ;
- l'intégrité de leur contenu ;
- leur lisibilité.

Ces garanties doivent être assurées depuis l'émission de la facture jusqu'à la fin de sa période de conservation S10.

Les plateformes doivent également mettre en œuvre des processus permettant le traitement :

- des factures électroniques ;
- des données de facturation ;
- des données de transaction ;
- des données de paiement.

Ces processus font partie des éléments contrôlés dans le cadre de l'immatriculation et des audits des plateformes agréées.

Conservation de certaines informations liées au fonctionnement du dispositif

La réglementation prévoit explicitement certaines obligations de conservation.

Par exemple, lorsqu'un assujetti autorise une plateforme à mettre à jour ses informations dans l'annuaire central, l'accord formel correspondant doit être conservé par la plateforme.

Cet accord doit être conservé pendant trois ans après la date à laquelle il cesse de produire ses effets S10.

Les audits des plateformes examinent également leurs mécanismes de traitement, de suivi et d'archivage ainsi que les mesures de sécurité appliquées aux factures et aux données.

Limite importante

Ces obligations ne permettent pas d'affirmer que chaque plateforme agréée doit conserver pendant une durée identique l'intégralité des données de facturation, de transaction et de paiement qu'elle traite.

Il faut distinguer :

- la conservation légale de la facture ;
- la conservation d'éléments techniques ou réglementaires par la plateforme ;
- le transit et le traitement des données réglementaires ;
- la conservation des données par l'administration fiscale.

2.3 Conservation des données par l'administration

Statut : À ÉTABLIR

Le chapitre 1 a établi que les données de facturation sont transmises à l'administration fiscale par les plateformes agréées.

La réglementation prévoit notamment que certaines données de facturation doivent être transmises par la plateforme de l'émetteur dans un délai de vingt-quatre heures suivant le dépôt de la facture S11.

L'existence de cette transmission est donc établie.

En revanche, les sources étudiées à ce stade ne permettent pas d'établir une durée générale unique pendant laquelle l'administration fiscale conserverait l'ensemble des données de facturation, de transaction et de paiement reçues dans le cadre de la réforme.

Il serait donc incorrect de déduire du délai de conservation imposé aux entreprises que la DGFiP conserve automatiquement ces mêmes données pendant une durée identique.

Question restant à documenter :

> Quelle est la durée de conservation, dans les systèmes de l'administration, des données de facturation, de transaction, de paiement et de cycle de vie transmises par les plateformes agréées et concentrées par le Portail Public de Facturation ?

2.4 Accès aux données

Statut : AVÉRÉ / À ÉTABLIR

La réforme organise plusieurs niveaux de traitement et de transmission des données.

Les textes permettent d'identifier les principaux acteurs intervenant dans leur circulation, mais ils ne permettent pas, à ce stade de cette analyse, d'établir de manière exhaustive quels agents ou services administratifs peuvent consulter individuellement chaque catégorie de données une fois celles-ci reçues par l'administration.

Les plateformes agréées

Les plateformes agréées occupent une position intermédiaire obligatoire dans le dispositif de facturation électronique S10.

Elles assurent notamment :

- la réception et le traitement des factures électroniques ;
- les contrôles de conformité prévus par la réglementation ;
- la transmission des factures vers les plateformes de leurs destinataires ;
- la transmission à l'administration des données réglementaires de facturation ;
- la transmission des données de transaction et de paiement lorsqu'elles relèvent du e-reporting.

Elles traitent donc les informations nécessaires à l'exécution de ces opérations S10.

Cet accès ne signifie cependant pas que les plateformes disposent d'un droit général de réutilisation des données pour toute autre finalité.

L'administration fiscale

Le Code général des impôts prévoit explicitement la transmission à l'administration des données issues du dispositif S7.

Pour la facturation électronique B2B, les données des factures électroniques sont transmises à l'administration par la plateforme agréée choisie par l'assujetti S7.

Pour les opérations relevant du e-reporting, les données de transaction et, dans les situations prévues par les textes, les données relatives aux paiements sont également transmises à l'administration S7.

La réglementation prévoit en outre une solution dédiée permettant le recueil S12 :

- des données de facturation ;
- des données de transaction ;
- des données de paiement ;
- de certaines informations relatives aux statuts de traitement.

Il est donc établi que l'administration fiscale est destinataire d'un ensemble structuré de données économiques provenant du dispositif.

L'annuaire central doit être distingué des données fiscales transmises

L'État met également à disposition des plateformes agréées un annuaire central destiné à permettre l'adressage des factures électroniques S12.

Cet annuaire contient notamment des informations permettant d'identifier les assujettis, les personnes morales de droit public et les plateformes agréées, ainsi que les informations nécessaires au routage des factures S12.

L'accès à cet annuaire par les plateformes ne doit pas être confondu avec un accès général aux données fiscales collectées par l'administration.

Il s'agit de deux fonctions différentes du dispositif :

- l'annuaire permet principalement l'identification et l'adressage des factures ;
- la solution dédiée recueille les données réglementaires destinées à l'administration S12.

Ce qui reste à établir

Les sources étudiées permettent donc d'établir la circulation des données entre les entreprises, les plateformes agréées et l'administration fiscale.

Elles ne permettent pas encore d'établir de manière suffisamment précise :

- quels services administratifs disposent d'un accès direct aux bases contenant ces données ;
- quelles catégories d'agents peuvent les consulter individuellement ;
- quelles habilitations techniques sont nécessaires ;
- si certains autres services ou administrations peuvent obtenir un accès direct ou indirect à ces données ;
- quelles traces et procédures de contrôle encadrent les consultations.

Ces éléments nécessitent une recherche spécifique sur les traitements de données concernés, leurs règles d'habilitation et les éventuels textes ou documents relatifs à leur protection.

Question restant à documenter :

> Quels services, agents ou organismes peuvent accéder aux données de facturation, de transaction et de paiement reçues par l'administration, et selon quelles règles d'habilitation et de traçabilité ?

2.5 Finalités officielles de la réforme

Statut : AVÉRÉ

La transmission des données à l'administration ne constitue pas uniquement une conséquence technique de la dématérialisation des factures.

L'administration fiscale présente explicitement plusieurs objectifs associés à la réforme et à l'exploitation des informations qu'elle permet de recueillir.

La Direction générale des Finances publiques identifie quatre objectifs officiels S5 :

1. renforcer la compétitivité des entreprises grâce aux gains liés à la dématérialisation ;
2. simplifier, à terme, les obligations déclaratives en matière de TVA, notamment grâce au pré-remplissage des déclarations ;
3. améliorer la lutte contre la fraude à la TVA ;
4. améliorer la connaissance en temps réel de l'activité des entreprises et le pilotage des politiques publiques.

Ces objectifs sont présentés directement par la DGFiP dans sa documentation consacrée à la réforme S5.

Exploitation automatique et continue des données

La documentation pédagogique publiée par la DGFiP apporte une précision supplémentaire concernant le quatrième objectif S6.

Elle indique que la disponibilité et l'exploitation de données obtenues de façon automatique et continue doivent faciliter le pilotage de l'économie par la puissance publique.

Les remontées d'informations issues de la facturation doivent notamment permettre une connaissance et une visibilité en temps réel de la conjoncture économique, notamment par secteur d'activité.

Il est donc officiellement établi que l'exploitation des données issues du dispositif ne répond pas exclusivement à une finalité de contrôle de la TVA.

Les données doivent également contribuer à la connaissance de l'activité économique et au pilotage des politiques publiques.

Distinction entre les finalités établies et leurs usages futurs

L'existence de cet objectif de pilotage des politiques publiques ne permet cependant pas de conclure que n'importe quelle politique publique pourrait utiliser librement les données collectées.

À ce stade, les sources étudiées établissent :

- l'objectif de lutte contre la fraude à la TVA ;
- l'objectif de pré-remplissage des déclarations de TVA ;
- l'objectif de connaissance en temps réel de l'activité des entreprises ;
- l'objectif de pilotage des politiques publiques ;
- l'exploitation de données obtenues de façon automatique et continue pour améliorer la connaissance de la conjoncture économique.

Elles n'établissent pas, à elles seules :

- l'utilisation des données pour une politique environnementale ;
- l'établissement d'une empreinte carbone individuelle ;
- l'utilisation des données pour limiter certaines transactions ;
- leur interconnexion avec une infrastructure monétaire numérique ;
- un droit général permettant à l'administration de réutiliser les données pour n'importe quelle finalité future.

Ces éventuelles possibilités doivent être étudiées séparément dans les chapitres consacrés aux données environnementales, aux infrastructures de paiement, aux interconnexions et aux garanties juridiques.

Conclusion intermédiaire

La réforme instaure donc non seulement un mécanisme de transmission de données à l'administration fiscale, mais prévoit officiellement que les informations obtenues contribuent à une connaissance plus rapide de l'activité économique.

Le pilotage des politiques publiques figure explicitement parmi les objectifs annoncés de la réforme.

AVÉRÉ :

> L'administration indique que les données obtenues automatiquement et de façon continue doivent notamment permettre d'améliorer la connaissance en temps réel de l'activité économique et de faciliter le pilotage de l'économie par la puissance publique.

À ÉTABLIR :

> Quelles politiques publiques peuvent juridiquement utiliser ces données, sous quelle forme, avec quel niveau de granularité et selon quelles limitations ?

2.6 Contrôle fiscal et lutte contre la fraude

Statut : AVÉRÉ / À ÉTABLIR

La lutte contre la fraude à la TVA constitue explicitement l'un des objectifs officiels de la réforme française de la facturation électronique S5.

La DGFiP présente en effet parmi les quatre objectifs de la réforme celui d'« améliorer la lutte contre la fraude à la TVA ».

Cette finalité doit être rapprochée de la nature des informations transmises à l'administration.

Comme documenté au chapitre 1, le dispositif organise la transmission électronique de données relatives :

- aux factures électroniques ;
- aux transactions relevant du e-reporting ;
- aux paiements ou encaissements dans les situations prévues par les textes.

Des données directement liées à la détermination de la TVA

Le Code général des impôts établit explicitement un lien entre certaines données transmises et la détermination de la taxe S7.

Pour les opérations pour lesquelles la TVA est exigible à l'encaissement, les données relatives au paiement sont communiquées à l'administration sous forme électronique S7.

Le texte précise que les données à transmettre sont celles nécessaires à la détermination de l'exigibilité de la taxe sur la valeur ajoutée S7.

Les données de transaction transmises dans le cadre du e-reporting comprennent également, selon les situations prévues par les textes, des informations telles que :

- la catégorie de transaction ;
- la base d'imposition hors taxe ;
- le taux d'imposition ;
- le montant de TVA correspondant ;
- le montant total de TVA due en France ;
- la date des transactions.

Le dispositif fournit donc à l'administration des données structurées directement exploitables pour la détermination de certains éléments relatifs à la TVA S7.

Une transmission organisée et automatisée

La réforme modifie également la manière dont ces informations parviennent à l'administration.

Les données réglementaires issues des factures électroniques sont extraites et transmises par les plateformes agréées.

Les données de transaction et de paiement relevant du e-reporting sont également transmises électroniquement par leur intermédiaire.

Il ne s'agit donc pas uniquement d'informations susceptibles d'être demandées ponctuellement par l'administration dans le cadre d'un contrôle.

Le dispositif prévoit leur transmission électronique selon les obligations, périodicités et modalités définies par les textes.

Surveillance des obligations de transmission

La DGFiP dispose également d'un service chargé de l'immatriculation et du suivi des plateformes agréées S13.

Parmi les missions officiellement attribuées à ce service figurent notamment :

- la surveillance des obligations de transmission pesant sur les plateformes agréées et leurs utilisateurs ;
- la mise en œuvre éventuelle de sanctions pécuniaires en cas de manquement ;
- le retrait éventuel de l'immatriculation d'une plateforme en cas de manquements répétés.

La transmission des données constitue donc elle-même une obligation faisant l'objet d'un dispositif de surveillance administrative S13.

Ce que ces éléments permettent d'établir

Il est établi que :

- la lutte contre la fraude à la TVA constitue un objectif officiel de la réforme S5 ;
- des données structurées relatives aux factures, transactions et paiements sont transmises électroniquement à l'administration S7 ;
- certaines de ces données sont explicitement définies comme nécessaires à la détermination de l'exigibilité de la TVA S7 ;
- les données de transaction comprennent des éléments permettant de connaître les bases imposables et les montants de TVA correspondants S7 ;
- le respect des obligations de transmission fait lui-même l'objet d'une surveillance par l'administration S13.

Ces différents éléments établissent donc un lien direct entre l'infrastructure de transmission mise en place par la réforme et les objectifs fiscaux liés à la TVA.

Traitement algorithmique des données de facturation électronique

La documentation disponible permet désormais d'établir que les données issues de la facturation électronique sont destinées à intégrer le traitement automatisé « ciblage de la fraude et valorisation des requêtes » (CFVR) de la DGFiP S37.

Dans son avis du 18 juin 2026, la CNIL indique que l'ajout de ces données augmente substantiellement le volume d'informations traité, la DGFiP estimant le volume des factures électroniques à environ 2 à 3 milliards par an S37.

Ces données doivent alimenter la plateforme sécurisée des données de la DGFiP et peuvent être exploitées afin d'identifier des anomalies et des entreprises présentant certains risques fiscaux S37.

Les résultats des requêtes peuvent également être croisés avec d'autres données du traitement CFVR. Celui-ci utilise notamment des méthodes algorithmiques et d'apprentissage, comprenant certaines méthodes

d'apprentissage non supervisé S37.

La CNIL souligne toutefois les risques de biais et d'amplification de ces biais et considère indispensable que les résultats issus des traitements algorithmiques ne remplacent pas l'analyse humaine préalable à l'ouverture d'un contrôle fiscal S37.

Ce que ces éléments ne permettent pas d'affirmer

Ces éléments ne permettent cependant pas d'affirmer que :

- chaque facture électronique déclenche automatiquement une analyse individuelle ou un contrôle fiscal ;
- chaque entreprise reçoit automatiquement un score de risque à partir de l'ensemble de ses factures ;
- les résultats algorithmiques entraînent automatiquement l'ouverture d'un contrôle ;
- les données de facturation sont systématiquement croisées avec l'ensemble des autres bases détenues par l'administration ;
- les données peuvent être réutilisées sans limitation pour des finalités étrangères à celles prévues par les traitements concernés.

L'existence d'un traitement algorithmique et de possibilités de croisement dans le cadre de CFVR est donc établie. L'étendue exacte des traitements, des rapprochements réalisés et des données effectivement mobilisées doit être distinguée de cette capacité documentée.

Conclusion intermédiaire

AVÉRÉ :

> Les données issues de la facturation électronique sont destinées à alimenter le traitement CFVR et la plateforme sécurisée des données de la DGFiP. Elles peuvent notamment être exploitées afin d'identifier des anomalies et certaines situations présentant un risque fiscal, dans un traitement utilisant des méthodes algorithmiques et d'apprentissage S37.

À ÉTABLIR :

> Quelle est l'étendue exacte des traitements appliqués aux données de facturation électronique dans CFVR, quelles autres catégories de données sont effectivement rapprochées de celles-ci et selon quelles modalités ces analyses interviennent-elles dans le ciblage des contrôles fiscaux ?

2.7 Connaissance de l'activité économique

Statut : AVÉRÉ / À ÉTABLIR

La connaissance en temps réel de l'activité des entreprises constitue explicitement l'un des objectifs officiels de la réforme S5.

La DGFiP indique également que la disponibilité et l'exploitation de données obtenues de façon automatique et continue doivent faciliter le pilotage de l'économie par la puissance publique S6.

Les remontées d'informations issues de la facturation doivent notamment permettre une connaissance et une visibilité en temps réel de la conjoncture économique, notamment par secteur d'activité S6.

Un objectif de pilotage économique explicitement documenté

L'objectif annoncé ne se limite pas à produire une connaissance statistique générale de l'économie.

Les documents préparatoires de la réforme indiquent que l'amélioration de la connaissance en temps réel de l'activité des entreprises doit permettre un pilotage de la politique économique « au plus près de la réalité économique des acteurs » S14.

L'évaluation préalable du dispositif fournit également un exemple concret d'utilisation envisagée de ces informations : les données recueillies pourraient enrichir les modèles d'analyse afin de faciliter la détection et l'accompagnement des entreprises en difficulté S14.

Il est donc établi que la remontée des données issues du dispositif a notamment été conçue pour améliorer les capacités d'analyse de la situation économique et contribuer au pilotage de politiques économiques.

Une infrastructure fournissant des données économiques structurées

Comme établi au chapitre 1, les données transmises à l'administration comprennent notamment, selon les opérations concernées, l'identification des entreprises participant à la transaction, les dates et numéros de facture, la catégorie de l'opération, les montants hors taxe, les taux et montants de TVA ainsi que certaines informations relatives aux paiements S1-S2-S3.

À compter du 1er septembre 2027, certaines opérations B2B comprennent également des données au niveau des lignes de facture, notamment la dénomination précise du bien ou du service, la quantité et le prix unitaire hors taxe S1-S2.

Ces données ne constituent donc pas uniquement des totaux fiscaux globaux : dans les situations prévues par les textes, elles décrivent également le contenu économique des transactions avec un niveau de granularité plus important.

Associée à une remontée automatisée et continue des informations S6, cette granularité fournit à l'administration une infrastructure de données permettant une connaissance plus détaillée et plus rapide de certaines composantes de l'activité économique.

Ce que ces éléments permettent d'établir

Il est établi que :

- la connaissance en temps réel de l'activité des entreprises constitue un objectif officiel de la réforme S5 ;
- les données obtenues de façon automatique et continue doivent contribuer à la connaissance de la conjoncture économique, notamment par secteur d'activité S6 ;
- le pilotage de l'économie par la puissance publique est explicitement mentionné dans la documentation de la DGFiP S6 ;
- les travaux préparatoires de la réforme évoquent un pilotage de la politique économique au plus près de la réalité économique des acteurs S14 ;
- l'enrichissement de modèles d'analyse afin de faciliter la détection et l'accompagnement des entreprises en difficulté est explicitement présenté comme un exemple d'utilisation possible des

données recueillies S14.

Ces éléments établissent donc que la collecte de données prévue par la réforme possède également une dimension d'observation et d'analyse de l'activité économique, distincte de son utilisation pour la TVA et la lutte contre la fraude.

Ce que ces éléments ne permettent pas d'affirmer

Ces sources ne permettent cependant pas, à elles seules, d'affirmer que :

- chaque entreprise fait l'objet d'une surveillance économique individuelle permanente ;
- les données de chaque facture sont actuellement utilisées pour attribuer automatiquement un profil économique ou un score à chaque entreprise ;
- l'ensemble des données disponibles est systématiquement utilisé dans les modèles d'analyse économique ;
- les données peuvent être utilisées librement pour n'importe quelle politique publique ;
- les données sont actuellement croisées avec des informations environnementales, monétaires ou relatives aux comportements individuels.

La nature exacte des traitements réalisés à partir de ces données, leur niveau d'agrégation, les modèles d'analyse effectivement utilisés et les règles juridiques encadrant ces usages doivent être distingués des possibilités offertes par l'infrastructure.

Conclusion intermédiaire

AVÉRÉ :

> La réforme prévoit que des données économiques obtenues de façon automatique et continue contribuent à améliorer la connaissance en temps réel de l'activité des entreprises et de la conjoncture économique, notamment par secteur d'activité, afin de faciliter le pilotage de l'économie et des politiques économiques S5-S6-S14.

AVÉRÉ :

> Les travaux préparatoires de la réforme mentionnent explicitement, à titre d'exemple, la possibilité d'enrichir des modèles d'analyse avec les données recueillies afin de faciliter la détection et l'accompagnement des entreprises en difficulté S14.

À ÉTABLIR :

> Quels modèles d'analyse sont effectivement alimentés par les données issues de la facturation électronique, avec quel niveau de granularité, sous quelle forme et selon quelles règles d'accès, d'agrégation et de réutilisation ?

2.8 Limites et éléments restant à établir

Statut : À ÉTABLIR

Les éléments documentés dans ce chapitre permettent d'établir l'existence d'un dispositif organisé de collecte, de transmission et d'exploitation de données économiques structurées par l'intermédiaire des plateformes agréées et de l'administration fiscale.

Ils permettent également d'identifier plusieurs objectifs officiels associés à la réforme, notamment la lutte contre la fraude à la TVA, le pré-remplissage des déclarations, la connaissance en temps réel de l'activité des entreprises et le pilotage des politiques publiques S5-S6.

Certaines caractéristiques essentielles du traitement de ces données restent cependant à documenter.

Durée de conservation par l'administration

Les obligations de conservation imposées aux entreprises et certaines obligations applicables aux plateformes agréées sont établies S8-S9-S10.

En revanche, les sources étudiées ne permettent pas encore d'établir une durée générale unique pendant laquelle l'administration fiscale conserve les données de facturation, de transaction, de paiement et de cycle de vie reçues dans le cadre de la réforme.

À ÉTABLIR :

> Quelle est la durée de conservation de chaque catégorie de données dans les systèmes de l'administration et quelles règles déterminent leur suppression ou leur archivage ?

Accès et habilitations

La circulation des données entre les entreprises, les plateformes agréées et l'administration est documentée S7-S10-S11-S12.

Les sources étudiées ne permettent cependant pas encore d'identifier de manière exhaustive les services, agents ou organismes pouvant consulter les différentes catégories de données une fois celles-ci reçues par l'administration.

À ÉTABLIR :

> Quels services et agents disposent d'un accès aux données, selon quelles habilitations, et quels mécanismes de journalisation et de contrôle permettent de tracer leurs consultations ?

Traitements automatisés et croisements de données

La transmission électronique et structurée des données est établie, de même que l'objectif d'une exploitation automatique et continue permettant notamment d'améliorer la connaissance de la conjoncture économique S4-S6.

Les travaux préparatoires de la réforme mentionnent également la possibilité d'enrichir des modèles d'analyse à partir des données recueillies, notamment afin de faciliter la détection et l'accompagnement des entreprises en difficulté S14.

L'existence de traitements automatisés appliqués aux données de facturation électronique n'est plus seulement une possibilité à établir. La CNIL confirme leur intégration au traitement CFVR, qui utilise notamment des méthodes algorithmiques et d'apprentissage pour l'analyse et le ciblage fiscal S37.

L'étendue exacte de ces traitements et des rapprochements effectivement réalisés reste cependant à documenter.

À ÉTABLIR :

> Quelles méthodes algorithmiques sont effectivement appliquées aux données issues de la facturation électronique dans CFVR, quelles autres catégories de données leur sont rapprochées et avec quel niveau de granularité ?

Croisement avec d'autres bases de données

L'existence d'une infrastructure permettant la transmission de données économiques structurées ne démontre pas que celles-ci sont systématiquement rapprochées d'autres bases détenues par l'administration ou par d'autres organismes publics.

Les sources étudiées dans ce chapitre ne permettent notamment pas d'établir l'existence d'un croisement systématique avec des données environnementales, sociales, bancaires, monétaires ou relatives à la consommation individuelle.

À ÉTABLIR :

> Avec quelles autres bases de données les informations issues de la facturation électronique peuvent-elles juridiquement ou techniquement être rapprochées, et quels croisements sont effectivement réalisés ?

Réutilisation pour le pilotage des politiques publiques

Le pilotage des politiques publiques et la connaissance en temps réel de l'activité des entreprises figurent explicitement parmi les objectifs officiels de la réforme S5-S6.

Cette formulation ne permet cependant pas, à elle seule, de déterminer l'ensemble des politiques publiques susceptibles d'utiliser les données collectées ni les conditions juridiques dans lesquelles une telle réutilisation pourrait intervenir.

Il convient notamment de distinguer les objectifs généraux annoncés pour la réforme des finalités juridiques précises attachées aux différents traitements de données.

À ÉTABLIR :

> Quelles sont les finalités juridiques précises des traitements concernés et dans quelles conditions les données peuvent-elles être réutilisées pour d'autres politiques publiques ?

Agrégation, anonymisation et granularité

Les sources étudiées établissent que certaines données sont transmises avec une granularité importante, notamment au niveau des lignes de facture pour certaines opérations B2B à compter du 1er septembre 2027 S1-S2.

Elles établissent également que le e-reporting B2C général repose sur des données agrégées par jour et ne permet donc pas, sur la seule base des éléments étudiés, d'affirmer que le détail de chaque achat individuel d'un particulier est transmis à l'administration S2.

En revanche, le niveau de granularité effectivement utilisé lors des analyses économiques ou statistiques réalisées à partir de ces données reste à documenter.

À ÉTABLIR :

> Les traitements destinés à la connaissance de l'activité économique et au pilotage des politiques publiques utilisent-ils des données individuelles, agrégées, anonymisées ou pseudonymisées, et à quel stade ces transformations interviennent-elles ?

Conclusion intermédiaire

Les principales incertitudes identifiées ne concernent donc plus l'existence de l'infrastructure de transmission ni la nature générale des données collectées, qui sont documentées, mais les conditions précises de leur conservation, de leur accès, de leur exploitation et de leur éventuelle réutilisation.

Ces questions devront être confrontées aux textes relatifs aux traitements de données, aux règles d'habilitation, aux garanties juridiques et aux éventuelles documentations techniques décrivant les systèmes effectivement utilisés.

Elles constituent également des points de contrôle essentiels pour les chapitres suivants, notamment lorsqu'une possibilité d'interconnexion avec une autre infrastructure sera étudiée.

2.9 Ce que ce chapitre permet d'établir

L'analyse des textes législatifs, réglementaires et des documents officiels permet désormais de distinguer les caractéristiques établies du dispositif des éléments qui restent à documenter.

AVÉRÉ

La réforme française de la facturation électronique met en place une infrastructure organisée permettant la transmission électronique à l'administration de données structurées relatives aux factures, aux transactions et, dans les situations prévues par les textes, aux paiements S4-S7.

Les plateformes agréées assurent le traitement et la transmission des informations nécessaires au fonctionnement de ce dispositif et sont soumises à des obligations réglementaires ainsi qu'à un mécanisme de surveillance administrative S10-S13.

Les entreprises restent soumises à leurs propres obligations de conservation des documents fiscaux. Le délai prévu par l'article L. 102 B du Livre des procédures fiscales évolue de six à dix ans à compter du 1er janvier 2027 dans les conditions prévues par le texte S8, tandis que les règles applicables aux factures imposent également des garanties relatives à l'authenticité de leur origine, à l'intégrité de leur contenu et à leur lisibilité S9.

Ces obligations de conservation ne permettent cependant pas de déduire une durée identique de conservation par l'administration des données qu'elle reçoit.

La lutte contre la fraude à la TVA, le pré-remplissage des déclarations de TVA, la connaissance en temps réel de l'activité des entreprises et le pilotage des politiques publiques figurent parmi les objectifs officiellement annoncés de la réforme S5.

La DGFiP indique également que la disponibilité et l'exploitation de données obtenues de façon automatique et continue doivent faciliter la connaissance de la conjoncture économique, notamment par secteur d'activité, ainsi que le pilotage de l'économie par la puissance publique S6.

Les travaux préparatoires de la réforme mentionnent en outre, à titre d'exemple, la possibilité d'enrichir des modèles d'analyse avec les données recueillies afin de faciliter la détection et l'accompagnement des entreprises en difficulté S14.

Il est donc établi que l'infrastructure ne répond pas uniquement à une fonction technique de transmission des factures : les données recueillies sont également destinées à contribuer à des objectifs fiscaux et à la connaissance de l'activité économique.

À ÉTABLIR

Les sources étudiées dans ce chapitre ne permettent pas encore d'établir avec suffisamment de précision :

- la durée de conservation de chaque catégorie de données dans les systèmes de l'administration ;
- les services et catégories d'agents pouvant accéder directement aux différentes données ;
- les règles précises d'habilitation, de journalisation et de contrôle des consultations ;
- l'étendue précise des traitements algorithmiques appliqués aux données de facturation électronique dans CFVR et les modalités exactes de leur rapprochement avec les autres données du traitement ;
- l'existence et la nature de rapprochements systématiques avec d'autres bases de données ;
- le niveau de granularité effectivement utilisé pour les analyses économiques et le pilotage des politiques publiques ;
- les mécanismes d'agrégation, d'anonymisation ou de pseudonymisation éventuellement appliqués ;
- les finalités juridiques précises attachées aux différents traitements et les conditions dans lesquelles les données peuvent être réutilisées pour d'autres politiques publiques.

Limite de l'analyse

L'existence d'une infrastructure permettant la collecte et l'exploitation de données économiques structurées ne démontre pas, à elle seule, l'existence d'un système général de surveillance économique individuelle.

Elle ne démontre pas non plus l'existence d'une interconnexion avec des données environnementales, une infrastructure monétaire numérique ou des mécanismes permettant de conditionner ou de restreindre

certaines transactions.

Ces hypothèses nécessitent l'existence d'autres infrastructures, de données compatibles et de mécanismes d'interconnexion qui doivent être documentés séparément.

Les chapitres suivants examineront donc successivement les données environnementales, les infrastructures numériques de paiement, les possibilités d'interconnexion et les garanties juridiques susceptibles d'encadrer ou de limiter ces usages.

Conclusion du chapitre

AVÉRÉ :

> La réforme française de la facturation électronique organise la transmission à l'administration de données économiques structurées et prévoit explicitement leur utilisation pour des objectifs fiscaux ainsi que pour améliorer la connaissance en temps réel de l'activité économique et le pilotage des politiques publiques S5-S6-S7.

AVÉRÉ :

> La documentation officielle prévoit une exploitation de données obtenues de façon automatique et continue, et les travaux préparatoires ont explicitement envisagé leur utilisation pour enrichir certains modèles d'analyse économique S6-S14.

À ÉTABLIR :

> Les conditions précises de conservation par l'administration, d'accès aux données, l'étendue et les modalités des traitements automatisés, de croisement avec d'autres bases et de réutilisation pour d'autres politiques publiques restent à documenter.

HYPOTHÈSE :

> Une éventuelle interconnexion future de cette infrastructure avec d'autres systèmes de données ne peut être déduite de la seule existence du dispositif de facturation électronique et doit être étudiée séparément.

Chapitre 3 — Données environnementales

> **Navigation :** ← Retour au sommaire

Ce chapitre examine les dispositifs permettant d'associer des données environnementales structurées à des produits, ainsi que leur niveau de granularité et les infrastructures prévues pour les rendre accessibles.

L'objectif est notamment de déterminer quelles informations environnementales peuvent être associées à un produit, sous quelle forme elles peuvent être identifiées ou consultées et si un lien avec les données économiques étudiées dans les chapitres précédents est officiellement prévu.

Une distinction essentielle doit être faite entre :

- les données environnementales relatives à un produit ;
- l'identification numérique d'un produit ;
- le calcul de l'empreinte environnementale ou carbone d'un produit ;
- l'attribution éventuelle de ces informations à une transaction ;
- l'établissement éventuel d'un profil environnemental individuel.

L'existence des premiers éléments ne démontre pas automatiquement l'existence des suivants.

Sommaire

- 3.1 — Le passeport numérique des produits
- 3.2 — Données environnementales pouvant être associées aux produits
- 3.3 — Identification et granularité des données
- 3.4 — Empreinte environnementale et empreinte carbone
- 3.5 — Accès et circulation des données
- 3.6 — Lien éventuel avec les données de transaction
- 3.7 — Ce qui est techniquement déductible
- 3.8 — Limites et éléments restant à établir
- 3.9 — Ce que ce chapitre permet d'établir

3.1 Le passeport numérique des produits

Statut : AVÉRÉ

L'Union européenne a établi un cadre juridique pour le passeport numérique de produit, ou Digital Product Passport, dans le règlement (UE) 2024/1781 relatif à l'écoconception des produits durables S15.

Le dispositif ne correspond pas uniquement à l'affichage d'informations environnementales destinées au consommateur. Il repose sur une infrastructure permettant d'associer à un produit un ensemble de données numériques structurées et accessibles selon des règles définies par la réglementation S15.

Un identifiant numérique associé au produit

Le passeport numérique de produit doit être relié, par l'intermédiaire d'un support de données, à un identifiant unique persistant du produit S15.

Selon les règles qui seront applicables à chaque groupe de produits, le passeport pourra être établi au niveau :

- du modèle ;
- du lot ;
- de l'article individuel.

Le niveau de granularité n'est donc pas nécessairement limité à une catégorie générale de produits : le cadre réglementaire permet qu'un passeport corresponde, lorsque les règles applicables au produit le prévoient, à un article individuel S15.

Des données conçues pour être exploitables par des systèmes informatiques

Les données contenues dans le passeport numérique de produit doivent reposer sur des standards ouverts et utiliser un format interopérable S15.

Elles doivent également être, lorsque cela est approprié :

- lisibles par machine ;
- structurées ;
- recherchables ;
- transférables au moyen d'un réseau ouvert et interopérable d'échange de données.

Le règlement prévoit également une interopérabilité technique, sémantique et organisationnelle entre les passeports numériques de produits S15.

Le dispositif constitue donc une infrastructure de données structurées conçue pour permettre leur traitement et leur circulation entre différents systèmes informatiques, selon les droits d'accès applicables.

Un registre numérique géré par la Commission européenne

Le règlement prévoit la mise en place par la Commission européenne d'un registre numérique des passeports de produits S15.

Ce registre contient au minimum les identifiants uniques prévus par le dispositif. Pour certains produits importés, il contient également le code de marchandise correspondant S15.

La Commission européenne assure la gestion du registre.

La Commission, les autorités nationales compétentes et les autorités douanières disposent d'un accès au registre pour l'exécution des missions qui leur sont attribuées par le droit de l'Union S15.

Un portail internet public doit également permettre aux parties prenantes de rechercher et de comparer certaines données contenues dans les passeports, dans les limites de leurs droits d'accès respectifs S15.

Une interconnexion avec une autre infrastructure publique est explicitement prévue

Le règlement prévoit explicitement une interconnexion entre le registre des passeports numériques de produits et le système européen d'échange de certificats du guichet unique pour les douanes, EU CSW-CERTEX S15.

Cette interconnexion doit permettre l'échange automatisé d'informations avec les systèmes douaniers nationaux S15.

Les contrôles correspondants doivent notamment permettre de vérifier électroniquement et automatiquement la correspondance entre certains identifiants communiqués lors de l'importation et les informations présentes dans le registre S15.

Il est donc établi que l'architecture du passeport numérique de produit n'est pas conçue comme un système nécessairement isolé : le règlement organise déjà son interconnexion avec une autre infrastructure numérique publique européenne pour certaines finalités douanières.

Limite à ce stade

Cette interconnexion avec les systèmes douaniers ne démontre pas l'existence d'une interconnexion avec les systèmes de facturation électronique, les plateformes agréées, les infrastructures bancaires ou les systèmes de paiement.

Elle démontre en revanche que le cadre technique et juridique du passeport numérique de produit prévoit des identifiants structurés, des mécanismes d'interopérabilité et au moins une interconnexion automatisée avec une autre infrastructure publique.

L'existence éventuelle d'autres connexions doit donc être recherchée séparément.

Conclusion intermédiaire

AVÉRÉ :

> L'Union européenne met en place une infrastructure de passeports numériques permettant d'associer des données structurées et interopérables à des produits identifiés de manière unique, avec une granularité pouvant, selon les règles applicables, atteindre l'article individuel S15.

AVÉRÉ :

> Le règlement prévoit un registre numérique géré par la Commission européenne et organise explicitement son interconnexion avec l'infrastructure européenne EU CSW-CERTEX afin de permettre des échanges automatisés d'informations avec les systèmes douaniers nationaux S15.

À ÉTABLIR :

> Existe-t-il d'autres infrastructures, standards, identifiants, projets, partenariats ou mécanismes d'interopérabilité permettant ou préparant un rapprochement entre les données du passeport numérique de produit et des données de facturation, de transaction ou de paiement ?

3.2 Données environnementales pouvant être associées aux produits

Statut : AVÉRÉ

Le passeport numérique de produit est destiné à rendre accessibles des informations relatives aux caractéristiques, à la composition, à la durabilité et aux impacts environnementaux des produits concernés S15-S16.

Le contenu exact d'un passeport n'est pas identique pour tous les produits. Les données obligatoires dépendent du groupe de produits et des exigences prévues par les actes européens applicables S15.

Des informations relatives aux impacts environnementaux

Selon la Commission européenne, un passeport numérique de produit peut notamment fournir, selon le produit et la législation applicable, des informations relatives :

- à l'empreinte carbone ;
- à l'empreinte environnementale ;
- à la durabilité ;
- à la réparabilité ;
- à la recyclabilité S16.

Le dispositif peut donc associer directement à un produit des informations permettant d'en caractériser certains impacts ou certaines performances environnementales.

L'existence d'une donnée relative à l'empreinte carbone d'un produit ne signifie cependant pas qu'une empreinte carbone individuelle est calculée pour son acheteur.

Il s'agit à ce stade d'une information associée au produit.

Composition, matériaux et substances

Les informations accessibles peuvent également concerner les matériaux et composants utilisés dans le produit S16.

Des informations relatives aux substances dangereuses ou préoccupantes peuvent également être concernées selon les exigences applicables S15-S16.

Le passeport peut ainsi fournir des informations structurées ne décrivant pas seulement le produit commercialement, mais également certaines caractéristiques de sa composition matérielle.

Durabilité, réparation et utilisation

Les informations susceptibles d'être accessibles comprennent également des éléments relatifs :

- à la durée de vie ou à la durabilité du produit ;
- à sa réparabilité ;
- aux instructions de réparation ;
- à la disponibilité de pièces détachées ;
- à son utilisation et à sa maintenance S16.

Ces informations doivent notamment permettre aux différents acteurs disposant des droits d'accès correspondants de mieux connaître les caractéristiques du produit pendant son cycle de vie.

Fin de vie, réemploi et recyclage

Le passeport numérique de produit peut également fournir des informations relatives :

- au démontage ;
- au réemploi ;
- au recyclage ;
- à la gestion du produit en fin de vie S16.

Le DPP accompagne ainsi potentiellement l'information relative au produit au-delà de sa seule mise sur le marché.

Une donnée environnementale associée à un produit identifiable

Le point important pour la suite de l'analyse résulte de la combinaison des éléments établis dans les sections 3.1 et 3.2.

Le cadre européen permet d'associer un passeport numérique à un produit identifié de manière unique, avec une granularité pouvant selon les règles applicables atteindre l'article individuel S15.

Ce passeport peut contenir, selon le groupe de produits concerné, des informations relatives à l'empreinte carbone ou environnementale, à la composition, à la durabilité, à la réparabilité et à la recyclabilité S15-S16.

Il est donc établi que l'infrastructure européenne permet d'associer des caractéristiques environnementales structurées à des produits numériquement identifiables.

Ce que cela ne permet pas d'affirmer

Ces éléments ne permettent pas d'affirmer :

- qu'une empreinte carbone est obligatoirement calculée pour chaque produit commercialisé dans l'Union européenne ;
- que chaque article individuel possède nécessairement un passeport individuel ;
- que l'empreinte carbone d'un produit est automatiquement rattachée à l'identité de son acheteur ;
- qu'un historique environnemental individuel des achats est constitué ;
- que ces données sont transmises à l'administration fiscale ;
- qu'elles sont actuellement rapprochées des données de facturation, de transaction ou de paiement.

Ces différents mécanismes doivent être recherchés séparément.

Conclusion intermédiaire

AVÉRÉ :

> Le cadre européen du passeport numérique de produit permet d'associer à des produits numériquement identifiables des informations environnementales structurées pouvant notamment concerner leur empreinte carbone ou environnementale, leur composition, leur durabilité, leur réparabilité et leur recyclabilité S15-S16.

AVÉRÉ :

> Selon les exigences applicables au groupe de produits concerné, le passeport peut être défini au niveau du modèle, du lot ou de l'article individuel S15.

À ÉTABLIR :

> Dans quelles catégories de produits l'empreinte carbone ou environnementale sera-t-elle effectivement obligatoire, selon quelle méthodologie, avec quelle granularité et sous quelle forme les valeurs correspondantes seront-elles enregistrées dans le passeport numérique de produit ?

À ÉTABLIR :

> Existe-t-il un mécanisme permettant de conserver ou de transmettre l'identifiant du produit issu du passeport numérique dans une facture électronique, une transaction commerciale ou un système de paiement ?

3.3 Identification et granularité des données

Statut : AVÉRÉ / DÉDUCTIBLE TECHNIQUEMENT

Le passeport numérique de produit et les standards utilisés dans les échanges commerciaux électroniques disposent de mécanismes permettant d'identifier les produits de manière structurée.

L'analyse de ces mécanismes fait apparaître un point de correspondance technique entre les deux infrastructures : l'utilisation possible d'identifiants standardisés de produits.

Des identifiants uniques pour le passeport numérique de produit

Le règlement (UE) 2024/1781 prévoit que le passeport numérique de produit est relié à un identifiant unique et persistant du produit S15.

Selon les exigences applicables au groupe de produits concerné, le passeport peut être établi au niveau du modèle, du lot ou de l'article individuel S15.

Le règlement prévoit également des identifiants uniques relatifs aux opérateurs économiques et aux installations associés au produit S15.

Ces mécanismes ont notamment pour objectif de permettre la traçabilité des produits et des acteurs concernés le long de la chaîne de valeur.

Le GTIN parmi les données du passeport numérique de produit

L'annexe III du règlement (UE) 2024/1781 prévoit parmi les données pouvant être incluses dans le passeport numérique de produit le Global Trade Item Number, ou GTIN, ou un identifiant équivalent pour les produits ou leurs parties S15.

Le GTIN constitue un identifiant standardisé utilisé dans les chaînes commerciales pour identifier des articles.

Le passeport numérique de produit peut donc comporter, en plus de son identifiant unique propre, un identifiant commercial standardisé du produit S15.

Des identifiants standardisés également présents dans les échanges commerciaux électroniques

Les standards de facturation électronique permettent également d'associer un identifiant standardisé à l'article figurant sur une ligne de facture.

Dans le modèle utilisé par Peppol BIS Billing, le terme métier BT-157 correspond à l'identifiant standard de l'article S17.

Cet identifiant est associé à un schéma d'identification enregistré S17.

Les flux commerciaux Peppol utilisent également ce mécanisme d'identification standardisée des produits dans d'autres documents de la chaîne commerciale, notamment les commandes, où le GTIN est explicitement prévu comme exemple d'identifiant standard d'article S17.

Il existe donc des mécanismes normalisés permettant de conserver une identification structurée d'un produit au cours de différentes étapes d'un échange commercial.

Un point de correspondance technique entre les infrastructures

Les éléments précédents permettent d'identifier une correspondance technique importante.

D'une part, le passeport numérique de produit peut contenir un GTIN ou un identifiant équivalent du produit ou de ses parties S15.

D'autre part, les standards utilisés pour les échanges commerciaux électroniques permettent de transporter un identifiant standardisé de l'article au niveau de la ligne de facture et dans d'autres documents commerciaux S17.

DÉDUCTIBLE TECHNIQUEMENT :

> Lorsqu'un produit référencé dans un passeport numérique de produit et un article figurant dans un document commercial électronique utilisent le même identifiant standardisé, notamment un GTIN, cet identifiant peut techniquement constituer une clé de rapprochement entre les deux ensembles de données.

Ce rapprochement ne nécessite pas nécessairement que les deux infrastructures utilisent la même base de données : l'existence d'un identifiant commun peut permettre à un système disposant des données nécessaires d'établir une correspondance entre les enregistrements.

Une granularité qui doit être distinguée

Cette possibilité technique doit cependant être interprétée avec prudence.

Un GTIN identifie généralement une référence commerciale et ne démontre pas à lui seul l'identification d'un exemplaire physique particulier.

Le règlement DPP distingue précisément plusieurs niveaux possibles de granularité : modèle, lot ou article individuel S15.

De même, la présence d'un identifiant standardisé dans un format de facture ne signifie pas que cet identifiant est obligatoirement renseigné dans chaque facture électronique.

La possibilité technique de rapprochement dépend donc notamment :

- de la présence effective d'un identifiant commun ;
- du niveau de granularité du passeport ;
- du niveau de granularité de l'identifiant présent dans le document commercial ;
- de la conservation de cet identifiant au cours des différentes étapes de la transaction.

Un rapprochement techniquement possible n'est pas un rapprochement avéré

Aucune des sources étudiées à ce stade ne permet d'établir que les plateformes agréées, le Portail Public de Facturation ou l'administration fiscale rapprochent effectivement les identifiants présents dans les factures avec les données contenues dans les passeports numériques de produits.

Il n'est pas non plus établi qu'un identifiant DPP ou qu'un GTIN soit systématiquement transmis à l'administration fiscale dans le cadre de la réforme française de la facturation électronique.

La présence d'identifiants compatibles dans plusieurs infrastructures constitue donc une possibilité technique de rapprochement et non la preuve de son utilisation.

Conclusion intermédiaire

AVÉRÉ :

> Le passeport numérique de produit repose sur des identifiants structurés et peut notamment comporter un GTIN ou un identifiant équivalent du produit ou de ses parties S15.

AVÉRÉ :

> Les standards de facturation électronique permettent de renseigner au niveau de la ligne de facture un identifiant standard de l'article, et les standards Peppol utilisent également des identifiants standardisés de produits, notamment le GTIN, dans différents documents commerciaux S17.

DÉDUCTIBLE TECHNIQUEMENT :

> Lorsqu'un même identifiant standardisé de produit est présent dans un passeport numérique de produit et dans un document commercial électronique, il peut techniquement servir de clé permettant de rapprocher les informations environnementales associées au produit des informations décrivant la transaction commerciale.

À ÉTABLIR :

> Des acteurs publics ou privés utilisent-ils, expérimentent-ils ou prévoient-ils effectivement cette correspondance entre identifiants de produits afin de relier les données du passeport numérique de produit aux données de commande, de facturation, de transaction ou de paiement ?

3.4 Empreinte environnementale et empreinte carbone

Statut : AVÉRÉ

L'existence d'informations environnementales associées aux produits ne repose pas uniquement sur des descriptions qualitatives telles que la réparabilité ou la recyclabilité.

L'Union européenne dispose également de méthodes permettant de calculer quantitativement les impacts environnementaux associés à certains produits et à leur cycle de vie S18.

Une méthode européenne d'empreinte environnementale des produits

La Commission européenne a développé la méthode Product Environmental Footprint (PEF), destinée à mesurer et à communiquer les impacts environnementaux potentiels d'un produit sur l'ensemble de son cycle de vie S18.

Cette méthode repose sur une analyse structurée prenant notamment en compte les matériaux composant le produit, les processus de fabrication, l'énergie utilisée, le transport et la fin de vie S18.

La méthodologie prévoit également que certaines données utilisées dans l'étude soient spécifiques au produit étudié. La nomenclature des matériaux doit notamment correspondre au produit concerné et la modélisation des procédés de fabrication doit reposer sur des données propres à l'entreprise dans les conditions prévues par la méthode S18.

Des règles spécifiques peuvent être établies pour certaines catégories de produits au moyen des Product Environmental Footprint Category Rules, ou PEFCR S18.

L'empreinte environnementale peut donc résulter d'un calcul structuré reposant sur des caractéristiques physiques et industrielles relatives au produit et à son cycle de vie.

L'empreinte carbone constitue un paramètre environnemental prévu par le règlement ESPR

Le règlement (UE) 2024/1781 prévoit que les exigences d'information applicables à certains groupes de produits peuvent porter sur différents paramètres environnementaux, parmi lesquels l'empreinte carbone et l'empreinte environnementale S15.

Selon les actes applicables aux groupes de produits concernés, ces informations peuvent notamment être rendues accessibles au moyen du passeport numérique de produit S15.

Le cadre ESPR établit donc la possibilité juridique d'associer une information quantitative relative à l'empreinte environnementale ou carbone à un produit numériquement identifiable.

Il ne signifie cependant pas qu'une empreinte carbone sera obligatoire pour chaque produit commercialisé dans l'Union européenne.

Le cas des batteries montre une application réglementaire concrète

Le règlement (UE) 2023/1542 relatif aux batteries fournit un exemple concret de mise en œuvre d'une empreinte carbone réglementaire associée à un produit S19.

Pour certaines catégories de batteries, une déclaration d'empreinte carbone est progressivement exigée S19.

Cette empreinte est exprimée en kilogrammes de CO_2 équivalent par kWh de l'énergie totale fournie par la batterie pendant sa durée de vie prévue S19.

La réglementation prévoit également une différenciation de l'empreinte selon plusieurs étapes du cycle de vie S19.

Le calcul prend notamment en compte :

- l'acquisition et le prétraitement des matières premières ;
- la production ;
- la distribution ;
- la production propre d'électricité lorsqu'elle est concernée ;
- la fin de vie S19.

La méthodologie réglementaire s'appuie sur la méthode d'évaluation de l'impact « changement climatique » issue du Product Environmental Footprint S19.

Une valeur liée au modèle et au site de production

Dans le cas des batteries concernées, la réglementation prévoit que la déclaration d'empreinte carbone soit spécifique à un modèle de batterie produit dans un site de fabrication déterminé S19.

Les données d'activité spécifiques à la batterie doivent être utilisées pour le calcul dans les conditions prévues par la réglementation S19.

Le texte prévoit également qu'une modification de la nomenclature des matériaux ou du mix énergétique utilisé pour produire un modèle de batterie entraîne un nouveau calcul de son empreinte carbone S19.

L'information environnementale peut donc atteindre un niveau de précision combinant une référence de produit, certaines caractéristiques de sa fabrication et un site de production déterminé.

Du calcul environnemental à la donnée numérique produit

Les éléments établis depuis le début de ce chapitre permettent désormais d'identifier plusieurs composantes complémentaires.

Le passeport numérique permet d'associer des données structurées à un produit identifiable S15.

Les informations susceptibles d'être associées au produit peuvent comprendre son empreinte carbone ou environnementale S15-S16.

Des méthodes européennes permettent de calculer les impacts environnementaux d'un produit à partir de données relatives à son cycle de vie S18.

Enfin, le règlement relatif aux batteries fournit déjà un exemple dans lequel une empreinte carbone quantitative est réglementairement calculée pour certaines catégories de produits S19.

Il est donc établi que l'Union européenne dispose à la fois d'infrastructures permettant d'identifier numériquement des produits et de méthodologies permettant d'associer à certains produits des indicateurs environnementaux quantifiés.

Une distinction essentielle avec l'empreinte d'un acheteur

L'empreinte carbone d'un produit et l'empreinte carbone d'une personne constituent deux notions différentes.

Les textes étudiés établissent l'existence de données environnementales relatives aux produits.

Ils ne permettent pas d'établir que ces valeurs sont additionnées en fonction des achats réalisés par une personne afin de constituer automatiquement une empreinte carbone individuelle.

Un tel mécanisme nécessiterait notamment qu'un système puisse établir un lien entre les produits acquis, leurs informations environnementales et un acheteur déterminé.

Cette question dépend donc directement des possibilités d'interconnexion étudiées dans la section précédente et dans les sections suivantes.

Conclusion intermédiaire

AVÉRÉ :

> L'Union européenne dispose d'une méthodologie structurée permettant de calculer l'empreinte environnementale de produits sur leur cycle de vie S18.

AVÉRÉ :

> Le cadre ESPR prévoit que des informations relatives à l'empreinte carbone ou environnementale puissent faire partie des exigences d'information applicables à certains groupes de produits S15.

AVÉRÉ :

> Le règlement européen relatif aux batteries fournit déjà un exemple concret dans lequel une empreinte carbone quantitative est associée à certaines catégories de produits selon une méthodologie réglementaire prenant notamment en compte le modèle de batterie, le site de production et différentes étapes de son cycle de vie S19.

DÉDUCTIBLE TECHNIQUEMENT :

> Lorsqu'un produit peut être identifié dans une transaction et qu'une donnée environnementale quantitative peut être retrouvée à partir de son identifiant, les deux informations peuvent techniquement être rapprochées afin d'associer la caractéristique environnementale du produit à la transaction correspondante.

À ÉTABLIR :

> Existe-t-il des dispositifs, projets ou expérimentations utilisant effectivement cette possibilité pour rapprocher automatiquement les données environnementales d'un produit de données de commande, de facture, de paiement ou d'identification d'un acheteur ?

3.5 Accès et circulation des données

Statut : AVÉRÉ / À ÉTABLIR

Le passeport numérique de produit ne repose pas sur un simple document numérique statique associé à un produit.

Son architecture prévoit différents acteurs, différents niveaux d'accès, des mécanismes d'identification et d'autorisation ainsi que des interfaces permettant l'échange automatisé d'informations entre systèmes S15-

S20.

Un système décentralisé

Le système du passeport numérique de produit repose sur une architecture décentralisée S20.

Le registre européen ne contient pas nécessairement l'intégralité des informations détaillées présentes dans chaque passeport.

Les données complètes du passeport restent sous la responsabilité de l'opérateur économique concerné et peuvent être hébergées directement par celui-ci ou par un prestataire de services de passeport numérique de produit S15-S20.

Le registre européen joue notamment un rôle d'indexation et conserve les identifiants uniques, les données d'enregistrement et certaines métadonnées prévues par la réglementation S15-S20.

Cette architecture distingue donc le registre central européen des systèmes dans lesquels sont conservées les informations détaillées associées aux produits.

Plusieurs catégories d'acteurs peuvent accéder aux données

Le règlement (UE) 2024/1781 prévoit que différentes catégories d'acteurs peuvent accéder gratuitement et facilement aux informations du passeport en fonction des droits qui leur sont attribués S15.

Ces acteurs comprennent notamment :

- les clients ;
- les fabricants ;
- les importateurs ;
- les distributeurs et revendeurs ;
- les réparateurs professionnels ;
- les opérateurs indépendants ;
- les reconditionneurs ;
- les remanufactureurs ;
- les recycleurs ;
- les autorités de surveillance du marché ;
- les autorités douanières ;
- certaines organisations de la société civile et organisations syndicales ;
- d'autres acteurs pertinents selon les règles applicables S15.

L'accès n'est donc pas nécessairement identique pour tous les utilisateurs.

Les droits permettant de consulter, introduire, modifier ou mettre à jour certaines informations dépendent du rôle de l'acteur et des règles applicables au groupe de produits concerné S15.

Une API permettant l'intégration avec les systèmes informatiques des opérateurs

Le règlement d'exécution relatif au registre prévoit une API permettant l'enregistrement des passeports numériques de produits et la réception d'informations provenant du registre S20.

La Commission précise que cette API permet aux opérateurs économiques d'intégrer, lorsque cela est approprié, les opérations d'enregistrement dans leurs systèmes numériques existants S20.

Lors de l'enregistrement d'un passeport, le registre génère un identifiant unique d'enregistrement qui peut être communiqué automatiquement à l'acteur concerné par l'interface utilisateur ou directement dans la réponse de l'API S20.

Le registre n'est donc pas conçu uniquement pour une utilisation humaine au moyen d'un portail web : son architecture permet également des échanges automatisés entre systèmes informatiques.

Identification, autorisation et délégation

Les opérateurs économiques souhaitant intervenir dans le registre doivent faire l'objet d'un processus de vérification S20.

D'autres acteurs de la chaîne de valeur pouvant effectuer certaines opérations dans le registre sont également soumis à un mécanisme de vérification S20.

Le dispositif prévoit des mécanismes d'identification et d'autorisation des utilisateurs ainsi que la possibilité, pour certains acteurs vérifiés, de déléguer des droits d'accès à des utilisateurs agissant pour leur compte S20.

Le règlement prévoit notamment le recours à des mécanismes d'identification électronique relevant du cadre européen applicable à l'identification électronique S20.

Une intégration avec d'autres systèmes d'information de l'Union est envisagée par le texte

Le règlement d'exécution prévoit explicitement le cas dans lequel le registre des passeports numériques de produits serait intégré à un autre système d'information de l'Union disposant d'un processus de vérification d'identité équivalent ou identique S20.

Dans cette situation, un opérateur économique ou un autre acteur de la chaîne de valeur déjà enregistré dans cet autre système n'a pas à effectuer une nouvelle procédure de vérification d'identité dans le registre DPP S20.

AVÉRÉ :

> Le cadre réglementaire prévoit donc explicitement la possibilité d'une intégration du registre DPP avec d'autres systèmes d'information de l'Union partageant des mécanismes compatibles de vérification des acteurs S20.

Cette disposition ne permet cependant pas d'affirmer que le registre est actuellement intégré à un système fiscal, bancaire ou de paiement particulier.

L'identification des systèmes concernés et des intégrations effectivement mises en œuvre doit être recherchée séparément.

Journalisation et versionnement

Le registre comprend un système de journalisation des opérations S20.

Les créations, modifications et suppressions de données d'enregistrement doivent être enregistrées et le registre prend en charge le versionnement des données ainsi qu'un horodatage des mises à jour S20.

Le règlement d'exécution prévoit également, lorsqu'aucune autre durée spécifique n'est définie par le droit de l'Union, la suppression automatique de certaines données d'enregistrement du passeport dix ans après leur enregistrement S20.

Il existe donc un mécanisme réglementaire de traçabilité des opérations réalisées dans le registre ainsi que des règles relatives à la durée de conservation de certaines données d'enregistrement.

Un portail public complète les mécanismes d'accès

Le règlement ESPR prévoit également un portail web public permettant aux parties prenantes de rechercher et de comparer certaines données contenues dans les passeports numériques de produits S15.

Les informations accessibles restent déterminées par les droits attribués aux différentes catégories d'acteurs S15.

L'existence de ce portail montre que certaines informations du système sont destinées à être consultables au-delà des seuls opérateurs économiques ou autorités publiques.

Une limite importante concernant les données personnelles des clients

Le règlement ESPR contient également une garantie importante pour l'analyse menée dans ce dépôt.

Les données personnelles relatives aux clients ne doivent pas être stockées dans le passeport numérique de produit sans leur consentement explicite, conformément aux règles européennes de protection des données S15.

AVÉRÉ :

> Le DPP n'est donc pas conçu, dans son cadre réglementaire actuel, comme un fichier contenant automatiquement l'identité de chaque acheteur d'un produit S15.

Cette restriction n'empêche pas qu'un produit puisse être identifié dans un autre système, par exemple un document commercial, mais un tel rapprochement constitue une opération distincte qui ne peut être déduite de la seule existence du DPP.

Conclusion intermédiaire

AVÉRÉ :

> Le système DPP repose sur une architecture décentralisée dans laquelle des informations détaillées peuvent être hébergées par les opérateurs économiques ou des prestataires spécialisés, tandis qu'un registre européen assure notamment l'enregistrement et l'indexation des passeports S15-S20.

AVÉRÉ :

> Le registre dispose d'une API, de mécanismes d'identification et d'autorisation, d'un référentiel sémantique, d'un système de journalisation et de mécanismes permettant des échanges automatisés avec les systèmes informatiques des acteurs S20.

AVÉRÉ :

> Le règlement d'exécution envisage explicitement l'intégration du registre avec d'autres systèmes d'information de l'Union disposant de mécanismes équivalents ou identiques de vérification d'identité S20.

AVÉRÉ :

> Les données personnelles relatives aux clients ne doivent pas être stockées dans le passeport numérique de produit sans leur consentement explicite S15.

À ÉTABLIR :

> Avec quels autres systèmes d'information de l'Union le registre DPP est-il actuellement intégré ou son intégration est-elle prévue, expérimentée ou étudiée ?

À ÉTABLIR :

> Quels systèmes exploités par des opérateurs économiques, prestataires DPP, plateformes commerciales, acteurs financiers ou autres intermédiaires utilisent les API et identifiants du DPP conjointement avec des données de commande, de facturation ou de paiement ?

3.6 Lien éventuel avec les données de transaction

Statut : AVÉRÉ / DÉDUCTIBLE TECHNIQUEMENT / À ÉTABLIR

Les sections précédentes ont établi que le passeport numérique de produit peut associer des informations environnementales structurées à un produit identifiable et que certains standards commerciaux permettent également d'identifier les produits au niveau des documents décrivant une transaction S15-S17.

La question est désormais de déterminer si ces deux catégories de données restent strictement séparées ou si des infrastructures, projets ou expérimentations prévoient déjà leur rapprochement.

Les données du DPP sont destinées à circuler dans la chaîne de valeur

Le passeport numérique de produit est conçu pour accompagner la circulation d'informations relatives au produit entre différents acteurs de sa chaîne de valeur S15.

Son architecture repose sur des identifiants structurés, des formats interopérables et des interfaces permettant des échanges automatisés entre systèmes S15-S20.

Cette circulation ne signifie pas qu'une donnée de transaction ou de paiement est automatiquement inscrite dans le DPP.

Elle permet cependant à différents systèmes de retrouver les informations associées à un produit lorsqu'ils disposent des identifiants et des droits d'accès nécessaires.

Des projets européens associent déjà traçabilité et preuve de transaction

Le projet européen e-Origin constitue un exemple concret dans lequel des informations relatives à une transaction commerciale sont échangées entre plusieurs catégories d'acteurs publics et privés S21.

Le pilote réunit notamment des administrations chargées de la TVA, des marketplaces, des vendeurs en ligne, des courtiers en douane et des autorités douanières S21.

L'infrastructure permet notamment aux vendeurs et marketplaces de stocker et partager une preuve de transaction commerciale et aux autorités douanières de reconnaître cette preuve afin de faciliter certaines opérations de dédouanement S21.

Le projet prévoit également des mécanismes permettant le partage sécurisé des informations tout en maintenant un contrôle sur les données sensibles et confidentielles S21.

Il est donc établi que des travaux européens portent déjà sur des infrastructures permettant à plusieurs catégories d'acteurs économiques et administratifs d'échanger des preuves numériques relatives à des transactions commerciales.

Le Digital Product Passport apparaît dans la même trajectoire de traçabilité

La documentation européenne relative à e-Origin indique également que le projet EBSI-ELSA vise à développer des capacités de traçabilité en utilisant le Digital Product Passport S21.

AVÉRÉ :

> Un même environnement européen de développement associe donc des travaux relatifs à la preuve numérique de transactions commerciales, des acteurs chargés de la TVA et des douanes, ainsi que le développement de capacités de traçabilité reposant sur le Digital Product Passport S21.

Cet élément constitue un rapprochement documentaire plus concret que la seule comparaison de deux architectures techniques.

Il ne permet cependant pas d'affirmer que les données environnementales contenues dans un DPP sont actuellement rattachées aux données fiscales d'une transaction ou transmises à une administration chargée de la TVA.

Un rapprochement peut également reposer sur l'identifiant du produit

Comme établi dans la section 3.3, le DPP peut comporter un GTIN ou un identifiant équivalent S15.

Les standards commerciaux électroniques permettent également de transporter des identifiants standardisés d'articles dans différents documents de la chaîne commerciale S17.

DÉDUCTIBLE TECHNIQUEMENT :

> Lorsqu'une preuve de transaction ou un document commercial contient un identifiant permettant de retrouver le produit correspondant dans un système DPP, il devient techniquement possible d'associer les informations décrivant la transaction aux informations environnementales accessibles pour ce produit.

Cette opération peut être réalisée sans que les informations relatives à l'acheteur soient nécessairement enregistrées dans le passeport numérique lui-même.

Un système disposant séparément de l'identité d'une partie à la transaction et de l'identifiant du produit peut techniquement effectuer le rapprochement entre les deux ensembles de données.

L'utilisation du DPP au-delà de la première mise sur le marché est déjà expérimentée

Des projets européens utilisent déjà le DPP comme support de traçabilité au cours du cycle de vie du produit S40.

Le projet européen CE-RISE développe et expérimente notamment l'utilisation du DPP afin de permettre la traçabilité des matériaux et d'évaluer les possibilités de réemploi, de réparation, de reconditionnement et de recyclage des produits S40.

Le projet européen QUASAR fournit un autre exemple concret : le DPP y est utilisé pour contribuer au suivi de panneaux photovoltaïques en fin de vie et à l'orientation vers des opérations de réemploi, de réparation ou de recyclage, tandis que des solutions de seconde vie sont également expérimentées S41.

Ces exemples établissent que l'utilisation du DPP est expérimentée au-delà de la seule première mise sur le marché et peut accompagner différentes étapes du cycle de vie d'un produit.

Ils ne démontrent cependant pas que les événements associés au cycle de vie du produit constituent systématiquement des transactions commerciales, que ces transactions sont centralisées par une administration fiscale ou qu'elles sont rattachées à l'identité permanente de leurs utilisateurs.

Une frontière importante : transaction, paiement et identité ne sont pas équivalents

Une donnée de transaction peut permettre d'établir qu'un échange commercial a eu lieu.

Une donnée de paiement décrit le règlement financier correspondant.

Une donnée d'identité permet d'identifier une personne physique ou morale.

Enfin, le DPP permet d'identifier et de documenter le produit.

Ces quatre catégories d'informations doivent être distinguées.

La possibilité technique de les rapprocher ne signifie pas qu'elles sont aujourd'hui réunies dans une base unique ni qu'un acteur déterminé dispose nécessairement de l'ensemble de ces informations.

Ce qui est désormais établi

Les éléments étudiés permettent néanmoins de dépasser l'hypothèse selon laquelle le DPP serait nécessairement isolé des infrastructures utilisées pour les échanges commerciaux.

Le DPP repose sur des identifiants et des mécanismes d'interopérabilité S15-S20.

Les standards commerciaux permettent également l'utilisation d'identifiants structurés de produits S17.

Enfin, des travaux européens associent déjà, dans un même environnement de développement, preuve numérique de transaction commerciale, acteurs administratifs chargés notamment de la TVA et des douanes, partage sécurisé de données et développement de capacités de traçabilité utilisant le DPP S21.

Conclusion intermédiaire

AVÉRÉ :

> Des projets européens développent des infrastructures permettant de stocker et partager des preuves numériques de transactions commerciales entre vendeurs, marketplaces et autorités publiques S21.

AVÉRÉ :

> Le projet e-Origin réunit notamment des acteurs chargés de la TVA et des douanes, tandis que les développements associés à EBSI-ELSA prévoient l'utilisation du Digital Product Passport pour renforcer les capacités de traçabilité S21.

DÉDUCTIBLE TECHNIQUEMENT :

> Lorsqu'un système de transaction et un système DPP disposent d'un identifiant commun permettant d'identifier le même produit, les données économiques de la transaction peuvent techniquement être rapprochées des données environnementales associées à ce produit.

À ÉTABLIR :

> Existe-t-il actuellement un dispositif dans lequel les données environnementales contenues ou référencées par un Digital Product Passport sont effectivement associées à une facture électronique, à une déclaration fiscale ou à une donnée de paiement ?

À ÉTABLIR :

> Des projets européens prévoient-ils à terme une interopérabilité directe entre les infrastructures DPP, les systèmes de facturation électronique, les systèmes fiscaux ou les infrastructures de paiement ?

3.7 Ce qui est techniquement déductible

Statut : DÉDUCTIBLE TECHNIQUEMENT

Les sections précédentes ont établi séparément plusieurs caractéristiques du passeport numérique de produit et des infrastructures numériques utilisées dans les échanges commerciaux.

Il est désormais possible d'examiner ce que leur combinaison rend techniquement possible, sans confondre cette possibilité avec l'existence effective d'un traitement ou d'une interconnexion.

Associer une donnée environnementale à un produit identifiable

Le passeport numérique de produit repose sur un identifiant unique et persistant et peut, selon les exigences applicables, être défini au niveau du modèle, du lot ou de l'article individuel S15.

Il peut contenir ou permettre d'accéder à des informations environnementales structurées relatives au produit, notamment son empreinte carbone ou environnementale lorsque les règles applicables le prévoient S15-S16.

Des méthodologies européennes permettent par ailleurs de calculer quantitativement certains impacts environnementaux des produits S18, et le règlement relatif aux batteries fournit déjà un exemple concret d'empreinte carbone réglementaire associée à certaines catégories de produits S19.

DÉDUCTIBLE TECHNIQUEMENT :

> Un système disposant de l'identifiant d'un produit et d'un accès aux données correspondantes peut techniquement retrouver les caractéristiques environnementales associées à ce produit.

Associer un produit à une transaction commerciale

Les standards utilisés dans les échanges commerciaux électroniques permettent de transporter des identifiants structurés de produits dans différents documents commerciaux S17.

Le DPP peut également comporter des identifiants commerciaux standardisés, notamment un GTIN ou un identifiant équivalent S15.

Lorsqu'un même identifiant ou un mécanisme de correspondance permet de désigner le produit dans les deux systèmes, celui-ci peut constituer une clé de rapprochement.

DÉDUCTIBLE TECHNIQUEMENT :

> Un système disposant d'un identifiant produit présent dans un document commercial peut techniquement rechercher les informations correspondant au même produit dans une infrastructure DPP.

Cette possibilité ne signifie pas que cet identifiant soit obligatoirement renseigné dans chaque facture ni transmis à l'administration fiscale.

Associer une caractéristique environnementale à une transaction

La combinaison des deux mécanismes précédents permet d'identifier une possibilité supplémentaire.

Si un produit présent dans une transaction peut être identifié et si une information environnementale peut être retrouvée à partir de cet identifiant, un système disposant des données et droits d'accès nécessaires peut techniquement associer la caractéristique environnementale du produit à la transaction correspondante.

Le rapprochement peut être représenté de manière simplifiée ainsi :

```
Transaction commerciale
   ↓
Identifiant du produit
   ↓
Correspondance avec le produit
   ↓
Passeport numérique de produit
   ↓
Données environnementales
```

DÉDUCTIBLE TECHNIQUEMENT :

> L'association d'une donnée environnementale de produit à une transaction commerciale ne nécessite pas nécessairement que la donnée environnementale soit directement inscrite dans la facture : un identifiant commun ou une table de correspondance peut permettre de retrouver cette information dans un système distinct.

L'identité de l'acheteur constitue une étape supplémentaire

Le règlement ESPR prévoit que les données personnelles relatives aux clients ne doivent pas être stockées dans le passeport numérique de produit sans leur consentement explicite S15.

Le DPP ne constitue donc pas, dans son cadre actuel, une base attribuant automatiquement chaque produit à son acheteur.

Cela n'empêche cependant pas qu'un autre système puisse disposer séparément d'informations relatives aux parties participant à une transaction.

DÉDUCTIBLE TECHNIQUEMENT :

> Si un système distinct dispose à la fois d'informations permettant d'identifier une partie à une transaction et de l'identifiant du produit concerné, l'identité n'a pas besoin d'être stockée dans le DPP pour qu'une correspondance technique entre la transaction et les informations du produit puisse être établie.

Cette possibilité technique ne démontre ni l'existence ni la légalité d'un tel traitement.

De transactions successives à un ensemble d'informations environnementales

Lorsqu'un système contient plusieurs transactions auxquelles peuvent être associés des produits identifiables, le même mécanisme de rapprochement peut techniquement être répété.

Il devient alors possible, sur le seul plan informatique, d'associer à plusieurs transactions les caractéristiques environnementales correspondantes des produits concernés.

Si ces caractéristiques comportent des valeurs quantitatives compatibles, des opérations statistiques ou d'agrégation peuvent techniquement être réalisées sur ces valeurs.

DÉDUCTIBLE TECHNIQUEMENT :

> À partir d'un ensemble de transactions comportant des produits identifiables et de données environnementales quantitatives accessibles pour ces produits, un système disposant des informations et droits nécessaires peut techniquement calculer des agrégats environnementaux correspondant à cet ensemble de transactions.

Cette déduction est importante mais doit être strictement limitée à sa portée technique.

Elle ne démontre pas qu'une empreinte carbone individuelle des achats est actuellement calculée, qu'un acteur public dispose de toutes les données nécessaires, qu'un tel traitement possède une base juridique ou qu'un dispositif de restriction des achats existe.

Les infrastructures sont conçues pour permettre des échanges automatisés

Le DPP utilise des données structurées, lisibles par machine et transférables dans un environnement interopérable S15.

Son registre et son architecture permettent également des échanges automatisés entre systèmes S20.

Une interconnexion automatisée avec les systèmes douaniers est explicitement prévue par le règlement ESPR S15.

Des projets européens tels qu'e-Origin travaillent par ailleurs sur la circulation de preuves de transactions commerciales entre acteurs économiques et administrations, tandis que les développements associés prévoient des capacités de traçabilité utilisant le DPP S21.

La possibilité de rapprochement décrite dans cette section ne repose donc pas sur l'hypothèse que toutes les informations devraient être réunies manuellement dans une base unique.

Elle repose sur des architectures utilisant des identifiants, des données structurées et des mécanismes d'interopérabilité permettant à des systèmes distincts d'échanger ou de retrouver des informations.

Une chaîne techniquement réalisable, mais non établie comme système existant

Les éléments étudiés permettent de représenter la chaîne technique suivante :

```
Identité ou entreprise
   ↓
Transaction
   ↓
Produit identifiable
   ↓
Identifiant produit
   ↓
Données du DPP
   ↓
Caractéristiques environnementales
   ↓
Valeur environnementale quantitative
   ↓
Agrégation éventuelle
```

Chaque liaison de cette chaîne correspond à une opération informatique réalisable lorsque les systèmes concernés disposent des identifiants, données, droits d'accès et mécanismes d'interopérabilité nécessaires.

Cette représentation ne signifie pas que l'ensemble de cette chaîne existe aujourd'hui dans un système unique ni qu'elle soit mise en œuvre par une administration.

Elle permet uniquement d'identifier précisément les composants et correspondances qui seraient nécessaires pour réaliser un tel traitement.

Ce qui manque encore pour passer de la possibilité à l'usage avéré

Pour établir l'existence effective d'un système reliant automatiquement transactions et données environnementales, il faudrait notamment identifier :

- un acteur disposant effectivement des deux catégories de données ou autorisé à les interroger ;
- un mécanisme concret de rapprochement des identifiants ;
- une infrastructure ou un traitement réalisant cette opération ;
- une finalité déterminée pour ce traitement ;
- une base juridique lorsqu'elle est nécessaire ;
- des documents techniques, réglementaires, contractuels, expérimentaux ou institutionnels attestant de sa mise en œuvre ou de sa préparation.

L'existence simultanée des composants techniques ne suffit donc pas à démontrer l'existence du système complet.

Conclusion intermédiaire

DÉDUCTIBLE TECHNIQUEMENT :

> Les infrastructures et standards étudiés permettent techniquement d'utiliser l'identifiant d'un produit comme point de correspondance entre une transaction commerciale et les informations environnementales associées à ce produit.

DÉDUCTIBLE TECHNIQUEMENT :

> Lorsque plusieurs transactions comportent des produits identifiables auxquels sont associées des valeurs environnementales quantitatives, ces valeurs peuvent techniquement être rapprochées et agrégées par un système disposant des données et droits d'accès nécessaires.

AVÉRÉ :

> Des mécanismes d'interopérabilité et d'échange automatisé font partie de l'architecture réglementaire du DPP, et une interconnexion avec les systèmes douaniers est explicitement organisée S15-S20.

AVÉRÉ :

> Des travaux européens associent déjà preuve numérique de transaction commerciale, acteurs administratifs chargés notamment de la TVA et des douanes et développement de capacités de traçabilité utilisant le Digital Product Passport S21.

À ÉTABLIR :

> Existe-t-il un acteur, un traitement, un projet ou une infrastructure réalisant ou préparant effectivement l'ensemble ou une partie substantielle de la chaîne permettant d'associer automatiquement des transactions à leurs caractéristiques environnementales ?

À ÉTABLIR :

> Existe-t-il un dispositif permettant d'agréger ces informations à l'échelle d'une entreprise ou d'une personne identifiée, et si oui, pour quelle finalité et sur quelle base juridique ?

3.8 Limites et éléments restant à établir

Statut : À ÉTABLIR

Les éléments étudiés dans ce chapitre établissent l'existence d'une infrastructure européenne permettant d'associer des données numériques structurées à des produits identifiables, ainsi que l'existence de méthodes permettant de quantifier certains de leurs impacts environnementaux S15-S18-S19.

Ils établissent également l'existence de mécanismes d'interopérabilité, d'identifiants standardisés et d'échanges automatisés permettant techniquement à différents systèmes de retrouver ou de rapprocher certaines informations relatives à un même produit S15-S17-S20.

Ces éléments ne permettent cependant pas d'établir que l'ensemble des possibilités techniques identifiées est actuellement mis en œuvre dans un système reliant automatiquement produit, transaction, acheteur et données environnementales.

Produits effectivement concernés par le DPP

Le règlement ESPR établit le cadre général du passeport numérique de produit, mais son application concrète dépend des exigences adoptées pour les différentes catégories de produits S15.

La présence d'un DPP, son niveau de granularité et la nature des informations qu'il contient ne doivent donc pas être considérés comme identiques pour tous les produits commercialisés dans l'Union européenne.

À ÉTABLIR :

> Quelles catégories de produits seront effectivement soumises à un passeport numérique, selon quel calendrier, avec quelles données obligatoires et à quel niveau de granularité : modèle, lot ou article individuel ?

Généralisation de l'empreinte carbone

Le cadre européen permet que l'empreinte carbone ou environnementale fasse partie des informations associées à certains produits S15-S16.

Des méthodologies européennes permettent déjà de calculer quantitativement certains impacts environnementaux S18, et le règlement relatif aux batteries fournit un exemple concret d'application réglementaire S19.

Ces éléments ne permettent cependant pas d'affirmer qu'une empreinte carbone quantitative sera calculée et enregistrée pour chaque produit commercialisé dans l'Union européenne.

À ÉTABLIR :

> Pour quelles catégories de produits une empreinte carbone ou environnementale quantitative deviendra-t-elle obligatoire, selon quelles méthodes et avec quel niveau de précision ?

Présence des identifiants dans les transactions

Le DPP peut comporter des identifiants standardisés de produits et les standards utilisés dans les échanges commerciaux électroniques permettent également de transporter des identifiants d'articles S15-S17.

Cette compatibilité constitue une possibilité technique de rapprochement.

Elle ne permet cependant pas d'affirmer qu'un identifiant commun est effectivement présent dans chaque facture, chaque transaction ou chaque passeport.

À ÉTABLIR :

> Dans quelles situations un identifiant permettant de retrouver directement ou indirectement le DPP d'un produit est-il effectivement conservé dans une commande, une facture électronique, une donnée de transaction ou un autre document commercial ?

Transmission des identifiants à l'administration fiscale

Le chapitre 1 a établi la nature des données réglementaires transmises à l'administration dans le cadre français de la facturation électronique.

Les éléments étudiés ne permettent pas d'établir que l'identifiant DPP, le GTIN ou un autre identifiant permettant de retrouver automatiquement le passeport numérique d'un produit soit systématiquement

transmis à l'administration fiscale.

Cette distinction est essentielle : la présence d'un identifiant dans un format de facture ne signifie pas nécessairement que cet identifiant appartient aux données réglementaires effectivement extraites et transmises à l'administration.

À ÉTABLIR :

> Un identifiant permettant de relier une ligne de facture à un produit disposant d'un DPP est-il transmis, conservé ou accessible dans les systèmes utilisés par les plateformes agréées, le Portail Public de Facturation ou l'administration fiscale ?

Interconnexion effective avec les systèmes de facturation

Les infrastructures DPP disposent de mécanismes d'interopérabilité et d'interfaces permettant des échanges automatisés S15-S20.

Des standards commerciaux permettent parallèlement l'utilisation d'identifiants structurés de produits S17.

Ces éléments rendent techniquement possible un rapprochement dans certaines conditions, mais aucune des sources étudiées ne permet d'établir l'existence d'une interconnexion générale entre le système DPP et l'infrastructure française de facturation électronique.

À ÉTABLIR :

> Existe-t-il un projet, une expérimentation, une spécification, un partenariat ou une infrastructure prévoyant explicitement un échange de données entre les systèmes DPP et les systèmes de facturation électronique ?

Interconnexion avec les systèmes de paiement

Les éléments étudiés dans ce chapitre ne permettent pas d'établir que les données du DPP sont automatiquement transmises à un établissement bancaire, à un prestataire de paiement ou à une infrastructure monétaire lors du règlement d'un achat.

Ils ne permettent pas non plus d'établir qu'une information environnementale associée à un produit intervient actuellement dans l'autorisation, le refus ou les conditions d'exécution d'un paiement.

À ÉTABLIR :

> Existe-t-il des projets, partenariats, expérimentations ou infrastructures reliant effectivement les identifiants ou données environnementales du DPP à des données ou mécanismes de paiement ?

Cette question sera examinée plus précisément dans le chapitre consacré aux paiements et à l'euro numérique.

Identification de l'acheteur

Le règlement ESPR prévoit que les données personnelles relatives aux clients ne doivent pas être stockées dans le passeport numérique de produit sans leur consentement explicite S15.

Le DPP ne constitue donc pas, dans son cadre réglementaire actuel, un registre attribuant automatiquement chaque produit à son acheteur.

Une association avec une personne ou une entreprise pourrait techniquement être réalisée par un système distinct disposant simultanément des informations relatives à la transaction et de l'identifiant du produit.

À ÉTABLIR :

> Existe-t-il des traitements dans lesquels l'identité d'un acheteur, les produits acquis et les données environnementales correspondantes sont effectivement rapprochés de manière automatisée ?

Agrégation environnementale des transactions

La section 3.7 a établi qu'il est techniquement possible, sous certaines conditions, d'associer des valeurs environnementales à plusieurs transactions puis d'effectuer des opérations d'agrégation sur ces valeurs.

Cette possibilité informatique ne démontre pas l'existence d'un dispositif calculant automatiquement une empreinte environnementale cumulée à partir des achats d'une entreprise ou d'une personne.

À ÉTABLIR :

> Existe-t-il un dispositif public ou privé utilisant les identifiants de produits et les données de transaction pour calculer automatiquement des indicateurs environnementaux cumulés correspondant aux achats d'une entreprise ou d'une personne ?

Utilisation de ces données pour une décision ou une restriction

Aucune des sources étudiées dans ce chapitre ne permet d'établir que les informations environnementales associées aux produits sont utilisées pour autoriser, refuser, limiter ou conditionner les achats d'une personne.

L'existence d'une donnée environnementale quantifiée et la possibilité technique de l'associer à une transaction ne suffisent pas à démontrer l'existence d'un mécanisme de décision ou de restriction.

Un tel système nécessiterait des composants supplémentaires, notamment un mécanisme de décision, une infrastructure capable d'agir sur la transaction ou le paiement ainsi qu'un cadre juridique permettant cette utilisation.

À ÉTABLIR :

> Existe-t-il des textes, projets, expérimentations ou infrastructures prévoyant l'utilisation de données environnementales associées aux produits ou aux transactions afin de déclencher automatiquement une décision, une condition ou une restriction ?

Acteurs communs et projets d'interconnexion

Les recherches ont fait apparaître des projets européens associant déjà traçabilité numérique, preuves de transactions commerciales, acteurs économiques et autorités publiques S21.

La présence d'acteurs ou d'infrastructures dans plusieurs dispositifs ne constitue cependant pas, à elle seule, la preuve d'un échange de données entre ces dispositifs.

Les partenariats, consortiums, marchés publics, expérimentations, standards et documentations techniques devront donc continuer à être examinés afin d'identifier d'éventuelles interconnexions concrètes.

À ÉTABLIR :

> Quels acteurs participent simultanément aux infrastructures de facturation, de traçabilité environnementale, de paiement ou d'identité numérique, et quels échanges de données entre ces infrastructures sont effectivement prévus ou réalisés ?

Conclusion intermédiaire

Les éléments restant à établir ne concernent plus seulement l'existence de données environnementales numériques ou la possibilité technique de les associer à des produits identifiables.

Ces éléments sont désormais documentés.

La question centrale devient celle des **liaisons effectivement mises en œuvre entre les infrastructures** : présence et circulation des identifiants, accès aux données, acteurs disposant de plusieurs catégories d'informations, traitements de rapprochement et finalités associées.

AVÉRÉ :

> Des produits peuvent être associés à des données environnementales structurées et quantitatives, des identifiants standardisés peuvent être utilisés dans plusieurs systèmes numériques et l'architecture DPP prévoit des mécanismes d'interopérabilité et d'échange automatisé S15-S17-S18-S19-S20.

DÉDUCTIBLE TECHNIQUEMENT :

> Lorsque les identifiants, données et droits d'accès nécessaires sont disponibles, les caractéristiques environnementales d'un produit peuvent techniquement être rapprochées des informations décrivant une transaction et, dans certaines conditions, agrégées sur plusieurs transactions.

À ÉTABLIR :

> Il reste à déterminer quels rapprochements sont effectivement réalisés ou préparés, par quels acteurs, pour quelles finalités, sur quelles bases juridiques et avec quelles possibilités d'action sur les transactions ou les paiements.

3.9 Ce que ce chapitre permet d'établir

L'analyse des textes réglementaires, des infrastructures techniques et des projets institutionnels étudiés dans ce chapitre permet désormais de distinguer plusieurs niveaux de certitude concernant les données

environnementales associées aux produits et leurs possibilités de rapprochement avec des données commerciales.

Ce qui est avéré

AVÉRÉ :

> L'Union européenne a établi un cadre juridique pour le passeport numérique de produit, reposant sur des données structurées, lisibles par machine, interopérables et associées à des produits numériquement identifiables S15.

AVÉRÉ :

> Selon les exigences applicables au groupe de produits concerné, le passeport numérique peut être défini au niveau du modèle, du lot ou de l'article individuel S15.

AVÉRÉ :

> Les informations susceptibles d'être associées à certains produits comprennent notamment des données relatives à leur composition, leur durabilité, leur réparabilité, leur recyclabilité ainsi qu'à leur empreinte carbone ou environnementale S15-S16.

AVÉRÉ :

> L'Union européenne dispose de méthodes permettant de calculer quantitativement certains impacts environnementaux des produits sur leur cycle de vie S18.

AVÉRÉ :

> Le règlement européen relatif aux batteries fournit déjà un exemple concret dans lequel une empreinte carbone quantitative est réglementairement associée à certaines catégories de produits selon une méthodologie définie S19.

AVÉRÉ :

> Le DPP peut comporter des identifiants commerciaux standardisés, notamment un GTIN ou un identifiant équivalent, tandis que les standards utilisés dans les échanges commerciaux électroniques permettent également de transporter des identifiants standardisés au niveau des articles S15-S17.

AVÉRÉ :

> L'architecture du DPP prévoit des mécanismes d'interopérabilité, des échanges automatisés, une API, des mécanismes d'identification et d'autorisation ainsi qu'un registre européen des passeports numériques de produits S15-S20.

AVÉRÉ :

> Le cadre réglementaire organise déjà une interconnexion automatisée avec les systèmes douaniers et envisage l'intégration du registre DPP avec d'autres systèmes d'information de l'Union disposant de mécanismes compatibles de vérification des acteurs S15-S20.

AVÉRÉ :

> Des travaux européens associent déjà preuve numérique de transaction commerciale, acteurs économiques, administrations chargées notamment de la TVA et des douanes et développement de capacités de traçabilité utilisant le Digital Product Passport S21.

Ce qui est techniquement déductible

Les éléments précédents permettent d'identifier plusieurs opérations techniquement réalisables sans qu'il soit nécessaire de supposer l'existence d'une base de données unique regroupant toutes les informations.

DÉDUCTIBLE TECHNIQUEMENT :

> Lorsqu'un même identifiant standardisé permet d'identifier un produit dans un document commercial et dans l'environnement DPP, cet identifiant peut techniquement servir de clé de rapprochement entre les informations relatives à la transaction et les informations environnementales associées au produit.

DÉDUCTIBLE TECHNIQUEMENT :

> Une donnée environnementale n'a pas besoin d'être directement inscrite dans une facture pour pouvoir être associée à une transaction : un système disposant de l'identifiant du produit et des droits d'accès nécessaires peut techniquement retrouver cette donnée dans un système distinct.

DÉDUCTIBLE TECHNIQUEMENT :

> De la même manière, l'identité de l'acheteur n'a pas besoin d'être stockée dans le DPP pour qu'un rapprochement soit techniquement réalisable si un autre système dispose séparément des informations permettant d'identifier la partie à la transaction et le produit concerné.

DÉDUCTIBLE TECHNIQUEMENT :

> Lorsque plusieurs transactions comportent des produits identifiables auxquels peuvent être associées des valeurs environnementales quantitatives, un système disposant des informations et droits nécessaires peut techniquement rapprocher puis agréger ces valeurs.

La chaîne technique théorique peut ainsi être représentée de manière simplifiée :

```
Acheteur ou entreprise
   ↓
Transaction
   ↓
Produit identifiable
   ↓
Identifiant produit
   ↓
Passeport numérique de produit
   ↓
Donnée environnementale
   ↓
Valeur environnementale quantitative
   ↓
Agrégation éventuelle
```

Cette représentation décrit une possibilité d'architecture et non un système dont l'existence complète aurait été établie.

Ce qui n'est pas établi

Les sources étudiées ne permettent pas d'affirmer :

- qu'un passeport numérique individuel sera créé pour chaque produit commercialisé dans l'Union européenne ;
- qu'une empreinte carbone quantitative sera obligatoire pour tous les produits ;
- qu'un GTIN, un identifiant DPP ou un identifiant équivalent sera systématiquement présent dans chaque facture électronique ;
- que cet identifiant sera systématiquement transmis à l'administration fiscale ;
- que les plateformes agréées ou l'administration fiscale interrogent actuellement les systèmes DPP à partir des informations présentes dans les factures ;
- que les données environnementales des produits sont actuellement rapprochées des données françaises de facturation ou de e-reporting ;
- qu'un établissement bancaire ou un système de paiement reçoit automatiquement les informations environnementales associées aux produits achetés ;
- qu'une empreinte carbone individuelle des achats est actuellement calculée par une administration à partir de ces infrastructures ;
- que des achats peuvent actuellement être autorisés, refusés ou limités en fonction de ces données environnementales.

Ces affirmations nécessiteraient des éléments supplémentaires qui ne figurent pas dans les sources étudiées.

Une garantie importante concernant l'identité des acheteurs

Le règlement ESPR prévoit que les données personnelles relatives aux clients ne doivent pas être stockées dans le passeport numérique de produit sans leur consentement explicite S15.

AVÉRÉ :

> Dans son cadre réglementaire actuel, le DPP ne constitue donc pas automatiquement un registre nominatif des produits détenus ou achetés par chaque personne.

Cette garantie doit être conservée dans l'analyse.

Elle ne répond cependant pas à la question distincte d'un rapprochement éventuellement effectué par un autre système disposant séparément de données d'identité, de transaction et d'identification du produit.

Bilan du chapitre

Le chapitre permet d'établir l'existence de plusieurs composants distincts :

- une identification numérique structurée des produits ;
- une granularité pouvant, selon les règles applicables, atteindre l'article individuel ;
- des données environnementales associables aux produits ;

- des méthodes permettant de quantifier certains impacts environnementaux ;
- des identifiants standardisés utilisables dans les chaînes commerciales ;
- des mécanismes d'interopérabilité et d'échange automatisé ;
- un registre européen des passeports numériques de produits entré en fonctionnement le 20 juillet 2026, accompagné d'un environnement de test S42 ;
- des connexions réglementairement prévues avec certaines infrastructures publiques, notamment douanières ;
- des projets européens rapprochant déjà traçabilité numérique et preuve de transaction commerciale.

Pris séparément, aucun de ces éléments ne démontre l'existence d'un système permettant de suivre automatiquement l'empreinte environnementale des achats d'une personne.

Pris ensemble, ils permettent cependant d'établir que plusieurs composants techniques nécessaires à la réalisation d'un rapprochement entre **produit, transaction et donnée environnementale** existent déjà ou sont prévus dans les infrastructures étudiées.

Conclusion du chapitre :

> **Il est avéré que l'Union européenne développe une infrastructure permettant d'associer des données environnementales structurées et, dans certains cas, quantitatives à des produits numériquement identifiables. Il est également avéré que cette infrastructure est conçue pour être interopérable avec d'autres systèmes numériques et que des projets européens travaillent déjà sur des environnements associant traçabilité et preuves de transactions commerciales S15-S20-S21.**

> **Il est techniquement déductible qu'un identifiant commun ou un mécanisme de correspondance puisse permettre d'associer une transaction à la donnée environnementale du produit concerné et, lorsque plusieurs transactions sont disponibles, d'agréger les valeurs correspondantes.**

> **Il n'est en revanche pas établi, à ce stade, qu'un tel mécanisme soit utilisé par l'administration fiscale pour établir une empreinte environnementale des achats d'une entreprise ou d'une personne, ni qu'il soit relié à un système permettant de conditionner ou de restreindre un paiement.**

Ces dernières questions nécessitent l'étude des infrastructures de paiement, des projets d'interconnexion et des garanties juridiques correspondantes. Elles seront examinées dans les chapitres suivants.

Chapitre 4 — Euro numérique et infrastructures de paiement

> **Navigation :** ← Retour au sommaire

Ce chapitre examine l'architecture envisagée pour l'euro numérique, les acteurs intervenant dans son fonctionnement, les données nécessaires à l'exécution des paiements ainsi que les mécanismes techniques permettant d'automatiser certaines opérations.

L'objectif est notamment de déterminer ce que l'infrastructure de l'euro numérique permettrait techniquement, quelles données pourraient être traitées par les différents acteurs et quelles garanties sont

prévues concernant la programmabilité de la monnaie, la protection des données et les possibilités de conditionnement des paiements.

Une distinction essentielle doit être faite entre :

- la programmabilité de la monnaie elle-même ;
- les paiements conditionnels ;
- l'automatisation de l'exécution d'un paiement ;
- les données utilisées pour vérifier une condition ;
- l'identification du payeur ou du bénéficiaire ;
- l'utilisation éventuelle d'informations provenant d'autres systèmes numériques.

L'existence d'un mécanisme permettant de déclencher automatiquement un paiement lorsqu'une condition est satisfaite ne signifie pas que la monnaie elle-même est programmable.

Sommaire

- 4.1 — Architecture générale de l'euro numérique
- 4.2 — Acteurs et infrastructures de paiement
- 4.3 — Données traitées lors des paiements
- 4.4 — Paiements en ligne et hors ligne
- 4.5 — Monnaie programmable et paiements conditionnels
- 4.6 — Conditions externes et automatisation des paiements
- 4.7 — Identité numérique et infrastructures de paiement
- 4.8 — Limites et garanties prévues
- 4.9 — Ce que ce chapitre permet d'établir

4.1 Architecture générale de l'euro numérique

Statut : AVÉRÉ / PROJET EN COURS

L'euro numérique est un projet de monnaie numérique de banque centrale destiné à compléter les espèces et les autres moyens de paiement existants dans la zone euro S22-S23.

Il ne s'agit pas d'un crypto-actif ou d'une monnaie émise par un établissement privé. Les unités d'euros numériques constitueraient une créance directe sur l'Eurosystème S23.

À la date des sources étudiées, l'euro numérique n'est pas encore émis. Le projet poursuit son développement technique et reste dépendant de l'adoption du cadre législatif européen correspondant S23.

Une infrastructure centrale de règlement

L'architecture technique actuellement envisagée repose sur une plateforme centralisée de règlement exploitée par l'Eurosystème S23.

L'Eurosystème traiterait et vérifierait les règlements ainsi que les avoirs en euros numériques enregistrés dans l'infrastructure S23.

La BCE précise que cette architecture ne repose pas sur une blockchain ou une technologie de registre distribué comme infrastructure fondamentale du système S23.

Elle reprend néanmoins certains principes techniques utilisés dans les systèmes distribués afin d'améliorer notamment la résilience et les performances.

AVÉRÉ :

> L'architecture actuellement envisagée pour l'euro numérique repose sur une infrastructure centrale de règlement contrôlée par l'Eurosystème S23.

Une distribution passant par des intermédiaires

L'existence d'une infrastructure centrale ne signifie pas que les utilisateurs disposeraient directement d'un compte auprès de la BCE pour leurs opérations quotidiennes.

La proposition de règlement prévoit que les services de paiement en euros numériques soient distribués par l'intermédiaire de prestataires de services de paiement S22.

Ces intermédiaires permettraient notamment :

- l'accès et l'utilisation de l'euro numérique ;
- l'initiation et la réception de paiements ;
- la fourniture des instruments permettant d'effectuer ces paiements ;
- la gestion des comptes de paiement en euros numériques ;
- les opérations permettant de charger ou décharger les avoirs correspondants S22.

La BCE indique également qu'un utilisateur pourrait accéder à l'euro numérique au moyen d'un compte mis en place auprès de sa banque ou d'un intermédiaire public S23.

L'architecture distingue donc au moins deux niveaux :

```
Utilisateur
   ↓
Prestataire de services de paiement
   ↓
Infrastructure de l'Eurosystème
   ↓
Règlement en euros numériques
```

Cette séparation entre relation avec l'utilisateur et règlement central deviendra importante pour déterminer quelles données sont accessibles aux différents acteurs.

Une monnaie inscrite au bilan de l'Eurosystème

Les euros numériques détenus par les utilisateurs constitueraient des engagements directs de l'Eurosystème S23.

Cette caractéristique distingue l'euro numérique de la monnaie scripturale habituellement détenue sur un compte bancaire commercial.

Le prestataire de services de paiement assurerait donc la relation avec l'utilisateur et la fourniture du service, tandis que la valeur monétaire correspondante resterait une créance sur la banque centrale.

AVÉRÉ :

> L'intermédiation par une banque ou un prestataire de paiement ne transforme pas l'euro numérique en monnaie bancaire privée : les avoirs correspondants resteraient une créance directe sur l'Eurosystème S23.

Une infrastructure conçue pour fonctionner à grande échelle

La BCE prévoit une architecture répartie entre plusieurs régions géographiques, chacune disposant de plusieurs serveurs, afin d'assurer la continuité du service et la résilience de l'infrastructure S23.

L'objectif est notamment de permettre au système de continuer à fonctionner en cas de défaillance affectant une partie de l'infrastructure.

L'euro numérique est donc envisagé comme une infrastructure européenne de paiement de détail destinée à fonctionner à grande échelle et non comme une expérimentation limitée à quelques acteurs.

Paiements en ligne et hors ligne

L'architecture prévoit deux modalités principales d'utilisation :

- les paiements en ligne ;
- les paiements hors ligne S23.

La possibilité d'effectuer des paiements hors ligne constitue une caractéristique importante du projet.

Dans cette situation, la BCE indique que les détails de la transaction seraient connus uniquement du payeur et du bénéficiaire, afin de fournir un niveau de confidentialité proche de celui des espèces.

Les paiements en ligne utilisent en revanche l'infrastructure de paiement et impliquent les intermédiaires nécessaires à leur exécution.

La distinction entre ces deux modes devra donc être conservée lorsque seront examinées les données accessibles aux différents acteurs.

Une architecture centralisée ne signifie pas une connaissance directe de l'identité par la BCE

La centralisation du règlement ne signifie pas que la BCE disposerait automatiquement de l'identité civile des utilisateurs correspondant à chaque transaction.

La BCE indique que les informations mises à disposition de l'Eurosystème seraient pseudonymisées et qu'elle ne devrait pas être en mesure d'identifier directement l'utilisateur à partir des données de paiement qu'elle reçoit S23.

Les intermédiaires assurant la relation avec l'utilisateur disposeraient en revanche des informations nécessaires au respect de leurs obligations légales.

Cette distinction sera examinée plus précisément dans la section consacrée aux données de paiement.

Une architecture encore en développement

L'euro numérique n'est pas actuellement une monnaie en circulation S23.

La BCE poursuit le développement technique du dispositif et indique viser une préparation permettant une éventuelle première émission en 2029, sous réserve notamment de l'adoption du cadre législatif européen S23.

Les spécifications techniques continuent donc d'évoluer.

Les éléments étudiés dans ce chapitre doivent être compris comme décrivant l'architecture actuellement proposée ou préparée et non comme le fonctionnement définitif d'un système déjà déployé.

Conclusion intermédiaire

AVÉRÉ :

> L'euro numérique est conçu comme une monnaie de banque centrale dont les avoirs constitueraient une créance directe sur l'Eurosystème S22-S23.

AVÉRÉ :

> L'architecture actuellement envisagée repose sur une plateforme centralisée de règlement contrôlée par l'Eurosystème, tandis que la distribution et la relation avec les utilisateurs passent par des prestataires de services de paiement S22-S23.

AVÉRÉ :

> L'infrastructure prévoit des paiements en ligne et hors ligne ainsi que des mécanismes techniques spécifiques destinés à assurer sa résilience S23.

AVÉRÉ :

> La BCE indique que l'Eurosystème ne devrait pas pouvoir identifier directement les utilisateurs à partir des données de paiement auxquelles il aurait accès, tandis que les intermédiaires conserveraient les informations nécessaires à leurs obligations légales S23.

À ÉTABLIR :

> Quelles données exactes circulent entre l'utilisateur, son prestataire de services de paiement et l'infrastructure centrale lors des différents types de transactions ?

À ÉTABLIR :

> Quels composants techniques disposent des informations permettant d'initier, vérifier, autoriser, régler ou éventuellement conditionner l'exécution d'un paiement ?

4.2 Acteurs et infrastructures de paiement

Statut : AVÉRÉ / PROJET EN COURS

L'architecture envisagée pour l'euro numérique ne repose pas sur une relation directe unique entre l'utilisateur et la Banque centrale européenne.

Elle fait intervenir plusieurs catégories d'acteurs assurant des fonctions distinctes dans l'accès au service, l'initiation des paiements, leur acceptation, leur contrôle et leur règlement S22-S24.

Cette répartition des fonctions est importante pour déterminer quelles informations sont accessibles à chaque acteur et à quel moment d'une transaction.

L'Eurosystème

L'Eurosystème constitue le niveau central de l'infrastructure.

Comme établi dans la section précédente, l'architecture actuellement envisagée prévoit une plateforme centrale permettant notamment le traitement et le règlement des opérations en euros numériques S23.

L'Eurosystème définit également les règles et spécifications communes nécessaires au fonctionnement du dispositif.

Le rulebook de l'euro numérique décrit notamment :

- les acteurs participant au dispositif ;
- les différents cas d'utilisation ;
- les flux de paiement de bout en bout ;
- les interfaces entre les différents composants ;
- les exigences techniques applicables aux prestataires de services de paiement ;
- les mécanismes de gestion des données ;
- les échanges de données ;
- les mécanismes de gestion du risque et de la fraude ;
- le règlement des transactions S24.

AVÉRÉ :

> L'Eurosystème ne constitue donc pas uniquement l'émetteur de la monnaie : il fournit également l'infrastructure centrale et définit les règles techniques communes permettant aux différents acteurs du système d'interagir S23-S24.

Les prestataires de services de paiement

La proposition de règlement prévoit que la distribution de l'euro numérique repose sur des prestataires de services de paiement S22.

Les utilisateurs établissent une relation contractuelle avec ces prestataires et non directement avec la Banque centrale européenne S22.

Les prestataires peuvent notamment permettre aux utilisateurs :

- d'accéder à l'euro numérique ;
- d'initier et recevoir des paiements ;
- de disposer d'instruments de paiement en euros numériques ;
- de gérer leur compte de paiement en euros numériques ;
- d'effectuer les opérations de chargement et de déchargement prévues par le dispositif S22.

Les prestataires de services de paiement constituent donc une couche d'intermédiation entre l'utilisateur et l'infrastructure centrale.

Le prestataire du payeur

Dans une transaction, le prestataire assurant la relation avec le payeur intervient dans l'initiation et le traitement du paiement S24.

Il constitue notamment le point de contact entre l'utilisateur, son instrument de paiement et les services nécessaires à l'exécution de l'opération.

La documentation technique du dispositif distingue explicitement les fonctions et exigences applicables aux prestataires distribuant l'euro numérique S24.

Ces prestataires doivent notamment interagir avec les services centraux nécessaires à l'accès au système, à la gestion de la liquidité et au traitement des transactions.

Ils restent également soumis aux obligations légales applicables aux prestataires de services de paiement.

Cette position est importante pour l'analyse des données : contrairement à l'Eurosystème, qui doit recevoir des informations pseudonymisées dans certaines situations, le prestataire assurant la relation avec l'utilisateur dispose des informations nécessaires pour fournir le service et satisfaire à ses obligations réglementaires.

Le prestataire du bénéficiaire

Une transaction commerciale peut également faire intervenir un prestataire situé du côté du bénéficiaire du paiement.

Le rulebook distingue ainsi les prestataires distribuant l'euro numérique des prestataires assurant les fonctions d'acquisition nécessaires à l'acceptation des paiements S24.

Dans une transaction commerciale, le prestataire acquéreur permet notamment l'interaction entre le dispositif d'acceptation du commerçant et l'infrastructure nécessaire au traitement du paiement.

L'architecture peut donc être représentée de manière simplifiée ainsi :

```
Payeur
   ↓
PSP du payeur
   ↓
Infrastructure de l'euro numérique
   ↓
PSP du bénéficiaire / acquéreur
   ↓
Commerçant ou bénéficiaire
```

Ce schéma est volontairement simplifié : les flux techniques peuvent faire intervenir plusieurs services communs supplémentaires.

Les dispositifs d'acceptation

L'infrastructure ne se limite pas aux banques et à l'Eurosystème.

Le rulebook prévoit également des spécifications relatives aux dispositifs permettant d'accepter les paiements en euros numériques S24.

Ces dispositifs peuvent notamment intervenir dans les paiements effectués auprès d'un commerçant.

Ils constituent le point technique où les informations nécessaires à la transaction sont présentées, échangées ou capturées avant leur transmission aux autres composants du système.

Le dispositif d'acceptation doit donc être distingué du système central de règlement : il intervient à proximité de l'acte commercial tandis que le règlement monétaire est réalisé dans une autre couche de l'infrastructure.

Des services communs entre les différents acteurs

Le rulebook prévoit également une catégorie de services communs utilisables par différents participants au dispositif S24.

Les spécifications techniques publiées par la BCE couvrent notamment :

- la gestion des accès ;
- la recherche et la résolution d'alias ;
- la gestion de la liquidité ;
- le traitement des paiements ;
- la gestion du risque et de la fraude ;
- les échanges de données ;
- le règlement des transactions S24.

L'existence de ces services montre que l'exécution d'un paiement ne correspond pas simplement à un transfert direct entre deux portefeuilles.

Elle implique plusieurs fonctions techniques pouvant intervenir successivement ou simultanément dans le traitement d'une opération.

Contrôle du risque, de la fraude et respect des obligations légales

Les prestataires de services de paiement restent responsables des contrôles qui leur sont imposés par la réglementation applicable.

La documentation technique du projet prévoit notamment des mécanismes relatifs à la gestion du risque et de la fraude S24.

Les versions du rulebook préparant l'architecture indiquent également que le prestataire du payeur doit effectuer, avant l'exécution finale d'une transaction, les contrôles légalement requis en matière de fraude, de lutte contre le blanchiment et le financement du terrorisme ainsi que, lorsque cela est applicable, les contrôles relatifs aux sanctions et embargos.

Le prestataire conserve la responsabilité de l'exécution ou de la non-exécution de la transaction conformément au cadre juridique applicable.

AVÉRÉ :

> L'exécution d'un paiement en euros numériques n'est donc pas conçue comme une opération techniquement aveugle : des contrôles réglementaires et des mécanismes de gestion du risque et de la fraude interviennent dans le traitement des transactions S24.

Ces contrôles correspondent à des obligations juridiques existantes et ne constituent pas, en eux-mêmes, une possibilité générale de conditionner les paiements selon n'importe quel critère.

Plusieurs acteurs peuvent donc intervenir sur une même transaction

L'architecture permet de distinguer plusieurs fonctions :

```
Utilisateur
   ↓
Instrument ou interface de paiement
   ↓
PSP distributeur / PSP du payeur
   ↓
Services communs
   ↓
Infrastructure centrale
   ↓
PSP acquéreur / PSP du bénéficiaire
   ↓
Dispositif d'acceptation
   ↓
Bénéficiaire
```

Tous ces acteurs ou composants ne disposent pas nécessairement des mêmes informations.

La connaissance de l'identité du payeur, du bénéficiaire, du montant, de l'instrument utilisé, du contexte commercial ou des informations techniques nécessaires au règlement peut être répartie entre plusieurs composants.

Il est donc nécessaire de distinguer l'existence globale d'une information dans la chaîne de paiement de son accessibilité effective par un acteur déterminé.

Une distinction essentielle entre connaissance et capacité d'action

La présence d'un acteur dans le traitement d'une transaction ne signifie pas automatiquement qu'il dispose de toutes les données relatives à cette transaction.

Inversement, un acteur n'a pas nécessairement besoin de connaître l'ensemble du contexte commercial pour effectuer une opération technique telle qu'une authentification, un contrôle, une autorisation ou un règlement.

Cette distinction sera particulièrement importante lorsque seront étudiés les paiements conditionnels.

Un système peut en effet recevoir le résultat d'une vérification externe sans nécessairement recevoir toutes les données ayant permis de produire ce résultat.

Une architecture de ce type peut être représentée ainsi :

```
Système externe
   ↓
Résultat d'une condition
   ↓
Composant de paiement
   ↓
Exécution ou absence d'exécution
```

Cette représentation décrit uniquement un principe d'architecture informatique. Elle ne signifie pas qu'un système externe utilisant des données environnementales, fiscales ou individuelles soit actuellement relié à l'euro numérique.

Conclusion intermédiaire

AVÉRÉ :

> L'architecture envisagée pour l'euro numérique répartit les fonctions entre plusieurs catégories d'acteurs et de composants, notamment l'Eurosystème, les prestataires de services de paiement, les prestataires intervenant du côté du payeur ou du bénéficiaire, les dispositifs d'acceptation et différents services communs S22-S24.

AVÉRÉ :

> Le rulebook prévoit des spécifications techniques distinctes concernant notamment les flux de bout en bout, les prestataires distributeurs et acquéreurs, les dispositifs d'acceptation, la gestion des données, les échanges de données, le risque et la fraude ainsi que le règlement S24.

AVÉRÉ :

> Des contrôles réglementaires et des mécanismes de gestion du risque et de la fraude peuvent intervenir avant l'exécution finale d'une transaction, conformément aux obligations applicables aux prestataires de services de paiement S24.

DÉDUCTIBLE TECHNIQUEMENT :

> La répartition des fonctions entre plusieurs composants permet qu'une décision ou une vérification nécessaire au traitement d'un paiement soit produite dans un système distinct puis communiquée au composant chargé de poursuivre ou non l'opération, sans que celui-ci ait nécessairement accès à l'ensemble des données ayant produit cette décision.

À ÉTABLIR :

> Quelles données exactes sont accessibles à chacun des acteurs intervenant dans une transaction en euros numériques et lesquelles sont échangées entre leurs différents systèmes ?

À ÉTABLIR :

> Quels services disposent techniquement de la capacité de bloquer, suspendre, différer ou déclencher une transaction, dans quelles situations et selon quelles règles ?

À ÉTABLIR :

> Des informations provenant de systèmes externes au paiement peuvent-elles être utilisées par certains composants de cette architecture pour déterminer l'exécution d'une opération, et si oui, dans quels cas ?

4.3 Données traitées lors des paiements

Statut : AVÉRÉ / PROJET EN COURS

La documentation technique publiée pour le projet d'euro numérique permet d'aller au-delà d'une description générale de l'architecture et d'examiner les catégories de données prévues pour assurer son fonctionnement S24-S25.

Le rulebook v0.91 comporte notamment un modèle de données, un dictionnaire de données ainsi que des spécifications consacrées aux échanges de données entre les différents composants du système S25.

Ces documents constituent encore des spécifications provisoires et non contraignantes. Ils décrivent néanmoins de manière détaillée les informations actuellement prévues dans la conception du dispositif.

Un modèle structuré des utilisateurs, comptes, appareils et transactions

Le modèle de données distingue plusieurs catégories d'entités nécessaires au fonctionnement de l'euro numérique S25.

Il comprend notamment :

- les utilisateurs ;
- les utilisateurs professionnels ;
- les comptes de paiement en euros numériques ;
- certains comptes de paiement en euros non numériques liés au dispositif ;
- les prestataires de services de paiement ;
- les appareils utilisés ;
- les alias ;
- les points d'interaction avec les commerçants ;
- les transactions ;
- les payeurs ;
- les bénéficiaires ;
- les données relatives aux litiges ;
- les données relatives au risque et à la fraude S25.

Le document précise que ce modèle représente les entités, leurs attributs essentiels et les relations existant entre elles.

Il ne doit cependant pas être interprété comme la représentation complète de toutes les bases de données du système ni comme l'indication que chaque acteur conserve l'intégralité de ces informations.

AVÉRÉ :

> La conception actuelle de l'euro numérique repose sur un modèle de données structuré reliant notamment utilisateurs, comptes, appareils, prestataires de services de paiement et transactions S25.

Des identifiants propres aux utilisateurs et aux comptes

Le modèle prévoit un identifiant unique de l'utilisateur de l'euro numérique ainsi qu'un identifiant du compte de paiement en euros numériques, désigné notamment sous le terme DEAN dans les spécifications S25.

Il prévoit également des alias pseudonymes.

Le rulebook définit l'alias comme un identifiant pseudonyme destiné à protéger l'identité de l'utilisateur lors du traitement des paiements. Selon la spécification, cet alias ne peut être rattaché à une personne physique ou morale identifiable que par le prestataire de services de paiement distribuant l'euro numérique ou par l'utilisateur concerné S25.

L'alias est destiné à constituer un identifiant principal pouvant être partagé dans certaines transactions.

AVÉRÉ :

> L'architecture distingue donc l'identité connue du prestataire de services de paiement de l'identifiant pseudonyme susceptible de circuler dans certains traitements de transaction S25.

Cette séparation constitue une mesure importante de protection de l'identité mais ne signifie pas que l'utilisateur soit anonyme vis-à-vis de son prestataire de services de paiement.

Des données détaillées décrivant la transaction

Le modèle définit une transaction comme la représentation d'un échange financier entre acteurs.

Les exemples mentionnés comprennent notamment les opérations de chargement et de déchargement, les paiements récurrents, les réservations, les paiements, les achats, les retraits et d'autres opérations S25.

Parmi les informations prévues figurent notamment :

- un identifiant de transaction ;
- un identifiant de transaction de bout en bout connu des prestataires concernés ;
- le montant de la transaction ;
- la date et l'heure de création ;
- la direction de la transaction ;
- la devise ;
- des informations complémentaires pouvant être renseignées par l'utilisateur lors de l'initiation ;
- le type de transaction ;
- la méthode d'initiation ;
- le statut de la transaction ;
- l'environnement dans lequel elle intervient S25.

Les types et environnements prévus permettent notamment de distinguer achat, remboursement, réservation, paiement de compte à compte, transaction P2P, commerce électronique, commerce mobile, paiement récurrent ou ordre permanent S25.

AVÉRÉ :

> Une transaction en euros numériques n'est donc pas représentée uniquement par un montant transféré : le modèle technique prévoit plusieurs attributs permettant de l'identifier, de la dater, de la catégoriser et d'en suivre le cycle de traitement S25.

Identification du payeur et du bénéficiaire

Le modèle prévoit des entités distinctes pour le payeur et le bénéficiaire S25.

Le payeur peut être une personne physique, une entreprise, une administration ou une autre autorité publique.

Le bénéficiaire peut également appartenir à ces différentes catégories.

Les spécifications prévoient des identifiants uniques du payeur et du bénéficiaire dans le modèle de données S25.

Cela ne signifie pas que leur identité civile complète soit communiquée à tous les composants du système.

Comme indiqué précédemment, l'architecture prévoit notamment l'utilisation d'alias pseudonymes et une répartition des informations entre les prestataires et l'infrastructure centrale.

AVÉRÉ :

> Le modèle de données permet techniquement de distinguer et d'identifier les parties participant à une transaction, tout en prévoyant des mécanismes destinés à limiter la circulation de leur identité directement identifiable S25.

Les appareils utilisés peuvent également être représentés

Le modèle prévoit des informations relatives aux appareils permettant d'interagir avec le système S25.

Un appareil peut notamment correspondre à une application, une carte ou un accès par navigateur.

Parmi les attributs prévus figurent notamment :

- un identifiant de l'appareil ;
- son type ;
- son adresse IP lorsqu'elle est applicable S25.

Ces informations peuvent notamment intervenir dans les processus techniques, de sécurité ou de gestion du risque.

Leur existence dans le modèle ne signifie pas nécessairement qu'elles sont transmises à tous les acteurs participant au règlement d'une transaction.

Le contexte commercial peut être catégorisé

La documentation prévoit également des données relatives au commerçant et à son activité S25.

Elle utilise notamment le **Merchant Category Code**, ou MCC, fondé sur la classification ISO 18245.

Ce code permet de classer un commerçant selon le type de biens ou de services correspondant à son activité, par exemple les transports, le commerce de détail ou la location de véhicules S25.

Le modèle prévoit également un identifiant du commerçant ainsi que l'identifiant de son compte de paiement en euros numériques.

AVÉRÉ :

> L'architecture actuellement documentée permet donc de connaître, dans certains flux, non seulement le montant et les parties à une transaction mais également une catégorie correspondant à l'activité commerciale du bénéficiaire S25.

Cette donnée ne décrit cependant pas le produit individuel acheté.

Un Merchant Category Code classe l'activité du commerçant ; il ne constitue pas un GTIN, un identifiant DPP ou un identifiant d'article.

Cette distinction est essentielle pour éviter de confondre **catégorie du commerçant** et **contenu détaillé du panier**.

Le Merchant Category Code circule dans la requête de paiement

La documentation va plus loin concernant le MCC.

Elle indique que, parmi les informations relatives au type d'activité du commerçant, **seul le Merchant Category Code est transmis dans la requête de paiement au Digital Euro Service Platform (DESP) et au prestataire de services de paiement distributeur**, et qu'il est transmis sous forme chiffrée S25.

AVÉRÉ :

> Dans l'architecture actuellement documentée, une information catégorisant l'activité du commerçant fait donc partie des données pouvant circuler dans la chaîne technique d'une requête de paiement S25.

Le chiffrement de cette information doit être pris en compte : sa présence dans un message ne signifie pas que chaque composant intermédiaire puisse nécessairement la lire ou l'exploiter.

Il faudra donc distinguer, pour chaque traitement, la circulation technique d'une donnée de sa capacité effective à être déchiffrée et utilisée par un acteur déterminé.

Des informations relatives au point d'interaction et à sa localisation

Le modèle décrit également le point d'interaction, ou POI, où une transaction peut être réalisée S25.

Celui-ci peut correspondre à un emplacement physique, comme un terminal de paiement dans un commerce, ou à un emplacement virtuel, comme une page de paiement en ligne ou une application mobile.

Parmi les informations envisagées figurent notamment :

- un identifiant du point d'interaction ;
- son type ;
- un identifiant de l'entité juridique ;
- un identifiant professionnel local, par exemple un SIRET en France ;
- un identifiant en ligne tel qu'un nom de domaine ou une adresse IP ;
- une adresse physique ;
- une ville ;
- un code postal ;
- un pays S25.

La documentation précise toutefois que plusieurs de ces informations doivent être gérées **en interne par le PSP acquéreur**, notamment à des fins de traçabilité, d'audit, de gestion des capacités d'acceptation et, pour certaines données, de gestion des pré-litiges ou litiges S25.

AVÉRÉ :

> Des informations permettant de caractériser ou localiser un point d'interaction commercial existent dans le modèle, mais la documentation prévoit que plusieurs d'entre elles restent gérées au niveau du PSP acquéreur plutôt que d'être nécessairement transmises à l'ensemble de l'infrastructure S25.

Lien avec un compte bancaire non numérique

Le modèle prévoit également la possibilité de relier un compte de paiement en euros numériques à un compte de paiement non numérique S25.

Pour ce dernier, la documentation mentionne notamment :

- l'IBAN ;
- les dates d'ouverture et de fermeture ;
- le solde ;
- la date correspondant au solde S25.

Cette relation intervient notamment dans les mécanismes permettant d'alimenter ou de désalimenter les avoirs en euros numériques.

AVÉRÉ :

> L'architecture prévoit donc une articulation technique possible entre le compte en euros numériques d'un utilisateur et un compte de paiement bancaire classique utilisé notamment pour les opérations de financement ou de déchargement S25.

Cette articulation ne signifie pas que l'Eurosystème dispose librement de l'ensemble des données du compte bancaire traditionnel : la répartition des données entre PSP et DESP reste déterminante.

Des données de risque et de fraude

Le modèle de paiement comprend également des données relatives à l'évaluation du risque et de la fraude S25.

Il prévoit notamment une entité correspondant à un **fraud and risk score** ainsi qu'un type permettant de classifier ce score.

Ces informations doivent être replacées dans la fonction de prévention et de détection de la fraude prévue par l'architecture de paiement.

AVÉRÉ :

> L'architecture prévoit donc l'utilisation de scores ou indicateurs structurés destinés à l'évaluation du risque et de la fraude dans le traitement des paiements S25.

La présence d'un score de risque ou de fraude ne démontre pas l'existence d'un score social, environnemental ou comportemental général.

Aucune des sources étudiées à ce stade ne permet d'affirmer qu'une donnée environnementale ou un profil environnemental entre dans le calcul de ces scores.

Des données pouvant servir à des rapports, requêtes et analyses

Les spécifications du service d'échange de données prévoient que le DESP puisse fournir aux participants différents rapports et mécanismes de requête S25.

La documentation indique explicitement que ces fonctions doivent répondre à des besoins **opérationnels, analytiques et statistiques** des participants.

Les rapports et requêtes prévus concernent notamment :

- les transactions ;
- les comptes ;
- certaines données de référentiel ;
- les litiges ;
- le calcul de certains frais ;
- la gestion du risque et de la fraude S25.

Certains rapports peuvent être détaillés, d'autres agrégés, et leur accès dépend du rôle du prestataire concerné.

La documentation prévoit par exemple des rapports détaillés de transactions pour les PSP éligibles ainsi qu'un rapport agrégé périodique relatif à la situation en matière de risque de fraude S25.

AVÉRÉ :

> L'infrastructure prévoit donc non seulement le traitement transactionnel immédiat des données mais également des mécanismes structurés permettant à certains participants autorisés d'obtenir des rapports et d'effectuer des requêtes à des fins opérationnelles, analytiques ou statistiques S25.

Cette capacité reste encadrée par les rôles et droits d'accès définis dans le système.

Le modèle distingue les données existantes de leur accessibilité effective

Un point méthodologique est essentiel.

Le modèle de données décrit les informations nécessaires aux différents processus mais précise qu'il ne représente pas l'intégralité d'un système d'information et qu'il ne détermine pas automatiquement les informations déjà gérées dans les systèmes existants S25.

De même, le service d'échange de données prévoit que les rapports et requêtes accessibles à un PSP dépendent de son rôle et des données auxquelles il est éligible.

Il faut donc distinguer trois niveaux :

```
Donnée prévue dans le modèle
   ↓
Donnée effectivement transmise dans un flux déterminé
   ↓
Donnée effectivement accessible et exploitable par un acteur déterminé
```

Ces trois niveaux ne doivent pas être confondus.

Ce que les données de paiement ne permettent pas encore d'établir

Les éléments étudiés permettent de documenter une granularité importante des informations nécessaires au fonctionnement du système.

Ils ne permettent cependant pas d'affirmer que le système de paiement connaît systématiquement le produit individuel acheté.

À ce stade, les données identifiées comprennent notamment le montant, la date et l'heure, les parties, les comptes ou alias nécessaires, le type et l'environnement de la transaction, certains éléments techniques ainsi que la catégorie d'activité du commerçant.

Aucune des sources étudiées dans cette section ne permet d'établir que la requête de paiement contient systématiquement :

- le GTIN du produit acheté ;
- l'identifiant de son passeport numérique de produit ;
- sa désignation détaillée ;
- son empreinte carbone ;
- les différentes lignes composant le panier ;
- les données fiscales détaillées d'une facture électronique.

À ÉTABLIR :

> Des données provenant du système commercial, d'une facture électronique, d'un DPP ou d'un autre système externe peuvent-elles être associées à l'identifiant de transaction ou utilisées par une autre couche de l'infrastructure sans être directement contenues dans le message de paiement ?

Conclusion intermédiaire

AVÉRÉ :

> Le modèle technique actuellement publié pour l'euro numérique prévoit des données structurées relatives aux utilisateurs, comptes, appareils, prestataires, payeurs, bénéficiaires et transactions S25.

AVÉRÉ :

> Les transactions disposent d'identifiants, dont un identifiant de bout en bout, et comportent notamment des informations relatives au montant, à la date et l'heure, au type, à l'environnement et au statut de l'opération S25.

AVÉRÉ :

> L'architecture prévoit des identifiants pseudonymes permettant de limiter la circulation de l'identité directement identifiable de l'utilisateur, tandis que son prestataire de services de paiement conserve la capacité de rattacher certaines informations à son client S25.

AVÉRÉ :

> Le Merchant Category Code permet de catégoriser l'activité commerciale du bénéficiaire et la documentation prévoit sa transmission chiffrée dans la requête de paiement au DESP et au PSP distributeur S25.

AVÉRÉ :

> Le modèle comprend également des informations relatives aux points d'interaction, à certains éléments de localisation, aux appareils et à des scores de risque et de fraude, avec une répartition de leur gestion entre les différents acteurs S25.

AVÉRÉ :

> Le DESP prévoit des rapports et mécanismes de requête destinés à certains PSP selon leurs droits et leurs rôles, notamment pour des besoins opérationnels, analytiques et statistiques S25.

NON ÉTABLI :

> Les sources étudiées ne permettent pas d'affirmer que l'infrastructure de paiement reçoit systématiquement l'identifiant précis du produit acheté, son DPP, son GTIN, son empreinte environnementale ou le détail complet du panier.

À ÉTABLIR :

> Quelles informations supplémentaires peuvent être associées à une transaction par les PSP, commerçants ou systèmes externes grâce aux identifiants de transaction prévus dans l'architecture ?

À ÉTABLIR :

> Quelles données sont effectivement accessibles au DESP, aux PSP distributeurs, aux PSP acquéreurs et aux autres services techniques, sous quelle forme et pendant quelle durée ?

À ÉTABLIR :

> Dans quelles situations les informations décrivant le contexte d'une transaction peuvent-elles participer à une décision automatisée concernant son traitement ?

4.4 Paiements en ligne et hors ligne

Statut : AVÉRÉ / PROJET EN COURS

L'architecture envisagée pour l'euro numérique distingue deux modes de fonctionnement présentant des caractéristiques techniques et des niveaux d'accès aux données différents :

- le paiement en ligne ;
- le paiement hors ligne S23-S26.

Cette distinction est essentielle pour l'analyse des possibilités de traitement des données.

Un paiement en ligne utilise les infrastructures et intermédiaires nécessaires à son traitement et à son règlement.

Un paiement hors ligne est au contraire conçu pour permettre le transfert de valeur sans connexion à Internet et sans intervention en temps réel de l'infrastructure centrale S26.

Le paiement en ligne

Dans le fonctionnement en ligne, les différents composants étudiés dans les sections précédentes interviennent dans le traitement de la transaction.

Selon le type d'opération, cela peut notamment impliquer :

- le prestataire de services de paiement du payeur ;
- le prestataire du bénéficiaire ;
- les services communs du dispositif ;
- le Digital Euro Service Platform ;
- l'infrastructure de règlement de l'Eurosystème S24-S25.

Les données nécessaires au traitement de la transaction peuvent alors circuler entre différents composants selon les règles, rôles et droits d'accès prévus par l'architecture.

Comme établi dans la section 4.3, ces données peuvent notamment comprendre des identifiants de transaction, le montant, la date et l'heure, le type et l'environnement de l'opération, les identifiants pseudonymes nécessaires au traitement ainsi que certaines informations relatives au contexte commercial S25.

La BCE indique toutefois que l'Eurosystème ne devrait pas pouvoir identifier directement le payeur ou le bénéficiaire à partir des informations reçues pour les paiements en ligne S23.

Le lien entre les identifiants pseudonymisés utilisés dans l'infrastructure et l'identité des utilisateurs resterait connu de leurs prestataires de services de paiement conformément aux obligations applicables S23.

AVÉRÉ :

> Le fonctionnement en ligne implique donc une circulation structurée de données nécessaires au paiement, mais l'architecture prévoit une séparation entre les informations directement identifiantes détenues par les PSP et les informations pseudonymisées accessibles à l'Eurosystème S23-S25.

Le paiement hors ligne

Le fonctionnement hors ligne repose sur une architecture différente.

La BCE prévoit qu'un paiement puisse être réalisé directement entre les appareils du payeur et du bénéficiaire sans connexion à Internet au moment de la transaction S26.

Dans les travaux techniques actuellement menés pour le pilote, les paiements hors ligne entre particuliers reposent notamment sur une communication de proximité utilisant le NFC.

La valeur nécessaire au paiement est conservée localement dans un environnement matériel sécurisé de l'appareil.

La BCE étudie notamment l'utilisation :

- d'éléments sécurisés intégrés, ou embedded Secure Elements ;
- d'eSIM ;
- d'autres composants matériels permettant de protéger les valeurs et opérations cryptographiques nécessaires au fonctionnement hors ligne S26.

Ces composants sont destinés à empêcher notamment l'extraction des clés cryptographiques, la modification frauduleuse du solde ou l'altération des opérations réalisées dans l'environnement sécurisé.

Un transfert direct entre appareils

Dans le mode hors ligne, le transfert ne nécessite pas l'intervention d'un système en ligne au moment du paiement S26.

La BCE décrit le mécanisme comme un transfert direct entre deux appareils de valeurs cryptographiquement sécurisées.

Le fonctionnement peut être représenté simplement ainsi :

```
Appareil du payeur
   ↓
Communication locale sécurisée
   ↓
Appareil du bénéficiaire
```

L'infrastructure centrale n'intervient donc pas en temps réel dans le traitement individuel de cette transaction.

AVÉRÉ :

> Un paiement hors ligne en euros numériques est conçu pour pouvoir être exécuté directement entre les appareils du payeur et du bénéficiaire sans transmission de la transaction à un système en ligne au moment du paiement S26.

Les détails de la transaction restent sur les appareils

La différence avec le paiement en ligne est particulièrement importante concernant les données.

La BCE indique que, pour les paiements hors ligne, les informations sensibles relatives à la transaction restent dans l'environnement sécurisé des appareils et ne sont accessibles ni à l'Eurosystème ni aux prestataires de services de paiement S26.

La documentation précise notamment que les informations relatives :

- aux biens achetés ou à l'objet du paiement ;
- au lieu où les biens ont été achetés ;
- au commerçant auprès duquel l'achat a été effectué ou à la personne ayant reçu le paiement,

ne sont pas accessibles à la BCE, aux banques ou aux PSP dans le cadre du paiement hors ligne S26.

AVÉRÉ :

> Dans l'architecture actuellement annoncée, les détails personnels d'un paiement hors ligne sont conçus pour être connus uniquement du payeur et du bénéficiaire S23-S26.

Cette caractéristique constitue une différence majeure avec le fonctionnement en ligne étudié précédemment.

Un niveau de confidentialité comparable aux espèces

La BCE présente explicitement le paiement hors ligne comme devant offrir un niveau de confidentialité comparable à celui des espèces S23-S26.

Le fonctionnement hors ligne empêche l'Eurosystème de relier directement la transaction à une personne.

Mais il va plus loin : contrairement au paiement en ligne, les PSP ne reçoivent pas non plus les détails personnels de la transaction elle-même pendant ou après son exécution S26.

La différence peut être résumée ainsi :

Paiement en ligne

Transaction traitée par l'infrastructure numérique :

- données nécessaires réparties entre plusieurs composants
- PSP capable d'identifier son client
- Eurosystème recevant des informations conçues pour ne pas lui permettre d'identifier directement l'utilisateur

Paiement hors ligne

Transaction exécutée localement entre appareils :

- détails personnels conservés sur les appareils
- PSP ne recevant pas les détails personnels de la transaction
- Eurosystème ne recevant pas les détails personnels de la transaction

Cette distinction constitue une garantie architecturale importante dans l'analyse des possibilités de traçage des paiements.

Les opérations de chargement et de déchargement restent distinctes

Le caractère privé du paiement hors ligne ne signifie cependant pas que l'utilisateur puisse acquérir ou convertir des euros numériques hors ligne sans aucune interaction avec son prestataire.

Les opérations permettant de charger des fonds dans la fonctionnalité hors ligne ou de les reconvertir vers d'autres formes de monnaie nécessitent l'intervention du prestataire de services de paiement S26.

La BCE indique que les contrôles relatifs à la lutte contre le blanchiment sont effectués par le PSP au moment de ces opérations de chargement et de déchargement, selon une logique comparable aux contrôles applicables aux retraits et dépôts d'espèces S23-S26.

Il faut donc distinguer :

Chargement des fonds → interaction avec le PSP
Paiement hors ligne → transfert local entre appareils
Déchargement des fonds → interaction avec le PSP

AVÉRÉ :

> La confidentialité du paiement hors ligne concerne la transaction réalisée entre les utilisateurs ; elle ne supprime pas les interactions réglementées avec le PSP nécessaires à l'entrée et à la sortie des fonds du dispositif hors ligne S23-S26.

Une valeur stockée localement implique des protections techniques spécifiques

La possibilité d'effectuer une transaction sans connexion nécessite que l'appareil puisse conserver et transférer de manière sécurisée la valeur correspondante.

Les travaux actuels de la BCE reposent notamment sur l'utilisation d'un élément matériel sécurisé S26.

Ce composant protège notamment :

- les clés cryptographiques ;
- la valeur disponible ;
- les opérations de débit et de crédit ;
- les informations critiques nécessaires au fonctionnement du mécanisme hors ligne S26.

L'objectif est notamment d'empêcher qu'un utilisateur puisse modifier artificiellement son solde ou reproduire la même valeur pour effectuer plusieurs paiements.

Le mode hors ligne n'est donc pas simplement un mode en ligne temporairement déconnecté : il nécessite une architecture technique spécifiquement conçue pour permettre un transfert de valeur local et sécurisé.

Une protection qui limite également certaines possibilités d'interconnexion

Les garanties du mode hors ligne ont une conséquence importante pour l'objet de cette enquête.

Si les détails d'une transaction restent exclusivement sur les appareils du payeur et du bénéficiaire et ne sont transmis ni au PSP ni à l'Eurosystème, les infrastructures externes ne disposent pas automatiquement des informations nécessaires pour rattacher ce paiement individuel à d'autres bases de données.

DÉDUCTIBLE TECHNIQUEMENT :

> L'architecture hors ligne actuellement décrite constitue donc un obstacle technique à un rapprochement centralisé systématique entre chaque paiement individuel et des informations provenant d'autres infrastructures, puisque les détails personnels de la transaction ne remontent pas dans l'infrastructure centrale.

Cette conclusion doit cependant rester limitée au fonctionnement hors ligne tel qu'il est actuellement conçu.

Elle ne permet pas de conclure que toutes les interactions entourant le paiement sont anonymes, puisque les opérations de chargement et de déchargement impliquent le PSP.

Elle ne permet pas non plus d'affirmer qu'aucune limite d'utilisation, règle de sécurité ou mécanisme antifraude ne puisse être appliqué au dispositif hors ligne.

Ces éléments doivent être examinés séparément.

Une architecture actuellement testée

Le fonctionnement hors ligne ne constitue plus uniquement une hypothèse conceptuelle.

La BCE prépare un pilote de l'euro numérique prévu à partir du second semestre 2027 et poursuit actuellement les travaux nécessaires à la mise en œuvre de la fonctionnalité hors ligne S26.

En août 2026, la BCE a notamment lancé une consultation technique concernant les standards nécessaires au déploiement du mode hors ligne dans les composants matériels sécurisés des smartphones.

Les travaux portent notamment sur les embedded Secure Elements et les eSIM.

AVÉRÉ :

> L'architecture hors ligne fait donc actuellement l'objet de travaux techniques concrets portant sur les composants matériels, les standards de sécurité et la préparation du pilote S26.

Elle reste néanmoins une fonctionnalité d'un projet qui n'est pas encore déployé comme moyen de paiement en circulation générale.

Ce que le mode hors ligne ne permet pas d'affirmer

L'existence d'une fonctionnalité hors ligne ne signifie pas que tous les paiements en euros numériques seront privés de la même manière.

Les paiements en ligne suivent une architecture différente.

Elle ne signifie pas non plus que le mode hors ligne sera nécessairement utilisable sans aucune limite de montant, de détention, de fréquence ou de sécurité.

Enfin, l'absence de remontée des détails personnels d'une transaction hors ligne ne permet pas de déduire que le commerçant ou le bénéficiaire ne dispose lui-même d'aucune information relative à l'achat dans ses propres systèmes commerciaux.

Un commerçant peut disposer séparément :

- d'un ticket de caisse ;
- d'une commande ;
- d'un compte client ;
- d'une facture ;
- d'un identifiant produit ;
- ou d'autres données commerciales.

NON ÉTABLI :

> Les sources étudiées ne permettent donc pas de conclure que le mode hors ligne rend impossible tout rapprochement effectué indépendamment par le commerçant ou par un autre système disposant séparément des données commerciales nécessaires.

Cette distinction est essentielle : la confidentialité du **rail de paiement** ne signifie pas nécessairement l'absence de données dans le **système commercial** situé autour de ce paiement.

Conclusion intermédiaire

AVÉRÉ :

> L'euro numérique est conçu pour permettre des paiements en ligne et hors ligne reposant sur des architectures différentes S23-S26.

AVÉRÉ :

> Le paiement hors ligne doit pouvoir être exécuté directement entre les appareils du payeur et du bénéficiaire sans connexion à Internet et sans intervention d'un système en ligne au moment de la transaction S26.

AVÉRÉ :

> La valeur et les informations sensibles nécessaires au paiement hors ligne doivent être protégées dans un environnement matériel sécurisé de l'appareil S26.

AVÉRÉ :

> Selon l'architecture annoncée par la BCE, les détails personnels des transactions hors ligne ne sont accessibles ni à l'Eurosystème ni aux PSP et restent connus du payeur et du bénéficiaire S23-S26.

AVÉRÉ :

> Les opérations permettant de charger ou décharger les fonds restent en revanche liées au PSP, qui effectue les contrôles réglementaires correspondants S23-S26.

DÉDUCTIBLE TECHNIQUEMENT :

> L'absence de transmission centrale des détails d'un paiement hors ligne limite fortement la possibilité d'effectuer, au niveau de l'infrastructure de paiement, un rapprochement centralisé systématique de cette transaction avec des données fiscales, commerciales ou environnementales externes.

NON ÉTABLI :

> Cette protection ne permet pas de conclure qu'aucun rapprochement ne puisse être réalisé indépendamment dans le système commercial du bénéficiaire lorsque celui-ci dispose de données permettant d'identifier la transaction, le produit ou le client.

À ÉTABLIR :

> Quelles limites de montant, de détention, de fréquence ou de fonctionnement seront finalement appliquées aux paiements hors ligne ?

À ÉTABLIR :

> Quelles informations relatives aux opérations de chargement et de déchargement seront conservées par les PSP et pendant quelle durée ?

À ÉTABLIR :

> Dans quelles conditions les mécanismes de sécurité, de lutte contre la fraude ou de gestion des limites peuvent-ils empêcher ou différer une opération hors ligne ?

À ÉTABLIR :

> Un paiement hors ligne peut-il participer à un mécanisme de paiement conditionnel ou les mécanismes conditionnels nécessitent-ils nécessairement une composante en ligne ?

4.5 Monnaie programmable et paiements conditionnels

Statut : AVÉRÉ / DÉDUCTIBLE TECHNIQUEMENT / PROJET EN COURS

La distinction entre monnaie programmable et paiement conditionnel constitue un élément central de l'architecture envisagée pour l'euro numérique.

La Banque centrale européenne exclut explicitement que l'euro numérique devienne une monnaie programmable S22-S27.

Parallèlement, l'architecture est conçue pour permettre des paiements conditionnels, c'est-à-dire des paiements dont l'exécution peut être déclenchée automatiquement lorsque certaines conditions prédéfinies sont remplies S27.

Ces deux mécanismes ne doivent pas être confondus.

La monnaie programmable est explicitement exclue

La BCE définit la monnaie programmable comme une monnaie dont l'utilisation serait intrinsèquement limitée selon certaines règles.

Une telle monnaie pourrait, par exemple, être conçue pour :

- ne permettre l'achat que de certains biens ou services ;
- ne pouvoir être utilisée que pendant une période déterminée ;
- ne pouvoir être dépensée que dans une zone géographique particulière ;
- ou imposer directement d'autres restrictions d'utilisation attachées aux unités monétaires S27.

La BCE indique explicitement que ce fonctionnement est incompatible avec les principes retenus pour l'euro numérique.

Les unités d'euros numériques doivent rester fongibles et conserver la même valeur que les autres formes de l'euro.

AVÉRÉ :

> L'Eurosystème exclut explicitement que les unités d'euros numériques comportent elles-mêmes des règles limitant les biens, services, périodes, lieux ou bénéficiaires pour lesquels elles peuvent être utilisées S22-S27.

La BCE présente cette garantie comme une différence fondamentale entre une monnaie et un bon ou voucher affecté à un usage déterminé.

Un paiement peut néanmoins être conditionnel

L'exclusion de la monnaie programmable ne signifie pas que tous les paiements doivent être exécutés immédiatement et sans condition.

La BCE définit les paiements conditionnels comme des paiements exécutés automatiquement lorsque des conditions prédéfinies sont remplies S27.

La condition ne modifie pas les propriétés des unités monétaires elles-mêmes.

Elle intervient dans le processus déterminant **quand un paiement déterminé doit être exécuté**.

La distinction peut être résumée ainsi :

Monnaie programmable

La règle est attachée à la monnaie elle-même.
Exemple : cette unité monétaire ne peut servir qu'à acheter une catégorie déterminée de biens.

Paiement conditionnel

La monnaie reste librement utilisable, mais une transaction déterminée n'est exécutée que lorsque la condition convenue pour cette transaction est satisfaite.
Exemple : le paiement d'un produit est libéré lorsque sa livraison est confirmée.

AVÉRÉ :

> La BCE distingue donc explicitement la restriction attachée à la monnaie, qu'elle exclut, de l'automatisation conditionnelle d'une transaction, qu'elle prévoit dans l'architecture de l'euro numérique S27.

La réservation des fonds constitue le mécanisme de base

L'architecture envisagée prévoit une fonctionnalité de réservation des fonds permettant de supporter les paiements conditionnels S27.

Lorsqu'un paiement conditionnel est initié, le montant correspondant peut être temporairement réservé sur le compte du payeur.

Le montant réservé réduit alors le solde disponible pour d'autres dépenses, mais il n'est pas immédiatement transféré au bénéficiaire.

Les fonds restent disponibles pour exécuter le paiement lorsque la condition prévue est satisfaite.

Le mécanisme peut être représenté ainsi :

```
Paiement initié
   ↓
Montant réservé
   ↓
Vérification de la condition
   ↓
Condition satisfaite     → fonds transférés au bénéficiaire
Condition non satisfaite → réservation annulée ou expirée
```

AVÉRÉ :

> L'infrastructure centrale envisagée fournit donc une capacité technique de réservation de fonds permettant de différer leur transfert jusqu'à la vérification d'une condition S27.

Une couche de règlement distincte d'une couche de conditionnalité

Le rapport de clôture de la phase de préparation décrit explicitement une séparation entre deux couches S27.

La première est la **couche de règlement**, située dans l'infrastructure back-end et fournie par l'Eurosystème.

La seconde est une **couche de conditionnalité**, développée par les acteurs du marché.

La couche de règlement assure le traitement monétaire.

La couche de conditionnalité détermine si les conditions prévues pour libérer les fonds sont satisfaites.

Le fonctionnement peut être représenté ainsi :

Couche de conditionnalité — acteurs du marché

```
Vérification d'un événement ou d'une condition
   ↓
Résultat de la vérification
   ↓
Fonction de réservation / infrastructure de paiement
   ↓
Couche de règlement — Eurosystème
   ↓
Transfert ou libération des fonds
```

AVÉRÉ :

> L'architecture actuellement décrite sépare donc techniquement la fonction monétaire de règlement et la logique permettant de déterminer si une condition associée à une transaction est remplie S27.

Cette séparation est essentielle.

Elle signifie que l'Eurosystème n'a pas nécessairement besoin de connaître ou d'évaluer lui-même la donnée ayant servi à vérifier la condition.

Une surveillance externe peut déclencher la condition

Le rapport de clôture de la BCE précise que cette architecture doit permettre une flexibilité pour un **monitoring externe capable de déclencher les conditions** S27.

Dans l'exemple donné par la BCE, un système peut déterminer qu'un train est effectivement arrivé.

Lorsque cette information confirme la condition prévue, les fonds réservés sont transférés au bénéficiaire.

Si le train n'arrive pas ou si la condition définie n'est pas satisfaite, la réservation peut être annulée ou expirer et les fonds redeviennent disponibles pour le payeur S27.

AVÉRÉ :

> Une information produite ou vérifiée en dehors de la couche de règlement peut donc techniquement participer au déclenchement ou à l'absence de déclenchement d'un paiement conditionnel S27.

Il s'agit ici d'un premier lien explicitement documenté entre **une donnée ou un événement externe au règlement monétaire** et **l'exécution d'une transaction**.

Des exemples déjà identifiés et expérimentés

Les travaux de la BCE et des acteurs du marché ont étudié plusieurs catégories de paiements conditionnels S27.

Parmi les exemples documentés figurent notamment :

- le paiement à la livraison ;
- le paiement à l'usage ;
- les paiements déclenchés par étapes ou milestones ;
- les remboursements automatiques ;
- les abonnements ;
- les paiements fractionnés ;
- les paiements machine-to-machine ;
- certains paiements liés à la consommation d'énergie S27.

Dans le cas du paiement à la livraison, la transaction peut être finalisée lorsque la livraison du produit est confirmée.

Dans un paiement machine-to-machine, une machine peut participer automatiquement au déclenchement d'un paiement lorsqu'un événement prévu survient.

La BCE et des acteurs du marché ont déjà testé la faisabilité de plusieurs de ces mécanismes dans un environnement simulant le back-end de l'euro numérique S27.

AVÉRÉ :

> Les paiements conditionnels ne constituent donc plus uniquement une possibilité abstraite décrite dans une proposition réglementaire : leur faisabilité technique a fait l'objet d'expérimentations avec des acteurs du marché dans l'environnement d'innovation de la BCE S27.

Ces expérimentations n'ont cependant pas utilisé de véritables euros numériques et ne constituent pas le déploiement d'un système en production.

La condition peut être vérifiée par un tiers

Les travaux antérieurs de la BCE fournissent également un exemple dans lequel le déclenchement d'un paiement à la livraison peut dépendre d'un tiers autre que le payeur ou le bénéficiaire, comme le service postal chargé de confirmer la livraison d'un produit S27.

Cette architecture introduit donc potentiellement un troisième acteur dans la décision technique permettant de poursuivre le paiement.

```
Payeur + bénéficiaire définissent ou acceptent la condition
   ↓
Tiers ou système externe vérifie l'événement
   ↓
Confirmation de la condition
   ↓
Paiement exécuté automatiquement
```

AVÉRÉ :

> La vérification d'une condition peut donc être réalisée à partir d'une information provenant d'un acteur ou d'un système distinct du payeur, du bénéficiaire et de la couche centrale de règlement S27.

Les acteurs du marché développent la logique conditionnelle

La BCE considère que les intermédiaires supervisés et autres acteurs du marché sont les mieux placés pour développer les services de paiement conditionnel S27.

L'infrastructure de l'euro numérique fournit notamment la fonctionnalité fondamentale de réservation des fonds.

Les acteurs du marché peuvent construire au-dessus de cette infrastructure des services à valeur ajoutée utilisant leurs propres logiques et les informations nécessaires aux cas d'usage concernés.

En juillet 2026, la BCE indiquait également que les banques pourraient utiliser l'infrastructure de l'euro numérique pour déclencher automatiquement des paiements lorsqu'une condition convenue est remplie et développer de nouveaux services en s'appuyant sur les données dont elles disposent S27.

AVÉRÉ :

> La logique conditionnelle n'est donc pas conçue comme une fonction exclusivement définie et opérée par la Banque centrale européenne : des banques, PSP et autres acteurs du marché peuvent développer des services conditionnels au-dessus de l'infrastructure commune S27.

Le premier pont technique avec des données externes

Les sections précédentes ont établi que l'architecture de paiement peut traiter différentes informations relatives aux transactions et que les acteurs du marché disposent de leurs propres systèmes et données.

La présente section ajoute un élément supplémentaire : la couche de conditionnalité peut utiliser la vérification d'un événement externe afin de déterminer si les fonds réservés doivent être transférés S27.

Le mécanisme général devient donc :

```
Donnée ou événement externe
   ↓
Vérification de la condition
   ↓
Couche de conditionnalité
   ↓
Instruction liée aux fonds réservés
   ↓
Exécution ou absence d'exécution du paiement
```

AVÉRÉ :

> Le principe selon lequel une information externe au règlement monétaire peut déclencher l'exécution d'un paiement conditionnel est explicitement prévu dans l'architecture étudiée S27.

Cette constatation constitue un **pont technique entre une information externe et l'exécution d'un paiement**.

Elle ne permet cependant pas de conclure que n'importe quelle information peut être utilisée comme condition.

Ce pont ne démontre pas l'utilisation de données environnementales

Aucune des sources étudiées dans cette section ne prévoit qu'un paiement soit conditionné par :

- l'empreinte carbone d'un produit ;
- un passeport numérique de produit ;
- un GTIN ;
- une empreinte environnementale cumulée ;
- un quota environnemental individuel ;
- une donnée fiscale issue de la facturation électronique ;
- ou un profil comportemental d'un utilisateur.

Les exemples actuellement documentés concernent principalement des événements directement liés à l'exécution d'un contrat ou d'un service : livraison, réalisation d'une prestation, utilisation d'un service, horaire, consommation ou événement vérifiable S27.

NON ÉTABLI :

> L'existence d'une couche de conditionnalité capable d'utiliser des informations externes ne démontre pas qu'elle soit actuellement conçue pour recevoir ou utiliser des données environnementales, fiscales ou des profils individuels.

Cette distinction est fondamentale pour l'analyse.

Mais la nature technique de la condition n'est pas intrinsèquement monétaire

La condition permettant de déclencher le paiement peut correspondre à un événement vérifié par un système distinct.

Le système de règlement n'a pas nécessairement besoin de connaître l'ensemble des informations ayant permis d'établir que cette condition est satisfaite.

DÉDUCTIBLE TECHNIQUEMENT :

> Une architecture de paiement conditionnel peut techniquement utiliser le résultat d'une vérification effectuée par un système externe sans que les données ayant servi à cette vérification soient directement intégrées dans l'infrastructure monétaire.

Par exemple, le système de paiement pourrait recevoir uniquement un résultat logique :

```
Condition vérifiée : OUI
 ou
Condition vérifiée : NON
```

sans recevoir nécessairement toutes les données ayant conduit à ce résultat.

Cette propriété technique signifie qu'une interconnexion n'exige pas nécessairement la fusion complète des bases de données concernées.

Qui décide de la condition constitue une question juridique distincte

La possibilité technique de construire une condition ne signifie pas que n'importe quel acteur puisse imposer arbitrairement cette condition à un utilisateur.

La BCE indique que les paiements conditionnels reposent sur des conditions prédéfinies et convenues et affirme que les utilisateurs restent libres de choisir l'utilisation de ces services S27.

Dans une communication de janvier 2026, la BCE a également précisé que les conditions d'un paiement ne pourraient être fixées que par le payeur et le bénéficiaire.

AVÉRÉ :

> Dans le cadre actuellement présenté par la BCE, les paiements conditionnels constituent des services volontaires reposant sur des conditions convenues entre les parties et ne donnent pas à l'Eurosystème un pouvoir général permettant de déterminer ce qu'un utilisateur peut acheter S27.

Cette garantie doit être distinguée de la capacité technique du système à exécuter automatiquement une transaction lorsque la condition convenue est satisfaite.

La frontière exacte avec une restriction externe doit rester surveillée

La distinction conceptuelle entre monnaie programmable et paiement conditionnel est claire :

- la monnaie programmable impose une restriction à l'unité monétaire elle-même ;
- le paiement conditionnel applique une logique à une transaction déterminée.

Mais du point de vue de l'utilisateur, une condition peut néanmoins avoir pour effet pratique qu'un paiement déterminé ne soit pas exécuté tant que le critère prévu n'est pas satisfait.

Cette observation ne permet pas de qualifier le système de monnaie programmable.

Elle montre seulement que **l'absence de programmabilité de la monnaie n'implique pas l'absence de logique programmable autour de l'exécution des paiements**.

DÉDUCTIBLE TECHNIQUEMENT :

> Une infrastructure peut donc simultanément utiliser une monnaie totalement fongible et non programmable tout en permettant à des services externes d'appliquer des règles automatisées à l'exécution de transactions particulières.

La question déterminante devient alors celle de la gouvernance de ces règles : qui peut définir une condition, avec quel consentement, à partir de quelles données et dans quel cadre juridique ?

Conclusion intermédiaire

AVÉRÉ :

> La BCE exclut explicitement que l'euro numérique soit une monnaie programmable limitant intrinsèquement les biens, services, périodes, lieux ou bénéficiaires pour lesquels les unités monétaires peuvent être utilisées S22-S27.

AVÉRÉ :

> L'architecture prévoit néanmoins des paiements conditionnels exécutés automatiquement lorsque des conditions prédéfinies sont satisfaites S27.

AVÉRÉ :

> Une fonctionnalité de réservation des fonds est prévue afin de conserver temporairement le montant nécessaire jusqu'à la vérification de la condition S27.

AVÉRÉ :

> La BCE décrit une architecture séparant une couche de règlement fournie par l'Eurosystème et une couche de conditionnalité développée par les acteurs du marché, avec la possibilité qu'une vérification externe déclenche la condition S27.

AVÉRÉ :

> Des paiements conditionnels ont déjà été expérimentés dans un environnement simulé avec des acteurs du marché, notamment pour des scénarios de paiement à la livraison, paiement à l'usage, paiements par étapes et autres services automatisés S27.

AVÉRÉ :

> La BCE indique que les banques et autres prestataires pourront développer des services conditionnels au-dessus de l'infrastructure commune et s'appuyer sur les données dont ils disposent pour proposer des services innovants S27.

DÉDUCTIBLE TECHNIQUEMENT :

> Une information provenant d'un système externe peut techniquement participer à l'exécution ou à la non-exécution d'une transaction sans que cette information soit nécessairement stockée dans la monnaie elle-même ni intégralement transmise à la couche de règlement.

NON ÉTABLI :

> Les sources étudiées ne permettent pas d'établir que des données environnementales, des DPP, des données fiscales ou un profil individuel soient utilisés comme conditions de paiement dans l'architecture actuellement prévue.

AVÉRÉ :

> Dans le cadre actuellement présenté par la BCE, les conditions sont conçues comme convenues par les parties et l'Eurosystème affirme ne pas disposer du pouvoir permettant de bloquer des catégories d'achats S27.

À ÉTABLIR :

> Quelles catégories de données externes peuvent techniquement être utilisées par les services développant la couche de conditionnalité ?

À ÉTABLIR :

> Quels acteurs peuvent fournir la preuve ou le résultat permettant de considérer une condition comme satisfaite ?

À ÉTABLIR :

> Quelles garanties juridiques empêchent qu'une condition initialement conçue comme volontaire ou contractuelle soit imposée par un intermédiaire, une réglementation ou un autre acteur ?

À ÉTABLIR :

> Existe-t-il des projets ou expérimentations reliant les paiements conditionnels à des infrastructures de facturation, de traçabilité des produits ou de données environnementales ?

4.6 Conditions externes et automatisation des paiements

Statut : AVÉRÉ / DÉDUCTIBLE TECHNIQUEMENT / À ÉTABLIR

La section précédente a établi que l'architecture envisagée pour l'euro numérique distingue une couche de règlement fournie par l'Eurosystème et une couche de conditionnalité développée par les acteurs du marché S27.

Les travaux menés dans le cadre de la plateforme d'innovation permettent d'aller plus loin : des acteurs du marché ont effectivement connecté leurs propres plateformes à un environnement simulant les interfaces de l'euro numérique afin d'expérimenter des paiements conditionnels S28.

Il devient donc possible de distinguer trois composants :

```
système ou plateforme externe
   ↓
logique permettant de vérifier une condition
   ↓
infrastructure permettant de réserver puis de transférer les fonds
```

Cette architecture a fait l'objet d'expérimentations techniques, même si l'euro numérique lui-même n'est pas encore en circulation S28.

Les plateformes des participants ont été connectées aux interfaces simulées

Dans le cadre du groupe de travail des « pioneers », la BCE a fourni aux participants un environnement simulant le back-end de l'euro numérique ainsi que des spécifications techniques et des interfaces de programmation S28.

Les participants ont pu connecter leurs propres plateformes à cet environnement au moyen d'API.

Ils agissaient, dans l'expérimentation, comme des prestataires développant leurs propres services au-dessus des fonctionnalités centrales fournies par l'Eurosystème.

AVÉRÉ :

> Des plateformes développées ou exploitées par des acteurs du marché ont donc effectivement été connectées, à titre expérimental, à des interfaces simulant l'infrastructure de l'euro numérique S28.

Il ne s'agit pas encore d'une connexion au futur système de production.

Cette expérimentation démontre néanmoins que l'architecture est conçue pour permettre à des systèmes externes développés par les acteurs du marché d'utiliser les fonctionnalités fournies par l'infrastructure commune.

L'Eurosystème fournit la fonction monétaire, le marché développe la condition

La répartition des responsabilités expérimentée reprend la séparation décrite précédemment S27-S28.

L'Eurosystème fournit les fonctions fondamentales nécessaires au traitement monétaire, notamment la réservation des fonds.

Les PSP et autres acteurs du marché développent la couche déterminant les conditions nécessaires à leur libération.

Le mécanisme peut être représenté ainsi :

```
**Infrastructure de l'Eurosystème**
réservation des fonds
   ↓
**Plateforme du PSP ou de l'acteur du marché**
définition et gestion de la condition
   ↓
**Information permettant de vérifier la condition**
   ↓
condition satisfaite
   ↓
instruction permettant la libération des fonds
```

AVÉRÉ :

> Dans les expérimentations réalisées, la logique déterminant la condition n'était donc pas nécessairement située dans l'infrastructure centrale de l'Eurosystème : elle pouvait être développée et gérée par les plateformes des acteurs du marché S28.

La condition peut dépendre d'un événement extérieur au paiement

Plusieurs scénarios étudiés montrent que la condition n'a pas besoin d'être une information produite par le système monétaire lui-même S27-S28.

Dans un paiement à la livraison, l'information déterminante est la confirmation de la livraison du produit.

Dans un remboursement lié à un transport, elle peut être liée à l'exécution, au retard ou à l'annulation du service.

Dans un paiement à l'usage, elle peut dépendre de l'utilisation effective d'un service ou d'un équipement.

Dans un paiement par étapes, elle peut dépendre de la réalisation successive d'objectifs ou de jalons prédéfinis S28.

AVÉRÉ :

> Les conditions étudiées peuvent donc dépendre de faits ou d'événements produits en dehors de l'infrastructure monétaire et vérifiés par la couche conditionnelle développée par les acteurs du marché S27-S28.

Un système externe n'a pas nécessairement besoin de transmettre toutes ses données

La séparation entre couche conditionnelle et couche de règlement permet qu'un système externe effectue lui-même certaines vérifications.

La couche monétaire n'a alors pas nécessairement besoin de recevoir l'ensemble des informations ayant permis d'effectuer cette vérification.

Le mécanisme peut être résumé ainsi :

```
système externe dispose d'une information
   ↓
système externe vérifie une règle
   ↓
résultat : condition satisfaite ou non satisfaite
   ↓
couche conditionnelle traite ce résultat
   ↓
fonds libérés ou maintenus réservés
```

DÉDUCTIBLE TECHNIQUEMENT :

> Une donnée utilisée pour déterminer l'exécution d'un paiement n'a donc pas nécessairement besoin d'être stockée dans l'infrastructure monétaire ni même transmise intégralement à celle-ci : un résultat de vérification peut techniquement suffire.

Cette propriété est importante pour l'étude des interconnexions.

L'absence d'une donnée dans le dictionnaire de données de l'euro numérique ne suffit pas, à elle seule, à démontrer que cette donnée ne puisse jamais participer indirectement à la logique d'un service de paiement développé autour de l'infrastructure.

Les paiements machine-to-machine étendent l'automatisation

Les expérimentations ont également étudié des scénarios liés à l'Industrie 4.0 et aux paiements machine-to-machine S28.

Dans ces scénarios, des équipements ou systèmes numériques peuvent participer automatiquement à l'initiation ou au déclenchement d'opérations financières.

Un exemple étudié concerne une machine détectant elle-même le besoin d'une pièce de remplacement et participant à l'automatisation du processus commercial correspondant.

Ces scénarios cherchent notamment à réduire les interventions manuelles et à permettre des règlements en temps réel ou fondés sur l'utilisation effective d'un service S28.

AVÉRÉ :

> Les travaux d'expérimentation ne se limitent donc pas à des paiements déclenchés manuellement par une personne : ils examinent également des chaînes dans lesquelles des systèmes ou machines peuvent participer automatiquement à l'initiation et au traitement d'une transaction S28.

Cette automatisation ne signifie pas qu'une machine puisse dépenser arbitrairement l'argent d'un utilisateur : elle intervient dans un cadre de service, de mandat, d'autorisation et de conditions préalablement définies.

Des jalons peuvent déterminer progressivement la libération des fonds

Les expérimentations ont étudié des paiements fondés sur des étapes ou « milestones » S28.

Dans ce type de scénario, la totalité des fonds n'est pas nécessairement libérée en une seule fois.

Le versement peut être effectué progressivement lorsque différents objectifs prédéfinis sont considérés comme atteints.

Un exemple étudié concerne une formation en ligne pour laquelle les fonds pourraient être libérés progressivement lorsque l'apprenant atteint certains objectifs.

Un autre exemple concerne le financement participatif, dans lequel des fonds pourraient être libérés selon l'avancement d'un projet S28.

AVÉRÉ :

> Une condition externe peut donc non seulement déterminer si un paiement doit être exécuté, mais également participer à la détermination du moment ou de l'étape à laquelle une partie des fonds doit être libérée S28.

Les paiements à l'usage reposent sur une donnée mesurable

Le paiement à l'usage constitue une autre catégorie étudiée par la plateforme S28.

Dans ce type de mécanisme, le montant ou le moment du paiement dépend de l'utilisation effective d'un bien ou d'un service.

La condition peut donc être alimentée par une information mesurant cette utilisation.

Cela peut concerner notamment des services de mobilité, des infrastructures ou certains équipements connectés.

DÉDUCTIBLE TECHNIQUEMENT :

> Lorsqu'un système externe est capable de mesurer un événement ou une quantité et de communiquer le résultat correspondant à la couche conditionnelle, cette information peut techniquement participer à l'automatisation du paiement.

Il s'agit d'un principe général de fonctionnement des paiements conditionnels et non de la preuve que toute catégorie de donnée puisse être utilisée sans restriction.

L'automatisation peut également concerner les remboursements

Les travaux de la BCE ne portent pas uniquement sur le déclenchement d'un paiement vers un commerçant S27-S28.

Ils examinent également l'automatisation de remboursements lorsque certaines conditions sont satisfaites.

Dans le domaine des transports, par exemple, une annulation ou un retard peut conduire à l'automatisation d'un remboursement.

Le même principe général s'applique :

```
événement externe
   ↓
vérification de la situation
   ↓
déclenchement automatique
   ↓
paiement ou remboursement
```

AVÉRÉ :

> L'utilisation d'une condition externe peut donc agir sur différents flux financiers, notamment la libération d'un paiement ou le déclenchement d'un remboursement S27-S28.

Le paiement peut être associé à des informations commerciales complémentaires

La plateforme d'innovation a également étudié des services complémentaires tels que les reçus électroniques S28.

La BCE présente les e-receipts comme une fonctionnalité susceptible d'être associée aux paiements en euros numériques afin de permettre notamment aux utilisateurs de suivre leurs dépenses et de gérer leurs garanties.

Cette fonctionnalité est distincte du règlement monétaire.

Elle montre cependant que les acteurs du marché envisagent des services dans lesquels une transaction de paiement peut être associée à des informations commerciales supplémentaires.

AVÉRÉ :

> Les travaux de la plateforme d'innovation envisagent donc également l'association d'un paiement en euros numériques avec des informations commerciales extérieures au strict transfert monétaire, notamment au moyen de reçus électroniques S28.

À ÉTABLIR :

> Quelle granularité ces reçus électroniques pourraient-ils contenir et pourraient-ils notamment inclure des références de produits, des lignes d'achat ou des identifiants standardisés ?

Le lien avec le produit devient techniquement concret dans certains scénarios

Le scénario de paiement à la livraison repose déjà sur une relation entre :

- une commande ;
- un produit acheté ;
- une livraison ;
- une transaction ;
- une condition ;
- et la libération des fonds S27-S28.

Le système doit être capable de déterminer que l'événement vérifié correspond à la transaction pour laquelle les fonds ont été réservés.

Il existe donc nécessairement, dans le service développé autour du paiement, un mécanisme permettant de rapprocher la condition vérifiée de la transaction concernée.

AVÉRÉ :

> Les scénarios expérimentés démontrent qu'une plateforme externe peut techniquement associer un événement commercial relatif à une commande ou à un service à la transaction dont l'exécution dépend de cet événement S28.

Cela ne signifie pas que l'infrastructure centrale connaît le détail du produit.

Le rapprochement peut être effectué dans la plateforme externe, qui transmet ensuite uniquement l'information nécessaire à la poursuite du paiement.

Le pont générique entre données externes et paiement est établi

À ce stade, plusieurs éléments peuvent être assemblés.

Le chapitre 4 a établi :

- qu'une transaction possède des identifiants structurés S25 ;
- qu'une architecture de réservation des fonds permet de différer leur transfert S27 ;
- qu'une couche de conditionnalité peut être développée par des acteurs du marché S27-S28 ;
- qu'un monitoring externe peut déclencher une condition S27 ;
- que les plateformes des participants ont effectivement été connectées aux interfaces simulées de l'euro numérique S28 ;
- que des événements commerciaux extérieurs au règlement ont été utilisés dans les scénarios de paiement conditionnel S28.

La chaîne suivante est donc désormais documentée dans son principe :

```
événement ou donnée provenant d'un système externe
   ↓
plateforme ou service de l'acteur du marché
   ↓
vérification d'une condition
   ↓
association avec la transaction correspondante
   ↓
utilisation de la fonctionnalité de réservation des fonds
   ↓
exécution, libération, maintien ou restitution des fonds selon le scénario
```

AVÉRÉ :

> L'architecture et les expérimentations étudiées établissent donc qu'un système externe à la couche de règlement peut fournir ou vérifier une information utilisée par un service conditionnel afin de déterminer l'exécution d'une transaction déterminée S27-S28.

Ce constat dépasse désormais la simple possibilité abstraite d'une architecture informatique : le mécanisme général a fait l'objet d'expérimentations techniques avec des plateformes d'acteurs du marché connectées à un environnement simulant l'euro numérique S28.

Le pont spécifique avec les données environnementales n'est pas établi

Cette conclusion ne doit cependant pas être étendue au-delà de ce que démontrent les sources.

Aucune des expérimentations étudiées ne permet d'établir qu'une condition de paiement a été alimentée par :

- un passeport numérique de produit ;
- un identifiant DPP ;
- un GTIN utilisé pour consulter un DPP ;
- l'empreinte carbone d'un produit ;
- une empreinte environnementale cumulée ;
- une donnée issue du système français de facturation électronique ;
- un profil environnemental individuel.

NON ÉTABLI :

> Le pont générique entre système externe et paiement conditionnel est documenté, mais le pont spécifique entre données environnementales ou fiscales et exécution d'un paiement ne l'est pas à ce stade.

Cette distinction constitue une limite essentielle de l'enquête.

La combinaison avec le chapitre 3 devient néanmoins techniquement analysable

Le chapitre 3 a établi séparément qu'un produit peut être associé à un identifiant numérique et à des données environnementales structurées et que, lorsque des identifiants compatibles existent, ces informations peuvent

techniquement être rapprochées d'une transaction commerciale.

Le présent chapitre établit maintenant qu'une information provenant d'un système externe peut être vérifiée dans une couche de conditionnalité et participer à l'exécution d'un paiement.

Ces deux constats ne démontrent pas leur interconnexion effective.

Ils permettent néanmoins d'identifier précisément le raccord technique qui serait nécessaire :

```
transaction ou commande
   ↓
produit identifiable
   ↓
système externe disposant d'une information relative au produit
   ↓
règle ou condition appliquée dans un service externe
   ↓
résultat de la vérification
   ↓
couche de conditionnalité du paiement
   ↓
exécution ou absence d'exécution selon la condition
```

DÉDUCTIBLE TECHNIQUEMENT :

> Si un acteur autorisé disposait d'une donnée environnementale relative à un produit et si cette donnée était utilisée comme critère d'une condition de paiement, l'architecture décrite pour les paiements conditionnels permettrait techniquement que le résultat de cette vérification participe à l'exécution de la transaction sans que la donnée environnementale soit intégrée à la monnaie elle-même.

Cette proposition décrit une possibilité technique résultant de la combinaison de composants documentés séparément.

Elle ne démontre ni l'existence d'un tel service, ni son autorisation juridique, ni son utilisation par une administration, une banque ou un PSP.

Une interconnexion ne nécessite pas nécessairement une base de données unique

Les résultats obtenus dans les chapitres 3 et 4 montrent également qu'une éventuelle interconnexion n'aurait pas nécessairement besoin de centraliser toutes les informations dans un système unique.

Un service pourrait théoriquement :

```
recevoir l'identifiant nécessaire à une transaction
   ↓
interroger un système externe autorisé
   ↓
vérifier une condition
   ↓
obtenir un résultat
   ↓
transmettre uniquement ce résultat au système chargé du paiement
```

DÉDUCTIBLE TECHNIQUEMENT :

> L'absence de fusion physique entre les bases de données environnementales, commerciales et monétaires ne suffit donc pas à exclure techniquement un mécanisme de décision reposant sur leur interopérabilité.

Cette déduction est cohérente avec les architectures étudiées : elles reposent précisément sur des identifiants, des API, des droits d'accès et des échanges entre composants spécialisés.

Le consentement et la gouvernance restent déterminants

La capacité technique d'utiliser une condition externe ne détermine pas qui possède le droit de définir cette condition.

Dans les cas d'usage actuellement présentés par la BCE, les paiements conditionnels constituent des services destinés à répondre à un besoin du payeur et du bénéficiaire S27.

Ils ne constituent pas un pouvoir général accordé à l'Eurosystème pour décider quels achats doivent être autorisés.

Une distinction doit donc être maintenue entre :

- une condition volontaire choisie dans un service ;
- une condition contractuelle imposée par les conditions d'utilisation d'un service ;
- une condition réglementaire imposée par le droit ;
- une décision prise par un intermédiaire conformément à ses obligations légales ;
- une restriction attachée à la monnaie elle-même.

Ces situations peuvent produire des effets techniques similaires sur une transaction mais reposent sur des bases juridiques et des acteurs décisionnaires différents.

À ÉTABLIR :

> Quelles garanties empêchent ou encadrent l'utilisation de la couche conditionnelle pour des critères autres que ceux volontairement acceptés par le payeur et le bénéficiaire ?

Les expérimentations continuent en 2026

Les travaux de la plateforme d'innovation ne se sont pas arrêtés à la première expérimentation S28.

La BCE a annoncé une nouvelle phase de collaboration avec les acteurs du marché en 2026.

Cette phase doit notamment approfondir les paiements conditionnels et d'autres services à valeur ajoutée, tels que les reçus électroniques, le partage de factures et les outils de gestion budgétaire.

La BCE indique également vouloir poursuivre l'exploration des paiements machine-to-machine, de l'intelligence artificielle appliquée aux paiements, des micropaiements et de différents cas d'usage B2B.

AVÉRÉ :

> L'intégration de services externes et l'automatisation des paiements constituent donc toujours un domaine actif de développement et d'expérimentation du projet en 2026 S28.

Les caractéristiques définitives des services qui en résulteront ne sont cependant pas encore établies.

Conclusion intermédiaire

AVÉRÉ :

> Des acteurs du marché ont connecté leurs propres plateformes, au moyen d'API, à un environnement simulant les interfaces de l'euro numérique afin de tester des paiements conditionnels S28.

AVÉRÉ :

> Dans l'architecture expérimentée, l'Eurosystème fournit les fonctionnalités monétaires fondamentales tandis que les PSP et autres acteurs du marché peuvent développer et gérer la logique déterminant les conditions de libération des fonds S27-S28.

AVÉRÉ :

> Les conditions expérimentées peuvent dépendre d'événements externes au règlement monétaire, notamment une livraison, l'utilisation d'un service, l'accomplissement d'une étape ou d'autres événements vérifiables S28.

AVÉRÉ :

> Des scénarios machine-to-machine ont également été étudiés, permettant à des systèmes ou équipements de participer automatiquement à certains processus commerciaux et de paiement S28.

AVÉRÉ :

> Le mécanisme générique permettant à un système externe de fournir ou vérifier une information participant à l'exécution d'un paiement conditionnel a donc dépassé le stade de la simple hypothèse technique et a fait l'objet d'expérimentations dans un environnement simulé S27-S28.

DÉDUCTIBLE TECHNIQUEMENT :

> Une donnée externe n'a pas nécessairement besoin d'être directement transmise ou stockée dans l'infrastructure monétaire : la couche conditionnelle peut techniquement effectuer ou recevoir une vérification et communiquer seulement le résultat nécessaire à l'exécution du paiement.

DÉDUCTIBLE TECHNIQUEMENT :

> La combinaison avec les infrastructures étudiées au chapitre 3 rend techniquement possible une architecture dans laquelle une caractéristique environnementale d'un produit serait vérifiée dans un système externe puis utilisée comme critère d'un service de paiement conditionnel.

NON ÉTABLI :

> Aucun élément étudié ne permet cependant d'établir qu'un DPP, un GTIN, une empreinte carbone, une donnée issue de la facturation électronique ou un profil environnemental individuel soit actuellement utilisé pour déclencher, empêcher ou modifier un paiement en euros numériques.

À ÉTABLIR :

> Existe-t-il des expérimentations, consortiums, marchés publics, spécifications ou partenariats reliant concrètement les infrastructures de traçabilité des produits, de facturation électronique ou de données environnementales aux services de paiement conditionnel ?

À ÉTABLIR :

> Les reçus électroniques envisagés avec l'euro numérique pourront-ils transporter des identifiants de produits ou d'autres informations permettant un rapprochement automatisé avec des systèmes commerciaux ou environnementaux ?

À ÉTABLIR :

> Quels acteurs sont présents simultanément dans les projets de DPP, de facturation électronique et d'euro numérique, et développent-ils des interfaces ou services permettant de relier ces infrastructures ?

4.7 Identité numérique et infrastructures de paiement

Statut : AVÉRÉ / PROJET EN COURS

L'identité numérique européenne constitue une infrastructure distincte de l'euro numérique.

Les sources officielles établissent cependant un raccord explicite entre l'European Digital Identity Wallet, ou EUDI Wallet, et les infrastructures de paiement S29.

La Commission européenne documente un cas d'usage spécifiquement consacré à l'authentification des paiements au moyen de l'EUDI Wallet.

La Banque centrale européenne prévoit parallèlement que les prestataires participant au pilote de l'euro numérique puissent utiliser ce wallet comme méthode d'authentification forte pour certaines transactions en ligne S29.

Le lien entre identité numérique et paiement n'est donc pas seulement techniquement déductible : il est explicitement prévu dans les architectures étudiées.

L'EUDI Wallet constitue une infrastructure européenne d'identité numérique

Le cadre européen relatif à l'identité numérique prévoit la mise à disposition de wallets permettant aux personnes physiques et morales de s'identifier et de présenter différentes attestations numériques S29.

Le wallet peut notamment contenir ou permettre de présenter :

- des données d'identité ;
- des attestations électroniques ;
- des justificatifs ou attributs vérifiables ;
- des éléments nécessaires à l'authentification auprès de services publics ou privés.

L'architecture repose sur des formats et protocoles communs permettant aux émetteurs, wallets et parties utilisatrices de vérifier cryptographiquement les informations présentées.

Son utilisation est prévue comme volontaire pour l'utilisateur.

L'EUDI Wallet est explicitement prévu pour les paiements

La Commission européenne documente un cas d'usage intitulé **Payment Authentication** permettant d'utiliser l'EUDI Wallet pour authentifier des paiements en ligne ou en magasin S29.

Cette architecture est conçue pour fonctionner avec les infrastructures de paiement existantes, notamment les paiements par carte et les paiements de compte à compte.

Le wallet ne constitue donc pas lui-même nécessairement le système transférant les fonds.

Il intervient comme composant permettant notamment d'authentifier le payeur et de présenter les preuves nécessaires à la transaction.

Le fonctionnement général peut être résumé ainsi :

```
utilisateur
   ↓
EUDI Wallet
   ↓
présentation d'une preuve ou d'une attestation
   ↓
banque / PSP / acquéreur / commerçant
   ↓
authentification du paiement
```

AVÉRÉ :

> Une infrastructure européenne d'identité numérique est explicitement conçue pour pouvoir intervenir directement dans le processus d'authentification d'un paiement S29.

Le wallet peut être relié à un payeur et à un compte

La documentation prévoit notamment des attestations d'authentification forte émises par les prestataires de services de paiement S29.

Ces attestations permettent d'établir un lien vérifiable entre :

- le wallet ;
- un payeur déterminé ;
- et un compte ou instrument de paiement déterminé.

Lorsqu'un paiement est initié, le wallet peut présenter l'attestation appropriée à la partie chargée de la vérifier, par exemple une banque, un acquéreur ou un commerçant.

AVÉRÉ :

> L'EUDI Wallet peut donc intervenir comme composant cryptographiquement vérifiable reliant l'utilisateur à l'authentification d'une opération de paiement et à l'instrument ou au compte concerné S29.

Cela ne signifie pas que l'ensemble des informations d'identité contenues dans le wallet soit transmis avec chaque paiement.

La divulgation sélective permet de présenter un attribut sans transmettre toute l'identité

L'architecture de l'EUDI Wallet repose notamment sur un principe de divulgation sélective S29.

L'utilisateur peut présenter uniquement l'information nécessaire à une interaction donnée plutôt que l'intégralité de son identité ou du document contenant cette information.

La Commission fournit notamment comme exemples :

- l'âge ;
- la résidence ;
- certaines informations issues d'un permis de conduire S29.

Dans un scénario d'achat soumis à une condition d'âge, le système peut ainsi vérifier que l'utilisateur remplit le critère requis sans nécessairement recevoir sa date de naissance complète.

Le principe peut être représenté ainsi :

```
wallet contenant une information vérifiable
   ↓
sélection de l'attribut nécessaire
   ↓
preuve du critère demandé
   ↓
service ou commerçant vérificateur
```

AVÉRÉ :

> L'infrastructure permet donc techniquement qu'un attribut relatif à une personne soit vérifié dans le contexte d'un paiement sans nécessiter la transmission de l'ensemble de son identité S29.

L'âge constitue déjà un exemple concret de critère associé à un achat

La documentation officielle fournit précisément l'exemple d'un achat nécessitant une vérification d'âge S29.

Dans le parcours présenté par la Commission, l'utilisateur effectue un achat en ligne et utilise son EUDI Wallet dans le processus d'authentification.

Le wallet affiche notamment le commerçant, le montant et les attributs demandés.

L'utilisateur peut ensuite présenter la preuve nécessaire.

AVÉRÉ :

> Un attribut personnel vérifiable provenant de l'infrastructure d'identité numérique peut donc déjà être intégré au parcours technique entourant un paiement afin de vérifier une condition applicable à l'achat S29.

Il est toutefois essentiel de distinguer ce mécanisme d'un paiement conditionnel au sens étudié dans les sections 4.5 et 4.6.

Dans cet exemple, la vérification d'âge répond à une exigence liée à l'accès ou à la vente du produit ; elle ne constitue pas la preuve que l'euro numérique lui-même applique une restriction d'achat.

Le raccord avec l'euro numérique est explicitement prévu

La relation entre l'EUDI Wallet et l'euro numérique n'est pas seulement une possibilité résultant de l'existence de deux infrastructures européennes compatibles.

La documentation de la BCE relative au pilote de l'euro numérique l'indique explicitement S29.

Les PSP participant au pilote pourront prendre en charge l'EUDI Wallet comme méthode d'authentification forte pour les transactions en ligne lorsque l'utilisateur utilise les instruments numériques du PSP.

Les PSP restent libres de choisir leurs méthodes d'authentification sous réserve du respect des exigences réglementaires applicables.

AVÉRÉ :

> L'utilisation de l'EUDI Wallet comme méthode d'authentification dans le pilote de l'euro numérique est explicitement prévue par la Banque centrale européenne S29.

Le raccord suivant est donc officiellement documenté :

```
EUDI Wallet
   ↓
authentification forte
   ↓
PSP
   ↓
paiement en euro numérique
```

Ce raccord est plus solide que les rapprochements hypothétiques étudiés avec d'autres infrastructures : il est directement décrit par la BCE pour le pilote.

Des pilotes européens ont déjà expérimenté identité et paiement

L'utilisation de l'EUDI Wallet dans les paiements a également fait l'objet de Large Scale Pilots européens S29.

Les projets européens ont notamment testé :

- l'initiation de paiements ;
- l'authentification forte ;
- les paiements en ligne ;
- les paiements en magasin ;
- la vérification d'âge associée à un paiement.

AVÉRÉ :

> Le raccord entre identité numérique européenne et infrastructure de paiement a donc dépassé le stade d'une simple spécification conceptuelle : il a déjà fait l'objet de pilotes européens S29.

Ces expérimentations ne constituent cependant pas la preuve d'un système généralisé reliant automatiquement toutes les informations d'identité à toutes les transactions.

Une même infrastructure peut présenter différents types d'attestations

L'EUDI Wallet n'est pas limité à une identité civile élémentaire.

Son architecture permet de stocker et présenter différents types d'attestations émises par des sources de confiance.

Cela signifie qu'un même mécanisme technique peut être utilisé pour présenter différents attributs selon le service concerné.

DÉDUCTIBLE TECHNIQUEMENT :

> Une infrastructure de paiement utilisant l'EUDI Wallet pour une authentification ou une vérification n'a pas nécessairement besoin d'accéder à l'ensemble des données détenues par le wallet : elle peut demander et recevoir uniquement l'attestation ou l'attribut nécessaire au processus concerné.

Cette logique est comparable, sur le plan architectural, à celle étudiée pour les paiements conditionnels : le composant prenant une décision n'a pas nécessairement besoin de disposer de toutes les données sources lorsque le système peut lui présenter une preuve vérifiable.

Le raccord identité → paiement est établi, mais sa portée doit être délimitée

À ce stade, la chaîne suivante peut être considérée comme documentée :

```
attribut ou identité vérifiable
   ↓
EUDI Wallet
   ↓
présentation d'une preuve
   ↓
PSP / banque / acquéreur / commerçant
   ↓
authentification ou vérification nécessaire au processus de paiement
```

Et, dans le cadre du pilote de l'euro numérique :

```
EUDI Wallet
   ↓
authentification forte
   ↓
PSP participant au pilote
   ↓
transaction en euro numérique
```

AVÉRÉ :

> Il existe donc un raccord institutionnel et technique explicitement prévu entre l'infrastructure européenne d'identité numérique et les infrastructures de paiement, y compris dans le cadre du pilote de l'euro numérique S29.

Ce raccord ne signifie pas qu'un profil complet accompagne chaque paiement

L'existence de ce lien ne doit pas conduire à considérer que l'ensemble des données détenues dans l'EUDI Wallet est automatiquement communiqué au PSP ou au commerçant.

La conception du wallet repose au contraire sur des principes de minimisation des données et de divulgation sélective S29.

Une vérification peut, par exemple, porter uniquement sur le fait qu'une personne satisfait un critère d'âge.

NON ÉTABLI :

> Les sources étudiées ne permettent pas d'affirmer que l'ensemble des attributs détenus dans un EUDI Wallet puisse être consulté par une banque, un PSP, un commerçant ou l'Eurosystème lors d'un paiement.

NON ÉTABLI :

> Elles ne permettent pas non plus d'établir qu'un historique général des achats soit enregistré dans l'EUDI Wallet à des fins de profilage individuel.

La combinaison avec les paiements conditionnels doit être distinguée de l'authentification

Les sections 4.5 et 4.6 ont établi qu'une donnée externe peut participer à la vérification d'une condition déclenchant un paiement conditionnel.

La présente section établit qu'un wallet d'identité peut fournir une preuve vérifiable dans le parcours d'un paiement.

Ces deux mécanismes sont techniquement compatibles dans leur principe, mais leur combinaison systématique n'est pas démontrée.

DÉDUCTIBLE TECHNIQUEMENT :

> Une attestation vérifiable fournie par une infrastructure d'identité peut techniquement constituer l'une des informations utilisées par un service externe pour vérifier qu'une condition nécessaire à une opération est satisfaite.

L'exemple de la vérification d'âge montre déjà qu'un attribut individuel peut intervenir dans un processus commercial associé à un paiement.

NON ÉTABLI :

> Cela ne démontre pas qu'un attribut environnemental, fiscal, social ou comportemental puisse actuellement être imposé comme condition générale d'utilisation de l'euro numérique.

Le rapprochement avec les autres infrastructures reste à établir

Les chapitres précédents ont maintenant identifié séparément plusieurs mécanismes :

Chapitre 1
données structurées relatives aux transactions et à la facturation

Chapitre 3
produits identifiables et données environnementales structurées

Chapitre 4.5–4.6
systèmes externes et conditions pouvant participer à l'exécution automatisée d'un paiement

Chapitre 4.7
identité ou attribut vérifiable pouvant intervenir directement dans le processus de paiement

L'existence séparée de ces quatre éléments ne démontre toujours pas leur interconnexion globale.

Elle réduit cependant progressivement le nombre de raccords purement hypothétiques.

Le raccord :

> **identité numérique → infrastructure de paiement**

est désormais **AVÉRÉ** S29.

Le raccord :

> **EUDI Wallet → authentification d'un paiement dans le pilote euro numérique**

est également **AVÉRÉ** S29.

Le raccord :

> **système externe → condition → exécution automatisée d'un paiement**

a été établi dans les sections précédentes S27-S28.

En revanche, le raccord :

> **données de facturation / DPP / données environnementales → attribut individuel → condition appliquée à un paiement**

reste **À ÉTABLIR**.

Conclusion intermédiaire

AVÉRÉ :

> L'EUDI Wallet est explicitement conçu pour être utilisé dans l'authentification de paiements en ligne et en magasin S29.

AVÉRÉ :

> Des attestations émises notamment par les PSP peuvent établir un lien vérifiable entre un wallet, un payeur et un compte ou instrument de paiement S29.

AVÉRÉ :

> L'architecture permet la présentation sélective de certains attributs personnels, notamment l'âge ou la résidence, sans nécessairement transmettre l'ensemble de l'identité de l'utilisateur S29.

AVÉRÉ :

> Des pilotes européens ont déjà expérimenté des paiements utilisant l'EUDI Wallet, y compris des scénarios associant paiement et vérification d'âge S29.

AVÉRÉ :

> La BCE prévoit explicitement que les PSP participant au pilote de l'euro numérique puissent utiliser l'EUDI Wallet comme méthode d'authentification forte pour les paiements en ligne S29.

DÉDUCTIBLE TECHNIQUEMENT :

> Une preuve ou un attribut vérifiable provenant d'une infrastructure d'identité peut techniquement être utilisé dans un processus de vérification entourant une transaction sans que l'ensemble des données sources soit communiqué au système de paiement.

NON ÉTABLI :

> Aucun élément étudié ne permet d'établir que l'EUDI Wallet soit actuellement destiné à fournir un profil environnemental, fiscal ou comportemental utilisé pour autoriser ou refuser des paiements en euros numériques.

À ÉTABLIR :

> Quels attributs autres que ceux actuellement documentés pour l'authentification pourront être demandés dans les futurs services de paiement utilisant l'EUDI Wallet ?

À ÉTABLIR :

> Dans quelles conditions juridiques un commerçant, une banque, un PSP ou un autre service pourra demander la présentation d'un attribut avant l'exécution d'une transaction ?

À ÉTABLIR :

> Existe-t-il des infrastructures ou projets européens permettant de relier des attestations détenues dans un wallet d'identité à des données de facturation, de produit ou environnementales ?

4.8 Limites et garanties prévues

Statut : AVÉRÉ / PROJET EN COURS / À ÉTABLIR

Les sections précédentes ont établi que l'architecture envisagée pour l'euro numérique comporte des capacités techniques importantes : traitement structuré des transactions, intervention de plusieurs prestataires, réservation de fonds, paiements conditionnels, utilisation d'informations provenant de systèmes externes et possibilité d'utiliser une infrastructure d'identité numérique dans le processus de paiement S22-S24-S25-S27-S28-S29.

Ces capacités ne peuvent cependant pas être analysées indépendamment des garanties juridiques et techniques prévues pour limiter leur utilisation.

Il faut notamment distinguer :

- ce qui est explicitement interdit ;
- ce qui est rendu plus difficile par l'architecture ;
- ce qui reste possible mais encadré par le droit ;
- et ce qui dépendrait d'une modification future du cadre juridique.

L'euro numérique ne doit pas être une monnaie programmable

La garantie la plus explicite concerne la programmabilité de la monnaie.

La proposition de règlement exclut que l'euro numérique soit conçu comme une monnaie comportant intrinsèquement des conditions limitant son utilisation à certains biens, services, lieux, personnes ou périodes S22.

Cette interdiction est également constamment affirmée par la Banque centrale européenne S23-S27.

AVÉRÉ :

> L'Eurosystème ne doit pas pouvoir attribuer à certaines unités d'euros numériques des règles déterminant les biens ou services pour lesquels elles peuvent être dépensées S22-S23-S27.

Une unité d'euro numérique doit rester fongible avec les autres unités.

Cette garantie interdit donc un scénario dans lequel la monnaie elle-même porterait, par exemple, une règle du type :

« cette unité ne peut pas acheter tel produit ».

Cette interdiction ne supprime pas les paiements conditionnels

Comme établi en 4.5 et 4.6, l'interdiction de la monnaie programmable ne supprime pas la possibilité de construire des services conditionnels autour du paiement S27-S28.

La différence juridique et technique est fondamentale :

restriction attachée à la monnaie → explicitement exclue

condition attachée à une transaction ou à un service → prévue dans l'architecture

AVÉRÉ :

> La garantie contre la monnaie programmable n'interdit donc pas toute logique automatisée autour de l'exécution d'un paiement S22-S27.

C'est précisément pour cette raison que la gouvernance de la couche de conditionnalité est importante.

Les conditions sont présentées comme devant être convenues par les parties

Dans le modèle présenté par la BCE, les paiements conditionnels correspondent à des services dans lesquels les conditions sont déterminées ou acceptées par les parties à la transaction S27.

L'Eurosystème fournit l'infrastructure monétaire nécessaire au règlement et à la réservation des fonds mais n'est pas présenté comme l'acteur définissant les critères commerciaux permettant leur libération.

AVÉRÉ :

> Dans le cadre actuellement présenté, l'Eurosystème ne dispose pas d'un pouvoir général lui permettant de définir les biens ou services qu'un utilisateur peut acheter au moyen de l'euro numérique S22-S27.

Cette garantie est importante.

Elle ne répond cependant pas entièrement à une autre question :

un critère peut-il devenir obligatoire parce qu'il résulte non de la BCE mais d'une obligation juridique ou réglementaire applicable au PSP, au commerçant ou à l'utilisateur ?

Cette question relève alors moins de la conception monétaire que du droit applicable à l'acteur exécutant le paiement.

À ÉTABLIR :

> Dans quelles conditions une règle extérieure au système monétaire pourrait-elle légalement imposer à un PSP ou à un autre intermédiaire de vérifier un critère avant d'exécuter une transaction ?

Les PSP disposent déjà de capacités de contrôle et de non-exécution

L'existence d'une monnaie non programmable ne signifie pas qu'un prestataire de services de paiement soit techniquement obligé d'exécuter toutes les transactions qui lui sont présentées.

Comme établi en 4.2, les PSP restent soumis à différentes obligations réglementaires concernant notamment :

- la lutte contre le blanchiment et le financement du terrorisme ;
- les sanctions et embargos ;
- la prévention de la fraude ;
- la sécurité ;
- certaines obligations fiscales S22-S24.

Dans certaines circonstances prévues par le droit, ces obligations peuvent conduire à empêcher, suspendre ou refuser une opération.

AVÉRÉ :

> L'interdiction de la monnaie programmable n'équivaut donc pas à une impossibilité technique ou juridique absolue de bloquer une transaction : des mécanismes de contrôle et de non-exécution existent déjà lorsqu'une base juridique le prévoit S22-S24.

La question centrale n'est donc pas uniquement :

« le paiement peut-il être bloqué ? »

mais également :

« qui possède le pouvoir de le bloquer, pour quel motif et sur quelle base juridique ? »

Des limites de détention sont prévues

La proposition de règlement prévoit également la possibilité d'appliquer des limites au montant d'euros numériques qu'un utilisateur peut détenir S22.

Ces limites doivent notamment permettre de préserver la stabilité financière et d'éviter une migration excessive des dépôts bancaires vers la monnaie de banque centrale.

Les PSP participent à l'application de ces limites.

Des mécanismes sont également prévus afin de vérifier qu'un utilisateur possédant plusieurs comptes en euros numériques ne puisse contourner la limite globale applicable S22.

AVÉRÉ :

> L'architecture prévoit donc déjà des règles quantitatives pouvant être vérifiées et appliquées automatiquement au niveau des avoirs en euros numériques S22.

Ces limites portent sur la **détention** d'euros numériques et non sur la nature des biens ou services achetés.

Elles ne constituent donc pas une restriction de consommation.

L'infrastructure peut vérifier une règle sans connaître tout son contexte

La vérification des limites illustre néanmoins un principe technique déjà rencontré dans les sections précédentes.

Plusieurs composants peuvent coopérer pour déterminer qu'une règle est satisfaite sans que chacun dispose de toutes les informations relatives à l'utilisateur.

Cette logique rejoint celle des paiements conditionnels et de l'identité numérique :

```
donnée ou attribut
   ↓
vérification d'une règle
   ↓
résultat exploitable par un autre composant
```

DÉDUCTIBLE TECHNIQUEMENT :

> L'architecture permet donc l'application automatisée de certaines règles sans nécessiter qu'un acteur unique centralise l'ensemble des données utilisées pour les vérifier.

Cette caractéristique constitue à la fois une possibilité technique et, lorsqu'elle repose sur la pseudonymisation ou la divulgation sélective, un mécanisme de protection des données.

La BCE ne doit pas pouvoir identifier directement les utilisateurs à partir des données centrales

La proposition de règlement prévoit que les données communiquées à la BCE et aux banques centrales nationales soient organisées de manière à ne pas leur permettre d'identifier directement les utilisateurs S22.

L'architecture prévoit notamment des mécanismes de séparation, de pseudonymisation et de protection cryptographique.

Comme établi en 4.3, les PSP conservent cependant la relation avec leurs clients et disposent des informations nécessaires à cette relation ainsi qu'au respect de leurs obligations réglementaires S22-S25.

AVÉRÉ :

> La conception actuelle cherche donc à empêcher que l'infrastructure centrale de l'Eurosystème constitue directement une base nominative complète des paiements individuels S22-S23.

Cela ne signifie pas qu'aucun acteur de la chaîne ne puisse identifier l'utilisateur.

La protection repose précisément sur une **répartition des informations entre différents acteurs**.

La séparation des données constitue une garantie, mais pas une absence de traitement

La pseudonymisation ne signifie pas que les transactions deviennent inexistantes ou techniquement impossibles à traiter.

Elle signifie que certains composants utilisent des identifiants qui ne permettent pas directement d'identifier la personne concernée.

Les PSP disposent parallèlement de la relation permettant d'identifier leurs propres clients.

AVÉRÉ :

> L'architecture repose donc davantage sur une séparation des connaissances et des responsabilités que sur l'absence totale de données S22-S25.

Cette distinction est importante pour l'analyse des interconnexions.

Un système distribué peut permettre plusieurs traitements sans qu'une base centrale unique contienne l'intégralité des informations.

Le mode hors ligne constitue la protection architecturale la plus forte

Le mode hors ligne étudié en 4.4 constitue une situation différente S23-S26.

Les détails personnels du paiement sont conçus pour rester sur les appareils du payeur et du bénéficiaire et ne pas être transmis aux PSP ou à l'Eurosystème.

AVÉRÉ :

> Dans l'architecture actuellement prévue, le mode hors ligne empêche donc l'infrastructure centrale d'exploiter systématiquement les détails individuels de chaque transaction hors ligne S23-S26.

Cette protection constitue un obstacle technique beaucoup plus important à un rapprochement centralisé que la simple pseudonymisation d'une transaction en ligne.

Les opérations de chargement et de déchargement restent néanmoins visibles du PSP et soumises aux contrôles réglementaires correspondants.

La minimisation des données est également prévue pour l'identité numérique

L'EUDI Wallet repose notamment sur la divulgation sélective S29.

Lorsqu'un service doit vérifier un attribut, l'objectif est de ne transmettre que l'information nécessaire.

Par exemple :

« utilisateur âgé de plus de 18 ans : OUI »

peut être suffisant sans transmettre la date de naissance complète.

AVÉRÉ :

> L'interconnexion entre identité numérique et paiement n'implique donc pas nécessairement la transmission de l'ensemble du profil d'identité de l'utilisateur S29.

Cette architecture limite la quantité de données exposées.

Elle confirme néanmoins également qu'une décision peut techniquement reposer sur un attribut personnel sans que le système prenant cette décision connaisse l'intégralité des données ayant permis de produire la preuve.

Les garanties reposent en partie sur le droit et peuvent donc évoluer avec lui

Une distinction fondamentale doit être faite entre une impossibilité technique et une interdiction juridique.

Certaines garanties sont profondément intégrées à l'architecture, notamment la protection du mode hors ligne.

D'autres reposent sur les règles définissant les finalités autorisées, les droits d'accès, les obligations des PSP ou les catégories de traitements autorisés.

DÉDUCTIBLE TECHNIQUEMENT :

> Lorsqu'une capacité technique existe mais que son utilisation est interdite ou limitée par le droit, la garantie dépend du maintien du cadre juridique qui encadre cette capacité.

Cela ne signifie pas que ce cadre soit destiné à être modifié.

Cela signifie simplement qu'une interdiction juridique ne doit pas être présentée comme une impossibilité technique.

Cette distinction est essentielle pour l'ensemble de cette enquête.

Les garanties actuelles empêchent plusieurs conclusions excessives

À partir des sources étudiées, il serait incorrect d'affirmer que :

- la BCE pourra décider arbitrairement ce qu'un citoyen peut acheter ;
- l'euro numérique comportera intrinsèquement un quota carbone ;
- chaque unité monétaire pourra être limitée à certains produits ;
- la BCE disposera nécessairement d'un historique nominatif complet des achats ;
- les données du DPP seront automatiquement transmises avec chaque paiement ;
- l'EUDI Wallet transmettra automatiquement l'ensemble des attributs personnels lors d'une transaction ;
- les paiements hors ligne permettront un suivi centralisé identique aux paiements en ligne.

NON ÉTABLI :

> Aucun des éléments étudiés ne démontre l'existence actuelle d'un système permettant d'attribuer à une personne un quota environnemental puis de bloquer automatiquement ses achats lorsque ce quota est atteint.

Mais les garanties ne suppriment pas les capacités techniques documentées

Inversement, il serait également incorrect de conclure que l'interdiction de la monnaie programmable rend techniquement impossible toute décision automatisée entourant un paiement.

Les sections précédentes ont établi séparément :

```
transactions structurées et identifiables [S25](#s25)
   ↓
réservation des fonds [S27](#s27)
   ↓
couche de conditionnalité externe à l'Eurosystème [S27](#s27)-[S28](#s28)
   ↓
vérification possible d'événements provenant de systèmes externes [S27](#s27)-
[S28](#s28)
   ↓
plateformes d'acteurs du marché connectées par API dans les expérimentations [S28]
(#s28)
   ↓
identité et attributs vérifiables pouvant intervenir dans le parcours de paiement
[S29](#s29)
```

AVÉRÉ :

> Les garanties entourant l'euro numérique limitent les usages autorisés de ces capacités mais ne suppriment pas l'existence des composants techniques permettant l'automatisation, la vérification de conditions et l'interaction avec des systèmes externes S22-S27-S28-S29.

La question centrale se déplace donc vers la gouvernance

Après examen des garanties, la question n'est plus seulement de savoir si l'infrastructure possède techniquement les composants permettant d'automatiser ou de conditionner certaines opérations.

Une partie de ces composants est désormais documentée.

La question devient :

```
qui peut définir la règle ?
   ↓
sur quelle base juridique ?
   ↓
à partir de quelles données ?
   ↓
avec quel consentement ou quelle obligation ?
   ↓
quel acteur vérifie la condition ?
   ↓
quel acteur possède la capacité d'agir sur la transaction ?
```

Cette distinction entre **capacité technique** et **autorité juridique** devra être centrale dans les chapitres consacrés aux interconnexions et aux garanties juridiques.

Conclusion intermédiaire

AVÉRÉ :

> La proposition relative à l'euro numérique interdit la monnaie programmable au sens d'unités monétaires comportant intrinsèquement des restrictions relatives aux biens, services, lieux, personnes ou périodes d'utilisation S22-S27.

AVÉRÉ :

> Cette interdiction n'empêche pas les paiements conditionnels, qui reposent sur une logique appliquée à une transaction ou à un service plutôt qu'à la monnaie elle-même S27-S28.

AVÉRÉ :

> Les PSP restent capables et, dans certaines situations, juridiquement tenus d'effectuer des contrôles pouvant conduire à la non-exécution d'une transaction, notamment dans les domaines de la fraude, des sanctions et de la lutte contre le blanchiment S22-S24.

AVÉRÉ :

> Des limites de détention d'euros numériques peuvent être définies et appliquées automatiquement, mais elles concernent le montant détenu et non les catégories de biens pouvant être achetées S22.

AVÉRÉ :

> L'architecture prévoit une séparation entre l'identité connue des PSP et les informations pseudonymisées traitées par l'infrastructure centrale, tandis que le mode hors ligne bénéficie d'une protection plus forte empêchant la remontée centrale des détails personnels de la transaction S22-S23-S26.

AVÉRÉ :

> L'EUDI Wallet repose notamment sur la minimisation des données et la divulgation sélective des attributs nécessaires S29.

DÉDUCTIBLE TECHNIQUEMENT :

> Les garanties juridiques encadrant une capacité technique ne doivent pas être confondues avec l'absence de cette capacité technique.

NON ÉTABLI :

> Aucun élément étudié ne permet d'établir l'existence d'un mécanisme actuel attribuant un quota environnemental individuel puis utilisant ce quota pour autoriser ou refuser des paiements.

À ÉTABLIR :

> Dans quelle mesure les règles encadrant les paiements conditionnels empêchent-elles juridiquement qu'une condition soit imposée autrement que par l'accord volontaire du payeur et du bénéficiaire ?

À ÉTABLIR :

> Une réglementation extérieure au cadre de l'euro numérique pourrait-elle légalement imposer à un PSP, à un commerçant ou à un autre intermédiaire de vérifier un attribut ou une condition avant l'exécution d'une transaction ?

À ÉTABLIR :

> Quelles garanties juridiques empêchent l'utilisation de données provenant d'autres infrastructures numériques comme critères décisionnels dans un service de paiement ?

À ÉTABLIR :

> Quelles garanties relèvent directement de l'architecture technique et lesquelles dépendent principalement du cadre juridique susceptible d'évoluer ?

4.9 Ce que ce chapitre permet d'établir

L'analyse de l'euro numérique montre qu'il ne s'agit pas uniquement d'un nouveau moyen de paiement reproduisant sous forme numérique le fonctionnement des espèces.

Le projet repose sur une infrastructure structurée faisant intervenir l'Eurosystème, des prestataires de services de paiement, des dispositifs d'acceptation, des services communs et différentes interfaces permettant aux acteurs du marché de développer des services complémentaires S22-S23-S24.

Les documents techniques et les expérimentations étudiés permettent également d'établir plusieurs capacités importantes concernant les données, l'automatisation des paiements et l'interaction avec des systèmes externes.

Ces capacités doivent cependant être distinguées des usages effectivement autorisés ou actuellement déployés.

Une infrastructure centralisée de règlement est prévue

AVÉRÉ :

> L'euro numérique est conçu comme une monnaie de banque centrale dont le règlement repose sur une infrastructure centralisée exploitée par l'Eurosystème et distribuée aux utilisateurs par l'intermédiaire de prestataires de services de paiement S22-S23-S24.

Cette architecture ne repose pas sur une blockchain ou une infrastructure DLT comme fondement du système S23.

L'utilisateur conserve principalement une relation avec son PSP, tandis que l'Eurosystème assure les fonctions centrales nécessaires au règlement et au fonctionnement de l'infrastructure.

Les paiements en ligne produisent des données structurées

AVÉRÉ :

> Le modèle technique actuellement publié prévoit des données structurées relatives aux utilisateurs, comptes, appareils, prestataires, payeurs, bénéficiaires et transactions S25.

Les transactions disposent notamment d'identifiants, d'un montant, d'une date et d'une heure, d'un type, d'un environnement et d'un statut.

Certaines informations permettent également de caractériser le contexte commercial.

Le Merchant Category Code permet notamment de catégoriser l'activité du commerçant et fait partie des informations prévues dans certains flux de paiement S25.

Cela ne signifie pas que l'infrastructure connaît systématiquement le produit précis acheté ou le contenu détaillé du panier.

Les données sont réparties entre plusieurs acteurs

AVÉRÉ :

> L'architecture ne prévoit pas qu'un acteur unique dispose nécessairement de l'ensemble des informations relatives à une transaction S22-S24-S25.

Les PSP connaissent leurs clients conformément à leurs obligations.

L'infrastructure centrale utilise notamment des identifiants pseudonymisés et des mécanismes destinés à empêcher l'Eurosystème d'identifier directement les utilisateurs à partir des informations qu'il reçoit S22-S23.

La présence d'une donnée quelque part dans la chaîne ne signifie donc pas qu'elle soit accessible à tous les participants.

Le mode hors ligne constitue une architecture distincte

AVÉRÉ :

> L'euro numérique est conçu pour permettre également des paiements hors ligne exécutés directement entre les appareils du payeur et du bénéficiaire sans intervention en temps réel de l'infrastructure centrale S23-S26.

Dans le modèle actuellement présenté, les détails personnels de ces transactions restent sur les appareils et ne sont accessibles ni à l'Eurosystème ni aux PSP.

Cette architecture constitue donc une limitation importante à la possibilité d'effectuer un rapprochement centralisé systématique des paiements hors ligne avec d'autres données.

L'euro numérique ne doit pas être une monnaie programmable

AVÉRÉ :

> La proposition de règlement et la Banque centrale européenne excluent explicitement une monnaie dont les unités comporteraient intrinsèquement des restrictions déterminant les biens, services, lieux, bénéficiaires ou périodes pour lesquels elles peuvent être utilisées S22-S23-S27.

L'euro numérique doit rester fongible.

Cette garantie exclut donc, dans le cadre actuellement proposé, un mécanisme dans lequel certaines unités monétaires seraient directement programmées pour interdire l'achat d'une catégorie de produits.

Les paiements conditionnels sont en revanche explicitement prévus

AVÉRÉ :

> L'interdiction de la monnaie programmable n'empêche pas l'existence de paiements conditionnels dont l'exécution dépend de conditions prédéfinies S27.

L'infrastructure prévoit notamment une fonctionnalité permettant de réserver des fonds puis de les transférer lorsque la condition correspondante est considérée comme satisfaite.

La BCE distingue ainsi :

programmation de la monnaie → exclue
programmation des conditions entourant une transaction → prévue

Cette distinction constitue l'un des résultats centraux du chapitre.

La logique conditionnelle peut être située en dehors de l'Eurosystème

AVÉRÉ :

> La BCE décrit une séparation entre une couche de règlement fournie par l'Eurosystème et une couche de conditionnalité pouvant être développée par des banques, PSP et autres acteurs du marché S27-S28.

La couche externe peut vérifier qu'un événement ou une condition est satisfait puis utiliser les fonctions fournies par l'infrastructure pour poursuivre le traitement du paiement.

L'Eurosystème n'a donc pas nécessairement besoin de connaître lui-même l'ensemble des données ayant permis de vérifier cette condition.

Un événement externe peut participer à l'exécution d'un paiement

AVÉRÉ :

> Les travaux de la BCE prévoient qu'un monitoring externe puisse déclencher une condition utilisée par un service de paiement conditionnel S27.

Les exemples étudiés comprennent notamment :

- la confirmation d'une livraison ;
- l'utilisation effective d'un service ;
- l'accomplissement d'une étape ;
- certains événements liés au transport ;
- des interactions machine-to-machine S27-S28.

Le principe général suivant est donc établi :

```
système ou événement externe
   ↓
vérification d'une condition
   ↓
service conditionnel
   ↓
action sur la transaction
```

Ce mécanisme a fait l'objet d'expérimentations

AVÉRÉ :

> Des acteurs du marché ont connecté leurs propres plateformes par API à un environnement simulant les interfaces de l'euro numérique afin d'expérimenter des services et paiements conditionnels S28.

Les PSP et autres participants pouvaient développer la logique conditionnelle au-dessus des fonctionnalités fondamentales fournies par l'environnement simulé.

Le pont générique entre **système externe** et **traitement conditionnel d'un paiement** ne relève donc plus uniquement d'une possibilité théorique d'architecture.

Il a fait l'objet d'expérimentations techniques.

Une donnée externe n'a pas nécessairement besoin d'entrer dans l'infrastructure monétaire

DÉDUCTIBLE TECHNIQUEMENT :

> Un système externe peut effectuer une vérification à partir de ses propres données puis communiquer uniquement le résultat nécessaire au service conditionnel.

Le fonctionnement peut donc être :

```
données conservées dans un système externe
   ↓
vérification d'une règle
   ↓
résultat de la vérification
   ↓
service conditionnel
   ↓
exécution ou absence d'exécution de la transaction
```

Cette architecture signifie qu'une éventuelle interconnexion ne nécessite pas nécessairement la création d'une base centrale regroupant toutes les informations concernées.

L'identité numérique possède également un raccord explicite avec le paiement

AVÉRÉ :

> L'EUDI Wallet est conçu pour pouvoir intervenir dans l'authentification de paiements et présenter des attestations ou attributs vérifiables aux acteurs concernés S29.

L'architecture permet notamment la divulgation sélective d'un attribut sans transmettre nécessairement l'ensemble de l'identité de l'utilisateur.

La vérification d'âge constitue déjà un exemple documenté d'attribut pouvant intervenir dans un parcours commercial associé à un paiement.

Le raccord entre EUDI Wallet et euro numérique est explicitement prévu

AVÉRÉ :

> La BCE prévoit que les PSP participant au pilote de l'euro numérique puissent utiliser l'EUDI Wallet comme méthode d'authentification forte pour les paiements en ligne S29.

La chaîne suivante est donc directement documentée :

```
identité ou attestation numérique
   ↓
EUDI Wallet
   ↓
PSP
   ↓
authentification
   ↓
paiement en euro numérique
```

Le raccord entre identité numérique européenne et infrastructure de paiement ne constitue donc pas uniquement une possibilité théorique.

Plusieurs capacités auparavant séparées peuvent maintenant être représentées ensemble

Les résultats du chapitre permettent de représenter l'architecture générale suivante :

```
Utilisateur
   ↓
identité / attribut vérifiable
   ↓
PSP ou service de paiement
   ↓
transaction structurée et identifiable
```

parallèlement :

```
système externe
   ↓
donnée ou événement vérifiable
   ↓
couche de conditionnalité
```

puis :

```
réservation des fonds
   ↓
condition satisfaite ou non satisfaite
   ↓
règlement ou absence de règlement
```

AVÉRÉ :

> Chacun des principaux composants de cette chaîne est documenté dans l'architecture ou dans les expérimentations étudiées S22-S24-S25-S27-S28-S29.

DÉDUCTIBLE TECHNIQUEMENT :

> Ces composants permettent techniquement de construire des services dans lesquels une information provenant d'un système externe participe à une décision automatisée concernant une transaction déterminée, sans rendre la monnaie elle-même programmable.

Le rapprochement avec les données environnementales reste le maillon manquant

Le chapitre 3 a établi séparément :

- l'existence du Digital Product Passport ;
- l'identification numérique de produits ;

- la possibilité d'associer certaines données environnementales structurées à ces produits ;
- l'existence de méthodes permettant de quantifier certaines empreintes environnementales ;
- des mécanismes d'interopérabilité, d'API et de registres ;
- la possibilité technique de rapprocher une transaction d'un produit identifiable lorsque les identifiants et droits d'accès nécessaires existent S15-S18-S19-S20-S21.

Le chapitre 4 établit maintenant séparément :

- l'existence de transactions de paiement structurées ;
- la réservation de fonds ;
- les paiements conditionnels ;
- une couche de conditionnalité externe ;
- l'utilisation possible d'informations provenant de systèmes externes ;
- des API permettant aux plateformes des acteurs du marché d'interagir avec l'environnement de paiement ;
- et un raccord explicite entre identité numérique et paiement S25-S27-S28-S29.

La combinaison technique peut donc être représentée ainsi :

```
produit identifiable
   ↓
donnée externe associée au produit
   ↓
système capable de vérifier une règle
   ↓
résultat de la vérification
   ↓
couche de conditionnalité
   ↓
transaction
   ↓
exécution ou absence d'exécution
```

DÉDUCTIBLE TECHNIQUEMENT :

> Si une donnée environnementale relative à un produit était rendue accessible à un service autorisé et si cette donnée devenait un critère valide d'une condition de paiement, l'architecture étudiée permettrait techniquement d'utiliser le résultat de cette vérification pour agir sur l'exécution d'une transaction sans programmer la monnaie elle-même.

Ce raccord spécifique n'est cependant pas établi

NON ÉTABLI :

> Aucun élément étudié dans ce chapitre ne démontre qu'une donnée issue d'un Digital Product Passport, un GTIN, une empreinte carbone, une donnée de facturation électronique ou une empreinte environnementale individuelle soit actuellement utilisée comme condition permettant d'autoriser, refuser ou modifier un paiement en euros numériques.

Il n'est pas davantage établi qu'une administration française ou européenne dispose d'un mécanisme permettant d'appliquer automatiquement un quota environnemental individuel aux achats d'une personne.

La possibilité technique résultant de l'assemblage de plusieurs composants ne doit donc pas être présentée comme un usage existant ou officiellement prévu.

Les garanties actuelles doivent être intégrées à cette conclusion

Plusieurs garanties s'opposent actuellement à une interprétation selon laquelle l'euro numérique constituerait directement un outil général de contrôle des achats :

- interdiction de la monnaie programmable S22-S27 ;
- conditions de paiement présentées comme convenues entre les parties S27 ;
- pseudonymisation et séparation des informations accessibles à l'Eurosystème S22-S23 ;
- minimisation et divulgation sélective dans l'EUDI Wallet S29 ;
- confidentialité renforcée des paiements hors ligne S23-S26.

AVÉRÉ :

> Le cadre actuellement proposé ne donne donc pas à l'Eurosystème un pouvoir général lui permettant de déterminer arbitrairement les biens et services qu'un utilisateur est autorisé à acheter.

Ces garanties ne doivent pas être confondues avec une impossibilité technique

Les mêmes sources établissent parallèlement l'existence :

- de contrôles pouvant conduire à la non-exécution de certaines transactions lorsqu'une base juridique le prévoit ;
- de règles quantitatives appliquées automatiquement aux avoirs ;
- de paiements conditionnels ;
- de services externes pouvant vérifier des conditions ;
- d'API permettant l'interaction avec des plateformes de marché ;
- d'attributs d'identité vérifiables utilisables dans le parcours de paiement S22-S24-S27-S28-S29.

DÉDUCTIBLE TECHNIQUEMENT :

> L'interdiction actuelle de certains usages ne signifie donc pas nécessairement que l'infrastructure serait techniquement incapable de mettre en œuvre une règle comparable si une base juridique et les droits d'accès correspondants existaient.

La distinction entre **capacité technique** et **autorité juridique** constitue ainsi l'une des conclusions principales de ce chapitre.

Conclusion du Chapitre 4

L'analyse permet d'écarter deux conclusions opposées.

La première serait d'affirmer que l'euro numérique constitue déjà une monnaie programmable permettant à une autorité de contrôler les achats individuels.

Les sources étudiées ne permettent pas de soutenir cette affirmation.

La seconde serait d'affirmer que l'architecture rend techniquement impossible l'utilisation de données ou de conditions externes dans l'exécution d'un paiement.

Les sources étudiées permettent au contraire d'établir que de tels mécanismes existent dans l'architecture envisagée et ont déjà fait l'objet d'expérimentations.

Le résultat peut donc être formulé ainsi :

AVÉRÉ :

> L'euro numérique n'est pas conçu comme une monnaie programmable.

AVÉRÉ :

> L'infrastructure est néanmoins conçue pour supporter des paiements conditionnels.

AVÉRÉ :

> La logique déterminant une condition peut être développée en dehors de l'Eurosystème par des acteurs du marché.

AVÉRÉ :

> Une information ou un événement provenant d'un système externe peut participer à la vérification d'une condition.

AVÉRÉ :

> Des plateformes externes ont déjà été connectées par API à un environnement simulant l'euro numérique afin d'expérimenter ces mécanismes.

AVÉRÉ :

> L'identité numérique européenne dispose d'un raccord officiel avec les infrastructures de paiement et son utilisation est explicitement prévue dans le pilote de l'euro numérique.

DÉDUCTIBLE TECHNIQUEMENT :

> Une information provenant d'une infrastructure distincte peut être vérifiée extérieurement puis utilisée sous forme de résultat dans un service conditionnel sans que la donnée source soit nécessairement intégrée à l'infrastructure monétaire.

DÉDUCTIBLE TECHNIQUEMENT :

> Les composants étudiés permettraient donc techniquement qu'une donnée relative à un produit ou à une autre caractéristique externe soit utilisée comme critère d'une transaction conditionnelle si un acteur autorisé disposait de cette donnée et d'une base permettant de l'utiliser.

NON ÉTABLI :

> Aucun élément étudié ne démontre actuellement l'utilisation d'un DPP, d'une donnée carbone, d'une donnée de facturation électronique ou d'un profil environnemental individuel comme critère d'autorisation ou de refus d'un paiement.

À ÉTABLIR :

> Existe-t-il des acteurs, projets, standards, infrastructures, appels d'offres ou expérimentations reliant concrètement les systèmes de facturation électronique, de Digital Product Passport, d'identité numérique et de paiement ?

À ÉTABLIR :

> Existe-t-il des identifiants, API ou infrastructures intermédiaires permettant de faire circuler ou vérifier une information entre ces différents systèmes ?

À ÉTABLIR :

> Des acteurs participant au développement de l'euro numérique interviennent-ils également dans les infrastructures de DPP, de facturation électronique ou de traitement des données environnementales ?

À ÉTABLIR :

> Les projets européens actuellement développés prévoient-ils explicitement une interopérabilité entre ces différentes infrastructures, même lorsque leurs finalités initiales restent distinctes ?

Ces questions constituent l'objet du chapitre suivant.

Chapitre 5 — Interconnexions

> **Navigation :** ← Retour au sommaire

Ce chapitre recherche les interconnexions existantes, prévues ou expérimentées entre les infrastructures étudiées dans les chapitres précédents.

L'existence simultanée de plusieurs infrastructures numériques ne démontre pas leur interconnexion.

L'analyse recherche donc des éléments permettant d'identifier des liens concrets entre ces infrastructures :

- standards et identifiants communs ;
- API et mécanismes d'interopérabilité ;
- projets pilotes et expérimentations ;
- consortiums et acteurs communs ;
- partenariats ;
- marchés publics et appels d'offres ;
- références explicites à d'autres infrastructures dans les documentations techniques.

La présence d'un même acteur dans plusieurs projets est documentée comme telle mais ne constitue pas, à elle seule, la preuve d'un échange de données entre ces infrastructures.

Une interconnexion n'est classée **AVÉRÉE** que lorsqu'une source permet d'établir l'existence effective ou explicitement prévue du lien étudié.

Sommaire

- 5.1 — Cartographie des raccords déjà établis
- 5.2 — European Business Wallets : identité, facturation et données de transaction
- 5.3 — Business Wallets, Digital Product Passport et infrastructures européennes
- 5.4 — Identifiants, standards et API communs
- 5.5 — Acteurs, consortiums et expérimentations communes
- 5.6 — Chaînes d'interconnexion documentées
- 5.7 — Le raccord environnement → paiement
- 5.8 — Limites de la démonstration
- 5.9 — Ce que ce chapitre permet d'établir

5.1 Cartographie des raccords déjà établis

Statut : AVÉRÉ / DÉDUCTIBLE TECHNIQUEMENT / À ÉTABLIR

Les quatre premiers chapitres ont étudié séparément plusieurs infrastructures numériques relatives aux transactions économiques, aux produits, à l'environnement, à l'identité et aux paiements.

Avant de rechercher de nouvelles interconnexions, il est nécessaire de distinguer les raccords déjà établis de ceux qui restent seulement techniquement possibles ou encore à démontrer.

Facturation électronique → administration fiscale

AVÉRÉ :

> La réforme française de la facturation électronique organise la transmission automatisée à l'administration fiscale de données structurées relatives aux factures, aux transactions et, dans certaines situations, aux paiements S1-S2-S3-S4.

Pour certaines opérations B2B, les données transmises atteignent le niveau des lignes de facture et comprennent notamment la désignation du bien ou du service, la quantité et le prix unitaire hors taxe.

Le premier raccord est donc directement établi :

```
facture / transaction
   ↓
plateforme agréée
   ↓
administration fiscale
```

Données fiscales → analyse économique et pilotage public

AVÉRÉ :

> Les objectifs officiels de la réforme comprennent, au-delà de la lutte contre la fraude et du pré-remplissage de la TVA, l'amélioration de la connaissance en temps réel de l'activité économique et le pilotage des politiques publiques S5-S6-S14.

Les travaux préparatoires mentionnent également l'utilisation des données recueillies afin d'enrichir certains modèles d'analyse.

Le raccord suivant est donc également documenté :

```
données économiques structurées
 ↓
traitements et analyses
 ↓
connaissance de l'activité économique / pilotage public
```

Cela ne permet pas de déduire que toutes les utilisations possibles de ces données seraient autorisées.

Produit → Digital Product Passport

AVÉRÉ :

> Le cadre européen du Digital Product Passport permet d'associer un produit, un modèle ou un lot à un ensemble structuré d'informations numériques au moyen d'identifiants uniques S15-S20.

Ces informations peuvent, selon la catégorie de produit et la réglementation applicable, inclure différentes caractéristiques techniques et environnementales.

Le raccord suivant est donc établi :

```
produit identifiable
   ↓
identifiant unique
   ↓
Digital Product Passport
   ↓
données structurées relatives au produit
```

Produit → données environnementales

AVÉRÉ :

> Certaines réglementations européennes permettent ou imposent déjà d'associer à certaines catégories de produits des informations environnementales quantitatives, notamment relatives à leur empreinte carbone S15-S18-S19.

Le règlement relatif aux batteries constitue un exemple concret de cette association.

Le raccord :

```
produit identifiable
   ↓
donnée environnementale quantitative
```

est donc établi pour les catégories de produits auxquelles les obligations correspondantes s'appliquent.

Il ne doit pas être généralisé à l'ensemble des produits commercialisés.

DPP → registre, API et systèmes externes

AVÉRÉ :

> L'architecture du Digital Product Passport prévoit un registre européen, des identifiants structurés, des mécanismes d'interopérabilité et des interfaces permettant l'échange automatisé de données S15-S20.

Le registre DPP est désormais opérationnel et la Commission indique qu'il repose notamment sur des API documentées et un référentiel sémantique destiné à faciliter l'interopérabilité entre systèmes.

L'architecture ne constitue donc pas uniquement un ensemble de fiches numériques destinées à être consultées manuellement.

Elle est conçue pour permettre des échanges structurés entre systèmes informatiques.

Transactions commerciales → DPP / traçabilité

AVÉRÉ :

> Des projets européens ont déjà rapproché des preuves de transactions commerciales, des acteurs administratifs chargés notamment de la TVA et des douanes et des mécanismes de traçabilité destinés à utiliser le Digital Product Passport S21.

Le projet e-Origin permet notamment de stocker et partager des preuves de transactions commerciales et de les faire reconnaître par les autorités douanières.

Son évolution dans le cadre du projet EBSI-ELSA prévoit le développement de capacités de traçabilité utilisant le Digital Product Passport.

Cela établit l'existence d'un rapprochement institutionnel entre plusieurs domaines auparavant étudiés séparément :

```
transaction commerciale
   ↓
preuve numérique de transaction
   ↓
infrastructure de traçabilité
   ↓
acteurs administratifs / douaniers
```

parallèlement :

> développement de capacités de traçabilité utilisant le DPP

NON ÉTABLI :

> Ce projet ne démontre pas que les données du DPP sont transmises à l'administration fiscale française avec les données de facturation électronique.

Système externe → condition de paiement

AVÉRÉ :

> L'architecture envisagée pour l'euro numérique prévoit une couche de conditionnalité développée par des acteurs du marché et capable d'utiliser la vérification d'un événement provenant d'un système externe S27-S28.

La BCE indique explicitement que cette architecture permet un monitoring externe susceptible de déclencher les conditions utilisées dans un paiement conditionnel.

Le raccord générique suivant est donc établi :

```
système externe
   ↓
information ou événement
   ↓
vérification d'une condition
   ↓
couche de conditionnalité
   ↓
traitement de la transaction
```

Plateforme externe → environnement euro numérique

AVÉRÉ :

> Des acteurs du marché ont connecté leurs propres plateformes au moyen d'API à un environnement simulant les interfaces de l'euro numérique afin d'expérimenter des paiements conditionnels S28.

Les scénarios étudiés comprennent notamment les paiements à la livraison, à l'usage ou par étapes ainsi que certaines interactions machine-to-machine.

Le raccord entre une plateforme extérieure et la logique conditionnelle entourant un paiement ne constitue donc plus uniquement une possibilité théorique.

Il a déjà fait l'objet d'expérimentations techniques.

Identité numérique → paiement

AVÉRÉ :

> L'European Digital Identity Wallet peut intervenir dans l'authentification de paiements et permettre la présentation d'attestations ou d'attributs vérifiables S29.

Le wallet permet notamment de présenter sélectivement certains attributs sans communiquer nécessairement l'intégralité de l'identité de l'utilisateur.

Le raccord suivant est donc établi :

```
identité / attribut vérifiable
   ↓
EUDI Wallet
   ↓
banque / PSP / acquéreur / commerçant
   ↓
processus de paiement
```

EUDI Wallet → euro numérique

AVÉRÉ :

> La Banque centrale européenne prévoit que les prestataires participant au pilote de l'euro numérique puissent utiliser l'EUDI Wallet comme méthode d'authentification forte pour certaines transactions en ligne S29.

La chaîne suivante est donc explicitement prévue :

```
EUDI Wallet
   ↓
authentification forte
   ↓
PSP
   ↓
paiement en euro numérique
```

Transaction → produit → donnée environnementale

Les chapitres précédents ont également identifié un raccord techniquement possible mais qui nécessite certaines conditions.

Une facture ou une transaction peut contenir un identifiant permettant de déterminer le produit concerné.

Le Digital Product Passport peut également utiliser un identifiant de produit tel qu'un GTIN ou un identifiant équivalent S15-S17.

DÉDUCTIBLE TECHNIQUEMENT :

> Lorsqu'un identifiant commun ou un mécanisme de correspondance existe et que les droits d'accès nécessaires sont réunis, une transaction commerciale peut techniquement être rapprochée des données environnementales associées au produit correspondant.

La chaîne devient alors :

```
transaction
   ↓
produit identifiable
   ↓
identifiant ou mécanisme de correspondance
   ↓
DPP ou autre source environnementale
   ↓
donnée environnementale
```

NON ÉTABLI :

> Les sources étudiées ne démontrent pas que l'administration fiscale française réalise actuellement ce rapprochement.

Donnée externe → décision automatisée concernant un paiement

Les travaux relatifs aux paiements conditionnels permettent également d'établir qu'un système externe n'a pas nécessairement besoin de transférer toutes ses données au système de paiement.

Il peut vérifier lui-même une condition puis communiquer uniquement le résultat nécessaire au service conditionnel.

DÉDUCTIBLE TECHNIQUEMENT :

> Une information provenant d'une infrastructure extérieure peut donc participer à une décision automatisée concernant une transaction sans que la donnée source soit nécessairement intégrée à l'infrastructure monétaire.

Ce principe est important pour la recherche des interconnexions.

L'absence d'une base de données centrale réunissant toutes les informations ne suffit pas à démontrer l'absence d'un raccord entre plusieurs infrastructures.

État de la chaîne après les quatre premiers chapitres

Les raccords établis peuvent désormais être représentés de manière simplifiée :

```
**Facturation électronique**
   ↓
données économiques structurées
   ↓
administration fiscale / analyse économique

**Produit identifiable**
   ↓
Digital Product Passport
   ↓
données structurées / données environnementales

**Identité numérique**
   ↓
EUDI Wallet
   ↓
authentification de paiement

**Système externe**
   ↓
vérification d'une condition
   ↓
service de paiement conditionnel

**Plateforme d'un acteur du marché**
   ↓
API
   ↓
environnement expérimental de l'euro numérique
```

Ces raccords ne forment pas encore, à eux seuls, une chaîne unique.

Les raccords restant à rechercher

Après les quatre premiers chapitres, plusieurs questions deviennent donc beaucoup plus précises.

À ÉTABLIR :

> Existe-t-il une infrastructure explicitement destinée à relier les données de facturation ou de transaction aux autres infrastructures numériques européennes étudiées ?

À ÉTABLIR :

> Existe-t-il un raccord documenté entre le Digital Product Passport et une infrastructure d'identité ou de portefeuille numérique utilisée par les entreprises ?

À ÉTABLIR :

> Les infrastructures de facturation électronique et de DPP sont-elles explicitement envisagées comme les composants d'un même écosystème interopérable ?

À ÉTABLIR :

> Des identifiants, attestations, API ou services intermédiaires permettent-ils de transporter ou de vérifier une information entre ces différents systèmes ?

À ÉTABLIR :

> Des acteurs ou consortiums interviennent-ils simultanément dans le développement des infrastructures de produit, de facturation, d'identité et de paiement ?

À ÉTABLIR :

> Existe-t-il un raccord concret permettant à une donnée environnementale relative à un produit d'atteindre directement ou indirectement la couche de conditionnalité d'un service de paiement ?

Conclusion intermédiaire

AVÉRÉ :

> Plusieurs raccords entre les infrastructures étudiées sont déjà explicitement documentés : facturation vers administration fiscale, produit vers DPP, DPP vers systèmes interopérables, identité numérique vers paiement, EUDI Wallet vers pilote de l'euro numérique et système externe vers paiement conditionnel.

AVÉRÉ :

> Des plateformes externes ont déjà interagi par API avec un environnement simulant l'euro numérique afin d'expérimenter des services conditionnels.

DÉDUCTIBLE TECHNIQUEMENT :

> Lorsqu'un identifiant ou mécanisme de correspondance existe, une transaction comportant un produit identifiable peut techniquement être rapprochée des informations environnementales correspondantes.

NON ÉTABLI :

> Aucun élément étudié jusqu'ici ne démontre une chaîne opérationnelle reliant directement les données françaises de facturation électronique, le Digital Product Passport ou une donnée environnementale à la décision d'autoriser ou de refuser un paiement.

Le chapitre doit maintenant rechercher les infrastructures intermédiaires susceptibles de relier ces différents ensembles.

La première d'entre elles apparaît dans les travaux récents de la Commission européenne : **l'European Business Wallet**.

5.2 European Business Wallets : identité, facturation et données de transaction

Statut : AVÉRÉ / PROJET EN COURS / À ÉTABLIR

La Commission européenne a proposé en novembre 2025 la création des **European Business Wallets**, une infrastructure numérique destinée aux opérateurs économiques et aux organismes publics S30.

Contrairement à l'EUDI Wallet étudié dans le chapitre 4, principalement orienté vers l'identité numérique des personnes physiques, le Business Wallet est conçu pour permettre aux entreprises et autres opérateurs économiques d'interagir numériquement avec d'autres entreprises et avec les administrations publiques.

Il constitue donc une nouvelle infrastructure intermédiaire entre plusieurs domaines étudiés séparément dans les chapitres précédents.

Une infrastructure d'identification et d'échange de données pour les entreprises

AVÉRÉ :

> Les European Business Wallets doivent permettre aux opérateurs économiques de s'identifier, de s'authentifier et d'échanger de manière sécurisée des données, documents et attestations électroniques vérifiables avec d'autres acteurs économiques et avec les administrations publiques S30.

Le dispositif ne constitue donc pas uniquement un portefeuille destiné à conserver des documents.

Il doit également fournir une couche d'échange numérique interopérable entre organisations.

La chaîne générale peut être représentée ainsi :

```
entreprise
   ↓
European Business Wallet
   ↓
identification / authentification / attestations vérifiables
   ↓
entreprise ou administration destinataire
```

Business Wallet → EUDI Wallet

Le Business Wallet est construit à partir du cadre européen d'identité numérique.

La proposition prévoit notamment que les European Digital Identity Wallets et les attestations électroniques d'attributs puissent être utilisés pour l'onboarding et la gestion des accès aux European Business Wallets S30.

AVÉRÉ :

> Un raccord explicite est donc prévu entre l'infrastructure EUDI étudiée dans le chapitre 4 et les European Business Wallets S30.

La chaîne devient :

```
EUDI Wallet / attestation électronique
   ↓
authentification et gestion des accès
   ↓
European Business Wallet
```

Cette relation est particulièrement importante puisque le chapitre 4 a déjà établi séparément un raccord entre l'EUDI Wallet et les infrastructures de paiement.

Elle ne démontre cependant pas qu'une donnée contenue dans un Business Wallet soit automatiquement transmise à un système de paiement.

Des identifiants fiscaux et économiques peuvent être utilisés comme attributs

La proposition mentionne plusieurs attributs pouvant être émis ou vérifiés au moyen des Business Wallets S30.

Parmi les exemples figurent notamment :

- le numéro d'identification TVA ;
- le numéro fiscal ;
- le Legal Entity Identifier (LEI) ;
- le numéro EORI utilisé dans le domaine douanier ;
- le numéro d'accise.

AVÉRÉ :

> Le Business Wallet est donc explicitement conçu pour manipuler des attributs permettant d'identifier juridiquement, fiscalement ou économiquement une entreprise S30.

Cela crée une infrastructure capable de faire circuler des preuves vérifiables concernant une même entité entre plusieurs contextes administratifs et économiques.

Business Wallet → ViDA → facturation électronique

La proposition établit un raccord particulièrement important avec **VAT in the Digital Age (ViDA)** S30.

ViDA modernise le système européen de TVA et prévoit notamment le développement de la facturation électronique et du reporting numérique.

La Commission indique que les European Business Wallets pourront permettre le stockage sécurisé et l'échange vérifiable d'attestations relatives à la TVA et de **données de transaction**, afin de soutenir le reporting en temps réel et la facturation de confiance S30.

AVÉRÉ :

> La Commission prévoit donc explicitement une articulation entre European Business Wallets, données de transaction, TVA, reporting numérique et facturation électronique S30.

La chaîne suivante n'est plus uniquement déductible :

```
entreprise
   ↓
European Business Wallet
   ↓
attestations TVA / données de transaction
   ↓
ViDA
   ↓
reporting numérique / facturation électronique
```

Il s'agit d'un raccord institutionnel explicitement décrit dans la proposition de la Commission.

Le Business Wallet n'est pas limité aux relations avec l'administration

L'infrastructure doit pouvoir être utilisée dans les relations entre entreprises mais également dans les interactions entre entreprises et administrations S30.

AVÉRÉ :

> Le même environnement de confiance est donc conçu pour permettre des échanges B2B et B2G.

Cette caractéristique est importante pour l'étude des interconnexions.

Une attestation ou une donnée vérifiable peut être utilisée dans plusieurs relations économiques sans nécessiter la création d'une infrastructure différente pour chaque administration ou partenaire commercial.

Cela ne signifie cependant pas qu'une donnée communiquée dans un contexte devienne automatiquement accessible dans tous les autres.

Les droits d'accès et les finalités restent déterminants.

Le Business Wallet constitue une couche intermédiaire

Les infrastructures étudiées jusqu'ici pouvaient sembler appartenir à des domaines séparés :

- identité
- fiscalité
- facturation
- douanes
- produits
- administrations
- transactions commerciales

La proposition Business Wallet adopte précisément une logique transversale.

Elle fournit une infrastructure commune d'identification, d'attestations et d'échange sécurisé permettant à différents systèmes de communiquer avec un même opérateur économique S30.

AVÉRÉ :

> L'Union européenne développe donc explicitement une infrastructure destinée à faciliter l'interopérabilité entre plusieurs systèmes administratifs et économiques auparavant distincts S30.

Un raccord important avec notre cartographie précédente

Après le chapitre 4, la chaîne suivante était déjà documentée :

```
EUDI Wallet
   ↓
authentification
   ↓
infrastructures de paiement
```

Le Business Wallet ajoute désormais une autre branche officiellement prévue :

```
EUDI Wallet / identité européenne
   ↓
European Business Wallet
   ↓
identité de l'entreprise / attributs vérifiables
   ↓
TVA / données de transaction / facturation / reporting
```

AVÉRÉ :

> L'infrastructure européenne d'identité constitue donc désormais un point commun documenté entre, d'une part, les mécanismes d'identification des opérateurs économiques et de facturation et, d'autre part, les infrastructures de paiement étudiées dans le chapitre précédent.

Cette constatation ne suffit pas à démontrer un échange direct de données entre facturation et paiement.

Elle établit cependant que ces domaines ne reposent plus nécessairement sur des infrastructures totalement indépendantes.

Une interconnexion ne nécessite pas nécessairement une base centrale commune

Le fonctionnement envisagé repose sur des attestations, identifiants et échanges vérifiables entre acteurs.

Une entreprise peut donc prouver une information à un autre système sans qu'une base centrale unique regroupe nécessairement toutes les informations concernées.

Ce principe rejoint plusieurs architectures étudiées précédemment :

```
information détenue par un système
   ↓
attestation ou preuve vérifiable
   ↓
présentation à un autre système
   ↓
vérification
   ↓
utilisation du résultat
```

DÉDUCTIBLE TECHNIQUEMENT :

> L'interopérabilité entre plusieurs infrastructures peut donc reposer sur l'échange d'attestations et de preuves vérifiables plutôt que sur la centralisation de toutes les données dans une base commune.

Ce que ce raccord ne démontre pas

L'existence des European Business Wallets ne permet pas d'affirmer que :

- les données françaises de facturation électronique seront automatiquement copiées dans un Business Wallet ;
- toutes les données de transaction seront accessibles à toutes les administrations ;
- les informations détenues dans un Business Wallet seront automatiquement transmises à une banque ou à l'Eurosystème ;
- une donnée environnementale sera utilisée comme condition de paiement ;
- l'EUDI Wallet permettra à lui seul de relier nominativement toutes les transactions économiques d'une entreprise ou d'une personne.

NON ÉTABLI :

> Aucun élément étudié ne démontre à ce stade une transmission automatique des données de facturation ou de transaction contenues ou vérifiées par un Business Wallet vers la couche de conditionnalité d'un paiement en euro numérique.

Mais la séparation institutionnelle entre plusieurs infrastructures se réduit

Le résultat de cette section est néanmoins important.

Avant l'étude des European Business Wallets, les infrastructures relatives à l'identité, à la facturation, aux données fiscales et aux paiements pouvaient encore être représentées comme plusieurs systèmes disposant essentiellement de raccords séparés.

La proposition de la Commission introduit une infrastructure transversale destinée précisément à permettre l'identification des opérateurs et l'échange sécurisé de données et d'attestations entre plusieurs de ces environnements.

AVÉRÉ :

> European Business Wallet ↔ EUDI Wallet S30

AVÉRÉ :

> European Business Wallet ↔ identité et attributs fiscaux de l'entreprise S30

AVÉRÉ :

> European Business Wallet ↔ ViDA S30

AVÉRÉ :

> European Business Wallet ↔ attestations TVA S30

AVÉRÉ :

> European Business Wallet ↔ données de transaction S30

AVÉRÉ :

> European Business Wallet ↔ reporting numérique / facturation de confiance S30

Ces raccords sont explicitement décrits dans les documents de la Commission.

Conclusion intermédiaire

AVÉRÉ :

> Les European Business Wallets sont conçus comme une infrastructure transversale permettant aux entreprises et administrations de s'identifier, s'authentifier et échanger des données et attestations vérifiables S30.

AVÉRÉ :

> Leur architecture est explicitement articulée avec le cadre EUDI et permet l'utilisation d'attributs fiscaux et économiques vérifiables S30.

AVÉRÉ :

> La Commission prévoit explicitement leur articulation avec ViDA ainsi que le stockage et l'échange vérifiable d'attestations TVA et de données de transaction afin de soutenir le reporting en temps réel et la facturation de confiance S30.

DÉDUCTIBLE TECHNIQUEMENT :

> Cette infrastructure fournit donc un mécanisme intermédiaire permettant à plusieurs systèmes économiques et administratifs de vérifier et réutiliser certaines informations relatives à une même entreprise sans nécessiter une base de données centrale commune.

NON ÉTABLI :

> Aucun élément étudié ne démontre encore qu'une donnée issue de cette infrastructure soit utilisée pour conditionner un paiement en euro numérique.

Un autre raccord doit maintenant être examiné.

La Commission associe également explicitement les European Business Wallets au **Digital Product Passport**.

5.3 Business Wallets, Digital Product Passport et infrastructures européennes

Statut : AVÉRÉ / PROJET EN COURS / DÉDUCTIBLE TECHNIQUEMENT / À ÉTABLIR

L'analyse des European Business Wallets fait apparaître un raccord supplémentaire avec le Digital Product Passport étudié dans le chapitre 3.

Ce rapprochement ne résulte pas uniquement de la compatibilité technique des deux infrastructures.

La proposition relative aux European Business Wallets mentionne explicitement le Digital Product Passport parmi les dispositifs avec lesquels des synergies sont recherchées S30.

La stratégie européenne pour le marché unique va plus loin en présentant le Digital Product Passport, l'eInvoicing, le futur European Business Wallet et plusieurs autres infrastructures comme les composants d'un même écosystème cohérent de solutions numériques destiné à créer des synergies S31.

Business Wallet → Digital Product Passport

La proposition de règlement relative aux European Business Wallets décrit explicitement leur articulation avec le Digital Product Passport S30.

La Commission rappelle que le DPP dépend d'un accès fiable aux données relatives notamment à la conformité et à la durabilité des produits.

Elle indique que les Business Wallets peuvent notamment :

- prouver l'identité juridique d'un opérateur économique ;
- prouver les droits d'accès qui lui ont été accordés ;
- permettre la signature et le scellement de déclarations de conformité ;
- permettre l'échange sécurisé et vérifiable de données relatives aux produits entre différents acteurs et États membres S30.

AVÉRÉ :

> La Commission prévoit explicitement une articulation entre European Business Wallets et Digital Product Passport afin de permettre l'identification des opérateurs, la vérification des droits d'accès et l'échange sécurisé et vérifiable de données relatives aux produits S30.

La chaîne suivante est donc documentée :

```
opérateur économique
   ↓
European Business Wallet
   ↓
identité juridique / droits d'accès
   ↓
Digital Product Passport
   ↓
données de conformité / durabilité / produit
```

Le raccord concerne notamment les données de durabilité

Ce point est particulièrement important pour l'objet de cette enquête.

Le rapprochement entre Business Wallet et DPP n'est pas présenté uniquement comme un mécanisme permettant d'identifier une entreprise.

La Commission mentionne explicitement l'accès aux données de **conformité et de durabilité** associées au Digital Product Passport S30.

AVÉRÉ :

> L'infrastructure Business Wallet est donc explicitement envisagée comme un mécanisme pouvant contribuer à l'accès sécurisé et vérifiable aux données de durabilité associées aux produits dans l'écosystème DPP S30.

Cela ne signifie pas que toutes les données environnementales d'un produit soient automatiquement transférées dans le Business Wallet.

Le wallet peut notamment intervenir comme infrastructure permettant de prouver l'identité, les droits d'accès et l'authenticité des échanges.

Business Wallet → DPP et Business Wallet → ViDA

La section précédente a établi séparément :

```
European Business Wallet
   ↓
ViDA
   ↓
attestations TVA / données de transaction / reporting / facturation
```

La présente section établit maintenant :

```
European Business Wallet
   ↓
Digital Product Passport
   ↓
données produit / conformité / durabilité
```

AVÉRÉ :

> Une même infrastructure européenne est donc explicitement articulée, d'une part, avec des données de transaction et de facturation et, d'autre part, avec le Digital Product Passport et ses données relatives aux produits S30.

Ce constat constitue un rapprochement institutionnel entre deux ensembles étudiés séparément dans les chapitres précédents.

Il ne démontre pas encore qu'une donnée précise issue d'une facture soit automatiquement rapprochée d'une donnée précise issue d'un DPP.

La Commission présente ces infrastructures comme un même écosystème numérique

La stratégie pour le marché unique adoptée en mai 2025 permet de dépasser la simple observation selon laquelle plusieurs projets européens évolueraient parallèlement S31.

La Commission regroupe notamment :

- le Single Digital Gateway ;
- le Once-Only Technical System ;
- le Digital Product Passport ;
- l'eInvoicing ;
- le futur European Business Wallet ;
- le Business Register Interconnection System ;
- l'identifiant européen unique des entreprises ;
- ainsi que d'autres initiatives destinées à simplifier l'échange de données et le reporting numérique S31.

Elle indique que ces outils doivent collectivement constituer un **écosystème cohérent de solutions numériques** et créer des synergies facilitant les activités économiques dans l'Union européenne S31.

AVÉRÉ :

> La Commission européenne ne présente donc pas le DPP, l'eInvoicing et le Business Wallet comme des infrastructures nécessairement isolées : elle les inscrit explicitement dans un même écosystème numérique destiné à créer des synergies S31.

Ce point modifie la qualification de l'analyse.

L'existence d'une convergence entre ces infrastructures ne relève plus uniquement d'une déduction fondée sur leur compatibilité technique.

AVÉRÉ :

> Une stratégie institutionnelle d'interopérabilité et de création de synergies entre plusieurs de ces infrastructures est explicitement documentée S31.

---

eInvoicing → réutilisation des données

La stratégie identifie également un obstacle à l'automatisation complète des processus économiques : la faible réutilisation des données issues de la facturation électronique dans d'autres processus S31.

La Commission cherche donc explicitement à augmenter cette réutilisation.

Sa documentation relative à l'eInvoicing indique que la facturation électronique doit permettre l'automatisation d'un ensemble plus large de processus comprenant notamment :

- le reporting TVA ;
- certaines procédures douanières ;
- le reporting environnemental, social et de gouvernance, ou ESG S31.

AVÉRÉ :

> Les données de facturation électronique ne sont donc pas envisagées uniquement pour produire, transmettre et comptabiliser une facture : leur réutilisation dans d'autres processus numériques fait explicitement partie de la stratégie européenne S31.

---

eInvoicing → reporting de durabilité

La Commission prévoit plus précisément de tester la réutilisation des données issues de l'eInvoicing pour le **reporting de durabilité** S31.

AVÉRÉ / PROJET PRÉVU :

> La stratégie européenne prévoit un pilote consacré à la réutilisation des données de facturation électronique pour le reporting de durabilité S31.

Ce raccord est particulièrement important pour la cartographie étudiée dans cette enquête.

Jusqu'ici, la relation suivante était seulement techniquement déductible :

```
données de transaction
   ↓
produit
   ↓
donnée environnementale
```

La stratégie introduit désormais un raccord institutionnel supplémentaire :

```
données d'eInvoicing
   ↓
réutilisation
   ↓
reporting de durabilité
```

Cela ne signifie pas qu'une empreinte carbone individuelle soit calculée à partir des factures.

Cela établit en revanche que la réutilisation de données de facturation à des fins liées à la durabilité fait explicitement partie des travaux annoncés par la Commission.

---

eInvoicing → données douanières

La même stratégie prévoit également d'améliorer la transparence douanière en reliant les données d'eInvoicing aux données douanières, en cohérence avec le développement de l'EU Customs Data Hub S31.

AVÉRÉ / PROJET PRÉVU :

> La Commission prévoit explicitement un rapprochement entre données de facturation électronique et données douanières S31.

La chaîne devient :

```
eInvoicing
   ↓
données structurées de transaction
   ↓
rapprochement avec les données douanières
   ↓
EU Customs Data Hub
```

Ce rapprochement rejoint les éléments du chapitre 3 relatifs aux infrastructures de traçabilité, au DPP et aux systèmes douaniers.

Il ne démontre cependant pas que toutes ces données soient déjà réunies dans un même système.

Plusieurs raccords auparavant hypothétiques deviennent institutionnellement documentés

Après les sections 5.2 et 5.3, la cartographie peut désormais être complétée :

```
EUDI / identité numérique
   ↓
European Business Wallet
```

```
European Business Wallet
   ↓
ViDA / TVA / données de transaction / facturation
```

```
European Business Wallet
   ↓
Digital Product Passport / données produit / conformité / durabilité
```

```
eInvoicing
   ↓
réutilisation prévue pour le reporting de durabilité
```

```
eInvoicing
   ↓
rapprochement prévu avec les données douanières
```

```
DPP + eInvoicing + Business Wallet + autres infrastructures
   ↓
écosystème numérique cohérent et création de synergies
```

AVÉRÉ :

> Les documents de la Commission établissent donc désormais des liens institutionnels explicites entre plusieurs infrastructures étudiées séparément dans les chapitres précédents S30-S31.

Ce que cela change dans l'enquête

Au terme du chapitre 3, le rapprochement entre données de transaction et données environnementales reposait principalement sur une possibilité technique :

```
identifier le produit dans une transaction
   ↓
retrouver son DPP
   ↓
accéder à la donnée environnementale correspondante
```

Les éléments étudiés dans cette section ajoutent désormais trois faits distincts :

AVÉRÉ :

> La Commission prévoit une articulation entre Business Wallet et DPP pour l'identité, les droits d'accès et l'échange sécurisé de données produit, notamment de conformité et de durabilité S30.

AVÉRÉ :

> La même infrastructure Business Wallet est articulée avec ViDA, les attestations TVA et les données de transaction S30.

AVÉRÉ / PROJET PRÉVU :

> La Commission prévoit de tester directement la réutilisation des données d'eInvoicing pour le reporting de durabilité S31.

La proximité entre données de transaction et données de durabilité n'est donc plus seulement le résultat d'un assemblage théorique réalisé dans cette enquête.

AVÉRÉ :

> La Commission européenne travaille explicitement sur la réutilisation et l'interopérabilité de ces catégories de données au sein d'un écosystème numérique commun S30-S31.

Ce que cela ne démontre toujours pas

Ces éléments ne permettent pas d'affirmer que :

- chaque ligne de facture sera automatiquement rapprochée d'un DPP ;
- chaque produit acheté sera associé à son empreinte carbone dans une base centrale ;
- une administration calculera une empreinte environnementale individuelle à partir des factures ;
- les données de durabilité seront transmises aux banques ou à l'Eurosystème ;
- une donnée environnementale issue d'un DPP sera utilisée comme condition d'un paiement ;
- le reporting de durabilité envisagé concerne un profil environnemental individuel des consommateurs.

NON ÉTABLI :

> Le raccord spécifique entre donnée environnementale d'un produit et couche de conditionnalité d'un paiement reste à démontrer.

Une chaîne institutionnelle apparaît néanmoins

Sans transformer les éléments précédents en preuve d'un usage qui n'est pas documenté, une chaîne institutionnelle plus précise peut désormais être représentée :

```
eInvoicing / données de transaction*
   ↓
réutilisation prévue des données
   ↘ reporting de durabilité
     ↘ **données douanières / EU Customs Data Hub
```

parallèlement :

```
      European Business Wallet
    ↙                         ↘
ViDA / transaction     DPP / produit / durabilité
```

le tout inscrit par la Commission dans :

un écosystème cohérent de solutions numériques destiné à créer des synergies

AVÉRÉ :

> L'existence d'une stratégie de rapprochement et de réutilisation des données entre plusieurs de ces infrastructures est désormais explicitement documentée S30-S31.

DÉDUCTIBLE TECHNIQUEMENT :

> Une infrastructure capable d'identifier l'opérateur, de vérifier ses droits d'accès et d'échanger des données produit peut servir de couche d'interopérabilité entre des systèmes de transaction et des systèmes contenant des informations de durabilité, lorsque les règles applicables autorisent cet échange.

Conclusion intermédiaire

AVÉRÉ :

> Les European Business Wallets sont explicitement articulés avec le Digital Product Passport et peuvent intervenir dans l'identification des opérateurs, la vérification des droits d'accès et l'échange sécurisé et vérifiable de données relatives aux produits, notamment de conformité et de durabilité S30.

AVÉRÉ :

> Les European Business Wallets sont parallèlement articulés avec ViDA, les attestations TVA et les données de transaction S30.

AVÉRÉ :

> La Commission inscrit le DPP, l'eInvoicing, le Business Wallet et plusieurs autres infrastructures dans un même écosystème cohérent de solutions numériques destiné à créer des synergies S31.

AVÉRÉ / PROJET PRÉVU :

> La Commission prévoit de tester la réutilisation des données d'eInvoicing pour le reporting de durabilité S31.

AVÉRÉ / PROJET PRÉVU :

> La Commission prévoit également de rapprocher les données d'eInvoicing des données douanières en lien avec l'EU Customs Data Hub S31.

DÉDUCTIBLE TECHNIQUEMENT :

> Ces mécanismes réduisent la distance technique et institutionnelle entre données décrivant une transaction, données décrivant un produit et données relatives à sa durabilité.

NON ÉTABLI :

> Aucun élément étudié ne démontre encore qu'une donnée environnementale provenant d'un DPP soit transmise à une infrastructure de paiement afin d'autoriser ou de refuser une transaction.

La question n'est désormais plus seulement de savoir si ces infrastructures peuvent communiquer.

La Commission documente elle-même leur interopérabilité, leur réutilisation et les synergies recherchées.

Il reste à déterminer **par quels identifiants, standards et API ces rapprochements peuvent concrètement être réalisés**.

5.4 Identifiants, standards et API communs

Statut : AVÉRÉ / DÉDUCTIBLE TECHNIQUEMENT / À ÉTABLIR

Les sections précédentes ont établi que la Commission européenne recherche explicitement des synergies entre plusieurs infrastructures numériques relatives à la facturation, aux entreprises, aux produits et à leur durabilité.

L'existence d'une volonté d'interopérabilité ne suffit cependant pas à démontrer qu'un rapprochement de données peut effectivement être réalisé.

Pour qu'une interconnexion fonctionne, plusieurs conditions techniques doivent généralement être réunies : les systèmes doivent pouvoir identifier les objets ou acteurs concernés, comprendre les données échangées, vérifier les droits d'accès et disposer d'interfaces permettant les échanges automatisés.

Les infrastructures étudiées disposent déjà de plusieurs de ces composants.

---

eInvoicing → modèle sémantique commun

AVÉRÉ :

> Le standard européen EN 16931 définit un modèle sémantique commun permettant aux systèmes émetteurs et récepteurs de comprendre et traiter automatiquement les informations contenues dans une facture électronique S32.

L'objectif du standard est précisément de réduire les différences entre formats et systèmes nationaux afin de permettre l'interopérabilité.

La chaîne technique générale est donc :

```
système de facturation A
   ↓
données structurées selon un modèle sémantique commun
   ↓
système de facturation B
```

La donnée n'est plus seulement destinée à être lue par une personne.

Elle est structurée afin de pouvoir être interprétée automatiquement par différents systèmes.

EN 16931 évolue vers d'autres usages de données

Les travaux européens de standardisation ne concernent plus uniquement l'échange traditionnel d'une facture entre fournisseur et client.

Le plan européen de standardisation 2026 prévoit de maintenir EN 16931 en cohérence avec ViDA et d'intégrer les besoins résultant de différentes politiques européennes.

Parmi les domaines explicitement mentionnés figurent :

- le reporting fiscal ;
- le reporting de durabilité ;
- les douanes ;
- d'autres processus automatisés.

AVÉRÉ :

> L'évolution du standard européen de facturation prend explicitement en compte des besoins provenant du reporting fiscal, du reporting de durabilité et des procédures douanières S32.

Cette évolution est cohérente avec les projets de réutilisation des données d'eInvoicing identifiés dans la section précédente.

Elle ne signifie pas que toutes les données nécessaires à ces usages soient déjà présentes dans chaque facture.

DPP → identifiant unique et persistant du produit

Le règlement européen relatif à l'écoconception impose qu'un Digital Product Passport soit relié à un **identifiant unique persistant du produit** S15-S32.

Cet identifiant est associé à un support de données permettant d'accéder au passeport.

AVÉRÉ :

> Le DPP repose donc sur un mécanisme permettant à différents systèmes de désigner de manière persistante le même produit, modèle ou lot selon les règles applicables S15-S32.

La chaîne est :

```
produit
   ↓
identifiant unique persistant
   ↓
Digital Product Passport
```

Ce mécanisme constitue une condition essentielle à tout rapprochement automatisé entre un produit physique et ses informations numériques.

DPP → standards ouverts et données interopérables

Le règlement impose également que les données du Digital Product Passport reposent sur des standards ouverts et soient, selon les cas :

- lisibles par machine ;
- structurées ;
- recherchables ;
- transférables ;
- accessibles au moyen d'un réseau ouvert et interopérable d'échange de données S15-S32.

AVÉRÉ :

> L'interopérabilité du DPP constitue donc une exigence réglementaire de son architecture et non une simple fonctionnalité facultative S15-S32.

Le système est conçu pour permettre l'utilisation automatisée des données par différents acteurs autorisés.

Le registre DPP dispose d'une API

Le règlement d'exécution (UE) 2026/1778 précise l'architecture du registre européen du Digital Product Passport S20-S32.

Le registre comprend notamment :

- une interface utilisateur sécurisée ;
- une API permettant l'enregistrement des Digital Product Passports et la réception d'informations provenant du registre ;
- une plateforme de vérification ;
- un mécanisme d'identification et d'autorisation des utilisateurs ;
- un système générant des identifiants uniques d'enregistrement ;
- un référentiel sémantique ;
- un système de journalisation S20-S32.

AVÉRÉ :

> Le registre DPP dispose donc d'une interface machine-to-machine explicitement conçue pour permettre des interactions automatisées avec d'autres systèmes S20-S32.

La chaîne suivante est directement prévue :

```
système externe autorisé
   ↓
API
   ↓
registre DPP
   ↓
enregistrement / vérification / informations
```

Le référentiel sémantique facilite la compréhension entre systèmes

Le registre DPP comprend également un référentiel sémantique destiné à définir de manière autoritative la signification, la structure, les versions et les exigences d'interopérabilité des données du passeport S20-S32.

AVÉRÉ :

> Le dispositif ne fournit donc pas seulement une interface technique permettant de transmettre des données ; il prévoit également une couche sémantique permettant aux systèmes de comprendre de manière cohérente les informations échangées S20-S32.

Deux conditions nécessaires à une interconnexion automatisée sont ainsi réunies :

```
interface technique commune
   +
compréhension sémantique commune
```

Le registre associe produit et opérateur économique vérifié

Le règlement d'exécution impose également la vérification des opérateurs économiques et des autres acteurs de la chaîne de valeur intervenant dans le registre S20-S32.

Lorsqu'un DPP est enregistré, le registre peut notamment associer :

- l'identifiant unique du produit ;
- l'identité de l'opérateur économique vérifié responsable ;
- certaines informations nécessaires à l'enregistrement ;
- un identifiant unique d'enregistrement S20-S32.

Une preuve électronique d'enregistrement peut également être générée.

AVÉRÉ :

> Le registre DPP établit donc une relation vérifiable entre un produit identifiable et un opérateur économique identifiable S20-S32.

La chaîne devient :

```
opérateur économique vérifié
   ↓
produit identifiable
   ↓
DPP
   ↓
identifiant d'enregistrement / preuve vérifiable
```

Les mécanismes d'identité numérique peuvent participer à la vérification des opérateurs

Le règlement d'exécution prévoit plusieurs mécanismes permettant de vérifier l'identité des opérateurs économiques.

Ils comprennent notamment, selon les situations, des moyens d'identification électronique conformes au cadre eIDAS ainsi que des attestations électroniques d'attributs S20-S32.

AVÉRÉ :

> L'infrastructure DPP et l'infrastructure européenne d'identité numérique partagent donc des mécanismes permettant l'identification ou la vérification des opérateurs économiques S20-S32.

Il ne s'agit pas encore nécessairement d'un raccord direct avec l'EUDI Wallet dans toutes les situations.

Mais l'utilisation du même cadre européen d'identité et d'attestations facilite l'interopérabilité entre ces environnements.

Business Wallet → attestations vérifiables

Les European Business Wallets reposent également sur des données et attestations électroniques vérifiables S30-S32.

Ces attestations peuvent représenter différents attributs relatifs à l'entreprise, à ses représentants, à ses rôles ou à ses autorisations.

L'architecture prévoit notamment :

- des formats structurés d'attributs ;
- des mécanismes de vérification ;
- la gestion des mandats et délégations ;
- des contrôles d'accès ;
- la traçabilité des autorisations ;
- des preuves cryptographiquement vérifiables S30-S32.

AVÉRÉ :

> Les échanges entre infrastructures ne reposent donc pas uniquement sur la transmission de données brutes mais peuvent également reposer sur la présentation et la vérification d'attestations numériques S30-S32.

Business Wallet → contrôle d'accès interopérable

La proposition prévoit des mécanismes permettant de déterminer en temps réel si un acteur possède les droits nécessaires pour accéder à une donnée ou exécuter une procédure S30-S32.

Les autorisations doivent notamment pouvoir être :

- vérifiées ;
- auditées ;
- révoquées ;
- tracées jusqu'à leur émetteur ;
- utilisées de manière interopérable entre États membres.

AVÉRÉ :

> L'interopérabilité recherchée concerne donc également les droits permettant d'accéder aux données et services, et pas uniquement les formats de données S30-S32.

Ce point est essentiel pour l'analyse des interconnexions.

Un système peut techniquement disposer d'une API permettant d'accéder à une donnée tout en empêchant cet accès lorsque l'acteur ne possède pas l'autorisation correspondante.

Business Wallet → European Digital Directory → API

La proposition relative aux European Business Wallets prévoit également la création d'un **European Digital Directory** S30-S32.

Ce répertoire doit comporter deux interfaces :

- un portail destiné aux utilisateurs ;
- une interface lisible par machine exposée au moyen d'une API pour les communications automatisées entre systèmes.

AVÉRÉ :

> L'écosystème Business Wallet prévoit donc lui aussi une interface machine-to-machine permettant la découverte et l'interaction automatisée entre acteurs et systèmes S30-S32.

La structure générale devient :

```
acteur / système
   ↓
European Digital Directory
   ↓
API
   ↓
identification / découverte / interaction avec l'acteur concerné
```

Les mêmes principes techniques apparaissent dans plusieurs infrastructures

Les systèmes étudiés ne reposent pas nécessairement sur les mêmes bases de données ni sur un identifiant universel unique.

Ils utilisent cependant des principes techniques convergents :

Infrastructure	Identification	Données structurées	Sémantique	API / échange automatisé	Autorisation
eInvoicing	entreprises / références de transaction	oui	EN 16931	échanges électroniques	selon systèmes
DPP	produit / opérateur	oui	référentiel sémantique	API du registre	oui
Business Wallet	entreprise / rôles / mandats	oui	attestations / vocabulaires	API / interfaces	oui
EUDI	personne / attributs	oui	attestations vérifiables	protocoles d'échange	oui
euro numérique	utilisateurs / PSP / transactions	oui	modèle de données	interfaces de paiement	oui

AVÉRÉ :

> Plusieurs infrastructures européennes utilisent donc simultanément des identifiants structurés, des modèles de données interprétables automatiquement, des mécanismes d'autorisation et des interfaces destinées aux échanges machine-to-machine S20-S25-S29-S30-S32.

L'Union européenne recherche explicitement l'interopérabilité entre ces systèmes

Cette convergence technique n'est pas uniquement accidentelle.

La Commission indique plus largement vouloir assurer une interopérabilité transfrontalière entre les solutions numériques publiques telles que :

- l'eInvoicing ;
- la signature électronique ;
- les soumissions électroniques ;
- le Digital Product Passport.

Elle présente parallèlement le European Business Wallet comme un élément central permettant aux entreprises d'interagir numériquement avec les administrations.

AVÉRÉ :

> La stratégie européenne recherche explicitement une interopérabilité entre plusieurs catégories de systèmes étudiées dans cette enquête S30-S31-S32.

Une convergence sémantique est également en cours pour les Business Wallets

Les travaux techniques relatifs aux European Business Wallets comprennent désormais le développement d'un vocabulaire sémantique destiné aux attestations électroniques utilisées dans les différents cas d'usage.

Ces travaux s'appuient notamment sur des standards de credentials vérifiables et sur des formats destinés à permettre l'interopérabilité des attributs.

AVÉRÉ / TRAVAUX EN COURS :

> La construction de l'écosystème Business Wallet comprend donc également une couche destinée à harmoniser la signification des données et attributs échangés entre systèmes.

Cette évolution rapproche son fonctionnement du principe déjà observé dans EN 16931 et dans le référentiel sémantique du DPP.

Existe-t-il un identifiant universel reliant automatiquement toutes les infrastructures ?

À ce stade, les sources étudiées ne permettent pas d'établir l'existence d'un identifiant unique universel qui serait présent simultanément dans :

```
facture
   +
DPP
   +
Business Wallet
   +
identité
   +
paiement
```

NON ÉTABLI :

> Aucun identifiant universel permettant de joindre automatiquement toutes les infrastructures étudiées n'a été identifié.

Cette absence est importante.

Elle empêche d'affirmer qu'un rapprochement complet serait automatique ou systématique.

Un identifiant universel n'est cependant pas techniquement indispensable

Une interconnexion entre systèmes ne nécessite pas obligatoirement qu'ils utilisent tous exactement le même identifiant.

Des mécanismes de correspondance peuvent relier plusieurs identifiants.

Par exemple :

```
identifiant entreprise dans le système A
   ↓
identité ou attestation vérifiable
   ↓
correspondance avec l'entreprise dans le système B
```

ou :

```
référence de produit dans une transaction
   ↓
mécanisme de correspondance
   ↓
identifiant unique du DPP
   ↓
informations relatives au produit
```

DÉDUCTIBLE TECHNIQUEMENT :

> Des attestations, référentiels ou services intermédiaires peuvent permettre de résoudre les correspondances entre plusieurs systèmes sans imposer un identifiant universel commun à l'ensemble de l'architecture.

C'est précisément l'une des fonctions que peuvent remplir des infrastructures d'identité, des registres ou des services d'interopérabilité.

Une API commune unique n'est pas davantage nécessaire

La même distinction s'applique aux interfaces.

Il n'est pas nécessaire qu'une seule API relie directement :

> facturation → DPP → Business Wallet → paiement

Une architecture distribuée peut fonctionner sous la forme :

```
système A
   ↓ API
service intermédiaire
   ↓ API
système B
   ↓ résultat vérifiable
système C
```

Cette logique est déjà observée dans les architectures étudiées précédemment.

DÉDUCTIBLE TECHNIQUEMENT :

> L'absence d'une API unique reliant directement toutes les infrastructures ne permet donc pas, à elle seule, de conclure à l'absence d'interconnexion.

La question des droits d'accès reste déterminante

La possibilité technique de rapprocher plusieurs données ne signifie pas que ce rapprochement soit juridiquement ou opérationnellement autorisé.

Les architectures DPP, EUDI et Business Wallet comprennent précisément des mécanismes destinés à contrôler les droits d'accès et les informations pouvant être communiquées.

AVÉRÉ :

> L'interopérabilité technique et l'autorisation d'accéder aux données constituent deux questions distinctes S20-S29-S30-S32.

Une chaîne peut donc être techniquement réalisable tout en restant juridiquement interdite ou inaccessible à certains acteurs.

Ce que cette section permet désormais d'établir

Après les sections précédentes, il était établi que la Commission recherchait des synergies entre plusieurs infrastructures.

Cette section montre que les principaux composants techniques permettant de réaliser de telles synergies existent également :

```
**identifiants**
   ↓
désigner les acteurs, produits et transactions

**modèles sémantiques**
   ↓
comprendre automatiquement les données

**attestations vérifiables**
   ↓
prouver une information sans nécessairement transférer toutes les données sources

**mécanismes d'autorisation**
   ↓
déterminer qui peut accéder à quoi

**API et interfaces machine-to-machine**
   ↓
permettre les échanges automatisés

**registres et répertoires**
   ↓
retrouver et vérifier les acteurs, produits ou services
```

AVÉRÉ :

> Ces composants existent dans plusieurs des infrastructures étudiées et sont explicitement développés dans une logique d'interopérabilité S20-S30-S32.

Conclusion intermédiaire

AVÉRÉ :

> L'eInvoicing repose sur un modèle sémantique européen commun destiné à permettre le traitement automatisé et interopérable des factures S32.

AVÉRÉ :

> Le DPP repose sur des identifiants uniques persistants, des données structurées et interopérables, une API, un référentiel sémantique et des mécanismes d'identification et d'autorisation S15-S20-S32.

AVÉRÉ :

> Les European Business Wallets reposent sur des attestations vérifiables, des mécanismes d'autorisation interopérables et des interfaces destinées aux communications automatisées entre systèmes S30-S32.

AVÉRÉ :

> Les politiques européennes de standardisation cherchent explicitement à rapprocher l'eInvoicing des besoins liés notamment au reporting fiscal, au reporting de durabilité et aux douanes S32.

DÉDUCTIBLE TECHNIQUEMENT :

> Les composants nécessaires à la construction de passerelles automatisées entre plusieurs infrastructures existent donc : identification, résolution de correspondances, sémantique commune, contrôle d'accès, attestations vérifiables et API.

NON ÉTABLI :

> Aucun identifiant universel ou API unique reliant automatiquement facturation, DPP, identité et paiement n'est établi par les sources étudiées.

La recherche d'une interconnexion ne peut donc pas se limiter à chercher une base de données, un identifiant ou une API unique.

Une architecture distribuée peut relier plusieurs systèmes au moyen de services intermédiaires, d'attestations, de correspondances d'identifiants et d'interfaces successives.

La prochaine étape consiste donc à rechercher si **les mêmes acteurs, consortiums et projets pilotes interviennent effectivement dans plusieurs de ces infrastructures**.

5.5 Acteurs, consortiums et expérimentations communes

Statut : AVÉRÉ / INDICE D'INTERCONNEXION / À ÉTABLIR

L'existence d'acteurs communs à plusieurs infrastructures ne démontre pas, à elle seule, que des données circulent entre ces infrastructures.

Elle constitue cependant un élément pertinent lorsque ces acteurs participent concrètement à la conception, à l'intégration ou à l'expérimentation de plusieurs systèmes étudiés dans cette enquête.

L'analyse des projets européens relatifs à l'euro numérique, à l'identité numérique et aux Business Wallets montre que ces travaux ne sont pas conduits uniquement par des institutions publiques indépendantes les unes des autres.

Ils associent également des banques, prestataires de paiement, entreprises technologiques, opérateurs économiques, fournisseurs de wallets et intégrateurs intervenant dans plusieurs écosystèmes S33.

Digital Euro Innovation Platform → acteurs privés

En 2025, la Banque centrale européenne a créé une plateforme d'innovation réunissant environ 70 participants du marché afin d'expérimenter des fonctionnalités et cas d'usage relatifs à l'euro numérique S28-S33.

Les participants comprennent notamment :

- des banques ;
- des prestataires de services de paiement ;
- des fintechs ;
- des entreprises technologiques ;
- des acteurs du commerce ;
- des fournisseurs d'infrastructures et de services numériques.

AVÉRÉ :

> La conception et l'expérimentation des services pouvant être développés autour de l'euro numérique associent directement des acteurs privés provenant de plusieurs secteurs économiques S28-S33.

Ces acteurs ne se limitent donc pas à observer le projet.

Dans le cadre du volet « pioneers », ils ont pu connecter leurs propres plateformes à l'environnement simulé fourni par la BCE afin d'expérimenter différentes fonctionnalités S28.

Plusieurs grands acteurs financiers et technologiques participent à l'expérimentation de l'euro numérique

La liste publiée par la BCE comprend notamment :

- Accenture ;
- CaixaBank ;
- equensWorldline ;
- KPMG ;
- SAP Fioneer ;
- Tata Consultancy Services ;
- Infineon ;
- plusieurs banques et prestataires européens de paiement S33.

Un consortium appelé **Digi-Trade** participe également aux deux volets de l'Innovation Platform.

Il réunit :

- Amazon ;
- CargoX ;
- Deutsche Bank ;
- Stripe ;
- Swift S33.

AVÉRÉ :

> Des acteurs majeurs du commerce électronique, de la banque, du paiement, de la messagerie financière et des infrastructures technologiques participent donc conjointement à l'expérimentation de services reposant sur l'environnement de l'euro numérique S33.

Cette participation ne démontre pas que leurs infrastructures commerciales existantes seront automatiquement reliées à l'euro numérique.

Elle établit en revanche qu'ils disposent d'un accès direct aux travaux expérimentaux permettant d'évaluer et de développer de futurs services autour de cette infrastructure.

WE BUILD → un consortium transversal

Le Large Scale Pilot **WE BUILD** constitue un autre élément important S33.

Ce projet européen rassemble plus de 200 organisations issues de plusieurs dizaines de pays.

Il comprend notamment :

- des autorités publiques ;
- des registres d'entreprises ;
- des administrations fiscales ;
- des banques et institutions financières ;
- des fournisseurs de wallets et services de confiance ;
- des entreprises technologiques ;
- des PME ;
- des organismes de recherche S33.

AVÉRÉ :

> Un même consortium européen réunit donc des acteurs publics, fiscaux, financiers, technologiques et économiques afin de développer et tester des infrastructures interopérables reposant sur l'EUDI Wallet et les European Business Wallets S33.

WE BUILD ne traite pas uniquement d'identité

La documentation officielle relative aux Large Scale Pilots présente WE BUILD comme un projet consacré à des cas d'usage relatifs aux entreprises **et aux paiements** S33.

Son architecture répartit les travaux entre plusieurs domaines.

Parmi eux figurent notamment :

Business
identité d'entreprise / représentation / partage de données

Supply Chain
processus relatifs aux chaînes d'approvisionnement et à la facturation électronique

Payments & Banking
paiements sécurisés / services bancaires / onboarding financier S33

AVÉRÉ :

> Des cas d'usage relatifs à la facturation électronique et des cas d'usage relatifs aux paiements et services bancaires sont donc développés au sein d'un même Large Scale Pilot européen et d'une même architecture générale d'interopérabilité S33.

Ce constat ne démontre pas qu'une facture soit utilisée comme condition d'un paiement.

Il établit cependant que les deux domaines sont expérimentés au sein du même programme technique.

Business Wallet → supply chain → eInvoicing

Le blueprint d'architecture de WE BUILD mentionne explicitement la facturation électronique parmi les processus couverts dans le domaine Supply Chain S33.

Le même projet développe parallèlement des mécanismes relatifs :

- à l'identité des entreprises ;
- aux mandats et représentations ;
- au partage de données ;
- aux relations entre acheteurs et fournisseurs ;
- aux paiements et services bancaires.

AVÉRÉ :

> La facturation électronique, l'identité des entreprises, le partage de données et les paiements ne sont donc plus étudiés uniquement dans des programmes européens séparés : ils apparaissent également comme différents cas d'usage d'un même environnement expérimental S33.

WE BUILD → administrations fiscales

La composition du consortium comprend également des administrations fiscales S33.

L'administration fiscale finlandaise indique par exemple participer directement à WE BUILD afin d'expérimenter :

- la transmission d'informations fiscales au moyen de wallets ;
- les déclarations de TVA transfrontalières ;
- l'émission et la réception de documents fiscaux numériques ;
- différents processus nécessitant des attestations fiscales.

AVÉRÉ :

> Des administrations fiscales participent donc directement à l'expérimentation des Business Wallets et à l'utilisation de données fiscales et d'attestations numériques dans cet environnement S33.

La chaîne expérimentale comprend ainsi :

```
entreprise
   ↓
Business Wallet
   ↓
donnée / attestation fiscale
   ↓
administration fiscale
```

WE BUILD → paiements

WE BUILD dispose également de travaux spécifiquement consacrés aux paiements.

Le consortium a créé en 2026 une communauté dédiée aux paiements afin de présenter et discuter les solutions techniques expérimentées autour des EUDI Wallets et Business Wallets pour les paiements et les services bancaires S33.

AVÉRÉ :

> Les EUDI Wallets et Business Wallets sont donc effectivement expérimentés dans des cas d'usage relatifs aux paiements et aux services bancaires au sein du consortium S33.

Les travaux portent notamment sur les exigences réglementaires, les standards, les architectures techniques et les interactions avec les institutions financières et prestataires de paiement.

Certains acteurs apparaissent dans plusieurs environnements

L'analyse des participants permet d'identifier plusieurs recoupements entre les écosystèmes.

CaixaBank participe à la Digital Euro Innovation Platform de la BCE S33.

La banque apparaît également dans les travaux et événements du consortium WE BUILD consacrés aux wallets et aux paiements.

Worldline, via equensWorldline, participe à la Digital Euro Innovation Platform S33.

Le groupe participe également aux Large Scale Pilots relatifs à l'EUDI Wallet, notamment WE BUILD, dans des travaux liés aux paiements.

Ces recoupements peuvent être représentés ainsi :

```
Digital Euro Innovation Platform
   ↕
acteurs bancaires / PSP / intégrateurs
   ↕
EUDI / WE BUILD
   ↕
Business Wallet / paiements / services bancaires
```

AVÉRÉ :

> Certains acteurs financiers et technologiques interviennent donc effectivement dans plusieurs initiatives européennes relatives à l'identité numérique, aux wallets et aux paiements S33.

Un même acteur dans deux projets ne prouve pas un échange de données

Cette distinction est essentielle.

Une entreprise peut participer simultanément à plusieurs projets européens pour des raisons différentes :

- expertise technique ;
- préparation réglementaire ;
- développement commercial ;
- recherche ;
- standardisation ;
- expérimentation.

NON ÉTABLI :

> La présence d'un acteur dans plusieurs projets ne permet pas d'affirmer que cet acteur transfère des données d'une infrastructure vers une autre.

Par exemple :

```
acteur A participe au projet X
   +
acteur A participe au projet Y
```

ne signifie pas automatiquement :

données du projet X → acteur A → projet Y

Pour établir un tel raccord, il faut identifier un cas d'usage, une interface, un flux, une architecture ou une documentation décrivant effectivement cet échange.

Le cas WE BUILD est plus fort qu'un simple recoupement d'acteurs

WE BUILD présente cependant une différence importante.

Il ne s'agit pas uniquement de constater que les mêmes entreprises participent séparément à plusieurs projets.

Les domaines étudiés sont réunis **dans un même consortium et dans une même architecture d'intégration**.

Le blueprint du projet distingue explicitement :

```
Business
   +
Supply Chain
   +
Payments & Banking [S33](#s33)
```

et prévoit une architecture commune destinée à assurer l'interopérabilité entre les différents cas d'usage.

AVÉRÉ :

> L'identité d'entreprise, le partage de données, les chaînes d'approvisionnement, la facturation électronique et les paiements sont donc testés comme différents composants d'un même écosystème de wallets interopérables S33.

Cette constatation constitue un élément d'interconnexion plus fort que la simple présence d'un acteur commun dans plusieurs programmes.

Un projet européen relie désormais explicitement Business Wallet et paiements

Les European Business Wallets étudiés en 5.2 étaient principalement apparus comme une infrastructure d'identité, d'attestations et d'échange de données pour les entreprises.

WE BUILD montre que cette infrastructure est également expérimentée dans des cas d'usage bancaires et de paiement S33.

La chaîne devient donc :

```
identité de l'entreprise
   ↓
European Business Wallet
   ↓
attestations / données d'entreprise
   ↓
services bancaires / paiements
```

AVÉRÉ :

> Le raccord fonctionnel entre Business Wallet et environnement bancaire ou de paiement fait donc déjà l'objet d'expérimentations dans un Large Scale Pilot financé par l'Union européenne S33.

La facturation et le paiement se trouvent désormais dans le même environnement expérimental

En combinant uniquement les éléments explicitement documentés dans WE BUILD :

```
European Business Wallet
   ↓
identité / représentation / partage de données
```

parallèlement :

```
Supply Chain
   ↓
facturation électronique
```

parallèlement :

```
Payments & Banking
   ↓
paiements / services financiers
```

AVÉRÉ :

> La facturation électronique et les paiements apparaissent donc désormais dans le même programme européen d'expérimentation des wallets S33.

NON ÉTABLI :

> Aucun élément étudié ne permet encore d'affirmer qu'une donnée provenant directement d'une facture électronique est utilisée comme critère d'autorisation ou de refus d'un paiement dans WE BUILD.

Des travaux rapprochent encore davantage identité et paiement

Les expérimentations relatives à l'EUDI Wallet ne sont pas uniquement conceptuelles.

Des travaux menés dans les Large Scale Pilots ont déjà porté sur l'authentification de paiements au moyen du wallet.

WE BUILD poursuit désormais cette trajectoire avec des cas d'usage consacrés aux paiements et services bancaires.

AVÉRÉ :

> L'identité numérique et les infrastructures de paiement font donc l'objet d'expérimentations conjointes impliquant banques, prestataires de paiement, fournisseurs de wallets et entreprises technologiques S29-S33.

La cartographie des acteurs devient transversale

Les projets étudiés font apparaître plusieurs catégories d'acteurs présentes à différents niveaux de l'écosystème :

```
**institutions européennes**
Commission européenne / BCE
   ↓
**administrations nationales**
registres / administrations fiscales / autorités publiques
   ↓
**banques et PSP**
   ↓
**fournisseurs de wallets et services de confiance**
   ↓
**intégrateurs et entreprises technologiques**
   ↓
**entreprises et commerçants**
```

AVÉRÉ :

> Les infrastructures étudiées sont donc développées dans un environnement institutionnel et industriel commun faisant intervenir simultanément acteurs publics, administrations fiscales, banques, prestataires de paiement et entreprises technologiques S33.

Cela ne démontre toujours pas une centralisation des données entre tous ces acteurs.

Cela établit cependant l'existence d'un espace commun de conception, de standardisation et d'expérimentation.

Ce que cela change dans l'enquête

Au début du chapitre 5, plusieurs infrastructures étaient encore reliées principalement par leurs caractéristiques techniques.

Les sections précédentes ont progressivement établi :

```
DPP + eInvoicing + Business Wallet
→ même stratégie européenne d'interopérabilité

eInvoicing
→ réutilisation prévue pour le reporting de durabilité

Business Wallet
→ DPP / données produit / durabilité

Business Wallet
→ ViDA / données de transaction

EUDI Wallet
→ paiement

système externe
→ paiement conditionnel

WE BUILD
→ Business + Supply Chain + eInvoicing + Payments & Banking
```

AVÉRÉ :

> Plusieurs domaines précédemment étudiés séparément se retrouvent désormais au sein de stratégies, architectures et programmes expérimentaux communs S30-S31-S32-S33.

Ce que cela ne permet toujours pas d'affirmer

Même avec ces nouveaux éléments, il n'est pas établi que :

- les données françaises de facturation électronique soient transmises aux infrastructures de paiement ;
- les données d'un DPP soient transmises à une banque ;
- une empreinte carbone soit utilisée dans une décision de paiement ;
- une administration fiscale puisse ordonner automatiquement le refus d'un achat sur la base d'une donnée environnementale ;
- les participants communs aux différents projets organisent un échange de données entre ces infrastructures.

NON ÉTABLI :

> Le raccord opérationnel spécifique environnement → condition de paiement reste à démontrer.

Conclusion intermédiaire

AVÉRÉ :

> La Digital Euro Innovation Platform associe banques, PSP, entreprises technologiques, fintechs et acteurs commerciaux à l'expérimentation de services pouvant être développés autour de l'euro numérique S28-S33.

AVÉRÉ :

> Certains acteurs financiers et technologiques participent à plusieurs initiatives relatives à l'identité numérique, aux wallets et aux paiements S33.

AVÉRÉ :

> WE BUILD réunit plus de 200 organisations publiques et privées et développe dans un même programme des cas d'usage relatifs aux entreprises, aux chaînes d'approvisionnement et aux paiements S33.

AVÉRÉ :

> La facturation électronique figure dans les cas d'usage Supply Chain tandis que les paiements et services bancaires disposent de leur propre domaine au sein du même projet S33.

AVÉRÉ :

> Des administrations fiscales, banques, institutions financières, fournisseurs de wallets et entreprises technologiques participent au même environnement expérimental S33.

AVÉRÉ :

> Le raccord fonctionnel entre Business Wallet, identité d'entreprise et services bancaires ou de paiement fait l'objet d'expérimentations S33.

INDICE D'INTERCONNEXION :

> La présence de plusieurs infrastructures et catégories d'acteurs dans un même programme réduit encore la séparation institutionnelle et technique entre les domaines étudiés, sans démontrer à elle seule qu'une donnée circule effectivement de l'un à l'autre.

NON ÉTABLI :

> Aucun flux opérationnel reliant directement une donnée environnementale issue d'un produit à une condition déterminant l'exécution d'un paiement n'est encore établi.

Les acteurs communs existent.

Les programmes communs existent.

Les architectures d'intégration existent.

Les cas d'usage relatifs à la facturation et aux paiements se trouvent désormais dans le même environnement expérimental.

La prochaine étape consiste donc à ne plus étudier séparément les composants, mais à reconstruire les **chaînes d'interconnexion effectivement documentées de bout en bout**.

5.6 Chaînes d'interconnexion documentées

Statut : AVÉRÉ / EXPÉRIMENTÉ / DÉDUCTIBLE TECHNIQUEMENT / À ÉTABLIR

Les sections précédentes ont identifié séparément des infrastructures interopérables, des identifiants, des API, des wallets, des acteurs communs et des programmes expérimentaux réunissant facturation, identité et paiement.

Il est désormais possible de rechercher non plus seulement des composants compatibles, mais des chaînes dans lesquelles plusieurs de ces composants interviennent effectivement au cours d'une même transaction ou d'un même processus.

Les travaux de WE BUILD permettent d'en documenter plusieurs.

Identité d'entreprise → compte bancaire → paiement → preuve de transaction

Le consortium WE BUILD présente en septembre 2026 une chaîne B2B utilisant l'European Business Wallet comme infrastructure de confiance commune S34.

Le parcours décrit suit une entreprise depuis son identification jusqu'à la preuve de la transaction.

Il comprend notamment :

```
entreprise
   ↓
identité / KYC / KYB transfrontalier
   ↓
European Business Wallet
   ↓
ouverture ou identification du compte bancaire
   ↓
attestation vérifiable d'IBAN
   ↓
paiement utilisant l'IBAN vérifié
   ↓
eReceipt
   ↓
preuve de la transaction
```

AVÉRÉ / EXPÉRIMENTÉ :

> WE BUILD documente donc une chaîne dans laquelle identité numérique d'entreprise, donnée bancaire vérifiée, paiement et justificatif électronique de transaction interviennent dans un même parcours B2B S34.

Ce raccord dépasse la simple présence de cas d'usage distincts dans un même consortium.

Les composants sont ici utilisés successivement dans le même processus transactionnel.

EUDI Wallet → authentification du paiement

Le cas PA4 documenté par un participant au consortium apporte un niveau de détail supplémentaire S34.

Un salarié agit pour le compte d'une entreprise.

Son EUDI Wallet permet de présenter les éléments nécessaires à son authentification et à son autorisation.

Le paiement peut être réalisé depuis un compte ou une carte associés au parcours.

La transaction contient notamment :

- le montant ;
- la devise ;
- le bénéficiaire ;
- le moyen de paiement sélectionné.

L'utilisateur confirme les données de transaction et la banque procède au règlement.

La chaîne expérimentée devient :

```
personne autorisée
   ↓
EUDI Wallet
   ↓
authentification forte
   ↓
données de transaction
   ↓
banque
   ↓
règlement du paiement
```

EXPÉRIMENTÉ :

> Le raccord entre identité numérique, autorisation de la personne agissant pour l'entreprise et paiement est donc matérialisé dans un parcours technique de démonstration S34.

Paiement → émission automatique d'un justificatif vérifiable

Une fois le paiement confirmé, le vendeur émet un eReceipt sous la forme d'un credential vérifiable S34.

Ce justificatif est envoyé directement vers le European Business Wallet de l'entreprise acheteuse.

La chaîne devient :

```
paiement confirmé
   ↓
vendeur / Business Wallet
   ↓
génération du eReceipt
   ↓
credential vérifiable
   ↓
European Business Wallet de l'acheteur
```

EXPÉRIMENTÉ :

> Un événement provenant directement du processus de paiement peut donc déclencher l'émission et le transfert automatisé d'un document transactionnel structuré vers le wallet de l'entreprise S34.

Le lien paiement → donnée transactionnelle structurée n'est donc plus seulement théorique dans ce cas d'usage.

Le justificatif contient le détail économique de la transaction

Le eReceipt utilisé dans la démonstration ne constitue pas uniquement une preuve indiquant qu'un montant global a été payé.

Selon la documentation technique publiée par le participant au projet, il contient notamment :

- l'identité du vendeur ;
- son numéro de TVA ;
- les lignes d'achat ;
- les montants hors taxe et toutes taxes comprises ;
- les sous-totaux de TVA par taux ;
- la référence du paiement S34.

EXPÉRIMENTÉ :

> Le même objet numérique peut donc établir un lien vérifiable entre le paiement et le contenu économique détaillé de la transaction S34.

La chaîne devient :

```
paiement
   ↓
référence de paiement
   ↓
eReceipt vérifiable
   ↓
lignes d'achat + montants + TVA + vendeur
```

Ce point est important pour l'enquête.

Dans ce cas expérimental, la couche transactionnelle et le détail des biens ou services achetés ne sont plus nécessairement deux ensembles dépourvus de relation technique.

Un justificatif vérifiable peut servir de pont entre eux.

Justificatif → comptabilité

Le Business Wallet peut également être relié aux systèmes utilisés par l'entreprise.

Dans la démonstration PA4, un connecteur transmet les eReceipts vers le système comptable afin de comptabiliser automatiquement les dépenses S34.

La chaîne devient :

```
paiement
   ↓
eReceipt vérifiable
   ↓
Business Wallet
   ↓
connecteur
   ↓
comptabilité
```

EXPÉRIMENTÉ :

> Les données issues de la transaction peuvent donc être réutilisées automatiquement par un système extérieur au wallet sans ressaisie manuelle S34.

Ce mécanisme confirme le rôle de couche d'interopérabilité attribué aux wallets dans les sections précédentes.

Justificatif → administration fiscale

Le cas expérimental décrit par le participant va encore plus loin.

Les justificatifs vérifiés peuvent être communiqués à un service fiscal de démonstration.

Celui-ci vérifie notamment :

- la signature du justificatif ;
- la confiance accordée à son émetteur ;
- son statut de révocation.

Le système peut ensuite utiliser les informations de TVA contenues dans les justificatifs pour effectuer un rapprochement de TVA S34.

La chaîne expérimentale complète devient :

```
achat B2B
   ↓
paiement
   ↓
eReceipt vérifiable
   ↓
European Business Wallet
   ↓
données détaillées de transaction
   ↓
système comptable
```

et :

```
eReceipt vérifiable
   ↓
service fiscal de démonstration
   ↓
vérification
   ↓
rapprochement de TVA
```

EXPÉRIMENTÉ — SOURCE PARTICIPANT :

> Un participant de WE BUILD documente donc une démonstration technique reliant de bout en bout paiement, justificatif structuré, wallet d'entreprise, comptabilité et traitement fiscal S34.

LIMITE :

> Cette démonstration ne constitue pas la preuve qu'une administration fiscale nationale utilise actuellement cette chaîne en production.

Paiement et fiscalité peuvent donc appartenir à une même chaîne technique

Cette distinction est importante par rapport aux chapitres précédents.

Jusqu'ici, l'enquête avait établi séparément :

```
paiement
→ données de paiement

facturation / transaction
→ données fiscales

Business Wallet
→ attestations et données d'entreprise
```

Le pilote permet désormais de représenter une chaîne expérimentale unique :

```
identité de l'entreprise
   ↓
identité / délégation de la personne
   ↓
EUDI Wallet
   ↓
compte ou carte
   ↓
paiement
   ↓
eReceipt vérifiable
   ↓
European Business Wallet
   ↓
détail de transaction / TVA
   ↓
comptabilité
   ↓
traitement fiscal expérimental
```

EXPÉRIMENTÉ :

> Le raccord technique paiement → justificatif structuré → données fiscales → traitement fiscal a donc fait l'objet d'une démonstration de bout en bout dans l'écosystème WE BUILD S34.

Ce raccord ne dépend pas d'une base centrale unique

Le parcours confirme également un principe identifié précédemment.

Les informations n'ont pas besoin d'être regroupées dans une base de données centrale unique.

Les différents composants peuvent échanger successivement des preuves ou credentials vérifiables.

Par exemple :

```
banque
→ confirmation du paiement

vendeur
→ émission du justificatif

wallet
→ conservation / présentation du credential

comptabilité
→ exploitation du justificatif

service fiscal
→ vérification du justificatif
```

AVÉRÉ / EXPÉRIMENTÉ :

> Une chaîne d'interconnexion peut donc fonctionner de bout en bout au moyen de plusieurs systèmes distribués sans nécessiter qu'un acteur central détienne l'intégralité des données de chaque étape S34.

Cette architecture distribuée rend particulièrement importante l'analyse des interfaces et des droits d'accès plutôt que la seule recherche d'une base de données centrale.

Facturation électronique et paiement : autre chaîne étudiée dans le même programme

WE BUILD ne limite pas ses travaux aux eReceipts.

La documentation du programme fait également apparaître parmi ses cas d'usage :

- Business Payments ;
- eInvoicing ;
- Foreign Tax Declaration S33-S34.

Des ateliers d'interopérabilité ont en outre porté sur les paiements professionnels, la facturation et les justificatifs numériques dans l'environnement des EUDI Wallets et Business Wallets.

AVÉRÉ :

> Paiement professionnel, facturation électronique et traitement fiscal font donc partie des domaines effectivement expérimentés dans le même programme européen S33-S34.

NON ÉTABLI :

> Les éléments étudiés ne permettent pas encore d'affirmer que la chaîne PA4 relative aux eReceipts constitue directement le futur mécanisme ViDA de facturation électronique ou le mécanisme français de facturation électronique.

Un pont important est désormais fermé

Au début du chapitre 5, plusieurs raccords restaient séparés :

- identité → paiement
- transaction → fiscalité
- Business Wallet → données d'entreprise

Le cas WE BUILD permet désormais de les réunir expérimentalement :

```
identité
   ↓
paiement
   ↓
preuve structurée de transaction
   ↓
Business Wallet
   ↓
données fiscales
   ↓
traitement fiscal
```

EXPÉRIMENTÉ :

> Il existe donc au moins un cas d'usage européen dans lequel ces domaines sont techniquement reliés de bout en bout.

Cela ne démontre aucune finalité de contrôle des achats.

Cela démontre en revanche que leur interconnexion technique ne constitue plus seulement une possibilité abstraite.

Il reste le raccord environnemental

Le chapitre 3 a établi séparément :

```
produit identifiable
   ↓
DPP
   ↓
données produit
   ↓
données de durabilité / environnementales
```

Les sections 5.2 et 5.3 ont ensuite établi :

```
Business Wallet
   ⇔
DPP / données produit / durabilité
```

et :

```
Business Wallet
   ⇔
transaction / TVA / facturation
```

La présente section établit désormais expérimentalement :

```
paiement
   ↓
justificatif comportant les lignes d'achat
   ↓
Business Wallet
   ↓
traitement comptable / fiscal
```

Il devient donc possible de juxtaposer les deux chaînes documentées :

```
DPP / données de durabilité
   ↕
European Business Wallet
```

et :

```
paiement
   ↓
eReceipt / lignes d'achat
   ↓
European Business Wallet
```

DÉDUCTIBLE TECHNIQUEMENT :

> Lorsqu'une ligne d'achat permet d'identifier le produit correspondant et que les droits d'accès nécessaires existent, le Business Wallet ou un service interconnecté dispose techniquement des composants permettant de rapprocher la preuve de transaction des informations correspondantes contenues dans l'écosystème DPP.

Ce rapprochement n'est plus déduit uniquement de la compatibilité théorique de deux formats.

Il repose désormais sur l'existence documentée d'un environnement wallet relié, d'un côté, aux données produit et de durabilité et, de l'autre, à des justificatifs détaillés issus d'un paiement.

Le dernier raccord vers le paiement conditionnel reste distinct

Le chapitre 4 a établi une autre chaîne :

```
système externe
   ↓
vérification d'une condition
   ↓
couche de conditionnalité
   ↓
paiement
```

Les travaux de la BCE ont également démontré expérimentalement que des plateformes d'acteurs du marché pouvaient communiquer par API avec un environnement simulant l'euro numérique S27-S28.

Nous disposons donc désormais de deux ensembles :

Ensemble A

```
produit / DPP / durabilité
   ↕
Business Wallet
   ↕
transaction détaillée / eReceipt
   ↕
paiement
```

Ensemble B

```
système externe
   ↓
condition externe
   ↓
couche de conditionnalité
   ↓
paiement
```

DÉDUCTIBLE TECHNIQUEMENT :

> Les architectures documentées contiennent donc les composants nécessaires pour qu'une information provenant d'un système extérieur soit vérifiée et utilisée dans un processus entourant l'exécution d'un paiement.

NON ÉTABLI :

> Aucun élément étudié ne démontre cependant que les données environnementales du DPP soient actuellement utilisées comme condition dans un paiement en euro numérique ou dans un autre système de paiement.

La différence entre « possible », « expérimenté » et « prévu »

À ce stade de l'enquête, trois niveaux doivent être strictement distingués.

EXPÉRIMENTÉ :

> identité → paiement → justificatif structuré → Business Wallet → comptabilité / traitement fiscal.

AVÉRÉ / PRÉVU :

> Business Wallet ↔ DPP / données produit et de durabilité.

AVÉRÉ / EXPÉRIMENTÉ :

> système externe → vérification d'une condition → paiement conditionnel.

Mais :

NON ÉTABLI :

> donnée environnementale → condition déterminant l'exécution d'un paiement.

Cette dernière flèche ne doit pas être ajoutée artificiellement à la chaîne tant qu'aucune source ne la documente.

Ce que cette section change dans la démonstration

Au début de l'enquête, il aurait été possible d'objecter que les différents systèmes étudiés n'avaient aucun lien entre eux :

« la facture est fiscale » ;

« le DPP est environnemental » ;

« le wallet sert à l'identité » ;

« le paiement appartient aux banques » ;

« l'euro numérique est une infrastructure monétaire distincte ».

Les sources étudiées permettent désormais d'écarter une version aussi absolue de cette séparation.

AVÉRÉ :

> La Commission recherche explicitement des synergies entre plusieurs de ces infrastructures S30-S31.

AVÉRÉ :

> Des standards, API, attestations et mécanismes d'interopérabilité permettent leurs interactions S20-S30-S32.

AVÉRÉ :

> Des programmes européens réunissent identité, facturation, fiscalité et paiement dans les mêmes environnements expérimentaux S33-S34.

EXPÉRIMENTÉ :

> Une chaîne de bout en bout reliant identité, paiement, justificatif détaillé, Business Wallet, comptabilité et traitement fiscal a été démontrée par des participants de WE BUILD S34.

NON ÉTABLI :

> L'utilisation d'une donnée environnementale comme critère de paiement reste, elle, non démontrée.

Conclusion intermédiaire

AVÉRÉ / EXPÉRIMENTÉ :

> Une infrastructure de wallet peut participer à une chaîne reliant l'identité d'une entreprise et de son représentant, un compte ou une carte, un paiement et une preuve structurée de la transaction S34.

EXPÉRIMENTÉ :

> Cette preuve peut contenir les lignes d'achat, les montants, les informations de TVA et une référence au paiement puis être transmise automatiquement au European Business Wallet de l'entreprise S34.

EXPÉRIMENTÉ :

> Des connecteurs permettent ensuite la réutilisation du justificatif par un système comptable et, dans le cas de démonstration étudié, par un service fiscal effectuant un rapprochement de TVA S34.

AVÉRÉ :

> Le même écosystème Business Wallet est parallèlement articulé avec le Digital Product Passport et ses données relatives aux produits et à leur durabilité S30.

AVÉRÉ / EXPÉRIMENTÉ :

> Une architecture distincte de paiement conditionnel permet par ailleurs à une condition vérifiée par un système externe d'intervenir dans l'exécution d'une transaction S27-S28.

DÉDUCTIBLE TECHNIQUEMENT :

> Les infrastructures étudiées permettent donc de construire une chaîne technique dans laquelle une transaction détaillée peut être reliée à un produit identifiable, le produit à des données externes et le résultat d'une vérification externe à une logique conditionnelle entourant un paiement.

NON ÉTABLI :

> Aucun document étudié ne démontre cependant que cette chaîne soit actuellement assemblée afin d'utiliser une donnée environnementale pour autoriser, refuser ou limiter un paiement.

Le nombre de raccords manquants s'est donc considérablement réduit.

Il reste maintenant à examiner précisément **le dernier raccord de la chaîne : environnement → paiement**, en recherchant non plus seulement s'il est techniquement possible, mais s'il existe un projet, un pilote, un standard ou une documentation qui l'expérimente ou le prévoit explicitement.

S35 CEN/TS 16931-8:2024 — eReceipts, identifiant DPP et informations environnementales du produit

Organisme : Comité européen de normalisation (CEN)

Document : CEN/TS 16931-8:2024 — Electronic invoicing — Part 8: Semantic data model of the elements of an e-receipt

Date : 2024

Utilisé dans : Chapitre 5

Éléments établis : modèle sémantique européen relatif aux justificatifs électroniques ; description d'un processus dans lequel l'acheteur sélectionne un moyen de paiement, effectue ou initie le paiement puis reçoit un eReceipt généré par le vendeur ; possibilité d'inclure dans certains environnements des informations spécifiques relatives au produit ; mention explicite du Digital Product Passport pour les catégories de produits concernées ; utilisation d'un identifiant DPP permettant de relier le justificatif aux informations vérifiées relatives au produit ; mention parmi ces informations de la durabilité des matériaux ainsi que des impacts sociaux et environnementaux liés aux matériaux, à la production, à l'utilisation et à la fin de vie du produit.

Précaution méthodologique : l'existence d'un champ ou mécanisme permettant de relier un eReceipt au DPP démontre la possibilité normalisée d'établir ce raccord. Elle ne démontre pas que chaque eReceipt contiendra un identifiant DPP, ni que les données environnementales correspondantes seront systématiquement récupérées, ni qu'elles seront utilisées par un système de paiement.

Référence : CEN/TS 16931-8:2024

5.7 Le raccord environnement → paiement

Statut : AVÉRÉ / EXPÉRIMENTÉ / DÉDUCTIBLE TECHNIQUEMENT / NON ÉTABLI

Les sections précédentes ont progressivement réduit le nombre de raccords manquants entre les infrastructures étudiées.

À l'issue de la section 5.6, deux chaînes distinctes étaient établies.

La première relie désormais expérimentalement le paiement au détail économique de la transaction :

```
paiement
   ↓
eReceipt
   ↓
lignes d'achat
   ↓
European Business Wallet
```

La seconde relie une information provenant d'un système extérieur à l'exécution d'un paiement conditionnel :

```
système externe
   ↓
vérification d'une condition
   ↓
couche de conditionnalité
   ↓
paiement
```

La question de cette section est donc volontairement limitée à une seule flèche :

> **Existe-t-il un mécanisme documenté permettant de relier une information environnementale relative au produit à la transaction ou à la condition déterminant l'exécution du paiement ?**

---

eReceipt → Digital Product Passport

Un élément supplémentaire apparaît dans les travaux européens de normalisation relatifs aux justificatifs électroniques S35.

Le modèle CEN/TS 16931-8:2024 décrit le processus économique dans lequel l'acheteur sélectionne un moyen de paiement, effectue ou initie le paiement, puis reçoit un eReceipt généré par le vendeur.

Le même document prévoit que, dans certains environnements, des informations spécifiques relatives au produit puissent être associées au justificatif.

Pour les catégories de produits soumises au Digital Product Passport, le standard mentionne explicitement l'utilisation d'un **identifiant DPP permettant de relier le justificatif aux informations vérifiées relatives au produit** S35.

AVÉRÉ :

> Un standard européen relatif aux eReceipts prévoit donc explicitement un raccord entre le justificatif d'une transaction et le Digital Product Passport du produit correspondant S35.

La chaîne devient :

```
achat
   ↓
paiement
   ↓
eReceipt
   ↓
identifiant DPP
   ↓
Digital Product Passport
```

Ce raccord est plus précis que la simple possibilité de faire correspondre ultérieurement une référence commerciale avec un identifiant produit.

Le mécanisme de liaison au DPP est directement envisagé dans le modèle du justificatif.

Le raccord donne accès à des informations environnementales

Le même standard explique l'intérêt de cette relation avec le DPP.

L'identifiant permet de relier le produit aux informations vérifiées concernant son cycle de vie.

Parmi les informations explicitement mentionnées figurent notamment :

- la durabilité de l'approvisionnement en matériaux ;
- les impacts sociaux des matériaux utilisés ;
- les impacts environnementaux des matériaux utilisés ;
- la production ;
- l'utilisation ;
- la fin de vie du produit S35.

AVÉRÉ :

> Le raccord eReceipt → identifiant DPP ne conduit donc pas uniquement vers une référence administrative du produit : il peut conduire vers des informations vérifiées comprenant des caractéristiques relatives à sa durabilité et à ses impacts environnementaux S35.

La chaîne suivante est ainsi explicitement documentée au niveau du modèle sémantique :

```
transaction
   ↓
eReceipt
   ↓
identifiant DPP
   ↓
produit
   ↓
informations vérifiées
   ↓
durabilité / impacts environnementaux
```

Paiement → eReceipt → DPP → environnement

Ce nouvel élément peut être rapproché de la chaîne expérimentée dans WE BUILD.

La section 5.6 a établi :

```
paiement
   ↓
eReceipt vérifiable
   ↓
lignes d'achat / informations de transaction
```

Le standard CEN/TS 16931-8 ajoute :

```
eReceipt
   ↓
identifiant DPP
   ↓
informations vérifiées du produit
   ↓
informations environnementales
```

AVÉRÉ / EXPÉRIMENTÉ SELON LES MAILLONS :

> Les composants documentés permettent donc désormais de construire une chaîne dans laquelle un paiement est relié à un justificatif électronique et dans laquelle un justificatif électronique peut lui-même être relié, au moyen d'un identifiant DPP, aux informations environnementales vérifiées du produit S34-S35.

La chaîne complète peut être représentée ainsi :

```
paiement
   ↓
eReceipt
   ↓
produit identifiable
   ↓
identifiant DPP
   ↓
Digital Product Passport
   ↓
données de durabilité / environnementales
```

LIMITE :

> Cette représentation assemble deux raccords documentés dans des contextes différents. Elle ne démontre pas qu'un même système opérationnel utilise actuellement l'intégralité de cette chaîne de bout en bout.

Le rapprochement transaction → environnement n'est donc plus uniquement hypothétique

Au début de l'enquête, le lien entre un achat et les caractéristiques environnementales du produit reposait sur une déduction :

```
transaction
   ↓
identifier le produit
   ↓
rechercher son DPP
   ↓
retrouver la donnée environnementale
```

Le standard relatif aux eReceipts apporte un élément supplémentaire.

AVÉRÉ :

> Le modèle européen prévoit directement qu'un identifiant DPP puisse être associé au justificatif afin de relier l'achat aux informations vérifiées relatives au produit S35.

Il n'est donc plus nécessaire de supposer qu'un rapprochement devrait obligatoirement être réalisé après la transaction à partir de bases indépendantes.

Le justificatif peut lui-même transporter le mécanisme permettant d'accéder au passeport du produit.

Une autre convergence existe avec la facturation électronique

Cette relation doit également être rapprochée des éléments établis en 5.3 et 5.4.

La Commission prévoit :

```
eInvoicing
   ↓
réutilisation des données
   ↓
reporting de durabilité
```

et les travaux de standardisation relatifs à EN 16931 prennent explicitement en compte les besoins provenant du reporting de durabilité S31-S32.

Le standard relatif aux eReceipts ajoute désormais :

```
eReceipt
   ↓
identifiant DPP
   ↓
informations environnementales du produit
```

AVÉRÉ :

> Plusieurs travaux européens distincts organisent donc le rapprochement entre données décrivant une transaction et informations relatives à la durabilité ou à l'environnement S31-S32-S35.

Cela ne démontre toujours pas l'établissement d'un profil environnemental individuel.

Le paiement conditionnel accepte une condition provenant de l'extérieur

De l'autre côté de la chaîne, les travaux de la BCE établissent que la logique conditionnelle n'a pas besoin d'être intégrée à la monnaie elle-même.

Le dispositif étudié sépare :

```
infrastructure de règlement
   +
couche de conditionnalité développée par le marché
```

Cette couche peut utiliser un monitoring extérieur afin de vérifier qu'une condition est satisfaite S27-S28.

Une fois cette condition vérifiée :

```
condition satisfaite
   ↓
libération des fonds
```

ou, si elle ne l'est pas :

```
condition non satisfaite
   ↓
annulation / expiration de la réservation
```

AVÉRÉ / EXPÉRIMENTÉ :

> La conception actuelle permet donc à une information vérifiée à l'extérieur de l'infrastructure de règlement d'intervenir dans la décision d'exécuter un paiement conditionnel S27-S28.

La nature de la condition n'est pas techniquement limitée à la livraison

Les exemples les plus fréquemment présentés par la BCE concernent la livraison d'un produit, l'arrivée d'un train, l'utilisation d'un service ou l'accomplissement d'une étape.

Ces exemples décrivent des cas d'usage.

Ils ne constituent pas une liste technique exhaustive des seules informations pouvant être vérifiées par une couche de conditionnalité.

Les travaux expérimentaux montrent que les prestataires peuvent développer la logique conditionnelle et que des plateformes externes peuvent intervenir dans sa vérification S27-S28.

DÉDUCTIBLE TECHNIQUEMENT :

> Une condition provenant d'une infrastructure environnementale pourrait techniquement être traitée selon le même principe si un prestataire développait un tel service, si la donnée correspondante était accessible et si cet usage était juridiquement autorisé.

Par exemple :

```
identifiant DPP
   ↓
service externe
   ↓
lecture d'une caractéristique environnementale
   ↓
évaluation d'une règle
   ↓
résultat de la vérification
```

Le système de paiement n'aurait pas nécessairement besoin de recevoir l'intégralité du DPP.

Il pourrait techniquement recevoir uniquement un résultat :

```
condition remplie
   ou
condition non remplie
```

Le dernier raccord technique peut donc être représenté

En assemblant uniquement les capacités documentées :

```
produit acheté
   ↓
eReceipt
   ↓
identifiant DPP
   ↓
Digital Product Passport
   ↓
donnée environnementale
   ↓
service externe de vérification
   ↓
résultat d'une condition
   ↓
couche de conditionnalité
   ↓
paiement
```

DÉDUCTIBLE TECHNIQUEMENT :

> Aucun obstacle architectural identifié dans les sources étudiées n'impose que la donnée vérifiée par le système externe soit une donnée de livraison plutôt qu'une autre donnée accessible à ce système.

Mais cette déduction doit immédiatement être séparée de la preuve d'un usage réel.

La recherche du cas environnemental dans les travaux de la BCE

Les documents de la Digital Euro Innovation Platform permettent de vérifier si cette possibilité a déjà été transformée en cas d'usage environnemental.

Les scénarios documentés portent notamment sur :

- la livraison ;
- les paiements à l'usage ;
- les paiements par étapes ;
- la mobilité et le transport ;
- le commerce électronique ;
- les services financiers ;

- certaines applications industrielles ;
- les interactions machine-to-machine S28.

Les travaux relatifs aux eReceipts mentionnent également un bénéfice environnemental résultant de la réduction de l'utilisation du papier.

NON ÉTABLI :

> Les documents étudiés de la Digital Euro Innovation Platform ne décrivent cependant pas de scénario dans lequel l'empreinte carbone, la performance environnementale, le DPP ou une autre donnée de durabilité d'un produit constitue la condition déclenchant ou empêchant un paiement S28.

Ce résultat négatif est important.

Il empêche de transformer la possibilité technique en affirmation d'un projet actuellement documenté.

L'euro numérique ne peut pas être utilisé comme monnaie programmable

Une autre limite doit rester explicitement présente.

La proposition de règlement relative à l'euro numérique exclut la **monnaie programmable** S22.

Cela signifie que les unités d'euro numérique ne doivent pas comporter intrinsèquement des restrictions déterminant :

- les catégories de biens pouvant être achetées ;
- les commerçants auprès desquels elles peuvent être utilisées ;
- la période pendant laquelle elles peuvent être dépensées ;
- ou d'autres limitations remettant en cause leur pleine fongibilité.

AVÉRÉ :

> L'Eurosystème ne prévoit donc pas de coder dans les unités monétaires elles-mêmes une règle du type « cet euro ne peut pas acheter un produit dont l'empreinte carbone dépasse X » S22-S27.

Paiement conditionnel et monnaie programmable restent cependant deux mécanismes différents

L'exclusion de la monnaie programmable ne supprime pas les paiements conditionnels.

La proposition européenne définit séparément l'opération de paiement conditionnelle comme une opération exécutée automatiquement lorsque des conditions prédéfinies convenues entre le payeur et le bénéficiaire sont remplies S22.

La BCE prévoit parallèlement que les prestataires de paiement puissent développer la couche de conditionnalité S27-S28.

La distinction est donc :

```
**MONNAIE PROGRAMMABLE**
règle intégrée dans l'unité monétaire
→ exclue

contre :

**PAIEMENT CONDITIONNEL**
règle appliquée au processus de transaction
→ prévu / expérimenté
```

AVÉRÉ :

> L'interdiction de la monnaie programmable ne constitue donc pas une interdiction générale de toute logique automatisée entourant l'exécution d'un paiement S22-S27-S28.

Les conditions sont présentées comme convenues entre les parties

Cette limite est également essentielle.

Dans la proposition législative, les conditions d'un paiement conditionnel sont définies comme des conditions prédéfinies **convenues par le payeur et le bénéficiaire** S22.

Les services supplémentaires étudiés par la BCE sont par ailleurs présentés comme des services développés par les acteurs du marché et utilisés volontairement par les utilisateurs.

AVÉRÉ :

> Les documents étudiés ne donnent donc pas à la BCE ou à l'Eurosystème un pouvoir général permettant d'imposer unilatéralement une condition environnementale aux achats des utilisateurs.

NON ÉTABLI :

> Aucun mécanisme permettant à une administration de transformer directement une donnée environnementale individuelle en interdiction de paiement imposée au payeur n'a été identifié.

La chaîne technique et la chaîne juridique doivent être séparées

Le résultat de l'analyse peut donc être représenté de deux manières différentes.

CAPACITÉ TECHNIQUE :

```
transaction
   ↓
eReceipt
   ↓
identifiant DPP
   ↓
donnée environnementale
   ↓
service externe
   ↓
condition
   ↓
paiement conditionnel
```

DÉDUCTIBLE TECHNIQUEMENT :

> Les composants permettant de construire cette chaîne existent séparément et les interfaces nécessaires à plusieurs de ses raccords sont documentées.

Mais :

USAGE ÉTABLI :

```
donnée environnementale
   ↓
condition environnementale imposée
   ↓
autorisation / refus du paiement
```

NON ÉTABLI :

> Aucun projet institutionnel, règlement, pilote ou documentation technique étudié ne démontre actuellement l'utilisation d'une donnée environnementale relative à un produit afin d'autoriser, refuser ou limiter un paiement.

Une différence importante apparaît néanmoins par rapport au début de l'enquête

Au début de l'analyse, presque toute la chaîne devait être reconstruite par hypothèse :

```
facture
   ?
produit
   ?
environnement
   ?
identité
   ?
paiement
```

À ce stade, les raccords documentés sont beaucoup plus nombreux :

```
facturation / transaction
   ↓
données structurées

produit
   ↓
DPP
   ↓
données environnementales

eReceipt
   ↓
identifiant DPP

Business Wallet
   ↔
DPP / durabilité

Business Wallet
   ↔
transaction / fiscalité

identité
   ↓
wallet
   ↓
paiement

paiement
   ↓
eReceipt détaillé

système externe
   ↓
condition
   ↓
paiement conditionnel
```

Le point restant non démontré n'est donc plus l'existence des infrastructures nécessaires.

Il est désormais beaucoup plus précis :

> **l'existence d'une règle ou d'un cas d'usage utilisant effectivement une donnée environnementale comme condition déterminant l'exécution d'un paiement.**

La frontière documentaire actuelle

La frontière entre ce qui est établi et ce qui ne l'est pas peut désormais être placée précisément.

AVÉRÉ :

> Un produit peut être relié à des données environnementales au moyen du Digital Product Passport S15-S19.

AVÉRÉ :

> Un eReceipt peut comporter un identifiant permettant de relier l'achat au DPP et à ses informations vérifiées relatives au produit S35.

EXPÉRIMENTÉ :

> Un paiement peut être relié à un eReceipt contenant le détail économique de la transaction S34.

AVÉRÉ / EXPÉRIMENTÉ :

> Un système extérieur peut vérifier une condition utilisée par une couche de conditionnalité entourant un paiement S27-S28.

DÉDUCTIBLE TECHNIQUEMENT :

> Une donnée environnementale accessible depuis le DPP pourrait être vérifiée par un service extérieur et son résultat utilisé comme condition technique selon la même architecture.

NON ÉTABLI :

> Les sources étudiées ne démontrent pas qu'un tel service environnemental soit actuellement prévu ou expérimenté pour déterminer l'exécution d'un paiement.

Conclusion intermédiaire

AVÉRÉ :

> Le standard européen relatif aux eReceipts prévoit explicitement qu'un identifiant DPP puisse relier un justificatif de transaction aux informations vérifiées du produit, comprenant notamment des informations relatives à sa durabilité et à ses impacts environnementaux S35.

EXPÉRIMENTÉ :

> Des travaux européens ont parallèlement démontré une chaîne reliant paiement, eReceipt détaillé et Business Wallet S34.

AVÉRÉ / EXPÉRIMENTÉ :

> L'architecture des paiements conditionnels permet à un système externe de vérifier une condition dont le résultat intervient dans l'exécution du paiement S27-S28.

DÉDUCTIBLE TECHNIQUEMENT :

> Les composants documentés permettent donc techniquement de construire une chaîne paiement ↔ transaction identifiable ↔ produit ↔ DPP ↔ donnée environnementale ainsi qu'une chaîne donnée externe → condition → paiement.

NON ÉTABLI :

> Aucun élément identifié ne démontre toutefois que ces deux chaînes soient actuellement raccordées afin qu'une donnée environnementale détermine l'autorisation, le refus ou la limitation d'un paiement.

AVÉRÉ :

> Dans le cadre juridique proposé pour l'euro numérique, les conditions d'un paiement conditionnel sont présentées comme prédéfinies et convenues entre le payeur et le bénéficiaire, tandis que la monnaie programmable limitant intrinsèquement les biens ou services pouvant être achetés est explicitement exclue S22.

La recherche du raccord environnement → paiement aboutit donc à un résultat nuancé mais précis :

> **la chaîne technique est reconstructible avec des composants et raccords désormais largement documentés ; son utilisation environnementale comme mécanisme de décision de paiement reste, elle, non établie.**

Cette frontière doit être conservée dans la conclusion de l'enquête.

La section suivante doit maintenant examiner les **limites de la démonstration**, afin de distinguer définitivement ce que l'architecture permet, ce qui a été expérimenté et ce qu'aucune source ne permet encore d'affirmer.

5.8 Limites de la démonstration

Statut : LIMITES ÉTABLIES / NON ÉTABLI

Les sections précédentes ont permis d'identifier de nombreux raccords entre les infrastructures étudiées.

Ces raccords ne doivent cependant pas être interprétés au-delà de ce que démontrent effectivement les sources.

Cette section fixe donc les limites de la démonstration avant d'en établir la synthèse.

Interopérabilité ne signifie pas échange systématique de données

Les infrastructures étudiées utilisent des identifiants, standards, API, attestations vérifiables et mécanismes d'autorisation permettant leur interopérabilité S20-S30-S32.

AVÉRÉ :

> Plusieurs de ces systèmes sont techniquement conçus pour pouvoir échanger ou vérifier des informations provenant d'autres systèmes.

Mais :

NON ÉTABLI :

> Cette interopérabilité ne signifie pas que toutes leurs données soient automatiquement mises en commun, transmises ou centralisées.

Une possibilité d'interconnexion doit donc être distinguée d'un flux réellement activé.

Un raccord entre deux systèmes ne démontre pas une chaîne complète

Plusieurs raccords ont été documentés séparément :

- transaction → eReceipt
- eReceipt → DPP
- DPP → données environnementales
- identité → paiement
- système externe → condition → paiement

L'existence de chacun de ces raccords ne suffit pas à démontrer qu'ils sont tous utilisés simultanément dans un même processus.

NON ÉTABLI :

> Aucun système opérationnel identifié dans les sources étudiées ne relie actuellement de bout en bout une donnée environnementale provenant du DPP à une décision autorisant ou refusant un paiement.

Standard prévu ne signifie pas utilisation systématique

Le standard relatif aux eReceipts prévoit la possibilité de relier un justificatif au Digital Product Passport au moyen d'un identifiant DPP S35.

Cela démontre l'existence d'un mécanisme normalisé permettant ce raccord.

Mais :

NON ÉTABLI :

> Tous les eReceipts ne contiendront pas nécessairement un identifiant DPP et tous les produits ne seront pas nécessairement soumis aux mêmes exigences de passeport numérique.

La possibilité normalisée d'inclure une donnée ne démontre donc pas son utilisation systématique.

Projet pilote ne signifie pas système déployé

Les expérimentations WE BUILD et celles de la Digital Euro Innovation Platform permettent de démontrer la faisabilité de plusieurs chaînes techniques S28-S33-S34.

Elles constituent des preuves d'expérimentation.

Elles ne constituent pas nécessairement des preuves de déploiement opérationnel.

NON ÉTABLI :

> Les processus expérimentés dans ces pilotes ne doivent pas être présentés comme des mécanismes déjà généralisés à l'ensemble des entreprises, administrations, banques ou utilisateurs européens.

Cette distinction est particulièrement importante pour les démonstrations utilisant des services fiscaux simulés ou des environnements de paiement expérimentaux.

Proposition législative ne signifie pas droit définitivement adopté

Les European Business Wallets étudiés dans ce chapitre reposent notamment sur une proposition de règlement présentée par la Commission européenne S30.

À la date de l'analyse, cette proposition suit encore la procédure législative européenne.

AVÉRÉ :

> Le projet permet d'établir l'orientation proposée, les fonctionnalités envisagées et l'architecture recherchée.

Mais :

NON ÉTABLI :

> Toutes les dispositions étudiées ne peuvent pas être présentées comme constituant déjà le droit définitif applicable dans leur rédaction actuelle.

Le texte final peut encore évoluer au cours de la procédure législative.

Possibilité technique ne signifie pas autorisation juridique

Une infrastructure peut techniquement permettre à deux systèmes de communiquer sans que tous les acteurs soient juridiquement autorisés à accéder aux données correspondantes.

Le DPP prévoit notamment des droits d'accès différenciés selon les données et catégories de produits S15-S20.

Les architectures EUDI et Business Wallet reposent également sur des mécanismes d'autorisation et de présentation sélective des informations S29-S30.

AVÉRÉ :

> L'accès technique à une infrastructure et le droit d'accéder à une donnée particulière constituent deux questions différentes.

Par conséquent :

DÉDUCTIBLE TECHNIQUEMENT :

> Une chaîne peut être architecturalement réalisable.

sans que cela permette d'affirmer :

> qu'un acteur déterminé possède juridiquement le droit de l'utiliser pour une finalité déterminée.

Le DPP n'est pas un profil individuel de consommation

Le Digital Product Passport décrit le produit, son modèle, son lot ou son article selon les règles applicables S15.

Le règlement prévoit en outre que les données personnelles relatives aux clients ne soient pas stockées dans le DPP sans leur consentement explicite S15.

AVÉRÉ :

> Le DPP constitue une infrastructure relative au produit et non, par nature, une base de données destinée à établir le profil individuel de son acheteur.

NON ÉTABLI :

> L'existence du DPP ne démontre donc pas l'existence d'un registre européen centralisé associant chaque individu à l'ensemble des produits qu'il achète.

Un rapprochement avec une transaction ou une identité nécessiterait des mécanismes supplémentaires ainsi qu'une base juridique ou un consentement approprié selon le cas.

Business Wallet ne signifie pas wallet individuel du consommateur

Les European Business Wallets sont destinés aux opérateurs économiques et aux interactions professionnelles ou administratives S30.

Ils doivent être distingués de l'EUDI Wallet destiné aux personnes physiques.

AVÉRÉ :

> Les chaînes B2B documentées dans WE BUILD ne démontrent pas qu'un mécanisme identique soit automatiquement appliqué aux achats personnels de chaque consommateur.

Cette distinction empêche de transposer directement un pilote B2B à un scénario de contrôle individuel de la consommation.

Données fiscales ne signifie pas connaissance exhaustive des achats individuels

Le chapitre 1 a montré que les données transmises dans le cadre français de la facturation électronique et du e-reporting diffèrent selon les opérations.

Les transactions B2C ne conduisent pas nécessairement à la transmission à l'administration fiscale du détail individualisé de chaque produit acheté par chaque consommateur S1-S2-S3-S4.

NON ÉTABLI :

> La réforme française de la facturation électronique ne peut donc pas être présentée, sur la base des sources étudiées, comme créant à elle seule un registre nominatif exhaustif des achats de chaque particulier.

Cette limite demeure même si d'autres infrastructures disposent séparément d'informations plus détaillées sur certains produits ou transactions.

Donnée environnementale disponible ne signifie pas profil carbone individuel

Le DPP et d'autres réglementations européennes permettent ou imposent, selon les produits concernés, la disponibilité de données relatives à la durabilité ou à certains impacts environnementaux S15-S18-S19.

Le rapprochement technique entre une transaction et ces informations peut également être envisagé ou normalisé S31-S35.

Mais :

NON ÉTABLI :

> Aucun mécanisme général établissant automatiquement un bilan carbone individuel à partir de l'ensemble des achats d'une personne n'a été identifié dans les sources étudiées.

Une telle finalité nécessiterait notamment l'identification des transactions pertinentes, leur attribution à une personne, la récupération des données environnementales correspondantes et une méthode permettant leur agrégation.

Paiement conditionnel ne signifie pas monnaie programmable

Le chapitre 4 a établi une distinction fondamentale S22-S27-S28.

L'euro numérique ne doit pas être conçu comme une monnaie programmable dont les unités seraient limitées à certains biens, commerçants, lieux ou périodes.

En revanche, des services de paiement conditionnel sont prévus et expérimentés.

La distinction est :

monnaie programmable
règle intégrée à l'unité monétaire
→ exclue

et :

paiement conditionnel
règle appliquée au processus entourant la transaction
→ prévu / expérimenté

AVÉRÉ :

> L'existence de paiements conditionnels ne permet donc pas d'affirmer que l'euro numérique lui-même pourra être programmé afin d'interdire certaines catégories d'achats S22-S27-S28.

Une condition technique possible ne signifie pas condition imposée

Les paiements conditionnels sont présentés comme reposant sur des conditions prédéfinies intervenant dans le processus de transaction S22-S27-S28.

Les acteurs du marché peuvent développer des services utilisant cette couche de conditionnalité.

DÉDUCTIBLE TECHNIQUEMENT :

> Une donnée accessible à un système extérieur pourrait techniquement servir à vérifier une condition si un service correspondant était développé.

Mais :

NON ÉTABLI :

> Aucun pouvoir général permettant à une administration d'imposer une condition environnementale à l'ensemble des paiements des utilisateurs n'a été identifié dans les sources étudiées.

La BCE n'a pas documenté de condition environnementale de paiement

Les expérimentations de la Digital Euro Innovation Platform comprennent différents scénarios de paiements conditionnels S28.

Les cas étudiés concernent notamment la livraison, l'utilisation d'un service, des étapes contractuelles, le transport ou des processus machine-to-machine.

NON ÉTABLI :

> Les documents étudiés ne présentent pas l'empreinte carbone, le DPP ou une autre caractéristique environnementale du produit comme condition déterminant l'exécution d'un paiement.

Cette absence constitue actuellement la principale limite documentaire de la chaîne étudiée.

Acteur commun ne signifie pas échange de données

Plusieurs banques, prestataires de paiement, entreprises technologiques et intégrateurs participent à différents projets européens S33.

Ces recoupements permettent d'identifier un environnement industriel commun.

Mais :

NON ÉTABLI :

> La participation d'une même organisation à plusieurs projets ne démontre pas qu'elle transfère des données entre ces projets ou leurs infrastructures.

Une interconnexion doit être établie à partir d'un flux, d'une interface, d'un cas d'usage ou d'une documentation décrivant effectivement le raccord.

Infrastructure distribuée ne signifie pas base centrale de surveillance

Les chaînes étudiées peuvent fonctionner au moyen :

- d'API ;
- d'attestations vérifiables ;
- de wallets ;
- de registres ;
- de services intermédiaires ;
- de mécanismes de vérification externes.

Une information peut donc être vérifiée sans nécessairement être copiée intégralement dans tous les systèmes intervenant dans le processus.

NON ÉTABLI :

> Les sources étudiées ne démontrent pas l'existence d'une base européenne centrale réunissant simultanément identité individuelle, historique complet des achats, données environnementales, données fiscales et données de paiement.

La possibilité d'interconnexion distribuée doit donc être distinguée de l'hypothèse d'une centralisation intégrale des données.

Finalité annoncée et capacité technique sont deux niveaux différents

L'enquête documente deux catégories d'éléments qu'il convient de ne pas confondre.

D'une part :

> **les finalités explicitement annoncées**

Par exemple :

- lutte contre la fraude ;
- simplification administrative ;
- reporting fiscal ;
- information sur les produits ;
- durabilité ;

- identité numérique ;
- interopérabilité ;
- innovation dans les paiements.

D'autre part :

> **les capacités techniques résultant de l'architecture**

Par exemple :

- rapprocher plusieurs identifiants ;
- interroger un registre ;
- vérifier une attestation ;
- relier un justificatif à un produit ;
- récupérer une information environnementale ;
- vérifier une condition externe ;
- automatiser certaines étapes d'une transaction.

DÉDUCTIBLE TECHNIQUEMENT :

> Une capacité peut exister avant qu'une finalité particulière ne lui soit attribuée.

Mais :

NON ÉTABLI :

> L'existence de cette capacité ne constitue pas une preuve que les institutions européennes ou nationales ont l'intention de l'utiliser pour une finalité non documentée.

Cette distinction constitue l'une des limites méthodologiques centrales de l'enquête.

La frontière de la démonstration

Après l'ensemble des recherches du chapitre 5, la frontière peut être placée précisément.

ÉTABLI OU EXPÉRIMENTÉ :

> facturation / transaction → données structurées

> produit → DPP → données environnementales

> eReceipt → identifiant DPP → informations du produit

> identité → wallet → paiement

> paiement → eReceipt détaillé

> Business Wallet ↔ données de transaction / fiscalité

> Business Wallet ↔ écosystème produit / durabilité

> système externe → vérification d'une condition → paiement conditionnel

Mais :

NON ÉTABLI :

> donnée environnementale → règle imposée → autorisation / refus d'un paiement

et :

NON ÉTABLI :

> ensemble de ces infrastructures → système centralisé de contrôle individuel de la consommation

---

Conclusion intermédiaire

Les recherches menées dans ce chapitre permettent donc d'aller beaucoup plus loin que le simple constat de l'existence parallèle de plusieurs infrastructures numériques.

Des raccords institutionnels, normatifs et techniques existent réellement.

Certains sont déjà prévus par les textes.

D'autres sont standardisés.

D'autres encore ont été expérimentés dans des pilotes européens.

Mais plusieurs limites demeurent essentielles :

> **interopérable** ne signifie pas **interconnecté en permanence** ;

> **interconnecté** ne signifie pas **centralisé** ;

> **techniquement possible** ne signifie pas **juridiquement autorisé** ;

> **expérimenté** ne signifie pas **déployé** ;

> **donnée environnementale accessible** ne signifie pas **profil carbone individuel** ;

> **paiement conditionnel** ne signifie pas **monnaie programmable** ;

> **capacité technique** ne signifie pas **intention politique**.

Enfin, la principale frontière documentaire reste inchangée :

> **les infrastructures permettant de relier transaction, produit, donnée environnementale et mécanisme de conditionnalité existent ou peuvent être raccordées techniquement, mais aucune source étudiée ne démontre actuellement qu'une donnée environnementale soit utilisée afin d'autoriser, refuser ou limiter le paiement d'un utilisateur.**

5.9 Ce que ce chapitre permet d'établir

Le chapitre 5 avait pour objectif de déterminer si les infrastructures étudiées précédemment devaient être considérées comme des systèmes indépendants ou si des interconnexions concrètes pouvaient être documentées entre elles.

Les recherches permettent désormais d'apporter une réponse plus précise.

Les systèmes ne forment pas une infrastructure unique et centralisée.

Ils ne sont cependant pas non plus totalement indépendants les uns des autres.

Des raccords institutionnels, normatifs et techniques existent entre plusieurs d'entre eux. Certains sont prévus par les textes, certains sont standardisés et d'autres ont déjà été expérimentés.

Un écosystème européen commun est explicitement recherché

La Commission européenne ne présente plus certaines de ces infrastructures uniquement comme des projets isolés.

Sa stratégie pour le marché unique rassemble notamment :

- le Digital Product Passport ;
- l'eInvoicing ;
- les European Business Wallets ;
- le Single Digital Gateway ;
- le Once Only Technical System ;
- les systèmes européens d'identification et d'échange de données.

La Commission indique que ces outils doivent collectivement former un **écosystème cohérent de solutions numériques** destiné à créer des synergies entre les différents systèmes S30-S31.

AVÉRÉ :

> L'existence d'une stratégie européenne visant l'interopérabilité et la création de synergies entre plusieurs infrastructures étudiées dans cette enquête est explicitement documentée.

Cette convergence institutionnelle ne démontre cependant pas que toutes les données de ces systèmes soient échangées entre elles.

Facturation électronique → autres usages de la donnée

La facturation électronique ne constitue pas uniquement un mécanisme de transmission d'un document entre vendeur et acheteur.

En France, les données structurées alimentent notamment l'administration fiscale S1-S2-S3-S4.

Au niveau européen, la Commission prévoit également de développer la réutilisation des données d'eInvoicing pour d'autres fonctions S31.

Parmi les orientations explicitement documentées figurent :

```
eInvoicing
   ↓
reporting TVA
```

mais également :

```
eInvoicing
   ↓
reporting de durabilité
```

et :

```
eInvoicing
   ↓
données douanières / EU Customs Data Hub
```

AVÉRÉ :

> La réutilisation des données de facturation électronique au-delà de la seule production de la facture fait partie des orientations européennes documentées S31.

Transaction → produit → environnement

Le chapitre 3 avait établi l'existence d'une infrastructure permettant d'associer un produit à un Digital Product Passport contenant, selon les catégories concernées, des informations relatives à sa durabilité ou à ses caractéristiques environnementales S15-S18-S19-S20.

Le chapitre 5 a identifié un raccord supplémentaire.

Le modèle européen relatif aux eReceipts prévoit qu'un justificatif puisse comporter un identifiant permettant de relier le produit acheté à son Digital Product Passport S35.

La chaîne devient :

```
transaction
   ↓
eReceipt
   ↓
identifiant DPP
   ↓
produit
   ↓
données de durabilité / environnementales
```

AVÉRÉ :

> Un mécanisme normalisé permettant de relier un justificatif transactionnel au Digital Product Passport et aux informations vérifiées du produit est documenté S35.

LIMITE :

> Cela ne signifie pas que tous les produits ou tous les justificatifs utiliseront systématiquement ce mécanisme.

Business Wallet → identité, transaction et données produit

Les European Business Wallets constituent un autre point de raccord important.

Les documents étudiés prévoient leur utilisation pour :

- identifier et authentifier les opérateurs économiques ;
- gérer des attestations vérifiables ;
- échanger des informations relatives à la TVA et aux transactions ;
- soutenir des processus liés à la facturation ;
- interagir avec le Digital Product Passport et certaines données relatives aux produits et à leur durabilité S30.

La chaîne institutionnelle peut donc être représentée ainsi :

```
identité de l'entreprise
   ↕
Business Wallet
   ↔ données fiscales / transactionnelles
   ↔ facturation
   ↔ DPP / données produit
```

AVÉRÉ :

> Le Business Wallet est conçu comme une infrastructure transversale permettant à plusieurs catégories de données d'entreprise d'être présentées, vérifiées ou échangées dans un environnement interopérable S30-S32.

LIMITE :

> Le projet législatif relatif aux European Business Wallets n'est pas encore un texte définitivement adopté dans sa rédaction actuelle.

Identité → paiement

Le raccord entre identité numérique et paiement est également explicitement documenté.

L'EUDI Wallet peut être utilisé pour l'authentification de paiements et la présentation sélective de certaines attestations S29.

Les travaux relatifs à l'euro numérique prévoient également son utilisation comme mécanisme possible d'authentification pour certaines transactions S22-S29.

La chaîne :

```
identité numérique
   ↓
EUDI Wallet
   ↓
authentification
   ↓
paiement
```

est donc :

AVÉRÉ / EXPÉRIMENTÉ :

> L'identité numérique européenne et les infrastructures de paiement font déjà l'objet de raccords et d'expérimentations communes S29.

Paiement → transaction détaillée → Business Wallet

Les expérimentations étudiées dans WE BUILD apportent un raccord supplémentaire.

Un parcours B2B relie :

```
identité de l'entreprise
   ↓
personne autorisée
   ↓
wallet
   ↓
compte ou carte
   ↓
paiement
   ↓
eReceipt vérifiable
   ↓
lignes d'achat / TVA / référence du paiement
   ↓
European Business Wallet
```

Le justificatif peut ensuite être réutilisé par des systèmes comptables et, dans la démonstration étudiée, par un service fiscal de rapprochement de TVA S34.

EXPÉRIMENTÉ :

> Une chaîne reliant identité, paiement, justificatif transactionnel détaillé, wallet d'entreprise et traitement comptable ou fiscal a donc fait l'objet d'une démonstration technique S34.

Cette chaîne ne doit cependant pas être présentée comme un système déjà généralisé ou déployé par les administrations fiscales européennes.

Système externe → condition → paiement

Les travaux relatifs à l'euro numérique établissent parallèlement qu'un paiement conditionnel peut dépendre d'une condition vérifiée à l'extérieur de l'infrastructure de règlement S22-S27-S28.

L'architecture peut être représentée ainsi :

```
événement ou information externe
   ↓
service de vérification
   ↓
condition satisfaite / non satisfaite
   ↓
couche de conditionnalité
   ↓
exécution du paiement
```

AVÉRÉ / EXPÉRIMENTÉ :

> Des systèmes externes peuvent intervenir dans la vérification d'une condition utilisée par un service de paiement conditionnel S27-S28.

La logique conditionnelle peut être développée par les acteurs du marché sans être intégrée à l'unité monétaire elle-même.

Les principales chaînes documentées

À l'issue du chapitre 5, les raccords peuvent être synthétisés ainsi :

```
**FACTURATION / TRANSACTION**
données structurées
   ↓
fiscalité
   ↓
réutilisation prévue pour d'autres reportings
```

```
**TRANSACTION / PRODUIT**
eReceipt
   ↓
identifiant DPP
   ↓
Digital Product Passport
   ↓
informations produit / durabilité / environnement
```

```
**ENTREPRISE**
identité
   ↓
European Business Wallet
   ↔ attestations
   ↔ transaction / TVA / facturation
   ↔ environnement produit / DPP
```

```
**IDENTITÉ / PAIEMENT**
EUDI Wallet
   ↓
authentification
   ↓
paiement
```

```
**PAIEMENT / JUSTIFICATIF**
paiement
   ↓
eReceipt vérifiable
   ↓
détail de transaction
   ↓
Business Wallet
   ↓
comptabilité / traitement fiscal expérimental
```

```
**PAIEMENT CONDITIONNEL**
système externe
   ↓
vérification d'une condition
   ↓
couche de conditionnalité
   ↓
paiement
```

La chaîne techniquement reconstructible

Ces raccords permettent désormais de reconstruire une chaîne beaucoup plus complète que celle disponible au début de l'enquête :

```
identité
   ↓
wallet
   ↓
transaction / paiement
   ↓
justificatif structuré
   ↓
produit identifiable
   ↓
Digital Product Passport
   ↓
donnée environnementale
```

Parallèlement :

```
donnée externe
   ↓
service de vérification
   ↓
résultat d'une condition
   ↓
paiement conditionnel
```

DÉDUCTIBLE TECHNIQUEMENT :

> Les architectures documentées permettent techniquement qu'une information relative à un produit soit récupérée depuis une infrastructure externe, évaluée par un service et transformée en résultat utilisable par une logique automatisée entourant une transaction.

Cette conclusion ne nécessite pas l'existence d'une base centrale réunissant toutes les informations.

Les différents systèmes peuvent fonctionner au moyen d'identifiants, API, wallets, attestations vérifiables et services intermédiaires S20-S30-S32.

Le raccord qui n'a pas été trouvé

Malgré les recherches menées dans les différentes infrastructures, aucun document étudié ne permet d'ajouter la flèche suivante comme élément avéré :

```
donnée environnementale
   ↓
condition environnementale
   ↓
autorisation / refus / limitation du paiement
```

NON ÉTABLI :

> Aucun règlement, projet institutionnel, standard ou pilote identifié dans cette enquête ne démontre actuellement qu'une donnée environnementale issue du DPP ou d'une infrastructure équivalente soit utilisée afin de déterminer l'exécution d'un paiement.

Les exemples de paiements conditionnels étudiés portent sur d'autres événements ou conditions S27-S28.

La présence des composants nécessaires ne constitue donc pas la preuve de leur assemblage pour cette finalité.

Ce qui change néanmoins par rapport à l'hypothèse initiale

Au début de l'enquête, une représentation possible aurait été :

```
facturation
   ?
produit
   ?
environnement
   ?
identité
   ?
paiement
```

Après analyse des sources officielles, la situation est différente.

Plusieurs points d'interrogation peuvent être remplacés par des raccords documentés :

```
transaction
   → eReceipt
   → DPP
   → données environnementales
```

et :

```
identité
   → wallet
   → paiement
```

ainsi que :

```
paiement
   → eReceipt détaillé
   → Business Wallet
```

et :

```
système externe
   → condition
   → paiement conditionnel
```

Enfin, la Commission documente elle-même une stratégie visant à créer des synergies entre plusieurs infrastructures numériques étudiées dans cette enquête S30-S31.

AVÉRÉ :

> L'hypothèse selon laquelle toutes ces infrastructures seraient nécessairement conçues et exploitées comme des systèmes totalement indépendants n'est donc pas compatible avec l'ensemble des documents étudiés.

Mais l'affirmation inverse serait également excessive.

NON ÉTABLI :

> Les sources ne démontrent pas l'existence d'une infrastructure unique réunissant toutes ces données ni d'un système européen de contrôle environnemental individuel des paiements.

Tableau de synthèse

Raccord étudié	Statut
Facturation électronique → administration fiscale	**AVÉRÉ**
Données fiscales → analyse économique / politiques publiques	**AVÉRÉ**
Produit → Digital Product Passport	**AVÉRÉ**
DPP → données de durabilité / environnementales	**AVÉRÉ**
DPP → registre / API / systèmes externes	**AVÉRÉ**
eReceipt → identifiant DPP	**AVÉRÉ**
eReceipt → informations environnementales via DPP	**AVÉRÉ**
eInvoicing → réutilisation pour reporting de durabilité	**PRÉVU / AVÉRÉ**
eInvoicing → rapprochement avec données douanières	**PRÉVU / AVÉRÉ**
Business Wallet → identité d'entreprise	**AVÉRÉ DANS LE PROJET**

Raccord étudié	Statut
Business Wallet → données TVA / transaction / facturation	**AVÉRÉ DANS LE PROJET**
Business Wallet → DPP / données produit	**AVÉRÉ DANS LE PROJET**
EUDI Wallet → authentification de paiement	**AVÉRÉ / EXPÉRIMENTÉ**
EUDI Wallet → euro numérique	**PRÉVU / EXPÉRIMENTÉ**
Paiement → eReceipt détaillé → Business Wallet	**EXPÉRIMENTÉ**
eReceipt → comptabilité / traitement fiscal	**EXPÉRIMENTÉ**
Système externe → condition → paiement	**AVÉRÉ / EXPÉRIMENTÉ**
Transaction → produit → donnée environnementale	**AVÉRÉ / DÉDUCTIBLE SELON LE RACCORDEMENT EFFECTIF**
Donnée environnementale → service externe de vérification	**DÉDUCTIBLE TECHNIQUEMENT**
Donnée environnementale → condition de paiement	**DÉDUCTIBLE TECHNIQUEMENT**
Donnée environnementale → refus ou limitation effective du paiement	**NON ÉTABLI**
Profil carbone individuel généralisé à partir des achats	**NON ÉTABLI**
Base centrale réunissant identité + achats + fiscalité + environnement + paiement	**NON ÉTABLI**
Contrôle institutionnel des achats selon leur impact environnemental	**NON ÉTABLI**

Conclusion du chapitre 5

Le chapitre 5 permet d'écarter deux conclusions opposées.

La première serait d'affirmer :

> **« Ces infrastructures n'ont aucun lien entre elles. »**

Cette affirmation est contredite par les sources.

Des raccords existent entre facturation, données transactionnelles, identité numérique, Business Wallets, Digital Product Passport, données de durabilité, fiscalité et paiement.

Certains raccords sont inscrits dans les textes ou standards.

D'autres font partie de stratégies européennes explicitement consacrées à l'interopérabilité.

D'autres ont déjà été matérialisés dans des expérimentations.

La seconde conclusion excessive serait d'affirmer :

> **« Un système européen utilise déjà toutes ces infrastructures pour surveiller l'empreinte environnementale individuelle et autoriser ou bloquer les achats. »**

Les sources étudiées ne permettent pas de soutenir cette affirmation.

Le résultat documentaire se situe entre ces deux positions.

AVÉRÉ :

> L'Union européenne développe plusieurs infrastructures numériques interopérables capables de relier identité, entreprises, transactions, produits, données fiscales et, selon les systèmes concernés, informations environnementales.

AVÉRÉ :

> La Commission européenne recherche explicitement des synergies et la réutilisation de données entre plusieurs de ces infrastructures.

AVÉRÉ / EXPÉRIMENTÉ :

> Des chaînes reliant identité, paiement, justificatif détaillé, wallet d'entreprise et traitement fiscal ont déjà été expérimentées.

AVÉRÉ :

> Un standard européen prévoit qu'un justificatif électronique puisse être relié au Digital Product Passport et aux informations environnementales vérifiées du produit.

AVÉRÉ / EXPÉRIMENTÉ :

> Des architectures de paiement conditionnel permettent qu'un événement ou une information vérifiée par un système externe intervienne dans l'exécution d'une transaction.

DÉDUCTIBLE TECHNIQUEMENT :

> Ces composants permettent de construire une architecture dans laquelle une donnée environnementale relative à un produit pourrait être interrogée par un service externe et son résultat utilisé dans une logique conditionnelle entourant un paiement.

NON ÉTABLI :

> Aucun élément étudié ne démontre que cette utilisation environnementale du paiement conditionnel soit actuellement prévue, expérimentée ou déployée.

NON ÉTABLI :

> Aucun élément étudié ne démontre l'existence d'un système centralisé attribuant à chaque individu un profil environnemental exhaustif de consommation utilisé pour contrôler ses paiements.

La conclusion du chapitre n'est donc pas que le scénario étudié existe.

Elle est plus précise :

> **une part importante de l'architecture qui rendrait techniquement possible l'interconnexion de données transactionnelles, produit, environnementales, identitaires et de paiement est désormais documentée ; plusieurs raccords sont explicitement prévus ou expérimentés ; mais le raccord décisif transformant une donnée environnementale en règle imposée d'autorisation ou de refus d'un paiement n'a pas été établi.**

Cette distinction entre **infrastructure existante**, **interopérabilité documentée**, **capacité technique** et **usage effectivement démontré** constitue le principal résultat du chapitre 5.

Chapitre 6 — Garanties juridiques

Navigation : ← Retour au sommaire

Les chapitres précédents ont permis d'identifier les données collectées, les infrastructures concernées et plusieurs possibilités ou mécanismes documentés d'interconnexion entre facturation, fiscalité, produits, données environnementales, identité numérique et paiement.

L'existence d'une capacité technique d'interconnexion ne signifie cependant pas que son utilisation soit juridiquement autorisée.

Ce chapitre examine donc les garanties juridiques susceptibles d'encadrer, limiter ou interdire certains traitements ou rapprochements de données identifiés au cours de l'enquête.

L'analyse recherche notamment :

- les bases juridiques permettant les traitements ;
- les finalités pour lesquelles les données peuvent être collectées et réutilisées ;
- le principe de limitation des finalités ;
- le principe de minimisation des données ;
- les conditions applicables au croisement de données provenant de systèmes différents ;
- les règles relatives au profilage et aux décisions automatisées ;
- les droits des personnes concernées ;
- les obligations de transparence ;
- les règles de conservation et d'accès ;
- les pouvoirs et positions des autorités de contrôle, notamment la CNIL ;
- les exigences de nécessité et de proportionnalité ;
- les éventuelles garanties spécifiques prévues pour l'identité numérique, le DPP et les infrastructures de paiement ;
- les possibilités et conditions d'une évolution future des finalités ou des bases juridiques.

L'objectif n'est pas de présumer qu'une violation existe.

Il est de déterminer, pour chaque capacité identifiée dans les chapitres précédents, si le droit actuel :

> **l'autorise explicitement ;**

> **l'autorise sous conditions ;**

> **la limite ;**

> **semble l'interdire ;**

> **ou ne permet pas encore de conclure.**

Une attention particulière sera portée à la différence entre une protection inscrite dans le droit actuel et une impossibilité technique.

Une règle juridique peut limiter aujourd'hui un traitement que l'architecture permettrait techniquement.

Inversement, l'existence d'une infrastructure technique ne permet pas de présumer qu'une évolution juridique autorisant de nouveaux usages interviendra ultérieurement.

Le chapitre cherchera donc à identifier à la fois les protections existantes et leurs limites, sans transformer une possibilité d'évolution du droit en intention institutionnelle établie.

Sommaire

- 6.1 — Cadre juridique applicable
- 6.2 — Finalité des traitements et réutilisation des données
- 6.3 — Croisement, rapprochement et interconnexion des données
- 6.4 — Profilage et décisions automatisées
- 6.5 — Nécessité, proportionnalité et minimisation
- 6.6 — Droits des personnes et contrôle par la CNIL
- 6.7 — Garanties propres aux infrastructures étudiées
- 6.8 — Évolution des finalités et du cadre juridique
- 6.9 — Vulnérabilités juridiques et limites de l'analyse
- 6.10 — Ce que ce chapitre permet d'établir

S36 Règlement général sur la protection des données — principes applicables aux traitements

Organisme : Union européenne

Document : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 — Règlement général sur la protection des données (RGPD)

Éléments utilisés : principes de licéité, loyauté et transparence ; limitation des finalités ; minimisation des données ; base juridique du traitement ; garanties applicables aux traitements réalisés dans le cadre d'une mission d'intérêt public ; décisions individuelles automatisées et profilage.

L'article 5 impose notamment que les données à caractère personnel soient collectées pour des finalités déterminées, explicites et légitimes et ne soient pas traitées ultérieurement d'une manière incompatible avec ces finalités.

Il impose également que les données soient adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités poursuivies.

L'article 22 prévoit par ailleurs un encadrement spécifique des décisions fondées exclusivement sur un traitement automatisé lorsqu'elles produisent des effets juridiques ou affectent significativement une

personne.

Lien officiel : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679

S37 CNIL — intégration des données de facturation électronique au traitement algorithmique CFVR

Organisme : Commission nationale de l'informatique et des libertés (CNIL)

Document : Délibération n° 2026-068 du 18 juin 2026 portant avis sur un projet d'arrêté modifiant le traitement automatisé de lutte contre la fraude « ciblage de la fraude et valorisation des requêtes » (CFVR)

Publication : 24 juillet 2026

Éléments établis :

- les données issues de la facturation électronique sont ajoutées aux catégories de données personnelles utilisées par CFVR ;
- la CNIL constate que cette nouvelle catégorie augmente substantiellement le volume de données traitées ;
- la DGFiP estime le volume des factures électroniques à environ 2 à 3 milliards par an ;
- leur volumétrie nécessite l'utilisation de la plateforme sécurisée des données de la DGFiP ;
- les données de facturation électronique doivent alimenter cette plateforme ;
- elles peuvent être exploitées afin d'identifier des anomalies et des entreprises présentant certains risques fiscaux ;
- les résultats des requêtes peuvent être croisés avec d'autres données du traitement ;
- à terme, l'ensemble des données du traitement CFVR a vocation à alimenter cette plateforme ;
- le traitement utilise des méthodes algorithmiques et d'apprentissage, comprenant notamment certaines méthodes d'apprentissage non supervisé ;
- la CNIL identifie explicitement des risques de biais et d'amplification de ces biais ;
- la CNIL considère indispensable que les résultats algorithmiques ne remplacent pas l'analyse humaine préalable à l'ouverture d'un contrôle fiscal ;
- la CNIL rappelle l'importance de la minimisation, de la limitation des accès, des durées de conservation, de l'information des personnes et de la sécurité des données.

Élément méthodologique important : cet avis ne conclut pas à l'illégalité du traitement. Il confirme cependant que les données issues de la facturation électronique sont effectivement destinées à alimenter une infrastructure d'analyse et de ciblage fiscal utilisant notamment des traitements algorithmiques.

Lien officiel : https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000054466005

S38 Décret relatif à la généralisation de la facturation électronique — prise en compte du RGPD et avis de la CNIL

Organisme : République française

Document : Décret n° 2022-1299 du 7 octobre 2022 relatif à la généralisation de la facturation électronique dans les transactions entre assujettis à la TVA et à la transmission des données de transaction

Éléments établis :

Le décret organisant la réforme vise explicitement le règlement général sur la protection des données.

Il a également été adopté après un avis de la Commission nationale de l'informatique et des libertés en date du 23 juin 2022.

La consultation de la CNIL et la référence au RGPD démontrent que la problématique de protection des données a été intégrée au processus réglementaire.

Elles ne signifient cependant pas que toute évolution ultérieure des traitements ou toute nouvelle réutilisation des données serait automatiquement compatible avec le RGPD.

Lien officiel : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000046383394

S39 Contrôle de proportionnalité des traitements de données par les pouvoirs publics

Organismes : Cour de justice de l'Union européenne / Conseil constitutionnel

Éléments établis :

La protection des données personnelles et de la vie privée n'interdit pas aux autorités publiques de mettre en œuvre des traitements de données poursuivant un objectif d'intérêt général.

Ces traitements doivent cependant respecter un contrôle de nécessité et de proportionnalité.

La jurisprudence européenne rappelle notamment que les limitations apportées à la protection des données doivent rester limitées à ce qui est strictement nécessaire et qu'un objectif d'intérêt général doit être mis en balance avec la gravité de l'ingérence dans les droits concernés.

Le Conseil constitutionnel applique également un contrôle tenant notamment compte des finalités poursuivies, de la nature et de l'étendue des données collectées ainsi que des garanties entourant leur utilisation.

Références officielles :

CJUE : jurisprudence relative aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.

Conseil constitutionnel : contrôle de nécessité et de proportionnalité des dispositifs de collecte et de traitement de données à caractère personnel.

6.1 Cadre juridique applicable

Statut : GARANTIES JURIDIQUES ÉTABLIES / POINTS DE VIGILANCE IDENTIFIÉS

Les chapitres précédents ont étudié principalement l'existence des données, leur circulation et les possibilités d'interconnexion entre différentes infrastructures.

Le Chapitre 6 pose une question différente :

> **le fait qu'un traitement soit techniquement réalisable et poursuive un objectif d'intérêt général suffit-il à le rendre juridiquement admissible ?**

La réponse est négative.

Plusieurs niveaux de droit encadrent les traitements étudiés.

Le RGPD s'applique aux données personnelles utilisées dans le dispositif

Le règlement général sur la protection des données s'applique lorsqu'une information concerne une personne physique identifiée ou identifiable S36.

Toutes les données contenues dans une facture ne constituent donc pas nécessairement des données personnelles.

Une facture concernant une société peut comporter principalement des informations relatives à une personne morale.

Mais les systèmes de facturation peuvent également contenir des informations permettant d'identifier directement ou indirectement des personnes physiques.

Ce point n'est plus seulement théorique concernant l'exploitation fiscale des données issues de la réforme.

La CNIL qualifie explicitement les données issues de la facturation électronique ajoutées au traitement CFVR de **données personnelles collectées** S37.

AVÉRÉ :

> Au moins une partie des données provenant de la réforme de la facturation électronique entre dans le champ de la protection des données personnelles.

Le dispositif ne se situe donc pas en dehors du RGPD au seul motif qu'il concerne principalement des transactions économiques entre entreprises.

La réforme dispose d'une base légale

Un premier argument doit immédiatement être écarté.

La transmission des données à l'administration n'est pas mise en œuvre sans fondement juridique.

Elle résulte notamment du Code général des impôts, de dispositions législatives et réglementaires organisant la facturation électronique et le e-reporting.

Le décret organisant le dispositif vise lui-même explicitement le RGPD et a été adopté après consultation de la CNIL S38.

ARGUMENT INSUFFISANT :

> « La collecte est obligatoire et réalisée sans consentement, donc elle viole nécessairement le RGPD. »

Le RGPD ne repose pas uniquement sur le consentement.

Un traitement peut notamment être fondé sur une obligation légale ou être nécessaire à l'exécution d'une mission d'intérêt public prévue par le droit S36.

L'absence de consentement des entreprises ou personnes concernées ne suffit donc pas, à elle seule, à rendre la réforme illégale.

L'existence d'une base légale ne donne cependant pas un droit illimité d'utilisation

C'est ici qu'apparaît une première distinction juridique importante.

Le RGPD impose que les données soient :

> collectées pour des finalités déterminées, explicites et légitimes ;

et :

> non réutilisées ultérieurement d'une manière incompatible avec ces finalités S36.

Il impose également que les données soient :

> adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités poursuivies S36.

Par conséquent :

```
base légale
   ≠
autorisation générale de réutilisation
```

et :

```
collecte légalement obligatoire
   ≠
possibilité illimitée de croiser les données pour toute politique publique future
```

GARANTIE JURIDIQUE ÉTABLIE :

> Une réutilisation ultérieure de données personnelles doit rester compatible avec le cadre juridique applicable, notamment les finalités et principes de nécessité, de proportionnalité et de minimisation.

Cette distinction devient particulièrement importante au regard des interconnexions étudiées dans le Chapitre 5.

Une découverte importante : les données de facturation alimentent effectivement un traitement algorithmique de ciblage fiscal

Le Chapitre 2 avait laissé ouverte la question des traitements automatisés réellement appliqués aux données issues de la réforme.

La documentation publiée en 2026 permet désormais d'apporter une réponse précise.

La CNIL a examiné l'intégration des données issues de la facturation électronique au traitement automatisé **CFVR — ciblage de la fraude et valorisation des requêtes** S37.

Cette évolution a ensuite été inscrite dans le cadre réglementaire par l'arrêté du 10 juillet 2026 modifiant l'arrêté portant création de CFVR S45.

Les données issues de la facturation électronique font donc désormais partie des catégories de données intégrées au dispositif CFVR.

La CNIL précise en outre qu'une partie des données de CFVR ainsi que les données issues de la facturation électronique doivent alimenter la plateforme sécurisée des données de la DGFiP afin d'y être exploitées, notamment en raison de leur volumétrie S37.

Elle relève que :

> leur ajout augmente substantiellement le volume de données traitées ;

et que la volumétrie concernée est de l'ordre de :

> **2 à 3 milliards de factures électroniques par an** S37.

Les résultats issus de l'exploitation réalisée sur cette plateforme peuvent ensuite alimenter CFVR et être rapprochés d'autres informations afin de contribuer notamment à l'identification d'anomalies et d'entreprises présentant certains risques fiscaux S37.

AVÉRÉ :

> L'intégration des données issues de la facturation électronique au traitement CFVR repose désormais sur un texte réglementaire adopté S45.

AVÉRÉ :

> Ces données sont destinées à être exploitées à grande échelle au sein de l'infrastructure d'analyse de données de la DGFiP pour des finalités liées au contrôle et au ciblage fiscal S37-S45.

GARANTIE JURIDIQUE ÉTABLIE :

> Cette intégration ne soustrait pas les traitements réalisés aux principes applicables de finalité, minimisation, sécurité, nécessité et proportionnalité S36-S43-S44.

Les données sont croisées avec d'autres résultats d'analyse

L'avis de la CNIL apporte un second élément important.

Les données exploitées sur la plateforme doivent permettre de produire des résultats qui peuvent être croisés avec les autres informations utilisées par CFVR afin d'obtenir notamment des listes d'entreprises considérées comme présentant certains risques fiscaux S37.

La CNIL indique également qu'à terme l'ensemble des données du traitement CFVR a vocation à alimenter la plateforme sécurisée des données.

La chaîne réellement documentée devient donc :

```
données de facturation électronique
   ↓
plateforme sécurisée des données DGFiP
   ↓
exploitation algorithmique
   ↓
rapprochement avec d'autres données / résultats
   ↓
détection d'anomalies
   ↓
identification d'entreprises présentant certains risques
   ↓
orientation possible du contrôle fiscal
```

AVÉRÉ :

> Le croisement et l'analyse automatisée de données issues de la facturation électronique avec d'autres informations fiscales ne constituent plus une simple possibilité technique.

Ils font partie des usages documentés du dispositif CFVR S37.

Le traitement dépasse les seules entreprises

L'historique de CFVR décrit par la CNIL mérite également d'être relevé.

Initialement développé pour les contribuables professionnels, le dispositif a ensuite été étendu aux personnes physiques impliquées dans le fonctionnement des entreprises, puis aux particuliers S37.

Cela ne signifie pas que chaque donnée de facturation électronique sera associée à chaque particulier.

Mais cela démontre que l'infrastructure analytique dans laquelle ces données viennent désormais s'insérer n'est pas limitée par nature aux seules personnes morales.

POINT DE VIGILANCE :

> L'intégration massive des données issues de la facturation électronique dans une infrastructure utilisant déjà différentes catégories de données relatives aux professionnels et aux personnes physiques renforce l'importance des règles de finalité, de minimisation, d'habilitation et de proportionnalité.

Des échanges avec d'autres administrations sont également documentés

La même délibération décrit des échanges entre la DGFiP et les organismes de sécurité sociale dans le cadre de CFVR S37.

Ces échanges disposent d'un fondement juridique spécifique et sont limités à certaines finalités.

La CNIL considère ces finalités légitimes dans le cadre juridique actuellement prévu.

AVÉRÉ :

> Des mécanismes juridiques permettent déjà à certaines données administratives de circuler entre organismes publics pour des finalités déterminées.

Mais la CNIL insiste précisément sur :

- la minimisation des données ;
- la limitation aux agents habilités ;
- le besoin d'en connaître ;
- la durée de conservation ;
- l'information des personnes ;
- la proportionnalité des échanges S37.

Cette observation est essentielle pour la suite de l'enquête.

GARANTIE JURIDIQUE ÉTABLIE :

> L'interconnexion entre administrations n'est pas juridiquement libre : elle doit reposer sur un fondement juridique et respecter des finalités et garanties déterminées.

Première zone de vulnérabilité : l'extension progressive des finalités

La réforme repose initialement sur des objectifs notamment fiscaux : modernisation de la collecte de TVA, lutte contre la fraude, pré-remplissage et amélioration de la connaissance de l'activité économique.

L'utilisation des données pour le ciblage fiscal possède donc un lien direct avec plusieurs finalités annoncées.

ARGUMENT INSUFFISANT À CE STADE :

> L'utilisation actuelle des données de facturation par CFVR constituerait nécessairement un détournement de finalité.

Les sources étudiées ne permettent pas de soutenir cette conclusion.

La lutte contre la fraude et le contrôle fiscal font précisément partie du cadre dans lequel ces traitements sont organisés.

En revanche, la question deviendrait juridiquement beaucoup plus sensible si les mêmes données étaient ultérieurement réutilisées pour une finalité substantiellement différente.

Par exemple :

```
collecte pour finalité fiscale
   ↓
conservation d'une infrastructure détaillée de transactions
   ↓
réutilisation pour une autre politique publique
   ↓
rapprochement avec d'autres catégories de données
```

Une telle évolution devrait être examinée au regard de la limitation des finalités, de sa base juridique, de sa nécessité et de sa proportionnalité S36-S43.

VULNÉRABILITÉ POTENTIELLE :

> La capacité technique de réutiliser les données ne constitue pas une base juridique permettant de leur attribuer librement de nouvelles finalités.

Deuxième zone de vulnérabilité : la volumétrie et la proportionnalité

La CNIL constate elle-même l'augmentation substantielle du volume de données provoquée par l'intégration de la facturation électronique à CFVR S37.

Le volume annoncé atteint plusieurs milliards de factures par an.

Or la jurisprudence relative à la protection de la vie privée et des données personnelles impose de mettre en balance :

> l'objectif d'intérêt général poursuivi

avec :

> la nature, l'étendue et la sensibilité des données traitées ainsi que la gravité de l'ingérence S39-S44.

La question juridique pertinente n'est donc pas simplement :

> « la lutte contre la fraude est-elle un objectif légitime ? »

Elle l'est.

La question est :

> **« l'étendue précise des données collectées, leur niveau de détail, leur durée de conservation, leurs croisements et leurs modalités d'exploitation sont-ils nécessaires et proportionnés à cet objectif ? »**

C'est sur ce terrain qu'un contrôle juridique devient réellement intéressant.

Troisième zone de vulnérabilité : la protection des données dès la conception et par défaut

Le principe de minimisation ne s'applique pas uniquement au choix initial des catégories de données collectées.

L'article 25 du RGPD impose également au responsable du traitement de mettre en œuvre des mesures techniques et organisationnelles permettant d'appliquer effectivement les principes de protection des données dès la conception et par défaut S43.

Le règlement précise que cette exigence concerne notamment :

- la quantité de données personnelles collectées ;
- l'étendue de leur traitement ;
- leur durée de conservation ;

- leur accessibilité.

Cette disposition est particulièrement pertinente concernant une infrastructure appelée à traiter plusieurs milliards de factures électroniques par an et à permettre leur exploitation au sein d'une plateforme disposant d'importantes capacités de calcul S37.

La question juridique ne porte donc pas uniquement sur l'existence d'une base permettant l'intégration des données.

Elle porte également sur la conception concrète de l'infrastructure :

> quelles données sont réellement nécessaires ?

> pendant combien de temps ?

> pour quels traitements ?

> accessibles à quels agents ?

> avec quel niveau de granularité ?

> et quelles mesures empêchent techniquement leur utilisation au-delà des finalités autorisées ?

La CNIL exige précisément que la plateforme sécurisée des données conserve un cloisonnement strict, que les données qui y sont versées soient uniquement traitées pour les finalités prévues et que son utilisation n'ouvre pas l'accès à de nouveaux destinataires non prévus S37.

GARANTIE JURIDIQUE ÉTABLIE :

> Le RGPD impose que la protection des données et la minimisation soient intégrées à la conception même du traitement et que, par défaut, seules les données nécessaires à chaque finalité spécifique soient traitées S43.

POINT DE VIGILANCE :

> L'augmentation de la capacité technique de stockage, de calcul ou de croisement ne constitue pas en elle-même une justification permettant d'élargir les données accessibles ou les traitements réalisés.

QUESTION JURIDIQUE À DOCUMENTER :

> Les mesures techniques et organisationnelles effectivement mises en œuvre dans CFVR et dans la plateforme sécurisée des données permettent-elles de démontrer, pour les données issues de la facturation électronique, l'application effective des principes de minimisation et de protection des données dès la conception et par défaut ?

Quatrième zone de vulnérabilité : la maîtrise des accès

La CNIL insiste également sur la nécessité de limiter les accès à un nombre restreint d'agents et au strict besoin d'en connaître S37.

Elle demande que la plateforme sécurisée :

> conserve un cloisonnement strict des données ;

> ne permette leur traitement que pour les finalités prévues ;

> n'ouvre pas l'accès à de nouveaux destinataires non prévus.

Cette exigence est particulièrement importante pour notre enquête.

Elle signifie qu'une infrastructure techniquement capable d'accueillir plusieurs catégories de données ne peut juridiquement devenir un espace général de réutilisation sans nouvel encadrement.

GARANTIE JURIDIQUE ÉTABLIE :

> Le cloisonnement des finalités et des accès constitue actuellement une protection juridiquement significative contre une réutilisation généralisée des données.

POINT DE VIGILANCE :

> Toute extension des catégories d'accédants, des finalités ou des données croisées doit être examinée séparément afin de déterminer si le fondement juridique et les garanties existantes demeurent suffisants.

Une distinction fondamentale apparaît

Le résultat de cette première analyse est différent de deux positions extrêmes.

Il serait juridiquement incorrect d'affirmer :

> **« La réforme viole le RGPD parce que les données sont transmises sans consentement. »**

Une base légale existe et le consentement n'est pas la seule base permettant un traitement.

Mais il serait également incorrect d'affirmer :

> **« Puisque la collecte est prévue par la loi, l'administration peut ensuite faire ce qu'elle souhaite avec les données. »**

Le RGPD et les exigences constitutionnelles et européennes de protection de la vie privée continuent d'encadrer :

- les finalités ;
- les catégories de données ;
- leur nécessité ;
- leur proportionnalité ;
- leur conservation ;
- leurs destinataires ;
- leurs croisements ;
- les décisions automatisées ;
- les mesures de sécurité.

Première conclusion juridique

AVÉRÉ :

> La réforme repose sur un cadre légal et réglementaire et a fait l'objet d'une consultation de la CNIL.

AVÉRÉ :

> Les données issues de la facturation électronique comprennent des données personnelles soumises aux garanties du RGPD.

AVÉRÉ :

> Ces données sont destinées à alimenter une infrastructure de la DGFiP permettant leur exploitation algorithmique à grande échelle pour le ciblage fiscal.

AVÉRÉ :

> La CNIL constate elle-même une augmentation substantielle de la volumétrie et identifie des risques relatifs à la minimisation, aux accès, à la conservation, à la sécurité, aux biais algorithmiques et à l'automatisation.

AVÉRÉ :

> Certains échanges et croisements entre administrations sont juridiquement possibles lorsqu'un texte les prévoit et que leurs finalités sont déterminées.

GARANTIE JURIDIQUE ÉTABLIE :

> Une collecte légalement instituée ne permet pas une réutilisation illimitée des données pour n'importe quelle finalité.

VULNÉRABILITÉ POTENTIELLE :

> Toute extension substantielle des finalités, des catégories de données, des destinataires ou des mécanismes de rapprochement doit pouvoir satisfaire aux exigences de base légale, de nécessité, de minimisation et de proportionnalité.

À ÉTABLIR :

> L'étendue exacte des garanties entourant chacun des traitements issus de la réforme et la possibilité de contester juridiquement certaines extensions ou modalités d'exploitation doivent être examinées dans les sections suivantes.

Ce que 6.1 change dans l'enquête

Un élément qui était encore partiellement ouvert dans les premiers chapitres peut désormais être précisé.

La chaîne suivante est documentée :

```
facturation électronique
   ↓
données personnelles et économiques à très grande échelle
   ↓
plateforme sécurisée des données DGFiP
   ↓
exploitation algorithmique
   ↓
croisements / analyses
   ↓
détection d'anomalies et ciblage fiscal
   ↓
décision humaine éventuelle d'engager un contrôle
```

La question juridique n'est donc plus de savoir si les données de facturation **peuvent techniquement être exploitées et croisées à grande échelle**.

Cette exploitation est désormais documentée dans le domaine fiscal.

La question devient :

> **jusqu'où cette exploitation peut-elle juridiquement aller avant de rencontrer les principes de limitation des finalités, de minimisation, de nécessité, de proportionnalité et de protection contre certaines décisions automatisées ?**

C'est cette frontière que les sections suivantes doivent rechercher.

6.2 Finalité des traitements et réutilisation des données

Statut : GARANTIES JURIDIQUES ÉTABLIES / LATITUDES JURIDIQUES IDENTIFIÉES / FRONTIÈRES À ÉTABLIR

Le principe de limitation des finalités constitue l'une des principales protections juridiques applicables aux architectures étudiées dans les chapitres précédents.

Mais sa portée doit être décrite avec précision.

Une interprétation trop simple consisterait à considérer que :

> **« toute nouvelle utilisation d'une donnée pour une finalité différente de celle annoncée lors de sa collecte est interdite. »**

Le RGPD ne pose pas une interdiction aussi absolue.

Il organise au contraire plusieurs mécanismes permettant, sous conditions, certains traitements ultérieurs S36-S43-S46.

Une finalité doit être déterminée, explicite et légitime

Le principe initial reste clair.

Les données personnelles doivent être collectées pour des finalités déterminées, explicites et légitimes et ne doivent pas être traitées ultérieurement d'une manière incompatible avec ces finalités S36-S43.

Cette règle empêche en principe qu'une infrastructure constituée pour un objectif déterminé devienne, par sa seule existence technique, une réserve générale de données utilisable pour n'importe quel objectif futur.

Elle impose donc de distinguer :

```
capacité technique de réutilisation
   ↓
finalité juridiquement définie
   ↓
base juridique
   ↓
nécessité / proportionnalité
   ↓
traitement autorisé
```

La première étape ne suffit jamais à démontrer les suivantes.

GARANTIE JURIDIQUE :

> La disponibilité technique d'une donnée ne constitue pas, à elle seule, une finalité ni une base juridique permettant son utilisation.

Une nouvelle finalité n'est cependant pas automatiquement interdite

L'article 6, paragraphe 4 du RGPD prévoit explicitement le cas dans lequel des données sont traitées ultérieurement pour une finalité autre que celle ayant justifié leur collecte initiale S46.

Lorsque ce traitement ultérieur ne repose ni sur le consentement de la personne concernée ni sur une disposition pertinente du droit de l'Union ou d'un État membre, le responsable du traitement doit notamment déterminer si cette nouvelle finalité est compatible avec la finalité initiale.

Le règlement prévoit plusieurs critères permettant cette appréciation :

- le lien entre la finalité initiale et la finalité ultérieure ;
- le contexte dans lequel les données ont été collectées ;
- la nature des données ;
- les conséquences possibles du nouveau traitement pour les personnes ;
- les garanties mises en œuvre, notamment le chiffrement ou la pseudonymisation S46.

Il existe donc juridiquement un :

> **test de compatibilité des finalités.**

LATITUDE JURIDIQUE :

> Une donnée collectée pour une finalité déterminée peut, sous certaines conditions, faire l'objet d'un traitement ultérieur compatible avec cette finalité.

Cela signifie que :

```
nouvelle utilisation
   ≠
illégalité automatique
```

Mais également que :

```
nouvelle utilisation
   ≠
compatibilité automatique
```

La compatibilité doit être appréciée au regard du traitement effectivement envisagé.

Une seconde voie existe : l'intervention du droit

L'article 6, paragraphe 4 révèle une seconde possibilité importante pour cette enquête.

Le mécanisme du test de compatibilité qu'il décrit concerne le cas dans lequel le traitement ultérieur n'est pas fondé notamment sur le droit de l'Union ou d'un État membre constituant une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs prévus par l'article 23 du RGPD S46.

Autrement dit, l'évolution des usages ne dépend pas uniquement de la compatibilité avec la finalité initiale.

Le droit peut également encadrer certains nouveaux traitements ou certaines restrictions dans les conditions prévues par le RGPD.

LATITUDE JURIDIQUE :

> Le cadre juridique peut évoluer et permettre certains traitements ultérieurs qui ne reposent pas uniquement sur la compatibilité avec la finalité initiale.

Cette latitude est fondamentale pour l'analyse des architectures étudiées dans ce dépôt.

Une infrastructure techniquement existante peut aujourd'hui être juridiquement limitée à certaines finalités, sans que cette limitation constitue nécessairement une impossibilité juridique définitive.

Une évolution du droit pourrait modifier les traitements autorisés.

Cela ne permet cependant pas de présumer qu'une telle évolution aura lieu.

Le domaine fiscal bénéficie explicitement de cette latitude

Cette possibilité n'est pas purement abstraite dans le domaine étudié.

L'article 23 du RGPD prévoit expressément que le droit de l'Union ou le droit national peut, sous certaines conditions, limiter la portée de plusieurs obligations et droits prévus par le règlement afin de garantir certains objectifs importants d'intérêt public S47.

Parmi les domaines explicitement mentionnés figurent notamment :

- les intérêts économiques ou financiers importants ;
- le domaine monétaire ;
- le domaine budgétaire ;
- le domaine fiscal ;
- la sécurité sociale ;
- certaines missions de contrôle, d'inspection ou de réglementation liées à l'exercice de l'autorité publique S47.

Cette possibilité reste conditionnée.

La mesure doit notamment :

> respecter l'essence des libertés et droits fondamentaux ;

et :

> être nécessaire et proportionnée dans une société démocratique S47.

GARANTIE JURIDIQUE :

> Le RGPD n'autorise pas une restriction générale et sans contrôle des droits au nom de l'intérêt fiscal.

LATITUDE JURIDIQUE :

> Le RGPD prévoit explicitement la possibilité pour le législateur d'aménager certaines protections ou certains droits lorsque des objectifs fiscaux ou des missions de contrôle le justifient, sous réserve notamment des exigences de nécessité et de proportionnalité.

Cette latitude est déjà utilisée dans le cadre CFVR

Le lien avec l'enquête devient particulièrement concret dans l'arrêté du 10 juillet 2026 modifiant CFVR S45-S47.

Cet arrêté :

- intègre les données issues de la facturation électronique parmi les données traitées ;
- étend ou précise plusieurs sources de données utilisées par le dispositif ;
- organise certains accès et transmissions ;
- et fait explicitement référence aux points e) et h) du paragraphe 1 de l'article 23 du RGPD S45-S47.

Il ne s'agit donc pas seulement d'une possibilité théorique contenue dans le règlement européen.

Le cadre réglementaire actuel de CFVR mobilise déjà les mécanismes juridiques permettant certaines limitations dans le contexte fiscal et des missions de contrôle.

AVÉRÉ :

> Le cadre juridique de CFVR fait explicitement référence aux possibilités de limitation prévues par l'article 23 du RGPD pour certains objectifs d'intérêt public et certaines missions de contrôle S45-S47.

Le droit peut donc déplacer la frontière sans supprimer toutes les garanties

Cette observation conduit à une distinction importante.

Il serait incorrect d'écrire :

> **« Les finalités annoncées aujourd'hui interdisent définitivement toute nouvelle utilisation future. »**

Le droit peut évoluer.

Il serait tout aussi incorrect d'écrire :

> **« Il suffit d'adopter un nouveau texte pour rendre juridiquement possible n'importe quelle utilisation des données. »**

Les nouvelles dispositions restent elles-mêmes soumises aux normes juridiques supérieures applicables.

Selon les situations, cela peut notamment inclure :

- le RGPD ;
- la Charte des droits fondamentaux de l'Union européenne ;
- le droit au respect de la vie privée ;
- le contrôle de nécessité ;
- le contrôle de proportionnalité ;
- le principe de minimisation ;
- les garanties applicables aux personnes concernées S39-S43-S44-S46-S47.

La véritable frontière n'est donc pas :

```
possible
   /
impossible
```

mais plutôt :

```
usage actuellement autorisé
   ↓
extension envisagée
   ↓
compatibilité éventuelle
   ou
nouvelle base juridique
   ↓
contrôle de nécessité
   ↓
contrôle de proportionnalité
   ↓
garanties applicables
```

Première vulnérabilité juridique : l'extension progressive peut être légale

Cette conclusion fait apparaître une vulnérabilité particulière.

Elle ne résulte pas nécessairement d'une violation du droit.

Elle résulte au contraire de la capacité du droit à faire évoluer progressivement le périmètre des traitements autorisés.

Une infrastructure peut ainsi connaître successivement :

```
finalité A
   ↓
extension compatible A → A+
   ↓
nouveau fondement juridique
   ↓
extension vers B
   ↓
nouveaux rapprochements autorisés
```

Chaque étape peut être juridiquement encadrée et pourtant conduire, dans le temps, à une architecture dont le périmètre est beaucoup plus large que lors de sa création.

VULNÉRABILITÉ JURIDIQUE :

> La limitation des finalités constitue une protection contre les réutilisations incompatibles non suffisamment fondées, mais elle ne garantit pas l'immuabilité du périmètre juridique d'un traitement.

IMPORTANT :

> Cette possibilité d'évolution ne démontre ni qu'une extension particulière est envisagée ni qu'elle serait juridiquement admissible.

Elle démontre seulement que :

> **la frontière juridique peut évoluer sans nécessiter de modifier l'architecture technique déjà disponible.**

Deuxième vulnérabilité : l'accumulation des extensions

L'analyse juridique d'une extension est généralement effectuée au regard d'un traitement et d'une finalité déterminés.

Mais l'enquête étudie également l'effet cumulé de plusieurs infrastructures et évolutions successives.

Une succession d'extensions individuellement justifiées peut progressivement augmenter :

- le nombre de données disponibles ;
- le nombre de sources ;
- le nombre de rapprochements possibles ;
- le nombre de destinataires ;
- la durée pendant laquelle certaines informations demeurent exploitables ;
- la capacité de profilage ou d'analyse.

La question devient alors :

> **à quel moment l'effet cumulé de plusieurs extensions juridiquement fondées modifie-t-il suffisamment la nature ou l'intensité du traitement pour imposer une nouvelle appréciation de nécessité et de proportionnalité ?**

À ÉTABLIR :

> Dans quelle mesure le droit applicable impose-t-il de réévaluer la proportionnalité non seulement de chaque extension prise isolément, mais également de l'architecture résultant de leur accumulation ?

Cette question devra être rapprochée des analyses de nécessité, de proportionnalité et d'impact étudiées dans les sections suivantes.

Une frontière essentielle pour les interconnexions du Chapitre 5

Cette analyse permet également de conserver une frontière méthodologique essentielle concernant les chaînes étudiées précédemment.

Le Chapitre 5 a identifié plusieurs capacités techniques ou expérimentales reliant notamment :

```
transaction
   ↓
produit
   ↓
DPP
   ↓
données environnementales
```

ainsi que :

```
données externes
   ↓
condition
   ↓
paiement conditionnel
```

L'existence du mécanisme de traitement ultérieur prévu par le RGPD ne permet pas de transformer ces possibilités techniques en usages juridiquement autorisés.

Elle ne permet pas davantage de conclure qu'une future base juridique sera créée pour les relier.

NON ÉTABLI :

> Aucun élément étudié dans cette section n'établit que les données environnementales du DPP puissent actuellement être utilisées afin de déterminer l'autorisation, le refus ou la limitation d'un paiement.

DÉDUCTIBLE JURIDIQUEMENT :

> Si une telle interconnexion impliquant des données personnelles devait être mise en œuvre, sa conformité devrait être examinée au regard de sa finalité, de sa base juridique et des garanties applicables, ainsi que, selon le mécanisme retenu, des exigences de nécessité, de proportionnalité et de minimisation.

Cette distinction empêche de confondre :

```
évolution juridiquement possible en théorie
   ↓
   et
usage juridiquement autorisé aujourd'hui
```

Conclusion de 6.2

AVÉRÉ :

> Le RGPD interdit les traitements ultérieurs incompatibles avec les finalités initiales lorsqu'aucun autre fondement pertinent ne permet le traitement S36-S43-S46.

AVÉRÉ :

> Le RGPD prévoit un mécanisme permettant d'évaluer la compatibilité d'une finalité ultérieure avec la finalité initiale S46.

AVÉRÉ :

> Le droit de l'Union ou le droit national peut également prévoir certaines limitations ou certains traitements dans les conditions prévues par le RGPD, notamment pour des objectifs importants relevant du domaine fiscal et pour certaines missions de contrôle S46-S47.

AVÉRÉ :

> Le cadre CFVR modifié en juillet 2026 fait explicitement référence aux points e) et h) de l'article 23, paragraphe 1 du RGPD S45-S47.

GARANTIE JURIDIQUE :

> Une extension des usages ne devient pas licite du seul fait qu'elle est techniquement possible ou qu'elle poursuit un objectif d'intérêt général.

LATITUDE JURIDIQUE :

> Le droit permet néanmoins certaines réutilisations compatibles et peut faire évoluer le périmètre des traitements autorisés, sous réserve des conditions et garanties applicables.

VULNÉRABILITÉ JURIDIQUE :

> La limitation des finalités protège contre certaines réutilisations, mais ne fige pas définitivement le périmètre juridique d'une infrastructure de données.

À ÉTABLIR :

> Jusqu'où des extensions successives de finalités, de sources de données et de destinataires peuvent-elles s'accumuler avant que leur effet global impose une nouvelle appréciation de nécessité et de proportionnalité ?

NON ÉTABLI :

> Rien dans les sources étudiées ici ne démontre qu'une évolution juridique soit actuellement envisagée afin de relier les données environnementales du DPP à l'autorisation, au refus ou à la limitation d'un paiement.

6.3 Croisement, rapprochement et interconnexion des données

Statut : INTERCONNEXIONS AVÉRÉES / GARANTIES DOCUMENTÉES / VULNÉRABILITÉS ET ANGLES MORTS IDENTIFIÉS

Les chapitres précédents ont montré que plusieurs infrastructures étudiées disposent de capacités de rapprochement ou d'interconnexion.

Dans le domaine fiscal, cette question n'est désormais plus seulement technique.

Le traitement CFVR constitue déjà une architecture alimentée par de nombreuses sources de données et permettant leur analyse ou leur rapprochement S37-S45.

L'enjeu juridique devient donc double :

> **quelles interconnexions sont effectivement autorisées ?**

et :

> **quelles garanties empêchent qu'une infrastructure de rapprochement de données à grande échelle devienne elle-même une source disproportionnée de risque, notamment en cas de compromission, de mésusage ou d'extension des accès ?**

CFVR constitue déjà une infrastructure multi-sources

L'arrêté modifiant CFVR en juillet 2026 ne se limite pas à l'ajout des données issues de la facturation électronique S45.

Le traitement est alimenté par de nombreuses autres sources.

La liste réglementaire comprend notamment des données issues :

- des dossiers fiscaux ;
- des déclarations fiscales ;
- du prélèvement à la source ;
- des données foncières et d'occupation des logements ;
- des successions ;
- des coordonnées de comptes bancaires déclarées par les foyers fiscaux ;
- des paiements transfrontaliers enregistrés dans CESOP ;
- de la TVA intracommunautaire ;
- des échanges de biens au sein de l'Union européenne ;
- des traitements relatifs aux quittus automobiles ;
- de traitements de données provenant d'organismes sociaux ;
- de données publiquement accessibles collectées sur certaines plateformes en ligne ;
- et désormais de la facturation électronique S45.

L'arrêté prévoit également des données concernant des personnes physiques nécessaires à certains travaux portant sur l'intensité de l'activité économique S45.

AVÉRÉ :

> CFVR n'est pas une base limitée aux seules données issues de la facturation électronique.

Il constitue une infrastructure analytique alimentée par un ensemble beaucoup plus large de sources fiscales, économiques, administratives et, dans certains cas, relatives à des personnes physiques.

Le croisement est une fonction documentée du dispositif

La CNIL décrit explicitement le fonctionnement prévu pour les nouvelles données de facturation électronique S37.

Une partie des données de CFVR ainsi que les données issues de la facturation électronique doivent alimenter la plateforme sécurisée des données de la DGFiP.

Les résultats des requêtes effectuées sur cette plateforme peuvent ensuite être croisés avec les données provenant de CFVR afin d'obtenir notamment des listes d'entreprises considérées comme présentant certains risques.

À terme :

> **l'ensemble des données de CFVR a vocation à alimenter cette plateforme** S37.

La chaîne documentée devient donc :

```
multiples sources administratives / fiscales
   ↓
CFVR
   ↓
données de facturation électronique
   +
autres données CFVR
   ↓
plateforme sécurisée des données
   ↓
requêtes / modèles / analyses
   ↓
croisement de résultats
   ↓
détection d'anomalies
   ↓
sélection de dossiers présentant certains risques
```

AVÉRÉ :

> Le rapprochement de plusieurs ensembles de données constitue une fonction effective et réglementairement organisée de CFVR S37-S45.

Il ne s'agit donc plus seulement d'une interconnexion techniquement envisageable.

Les échanges entre administrations élargissent encore le périmètre

Les interconnexions documentées dépassent également la seule DGFiP.

L'article L. 152 du livre des procédures fiscales permet certains échanges entre l'administration fiscale et les organismes de sécurité sociale.

Le dispositif CFVR a été adapté en conséquence S37-S45.

Les données peuvent être transmises aux organismes sociaux pour certaines missions de contrôle de l'assiette des cotisations.

En sens inverse, certaines données communiquées par ces organismes peuvent également alimenter CFVR.

La CNIL mentionne notamment des informations relatives :

- au travail dissimulé ;
- aux rémunérations ;
- aux résultats de contrôles fiscaux S37.

AVÉRÉ :

> Il existe donc une circulation juridiquement organisée dans les deux sens entre l'administration fiscale et certains organismes sociaux.

Cette circulation repose sur une base légale et sur des finalités déterminées.

Le périmètre des personnes ayant accès au système évolue également

L'arrêté de juillet 2026 prévoit plusieurs catégories d'agents habilités pouvant accéder aux données nécessaires aux travaux de modélisation et de visualisation S45.

Il comprend notamment des agents appartenant :

- au réseau national d'analyse de données ;
- aux structures de programmation interrégionales ;
- à certains services nationaux spécialisés ;
- à des directions départementales des finances publiques ;
- à la direction nationale des enquêtes fiscales.

Les résultats utiles sont également accessibles, dans la limite du besoin d'en connaître, à certains agents chargés de la gestion, de la programmation et du contrôle des dossiers ainsi qu'à certains agents habilités des organismes de sécurité sociale S45.

La CNIL indique que les membres du réseau national doivent être individuellement habilités, formés et supervisés et que certaines requêtes peuvent être validées ou refusées par le bureau compétent S37.

GARANTIE JURIDIQUE ET ORGANISATIONNELLE :

> Les accès ne sont pas présentés comme ouverts indistinctement à l'ensemble des agents publics.

Ils reposent sur des habilitations et doivent être limités au besoin d'en connaître S37-S45.

Le croisement à grande échelle constitue lui-même un facteur de risque reconnu

Cette architecture doit cependant être rapprochée des critères utilisés par la CNIL en matière d'analyse d'impact.

Parmi les critères permettant d'identifier des traitements susceptibles d'engendrer un risque élevé figurent notamment :

- le traitement à grande échelle ;
- le croisement ou la combinaison d'ensembles de données ;
- l'évaluation ou le scoring ;

- l'usage de technologies ou méthodes innovantes S49.

CFVR présente publiquement plusieurs caractéristiques correspondant à ces critères :

```
volume massif
   +
croisements de données
   +
analyse / ciblage
   +
méthodes algorithmiques
```

La CNIL constate elle-même que l'arrivée de la facturation électronique augmente **substantiellement** le volume de données traitées et évoque plusieurs milliards de factures par an S37.

POINT DE VIGILANCE MAJEUR :

> L'augmentation simultanée de la volumétrie, du nombre de sources et des capacités de rapprochement augmente non seulement la puissance analytique du système, mais également les conséquences potentielles d'une erreur, d'un mésusage ou d'une compromission.

Première vulnérabilité : la concentration accroît l'impact potentiel d'une compromission

Une base ou une plateforme capable de rapprocher de nombreuses catégories de données présente un risque différent de plusieurs bases strictement cloisonnées.

Une compromission ne porterait plus nécessairement sur une seule information isolée.

Selon les accès effectivement obtenus, elle pourrait permettre de rapprocher plusieurs catégories d'informations.

Le RGPD impose précisément que le niveau de sécurité soit adapté :

- à la nature des données ;
- à leur portée ;
- au contexte du traitement ;
- à la probabilité du risque ;
- à sa gravité S48.

La CNIL va ici beaucoup plus loin qu'une formule générale.

Dans son avis concernant CFVR, elle relève explicitement :

> le volume massif des données ;

> leur sensibilité ;

> l'évolution de la menace ;

> et l'évolution des modes opératoires d'attaque informatique S37.

VULNÉRABILITÉ JURIDIQUE ET TECHNIQUE :

> Plus l'architecture concentre des données, des sources et des possibilités de rapprochement, plus le niveau de sécurité qui peut raisonnablement être exigé augmente.

Cela ne signifie pas que CFVR est actuellement compromis ou insuffisamment sécurisé.

Cela signifie que :

> **le changement d'échelle modifie également le niveau de risque dont l'administration doit pouvoir démontrer la maîtrise.**

La CNIL demande elle-même des protections renforcées contre les accès compromis

L'avis de la CNIL apporte ici un élément particulièrement concret S37.

Elle accueille favorablement l'engagement du ministère de systématiser :

- la double authentification ;
- l'accès uniquement depuis des terminaux sécurisés.

Mais la CNIL va plus loin concernant les journaux de connexion et d'activité.

Elle considère que la journalisation doit s'accompagner de mécanismes permettant notamment :

- une analyse proactive des événements ;
- la détection de comportements inattendus ;
- la génération d'alertes ;
- le blocage immédiat des comptes concernés jusqu'à la levée du doute par la hiérarchie S37.

GARANTIE DOCUMENTÉE :

> La double authentification et l'utilisation de terminaux sécurisés font l'objet d'un engagement du ministère relevé positivement par la CNIL.

ANGLE MORT DOCUMENTAIRE :

> Dans son avis publié en 2026, la CNIL invite spécifiquement le ministère à mettre en œuvre des mécanismes proactifs d'analyse des journaux, d'alerte et de blocage des comptes en cas de comportement inattendu.

Les sources publiques étudiées ici ne permettent pas encore d'établir si l'ensemble de ces mécanismes recommandés est effectivement déployé sur tous les environnements concernés.

À ÉTABLIR :

> Les mécanismes proactifs de détection et de blocage demandés par la CNIL ont-ils depuis été effectivement déployés, avec quelle couverture et selon quelles procédures ?

Voilà une question très concrète qui peut être adressée à l'administration.

Deuxième vulnérabilité : le risque ne provient pas uniquement d'une attaque extérieure

La sécurité d'une infrastructure de cette nature ne concerne pas uniquement un pirate obtenant un accès depuis Internet.

L'article 32 du RGPD couvre également les risques d'accès ou de divulgation non autorisés S48.

La maîtrise des habilitations devient donc fondamentale.

Une infrastructure réunissant :

```
plus de données
   +
plus de sources
   +
plus d'analyses
   +
plusieurs catégories d'accédants
```

augmente mécaniquement le nombre de situations dans lesquelles une habilitation erronée, un compte compromis, une mauvaise configuration ou un usage abusif pourrait avoir des conséquences importantes.

C'est précisément pour cette raison que la CNIL insiste sur :

- la limitation du nombre d'agents ;
- l'habilitation individuelle ;
- le strict besoin d'en connaître ;
- la supervision ;
- la journalisation ;
- l'analyse des comportements S37-S50.

VULNÉRABILITÉ :

> La sécurité du système dépend non seulement de la protection de son périmètre informatique mais également de la qualité permanente de la gestion des identités, des habilitations et de la détection des usages anormaux.

Troisième vulnérabilité : l'interconnexion étend la surface de confiance

Les échanges avec d'autres administrations ajoutent une autre dimension.

La CNIL prend acte de l'utilisation d'un outil sécurisé de transfert de fichiers avec chiffrement conforme à l'état de l'art pour les échanges avec les organismes sociaux S37.

C'est une garantie importante.

Mais une interconnexion crée nécessairement plusieurs environnements impliqués :

```
organisme A
   ↓
mécanisme de transfert
   ↓
organisme B
```

La sécurité globale ne dépend donc plus uniquement de l'infrastructure initiale.

Elle dépend également :

- des habilitations de chaque organisme ;
- de la sécurité des équipements de chaque organisme ;
- des copies éventuellement produites ;
- des durées de conservation ;
- de la suppression effective ;
- de la journalisation ;
- de la capacité de détecter un usage ou un transfert anormal.

GARANTIE DOCUMENTÉE :

> Les échanges DGFiP / organismes sociaux doivent utiliser un mécanisme de transfert sécurisé et chiffré S37.

VULNÉRABILITÉ STRUCTURELLE :

> Toute multiplication des destinataires ou des environnements dans lesquels les données sont accessibles étend la surface sur laquelle les garanties de confidentialité, d'intégrité et de contrôle des accès doivent être maintenues.

Il ne s'agit pas d'une preuve de faiblesse actuelle d'un organisme déterminé.

Il s'agit d'une conséquence de l'architecture distribuée elle-même.

Un angle mort très concret apparaît sur la conservation des données échangées

L'avis de la CNIL contient une observation particulièrement intéressante concernant les échanges avec les organismes sociaux S37.

La Commission constate que le projet d'arrêté qui lui avait été soumis :

> **ne précisait pas la durée de conservation des données transmises dans le cadre de ces communications.**

Elle rappelle alors que les échanges entre administrations ne sont permis que si leurs modalités restent proportionnées aux objectifs poursuivis et insiste sur la nécessité de limiter la conservation à la durée nécessaire S37.

ANGLE MORT DOCUMENTAIRE IDENTIFIÉ :

> Le texte soumis à la CNIL ne déterminait pas lui-même la durée de conservation des données transférées entre la DGFiP et les organismes de sécurité sociale.

Cela ne démontre pas que les données sont conservées sans limite.

Des durées peuvent être prévues dans d'autres textes, conventions, politiques internes ou traitements destinataires.

Mais cela produit une question juridiquement vérifiable :

À ÉTABLIR :

> Pour chaque catégorie de données transférée entre CFVR et les organismes sociaux, quelle est la durée maximale de conservation applicable chez le destinataire, par quel texte ou document est-elle déterminée, et comment sa suppression effective est-elle contrôlée ?

Ce point peut être beaucoup plus intéressant qu'une critique générale de la conservation.

Quatrième vulnérabilité : une modification du risque peut imposer une nouvelle appréciation

Le RGPD contient un mécanisme particulièrement pertinent pour suivre l'évolution de ce type d'architecture.

L'article 35 prévoit que, lorsqu'une analyse d'impact existe, le responsable du traitement doit réexaminer si le traitement demeure conforme à cette analyse lorsqu'une modification du risque intervient S48.

Or plusieurs transformations sont maintenant documentées :

- arrivée d'une nouvelle catégorie massive de données ;
- plusieurs milliards de factures supplémentaires ;
- utilisation d'une infrastructure de calcul renforcée ;
- croisement avec d'autres informations ;
- développement de nouvelles méthodes d'apprentissage ;
- extension organisationnelle du réseau d'analyse ;
- nouvelles relations avec des organismes sociaux S37-S45.

QUESTION JURIDIQUE MAJEURE :

> Ces évolutions ont-elles été intégrées à une AIPD existante ou ont-elles donné lieu à une nouvelle analyse ou à une réévaluation formelle du risque conformément à l'article 35 du RGPD ?

Les sources publiques étudiées ne permettent pas, à ce stade, de répondre complètement à cette question.

ANGLE MORT DOCUMENTAIRE :

> L'existence possible d'une AIPD interne ne doit pas être confondue avec son absence. En revanche, nous ne disposons pas encore d'un document public permettant d'établir précisément quelle analyse d'impact couvre l'ensemble de la chaîne CFVR + PSD + facturation électronique + nouveaux croisements + échanges inter-administrations.

Cette distinction est essentielle.

Une AIPD serait particulièrement pertinente au regard des critères de la CNIL

Sans préjuger de l'analyse juridique déjà réalisée par la DGFiP, plusieurs critères de risque élevé décrits par la CNIL apparaissent objectivement dans la documentation publique S37-S49 :

```
traitement à grande échelle        ✓

croisement d'ensembles de données  ✓

évaluation / ciblage               ✓

méthodes algorithmiques            ✓
```

La présence de ces caractéristiques rend particulièrement importante la possibilité de vérifier :

- la description exacte du traitement étudié dans l'AIPD ;
- les catégories de données couvertes ;
- les interconnexions prises en compte ;
- les risques de compromission ;
- les risques liés aux habilitations ;
- les risques de corrélation excessive ;
- les mesures de réduction de ces risques ;
- les modifications successives de l'analyse.

À ÉTABLIR :

> Quelle AIPD couvre aujourd'hui l'exploitation des données de facturation électronique dans CFVR et la PSD ?

> Quelle est sa date de dernière révision ?

> Intègre-t-elle l'arrivée de plusieurs milliards de factures par an ?

> Intègre-t-elle les croisements réalisés sur la PSD ?

> Intègre-t-elle les échanges avec les organismes sociaux ?

> Intègre-t-elle l'évolution des méthodes algorithmiques et l'élargissement du réseau d'analystes ?

Cinquième vulnérabilité : le cloisonnement devient une garantie critique

La CNIL impose une condition particulièrement forte concernant la plateforme sécurisée des données S37.

Elle considère que son utilisation suppose :

- un cloisonnement strict ;
- que les données versées soient uniquement traitées pour les finalités actuellement prévues ;
- qu'aucun nouvel accédant non prévu ne puisse y accéder ;
- que les protections techniques soient équivalentes à celles existant hors de la PSD.

Cette formulation montre que le cloisonnement n'est pas une question accessoire.

Il constitue l'une des garanties permettant que la concentration technique ne conduise pas à une ouverture fonctionnelle des données.

GARANTIE JURIDIQUE ET TECHNIQUE :

> La PSD ne doit pas devenir, du seul fait qu'elle accueille plusieurs ensembles de données, une infrastructure permettant leur utilisation générale par des utilisateurs ou pour des finalités non autorisés.

VULNÉRABILITÉ POTENTIELLE :

> La solidité juridique de l'architecture dépend donc directement de garanties techniques de cloisonnement qui ne sont pas entièrement vérifiables depuis la documentation publique étudiée.

À ÉTABLIR :

> Comment les séparations entre jeux de données, finalités, traitements et profils d'accès sont-elles techniquement implémentées et auditées dans la PSD ?

Le problème de sécurité ne peut donc pas être réduit à « tout peut être piraté »

Il serait trop faible juridiquement d'affirmer :

> **« Tout système informatique peut être piraté, donc cette architecture est dangereuse. »**

Le risque zéro n'existe pas et le RGPD n'exige pas l'impossibilité absolue d'une compromission.

L'exigence juridique est différente.

Elle porte sur l'adéquation entre :

```
niveau de risque
   ↓
mesures mises en œuvre
   ↓
état de l'art
   ↓
surveillance
   ↓
réévaluation régulière
   ↓
capacité à démontrer la conformité
```

S48-S50

C'est donc sur ce terrain que l'analyse doit se placer.

Ce que 6.3 permet déjà de faire relever

Plusieurs questions précises peuvent maintenant être adressées à la DGFiP, à la CNIL ou au législateur :

> **1. Quelle AIPD couvre actuellement CFVR après l'intégration de la facturation électronique et son exploitation dans la PSD ?**

> **2. Quand cette AIPD a-t-elle été réévaluée pour la dernière fois au regard du changement massif de volumétrie et des nouvelles interconnexions ?**

> **3. Les mécanismes proactifs de détection des comportements anormaux et de blocage immédiat des comptes recommandés par la CNIL sont-ils intégralement déployés ?**

> **4. Quelle durée maximale de conservation s'applique aux données transférées entre la DGFiP et chaque organisme de sécurité sociale ?**

> **5. Comment la suppression effective des copies reçues par les organismes destinataires est-elle contrôlée ?**

> **6. Comment le cloisonnement entre jeux de données, finalités et catégories d'utilisateurs est-il techniquement garanti et audité dans la PSD ?**

> **7. Quels audits indépendants ou tests réguliers permettent de démontrer que le niveau de sécurité demeure adapté à l'évolution des menaces ?**

Ces questions ne présument aucune violation.

Elles demandent la démonstration des garanties que le droit rend précisément pertinentes.

Conclusion de 6.3

AVÉRÉ :

> CFVR rapproche déjà de nombreuses sources fiscales, économiques, administratives et sociales et intègre désormais les données issues de la facturation électronique S37-S45.

AVÉRÉ :

> Les données de facturation électronique doivent être exploitées dans la PSD et leurs résultats peuvent être croisés avec d'autres informations utilisées par CFVR S37.

AVÉRÉ :

> Des échanges bidirectionnels de certaines données sont juridiquement organisés entre la DGFiP et des organismes de sécurité sociale S37-S45.

AVÉRÉ :

> La CNIL considère explicitement que le volume massif, la sensibilité des données et l'évolution des modes d'attaque informatique imposent une vigilance particulière S37.

GARANTIE JURIDIQUE :

> Le RGPD impose un niveau de sécurité adapté au risque ainsi qu'une réévaluation lorsque l'évolution des opérations entraîne une modification du risque S48.

GARANTIE DOCUMENTÉE :

> La CNIL relève notamment des engagements concernant la double authentification, les terminaux sécurisés, le cloisonnement et la limitation des habilitations S37.

ANGLE MORT DOCUMENTAIRE :

> Les sources publiques étudiées ne permettent pas encore d'établir si toutes les mesures proactives de détection et de blocage recommandées par la CNIL ont effectivement été déployées.

ANGLE MORT DOCUMENTAIRE :

> Le projet examiné par la CNIL ne précisait pas la durée de conservation des données transmises aux organismes sociaux ; il reste à établir précisément le régime applicable à chaque copie détenue par les destinataires S37.

ANGLE MORT DOCUMENTAIRE :

> Nous n'avons pas encore identifié une AIPD publique permettant de vérifier précisément comment l'ensemble des évolutions CFVR + PSD + facturation électronique + nouveaux croisements + échanges inter-administrations a été évalué.

VULNÉRABILITÉ JURIDIQUE :

> L'accroissement simultané de la volumétrie, du nombre de sources, des capacités de rapprochement et des catégories d'accédants augmente les conséquences potentielles d'une compromission ou d'un mésusage et renforce donc les exigences de sécurité, de cloisonnement et de réévaluation du risque.

À ÉTABLIR :

> L'administration peut-elle démontrer que les mesures techniques, organisationnelles et les analyses d'impact ont été réévaluées à la hauteur du changement d'échelle introduit en 2026 ?

NON ÉTABLI :

> Aucun élément identifié ne permet d'affirmer que CFVR ou la PSD ont subi une compromission ou que les mesures de sécurité actuellement déployées seraient juridiquement insuffisantes.

6.4 Profilage et décisions automatisées

Statut : TRAITEMENTS ALGORITHMIQUES AVÉRÉS / GARANTIE HUMAINE DOCUMENTÉE / FRONTIÈRE JURIDIQUE IDENTIFIÉE / VULNÉRABILITÉS À ÉTABLIR

Les sections précédentes ont établi que les données issues de la facturation électronique doivent être exploitées à grande échelle, croisées avec d'autres informations et utilisées dans un traitement permettant notamment d'identifier des anomalies et des entreprises présentant certains risques fiscaux S37-S45.

Cette architecture conduit directement à une question juridique supplémentaire :

> **à partir de quel moment un traitement qui analyse, classe ou sélectionne des personnes ou entreprises cesse-t-il d'être une simple aide à la décision et devient-il suffisamment déterminant pour relever des protections applicables aux décisions automatisées ?**

Cette frontière est particulièrement importante parce que le droit européen ne regarde pas uniquement l'existence formelle d'un algorithme.

Il s'intéresse également à son rôle concret dans la décision qui en résulte.

Profilage et décision automatisée ne sont pas synonymes

Une première distinction doit être conservée.

Le profilage consiste à utiliser des données personnelles afin d'évaluer certains aspects personnels concernant une personne physique.

Une décision automatisée peut être fondée sur un profilage, mais les deux notions ne se confondent pas S36-S43.

Un traitement peut donc :

```
analyser des données
   ↓
produire un score / signal / classification
   ↓
sans prendre lui-même
une décision produisant un effet juridique
```

Inversement, une décision peut être entièrement automatisée sans nécessairement reposer sur un profilage préalable.

GARANTIE MÉTHODOLOGIQUE :

> L'existence d'algorithmes, de modèles ou de classifications ne suffit pas, à elle seule, à démontrer l'existence d'une décision individuelle automatisée interdite ou spécialement encadrée par l'article 22 du RGPD.

L'article 22 fixe cependant une frontière importante

L'article 22 du RGPD reconnaît à la personne concernée le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, lorsque cette décision :

- produit des effets juridiques la concernant ;
- ou l'affecte de manière significative de façon similaire S36-S43.

Des exceptions existent.

Une telle décision peut notamment être autorisée lorsqu'elle est prévue par le droit de l'Union ou d'un État membre et que des mesures appropriées protègent les droits, libertés et intérêts légitimes des personnes S43.

Le principe n'est donc pas :

```
algorithme
   =
interdiction
```

La question juridique est plus précise :

```
traitement automatisé
   ↓
décision
   ↓
caractère exclusivement automatisé
   ↓
effet juridique ou significatif
   ↓
article 22
```

CFVR se situe actuellement en amont de cette frontière selon le dispositif documenté

La documentation publique relative à CFVR contient ici une garantie particulièrement importante.

La CNIL indique que le traitement a pour objet :

> d'orienter et d'éclairer l'analyse des agents,

et précise que :

> **les agents seuls peuvent décider d'engager une procédure de contrôle fiscal** S37.

Elle insiste à nouveau sur cette séparation lors de l'examen des méthodes algorithmiques.

Les signalements générés par CFVR doivent demeurer un outil permettant aux agents d'apprécier l'opportunité d'ouvrir ou non un contrôle.

Ils ne doivent pas remplacer leur analyse S37.

AVÉRÉ :

> Le fonctionnement juridiquement et organisationnellement documenté de CFVR ne prévoit pas qu'un algorithme décide seul de l'ouverture d'un contrôle fiscal.

GARANTIE JURIDIQUE ET ORGANISATIONNELLE :

> Une analyse humaine doit intervenir avant l'ouverture du contrôle.

Cette garantie interdit donc d'affirmer, sur la base des sources actuellement disponibles :

> **« CFVR ouvre automatiquement les contrôles fiscaux. »**

Cette affirmation n'est pas établie.

Mais la CNIL considère elle-même cette intervention humaine comme indispensable

La formulation utilisée par la CNIL est particulièrement importante.

Elle considère :

> **indispensable à l'équilibre du dispositif**

que les signalements générés ne puissent en aucun cas remplacer l'analyse réalisée par les agents S37.

Elle demande également au ministère de garantir :

> **une surveillance et une décision humaine effectives** S37.

Elle recommande notamment :

- une documentation adaptée pour les analystes ;
- des formations régulières ;
- une analyse fiscale des pièces de chaque dossier ;
- la prise en compte des dernières déclarations disponibles S37.

La CNIL qualifie ces mesures d'essentielles pour prévenir :

> **l'automatisation de l'ouverture des contrôles fiscaux** S37.

Cette formulation révèle une frontière juridique et organisationnelle très claire.

```
CFVR
   ↓
signalement algorithmique
   ↓
ANALYSE HUMAINE EFFECTIVE
   ↓
décision éventuelle
```

La solidité de la garantie dépend donc de ce qui se passe réellement dans l'étape centrale.

SCHUFA empêche de réduire la question à la présence formelle d'un humain

La jurisprudence de la Cour de justice apporte ici un élément majeur.

Dans l'affaire SCHUFA, la Cour devait examiner un système dans lequel une société produisait automatiquement une valeur de probabilité concernant une personne, puis transmettait cette valeur à un tiers qui prenait formellement la décision finale S51.

Il existait donc bien deux étapes :

```
système automatisé
   ↓
score
   ↓
tiers
   ↓
décision
```

La Cour a néanmoins considéré que l'établissement automatisé du score pouvait constituer lui-même une décision individuelle automatisée au sens de l'article 22 lorsque la décision du tiers dépendait **de manière déterminante** de cette valeur S51.

PRINCIPE JURISPRUDENTIEL :

> L'existence d'un décideur humain ou d'un tiers en bout de chaîne ne suffit donc pas nécessairement à exclure l'article 22 lorsque le résultat automatisé joue en pratique un rôle déterminant dans la décision finale.

Cette jurisprudence ne concernait pas CFVR et ne permet pas de transposer automatiquement sa conclusion au contrôle fiscal.

Mais elle fournit un critère particulièrement pertinent pour examiner ce type d'architecture.

Première vulnérabilité juridique : l'intervention humaine doit être réelle, pas seulement formelle

La question concernant CFVR devient donc plus précise.

Elle n'est pas seulement :

> **« un humain clique-t-il sur le bouton final ? »**

Elle est :

> **« cet humain dispose-t-il réellement des informations, du temps, de la compétence et de l'autonomie nécessaires pour remettre en cause le signal produit par le système ? »**

La CNIL semble elle-même identifier cette difficulté puisqu'elle demande une surveillance et une décision humaine **effectives** S37.

VULNÉRABILITÉ JURIDIQUE :

> Si l'analyse humaine devenait purement formelle et que les signalements algorithmiques déterminaient en pratique l'ouverture des contrôles, la qualification juridique du processus devrait être réexaminée au regard notamment de l'article 22 et de la jurisprudence SCHUFA S43-S51.

NON ÉTABLI :

> Les sources étudiées ne démontrent pas qu'une telle automatisation de fait existe actuellement dans CFVR.

À ÉTABLIR :

> Quelle proportion des signalements CFVR proposés aux agents est finalement retenue ou rejetée après analyse humaine ?

> Quels éléments permettent de mesurer concrètement la capacité des agents à écarter une recommandation algorithmique ?

> Existe-t-il des indicateurs permettant d'identifier une validation quasi systématique des signalements par certains modèles, services ou catégories d'agents ?

Ces données permettraient de mesurer l'effectivité réelle de la garantie humaine.

Une deuxième vulnérabilité apparaît : la boucle de rétroaction algorithmique

La CNIL identifie explicitement un autre problème S37.

Les résultats des contrôles fiscaux passés sont utilisés pour développer les modèles employés dans CFVR.

Cela crée potentiellement une boucle :

```
modèle
   ↓
sélection d'une population
   ↓
contrôles
   ↓
résultats des contrôles
   ↓
nouvelles données d'apprentissage
   ↓
nouveau modèle
   ↓
nouvelle sélection
```

Le problème apparaît lorsqu'un biais initial influence les contrôles réalisés.

Les populations davantage contrôlées produisent mécaniquement davantage de données issues de contrôles.

Ces données peuvent ensuite alimenter les modèles futurs.

La CNIL décrit précisément le risque d'une amplification conduisant à une concentration des contrôles sur certaines populations ou catégories d'entités qui ne serait plus justifiée par la prévalence actualisée de la fraude S37.

AVÉRÉ :

> La CNIL identifie explicitement un risque d'amplification des biais dans CFVR en raison de la réutilisation des résultats des contrôles passés pour développer les modèles.

Ce n'est donc pas une vulnérabilité hypothétique inventée par l'enquête.

La garantie des 50 % est intéressante mais reconnue comme insuffisante à elle seule

Le ministère a introduit une garantie particulière.

Il limite à 50 % le taux de contrôles fiscaux ouverts par les agents à la suite de l'analyse de signaux provenant de CFVR S37.

La CNIL considère cette mesure utile pour limiter le développement de biais significatifs.

Mais elle ajoute immédiatement que :

> **cette limitation ne permet pas, à elle seule, de parer à tout risque de biais significatif** S37.

Elle demande donc également :

- des analyses portant sur l'explicabilité des algorithmes ;
- des travaux critiques sur les biais susceptibles d'émerger ;
- un suivi de l'efficacité des garanties S37.

Le ministère s'est engagé à réaliser ces études et à en rendre compte dans les bilans d'activité de CFVR.

GARANTIE DOCUMENTÉE :

> Le ministère limite à 50 % la part des contrôles ouverts à la suite de signaux CFVR.

LIMITATION EXPLICITEMENT RECONNUE :

> La CNIL considère elle-même que cette garantie ne suffit pas à éliminer tous les risques de biais.

À ÉTABLIR :

> Les études annoncées sur l'explicabilité et les biais ont-elles été réalisées ?

> Quels résultats ont-elles produits ?

> Quels indicateurs permettent de vérifier que certaines populations ou catégories d'entités ne sont pas progressivement surreprésentées dans les contrôles du seul fait d'une boucle d'apprentissage ?

L'apprentissage non supervisé augmente encore l'enjeu

La CNIL relève également le développement de nouvelles méthodes d'apprentissage dans CFVR, notamment des méthodes dites non supervisées S37.

Dans ce type de méthode, le modèle cherche notamment à distinguer des comportements considérés comme normaux ou anormaux sans étiquetage préalable.

La CNIL considère que :

- l'élargissement massif des données ;
- le développement de ces nouvelles méthodes ;

ont pour effet d'amplifier les risques associés aux algorithmes et aux biais S37.

Cette évolution est particulièrement importante avec l'arrivée des données issues de plusieurs milliards de factures.

La chaîne devient :

```
données massives
   ↓
détection automatisée de structures / anomalies
   ↓
classification ou signalement
   ↓
liste d'entreprises considérées à risque
   ↓
analyse humaine
   ↓
contrôle éventuel
```

POINT DE VIGILANCE MAJEUR :

> Plus le fonctionnement du modèle devient complexe et dépend de relations détectées automatiquement dans de très grands volumes de données, plus la capacité à comprendre, contrôler et expliquer les raisons d'un signalement devient juridiquement et opérationnellement importante.

Troisième vulnérabilité : l'explicabilité devient une garantie centrale

Le droit européen contient désormais une jurisprudence particulièrement précise sur l'explication des décisions automatisées S52.

Dans l'affaire C-203/22, la Cour de justice précise que, lorsque le régime concerné s'applique, la personne doit pouvoir obtenir des informations lui permettant de comprendre :

- la procédure effectivement utilisée ;
- les principes appliqués ;
- la manière dont ses données ont contribué au résultat S52.

La Cour précise également que :

> la complexité du traitement ne dispense pas de fournir une explication intelligible.

Une formule mathématique complexe ne constitue pas nécessairement une explication suffisante.

La description exhaustive de toutes les opérations techniques ne l'est pas davantage S52.

GARANTIE JURIDIQUE :

> Lorsqu'une décision relève du régime des décisions automatisées du RGPD, la complexité d'un algorithme ne peut pas être utilisée comme justification permettant de rendre son résultat juridiquement inexplicable.

Une tension apparaît avec les modèles complexes

Cette jurisprudence produit une question importante pour l'évolution de CFVR.

La CNIL demande précisément au ministère de travailler sur :

> **l'explicabilité des algorithmes** S37.

Dans le même temps, CFVR développe :

- des méthodes d'apprentissage ;
- des méthodes non supervisées ;
- des analyses sur des volumes massifs ;
- des rapprochements entre de multiples sources S37-S45.

Il apparaît donc une tension structurelle :

```
augmentation de la complexité
   ↓
augmentation des capacités de détection
   ↓
mais
   ↓
nécessité de conserver
compréhension
contrôle
explicabilité
contestabilité
```

VULNÉRABILITÉ JURIDIQUE POTENTIELLE :

> Une architecture dont les résultats deviendraient suffisamment déterminants pour produire ou conditionner des décisions significatives devrait rester capable de fournir les garanties de transparence et d'explication requises par le droit applicable.

NON ÉTABLI :

> Les sources étudiées ne permettent pas de conclure que les modèles CFVR sont aujourd'hui juridiquement inexplicables.

Quatrième vulnérabilité : la qualité des données peut influencer directement le ciblage

L'intervention humaine documentée par la CNIL comprend une précaution révélatrice.

Les agents doivent notamment vérifier :

> que les dernières déclarations déposées ont bien été prises en compte S37.

Cette exigence montre qu'un signalement algorithmique peut être influencé par l'état des données disponibles au moment de son calcul.

Or les données de facturation électronique vont considérablement augmenter la quantité et la granularité des informations exploitables.

Une erreur peut provenir :

```
donnée incorrecte
   ↓
rapprochement
   ↓
anomalie détectée
   ↓
signalement
   ↓
entreprise sélectionnée
```

La garantie humaine doit donc permettre de casser cette chaîne avant qu'un signal algorithmique erroné ne produise des conséquences injustifiées.

VULNÉRABILITÉ :

> Plus le nombre de sources et de données utilisées augmente, plus la maîtrise de leur exactitude, de leur actualité et de leur contexte devient déterminante pour la qualité du résultat algorithmique.

La frontière juridique devient particulièrement importante si les conséquences évoluent

Aujourd'hui, la documentation établit principalement :

```
signalement
   ↓
orientation d'un agent
   ↓
analyse humaine
   ↓
contrôle fiscal éventuel
```

Cette architecture bénéficie précisément de l'existence de cette étape humaine.

Mais la jurisprudence SCHUFA montre qu'une autre configuration doit être analysée différemment :

```
résultat automatisé
   ↓
résultat déterminant
   ↓
décision ayant un effet significatif
```

S51

La question ne concerne donc pas uniquement CFVR aujourd'hui.

Elle concerne également toute évolution future dans laquelle un score ou une classification issus d'une infrastructure publique deviendraient déterminants pour :

- déclencher automatiquement une procédure ;
- refuser un droit ou un service ;
- modifier les conditions d'accès à un service ;
- produire une conséquence financière ;
- imposer une restriction ;
- ou conditionner une autre décision produisant un effet significatif sur une personne.

FRONTIÈRE JURIDIQUE :

> Plus le résultat algorithmique devient déterminant dans la production d'une conséquence individuelle significative, plus la question de l'application de l'article 22 et des garanties associées devient centrale S43-S51.

Cette frontière est essentielle pour le pont avec les autres infrastructures de l'enquête

Cette conclusion fournit un élément juridique important pour les architectures étudiées dans le Chapitre 5.

Les chapitres précédents ont identifié séparément des capacités concernant :

- les transactions ;
- la facturation électronique ;
- l'identité ;
- les produits ;
- le passeport numérique de produit ;
- les données environnementales ;
- certaines conditions de paiement.

Aucun élément étudié ne démontre actuellement l'existence d'un système utilisant l'ensemble de ces données afin de produire automatiquement une décision individuelle.

Mais le cadre juridique permet désormais d'identifier ce qu'il faudrait rechercher si de telles infrastructures étaient rapprochées.

La chaîne juridiquement sensible serait :

```
données économiques
   +
données transactionnelles
   +
données d'identité
   +
données produit
   +
données environnementales
   ↓
profil / score / classification
   ↓
résultat automatisé
   ↓
influence déterminante
   ↓
décision produisant
un effet juridique ou significatif
```

À ce stade, plusieurs protections devraient alors être examinées simultanément :

- finalité du traitement ;
- base juridique ;
- minimisation ;
- proportionnalité ;
- exactitude des données ;
- transparence ;
- explicabilité ;
- intervention humaine ;
- contestation ;
- article 22 du RGPD lorsque ses conditions sont réunies S43-S44-S46-S48-S51-S52.

DÉDUCTIBLE JURIDIQUEMENT :

> L'interconnexion technique de plusieurs infrastructures ne suffit pas à rendre juridiquement admissible une décision résultant de leur combinaison.

DÉDUCTIBLE JURIDIQUEMENT :

> Si leur combinaison devait produire un score ou une classification jouant un rôle déterminant dans une décision individuelle significative, l'existence formelle d'un intermédiaire humain ne suffirait pas nécessairement à écarter les protections applicables aux décisions automatisées S51.

NON ÉTABLI :

> Aucun élément étudié ne démontre actuellement qu'un score environnemental, un DPP ou une donnée issue de la facturation électronique détermine l'autorisation ou le refus d'un paiement ou d'un autre droit individuel.

Cette frontière doit impérativement être conservée.

Une vulnérabilité plus profonde apparaît néanmoins

Les infrastructures étudiées montrent progressivement trois phénomènes distincts :

```
1. augmentation des données disponibles

2. augmentation des possibilités de rapprochement

3. augmentation des capacités algorithmiques
```

Pris séparément, chacun peut disposer d'un fondement juridique et de garanties propres.

Mais leur combinaison augmente la possibilité technique de produire des classifications de plus en plus fines.

Le droit ne prohibe pas cette évolution par principe.

Il impose cependant que les garanties évoluent avec la nature et l'influence du traitement.

VULNÉRABILITÉ STRUCTURELLE :

> Une architecture peut rester juridiquement présentée comme une aide à la décision tant que l'intervention humaine demeure réelle et déterminante. La frontière devient beaucoup plus sensible si l'accroissement de la précision, du volume ou de l'autorité accordée aux résultats algorithmiques transforme progressivement cette intervention humaine en validation essentiellement formelle.

C'est précisément cette évolution qu'il faudrait pouvoir mesurer dans le temps.

Questions permettant de tester cette garantie

L'analyse permet maintenant de formuler plusieurs questions vérifiables :

> **1. Quel est le taux de rejet par les agents des dossiers proposés par CFVR après analyse humaine ?**

> **2. Ce taux est-il suivi modèle par modèle et catégorie de signalement par catégorie de signalement ?**

> **3. Quels mécanismes permettent de détecter une dépendance excessive des agents aux recommandations algorithmiques ?**

> **4. Les études sur les biais et l'explicabilité annoncées à la CNIL ont-elles été réalisées et leurs résultats sont-ils communicables ?**

> **5. Comment est mesurée la surreprésentation éventuelle de certaines catégories de contribuables ou d'entreprises dans les signalements ?**

> **6. Comment l'administration vérifie-t-elle qu'une corrélation détectée par un modèle reste liée à une prévalence réelle et actualisée de la fraude ?**

> **7. Quelle information peut être fournie à une personne qui souhaite comprendre le rôle joué par un traitement algorithmique dans la sélection de son dossier ?**

> **8. Quelles garanties empêchent qu'une évolution future transforme une recommandation algorithmique en déclenchement automatique ou quasi automatique d'une procédure ?**

Ces questions ne présument aucune violation.

Elles permettent de tester l'effectivité des garanties invoquées.

Conclusion de 6.4

AVÉRÉ :

> CFVR utilise des méthodes algorithmiques pour identifier des anomalies et orienter la programmation du contrôle fiscal S37-S45.

AVÉRÉ :

> Le développement de méthodes d'apprentissage non supervisé et l'élargissement massif des données conduisent la CNIL elle-même à considérer que les risques algorithmiques et les risques de biais sont amplifiés S37.

AVÉRÉ :

> Les résultats des contrôles antérieurs sont utilisés pour développer les modèles, ce qui expose selon la CNIL le dispositif à un risque d'amplification des biais dans le temps S37.

GARANTIE DOCUMENTÉE :

> Les signalements CFVR ne doivent pas remplacer l'analyse des agents et l'ouverture d'un contrôle fiscal doit actuellement résulter d'une décision humaine S37.

GARANTIE DOCUMENTÉE :

> Le ministère limite à 50 % le taux de contrôles ouverts à la suite de signaux provenant de CFVR S37.

LIMITATION EXPLICITEMENT RECONNUE :

> La CNIL considère que cette limite de 50 % ne suffit pas, à elle seule, à prévenir tous les risques de biais significatifs et demande des travaux supplémentaires sur l'explicabilité et les biais S37.

PRINCIPE JURISPRUDENTIEL :

> Selon la CJUE, un résultat automatisé peut lui-même relever de la notion de décision automatisée lorsque la décision ultérieure dépend de manière déterminante de ce résultat S51.

GARANTIE JURIDIQUE :

> Lorsque le régime des décisions automatisées s'applique, la complexité technique du système ne supprime pas les exigences de transparence et d'explication S52.

VULNÉRABILITÉ JURIDIQUE :

> La protection reposant sur l'intervention humaine dépend de son effectivité réelle. Une validation humaine essentiellement formelle d'un résultat algorithmique déterminant pourrait nécessiter une réévaluation de la qualification juridique du processus.

ANGLE MORT DOCUMENTAIRE :

> Les sources publiques étudiées ne permettent pas de mesurer précisément le taux de rejet des signalements CFVR par les agents ni, par conséquent, le degré d'influence pratique des recommandations algorithmiques sur les décisions d'ouverture de contrôle.

À ÉTABLIR :

> Les études annoncées sur l'explicabilité et les biais permettent-elles de démontrer que l'élargissement massif des données et le développement de nouvelles méthodes n'entraînent pas une concentration injustifiée des contrôles sur certaines populations ou catégories d'entités ?

À ÉTABLIR :

> Quels mécanismes permettent de démontrer que l'intervention humaine demeure substantielle lorsque les capacités prédictives et la complexité des modèles augmentent ?

DÉDUCTIBLE JURIDIQUEMENT :

> Si une infrastructure future combinait des données économiques, transactionnelles, d'identité, de produit ou environnementales afin de produire un résultat déterminant pour une décision individuelle significative, cette chaîne devrait être examinée au regard des garanties applicables aux traitements automatisés, indépendamment de la seule présence formelle d'un humain en bout de chaîne S51.

NON ÉTABLI :

> Aucun élément étudié ne permet actuellement d'affirmer que CFVR prend automatiquement la décision d'ouvrir un contrôle fiscal ou qu'une donnée environnementale, un DPP ou une donnée de facturation détermine automatiquement l'accès à un paiement, un service ou un droit.

6.5 Nécessité, proportionnalité et minimisation

Statut : OBLIGATIONS JURIDIQUES ÉTABLIES / CHANGEMENT D'ÉCHELLE AVÉRÉ / JUSTIFICATIONS À ÉTABLIR

Les sections précédentes ont établi plusieurs éléments importants.

Les données issues de la facturation électronique doivent alimenter une infrastructure permettant leur exploitation algorithmique à grande échelle.

Elles rejoignent un traitement déjà alimenté par de nombreuses autres sources.

Des rapprochements sont réalisés afin notamment de détecter des anomalies et d'identifier des entreprises présentant certains risques fiscaux.

La volumétrie annoncée atteint plusieurs milliards de factures électroniques par an S37-S45.

La question juridique devient alors différente.

Elle n'est plus seulement :

> **« la lutte contre la fraude constitue-t-elle une finalité légitime ? »**

Cette finalité est établie.

La question devient :

> **« l'ensemble des données collectées, leur granularité, leurs croisements, leurs durées de conservation et leurs modalités d'exploitation sont-ils nécessaires et proportionnés à cette finalité ? »**

Cette distinction est essentielle.

Une finalité légitime ne suffit pas à démontrer la nécessité de chaque donnée

Le principe de minimisation prévu par l'article 5 du RGPD impose que les données personnelles soient :

> **adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités poursuivies** S36-S43.

Cette exigence porte donc non seulement sur l'existence d'une finalité légitime, mais également sur le rapport entre cette finalité et les données effectivement utilisées.

La chaîne juridique n'est pas :

```
objectif d'intérêt général
   ↓
toutes les données susceptibles d'être utiles
```

Elle est :

```
objectif précisément déterminé
   ↓
données nécessaires
   ↓
quantité nécessaire
   ↓
durée nécessaire
   ↓
accès nécessaires
   ↓
traitements nécessaires
```

GARANTIE JURIDIQUE :

> L'utilité potentielle d'une donnée ne suffit pas nécessairement à démontrer sa nécessité juridique.

La CJUE applique directement cette exigence aux administrations fiscales

L'arrêt C-175/20 est particulièrement important pour cette enquête parce qu'il concerne précisément une administration fiscale S53.

La Cour de justice y rappelle que les limitations à la protection des données doivent rester limitées à ce qui est strictement nécessaire.

Elle en déduit qu'un responsable du traitement, même lorsqu'il agit dans le cadre d'une mission d'intérêt public :

> **ne peut procéder de manière générale et indifférenciée à la collecte de données personnelles** S53.

Il doit également :

> **s'abstenir de collecter les données qui ne sont pas strictement nécessaires aux finalités du traitement** S53.

La Cour ajoute que le responsable doit rechercher une minimisation aussi importante que possible de la quantité de données collectées.

PRINCIPE JURISPRUDENTIEL :

> Une administration fiscale ne dispose donc pas, du seul fait de sa mission de lutte contre la fraude, d'un droit général à collecter indifféremment toutes les données personnelles susceptibles de présenter un intérêt analytique.

La charge de la démonstration constitue un élément particulièrement important

La Cour ajoute une exigence essentielle.

Le responsable du traitement doit pouvoir démontrer le respect des principes prévus par l'article 5 du RGPD S53.

Concernant la minimisation, elle indique qu'il appartient à l'administration concernée d'établir qu'elle a cherché à minimiser autant que possible la quantité de données collectées.

Concernant la durée, elle précise également que la période concernée ne peut dépasser celle qui est strictement nécessaire à l'objectif d'intérêt général poursuivi S53.

La question n'est donc pas uniquement :

> **« peut-on démontrer que ces données sont utiles ? »**

Elle devient :

> **« peut-on démontrer pourquoi cette quantité précise de données est nécessaire ? »**

et :

> **« peut-on démontrer pourquoi une quantité moindre, une granularité inférieure ou une période plus courte ne permettrait pas d'atteindre suffisamment l'objectif poursuivi ? »**

GARANTIE JURIDIQUE :

> Le principe de responsabilité impose au responsable du traitement d'être en mesure de démontrer le respect de la minimisation.

Cette jurisprudence rencontre directement le changement d'échelle de CFVR

La CNIL constate que l'arrivée des données issues de la facturation électronique augmente substantiellement le volume de données traitées dans CFVR S37.

Elle indique que le volume des factures électroniques est estimé à :

> **2 à 3 milliards par an** S37.

La volumétrie est telle que le ministère indique que ces données ne pourraient pas être exploitées dans l'infrastructure CFVR existante.

Une infrastructure disposant d'une puissance de calcul renforcée, la PSD, devient nécessaire précisément pour permettre leur exploitation S37.

La chaîne documentée est donc :

```
nouvelle catégorie de données
   ↓
augmentation substantielle du volume
   ↓
2 à 3 milliards de factures / an
   ↓
infrastructure existante insuffisante
   ↓
PSD à puissance de calcul renforcée
   ↓
exploitation
   ↓
croisement des résultats
   ↓
ciblage fiscal
```

AVÉRÉ :

> L'intégration de la facturation électronique ne constitue pas une augmentation marginale du traitement.

Elle entraîne un changement d'échelle suffisamment important pour nécessiter une infrastructure de calcul renforcée S37.

Première vulnérabilité : le changement d'échelle doit pouvoir être justifié donnée par donnée

Le changement d'échelle ne constitue pas en lui-même une violation du principe de minimisation.

Une collecte massive peut être nécessaire lorsqu'une mission légitime ne peut raisonnablement être accomplie autrement.

Mais C-175/20 interdit de raisonner uniquement à partir de l'intérêt général poursuivi S53.

Il faut également examiner les données effectivement nécessaires.

La question devient donc :

> **Toutes les catégories de données personnelles provenant de la facturation électronique qui sont intégrées ou exploitées dans cette chaîne sont-elles nécessaires aux modèles et analyses poursuivis ?**

Et plus précisément :

> **Chaque champ personnel exploité apporte-t-il une contribution nécessaire à une finalité déterminée ?**

> **Certaines analyses pourraient-elles fonctionner avec moins de champs ?**

> **Certaines données pourraient-elles être agrégées, pseudonymisées ou supprimées avant l'exploitation ?**

> **La même efficacité pourrait-elle être obtenue sans conserver certains éléments au niveau transactionnel ?**

VULNÉRABILITÉ JURIDIQUE :

> Plus une infrastructure absorbe systématiquement de données, plus la démonstration de nécessité ne peut raisonnablement se limiter à l'affirmation générale que ces données peuvent améliorer la lutte contre la fraude.

À ÉTABLIR :

> Quelle démonstration documentée justifie, catégorie par catégorie, les données personnelles issues de la facturation électronique effectivement nécessaires aux traitements réalisés dans la PSD et CFVR ?

La jurisprudence oblige également à rechercher si un ciblage plus limité est possible

L'arrêt C-175/20 contient ici un raisonnement particulièrement intéressant S53.

Dans cette affaire, la Cour demande précisément s'il serait possible d'atteindre l'objectif fiscal sans disposer potentiellement des données relatives à toutes les annonces concernées.

Elle envisage explicitement la possibilité de :

> **cibler certaines annonces au moyen de critères spécifiques** S53.

Le principe est important.

Lorsque l'objectif peut être atteint par une collecte plus ciblée, la collecte généralisée devient plus difficile à justifier.

Appliqué à l'architecture étudiée, cela produit une question qui n'est plus théorique :

```
exploitation de données de facturation
à très grande échelle
   VS
sélection préalable
de catégories / opérations / situations
présentant des critères de risque
```

QUESTION JURIDIQUE MAJEURE :

> L'exploitation de la masse des données de facturation électronique est-elle nécessaire pour les finalités poursuivies ou certaines analyses pourraient-elles être réalisées à partir d'une sélection préalable moins intrusive ?

La réponse nécessite des informations techniques et statistiques qui ne sont pas présentes dans les sources publiques étudiées.

ANGLE MORT DOCUMENTAIRE :

> Nous n'avons pas encore identifié de démonstration publique comparant l'exploitation massive prévue avec des architectures moins intrusives permettant éventuellement d'obtenir des résultats comparables.

Deuxième vulnérabilité : la minimisation concerne également la granularité

Deux traitements peuvent exploiter le même nombre de documents tout en présentant des niveaux d'ingérence très différents.

Il faut distinguer :

```
existence d'une facture
```

de :

```
contenu détaillé de la facture
```

et encore de :

```
contenu détaillé
   +
historique
   +
contreparties
   +
rapprochements avec d'autres bases
```

Le principe de minimisation s'applique à la quantité de données, mais également à l'étendue du traitement et à leur accessibilité S43.

La question pertinente n'est donc pas uniquement :

> **combien de factures sont traitées ?**

Elle est également :

> **quel niveau de détail provenant de chacune de ces factures est réellement nécessaire pour chaque modèle ou requête ?**

VULNÉRABILITÉ JURIDIQUE :

> Une justification portant sur la nécessité d'utiliser les factures ne démontre pas automatiquement la nécessité d'utiliser chaque donnée personnelle qu'elles contiennent.

Troisième vulnérabilité : le rapprochement change l'intensité du traitement

Une donnée isolée et la même donnée rapprochée de nombreuses autres informations ne présentent pas nécessairement la même intensité d'ingérence.

CFVR permet précisément de rapprocher plusieurs sources S37-S45.

La PSD doit progressivement accueillir l'ensemble des données du traitement CFVR S37.

Ainsi :

```
donnée A
   +
donnée B
   +
donnée C
   +
facturation électronique
   +
historique fiscal
   +
autres sources
   ↓
capacité d'inférence accrue
```

Le principe de minimisation doit donc être examiné non seulement au niveau de chaque base prise séparément, mais également au regard des traitements effectivement réalisés à partir de leur combinaison.

VULNÉRABILITÉ STRUCTURELLE :

> Des données individuellement nécessaires à plusieurs traitements peuvent produire, lorsqu'elles sont rapprochées, une capacité d'analyse beaucoup plus intrusive que celle résultant de chacune des sources prises isolément.

À ÉTABLIR :

> Comment la nécessité et la proportionnalité sont-elles appréciées pour les combinaisons de données et non uniquement pour chaque source prise séparément ?

Le Conseil constitutionnel impose également un contrôle de proportionnalité

Cette exigence ne provient pas uniquement du RGPD et de la jurisprudence européenne.

Le Conseil constitutionnel rattache la protection des données personnelles au droit au respect de la vie privée garanti par l'article 2 de la Déclaration des droits de l'homme et du citoyen S44.

Il juge que :

> **la collecte, l'enregistrement, la conservation, la consultation et la communication de données personnelles doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif** S44.

Le contrôle porte donc sur plusieurs opérations successives :

```
collecte
   ↓
enregistrement
   ↓
conservation
   ↓
consultation
   ↓
communication
```

GARANTIE CONSTITUTIONNELLE :

> La présence d'un motif d'intérêt général ne dispense pas le dispositif d'un contrôle portant sur l'adéquation et la proportionnalité de ses modalités concrètes.

Quatrième vulnérabilité : la conservation doit être justifiée séparément

Une donnée nécessaire aujourd'hui ne devient pas automatiquement nécessaire pendant toute la durée techniquement possible de sa conservation.

Le principe de limitation de la conservation impose que les données permettant l'identification des personnes ne soient pas conservées plus longtemps que nécessaire au regard des finalités poursuivies S43.

C-175/20 applique également la logique de stricte nécessité à la période concernée par une collecte fiscale S53.

Cette question devient particulièrement importante dans une infrastructure algorithmique.

Plus l'historique disponible est long :

```
plus de données historiques
   ↓
plus de comparaisons possibles
   ↓
plus de modèles possibles
   ↓
plus de capacités d'inférence
```

Mais :

```
utilité analytique
   ≠
nécessité juridique automatique
```

VULNÉRABILITÉ JURIDIQUE :

> Une durée longue doit pouvoir être justifiée par rapport aux finalités poursuivies et ne peut reposer uniquement sur l'intérêt potentiel de disposer d'un historique plus riche.

Un premier point concret existe déjà concernant les échanges sociaux

La CNIL a précisément appliqué ce raisonnement aux échanges entre la DGFiP et les organismes de sécurité sociale S37.

Elle constate que le projet qui lui avait été soumis ne précisait pas la durée de conservation des données transmises.

Elle rappelle alors que les échanges entre administrations ne sont permis que lorsque leurs modalités restent proportionnées aux objectifs poursuivis.

Elle demande que la conservation soit limitée à la durée nécessaire S37.

Le ministère s'est engagé à prévoir une durée maximale de dix ans.

Mais la CNIL demande également quelque chose de plus précis :

> que les durées applicables soient déterminées **catégorie de données par catégorie de données** dans les conventions conclues avec les organismes sociaux S37.

Cette précision est particulièrement intéressante.

Elle montre que :

```
une durée maximale générale
   ≠
justification individualisée
de la durée nécessaire
pour chaque catégorie
```

AVÉRÉ :

> La CNIL demande elle-même une appréciation plus granulaire des durées de conservation pour les données échangées avec les organismes sociaux S37.

Cinquième vulnérabilité : « au maximum dix ans » ne signifie pas « dix ans nécessaires »

Cette distinction doit être conservée.

Le fait qu'une réglementation autorise une conservation jusqu'à une certaine durée ne signifie pas nécessairement que toutes les catégories de données doivent effectivement être conservées pendant cette durée.

Le principe de minimisation et de limitation de la conservation conduit à rechercher la durée nécessaire au traitement concerné S43-S53.

Ainsi :

```
durée maximale juridiquement possible
   ≠
durée nécessaire pour chaque donnée
```

QUESTION À ÉTABLIR :

> Parmi les données susceptibles d'être conservées jusqu'à dix ans, lesquelles nécessitent effectivement cette durée et lesquelles pourraient être supprimées ou anonymisées plus tôt ?

Sixième vulnérabilité : l'accumulation progressive peut déplacer le contrôle de proportionnalité

Le 6.2 avait identifié une question laissée volontairement ouverte :

> jusqu'où des extensions successives de finalités, de sources et de destinataires peuvent-elles s'accumuler avant que leur effet global impose une nouvelle appréciation de nécessité et de proportionnalité ?

Cette question devient ici beaucoup plus concrète.

CFVR n'est plus le traitement qu'il était lors de sa création.

Son périmètre a évolué.

Ses sources ont évolué.

Ses méthodes ont évolué.

Ses capacités de calcul ont évolué.

Les catégories d'agents impliqués ont évolué.

Les échanges inter-administrations ont évolué.

Et plusieurs milliards de factures électroniques viennent désormais rejoindre cette architecture S37-S45.

On peut donc représenter l'évolution ainsi :

```
traitement initial
   ↓
nouvelles sources
   ↓
nouveaux rapprochements
   ↓
nouveaux algorithmes
   ↓
nouveaux accédants
   ↓
nouveaux échanges
   ↓
nouvelle infrastructure de calcul
   ↓
plusieurs milliards de factures / an
```

Chaque extension peut disposer séparément d'un fondement juridique.

Mais cela ne répond pas entièrement à une autre question :

> **l'architecture résultante demeure-t-elle, dans son ensemble, nécessaire et proportionnée ?**

VULNÉRABILITÉ JURIDIQUE STRUCTURELLE :

> L'appréciation isolée de chaque extension peut ne pas suffire à rendre compte de l'intensité globale du traitement résultant de leur accumulation.

Le principe de responsabilité renverse ici une partie du raisonnement

L'un des apports les plus importants de C-175/20 est que la démonstration de la minimisation incombe au responsable du traitement S53.

Cela change la manière de formuler les questions de cette enquête.

Nous n'avons pas nécessairement à démontrer :

> **« cette donnée est inutile ».**

La question juridiquement pertinente peut être :

> **« quelle démonstration établit que cette donnée est nécessaire ? »**

De même, il n'est pas nécessaire d'affirmer :

> **« cette durée est excessive ».**

On peut demander :

> **« quelle démonstration établit que cette durée est nécessaire à cette finalité ? »**

Ou encore :

> **« quelle démonstration établit que le même objectif ne pourrait pas être atteint avec une quantité moindre de données ? »**

C'est une différence méthodologique fondamentale.

Septième vulnérabilité : les capacités techniques ne constituent pas la mesure de la nécessité

La CNIL explique que la PSD est nécessaire techniquement parce que la volumétrie des données de facturation électronique dépasse les capacités de l'environnement CFVR existant S37.

Cela établit :

> **la nécessité technique d'une infrastructure plus puissante pour traiter le volume envisagé.**

Cela ne répond cependant pas à une question différente :

> **la nécessité juridique de traiter l'intégralité du volume envisagé.**

Les deux raisonnements ne doivent pas être confondus.

```
« nous avons besoin de la PSD
pour traiter autant de données »
   ≠
« nous avons démontré qu'il est nécessaire
de traiter autant de données »
```

VULNÉRABILITÉ DOCUMENTAIRE :

> Les sources étudiées expliquent pourquoi une puissance de calcul renforcée est nécessaire pour exploiter la volumétrie prévue, mais elles ne permettent pas, à elles seules, de démontrer pourquoi cette volumétrie précise constitue le niveau minimal nécessaire à chaque finalité poursuivie.

Cette distinction est particulièrement importante.

Ce raisonnement devient crucial pour les autres infrastructures de l'enquête

Le principe de nécessité ne concerne pas uniquement CFVR.

Il fournit également un test juridique pour toute interconnexion future impliquant des données personnelles.

Les chapitres précédents ont identifié différentes infrastructures relatives notamment :

- aux transactions ;
- à la facturation ;
- à l'identité ;
- aux produits ;
- au DPP ;
- aux informations environnementales ;
- à certaines infrastructures de paiement.

L'existence séparée de bases juridiques permettant certains traitements dans chacune de ces infrastructures ne suffirait pas nécessairement à justifier leur combinaison.

La question devrait être reposée pour le traitement résultant :

```
donnée nécessaire dans système A
   +
donnée nécessaire dans système B
   +
donnée nécessaire dans système C

   ≠ automatiquement

combinaison A + B + C nécessaire
```

DÉDUCTIBLE JURIDIQUEMENT :

> La nécessité de collecter une donnée dans son système d'origine ne démontre pas automatiquement la nécessité de la rapprocher des données d'une autre infrastructure.

C'est une frontière juridique importante pour le pont construit dans cette enquête.

Application au pont environnement / identité / paiement

Aucun élément étudié ne démontre actuellement l'existence d'un traitement combinant l'ensemble de ces infrastructures afin de produire une décision individuelle.

Mais si une évolution future conduisait par exemple à :

```
identité
   +
transaction
   +
produit
   +
DPP
   +
information environnementale
   +
paiement
   ↓
analyse / classification
   ↓
conséquence individuelle
```

la seule existence d'une base juridique propre à chaque composant ne suffirait pas nécessairement à établir la nécessité et la proportionnalité du traitement résultant.

Il faudrait notamment examiner :

- la finalité précise du rapprochement ;
- les données strictement nécessaires ;
- la granularité nécessaire ;
- la durée nécessaire ;
- les personnes pouvant y accéder ;
- les alternatives moins intrusives ;
- les conséquences pour les personnes ;
- les garanties contre les usages secondaires S43-S44-S53.

DÉDUCTIBLE JURIDIQUEMENT :

> Plus plusieurs infrastructures sont rapprochées, plus la justification doit porter sur le traitement résultant de leur combinaison et non uniquement sur la légalité individuelle de chacun de leurs composants.

NON ÉTABLI :

> Rien dans les sources étudiées ne démontre actuellement qu'une telle interconnexion globale soit mise en œuvre ou juridiquement prévue.

Une véritable ligne de contrôle apparaît

Après 6.1 à 6.5, le raisonnement juridique peut maintenant être résumé ainsi :

```
base juridique
   ↓
finalité légitime
   ↓
   MAIS
   ↓
données nécessaires ?
   ↓
quantité nécessaire ?
   ↓
granularité nécessaire ?
   ↓
croisements nécessaires ?
   ↓
durée nécessaire ?
   ↓
accédants nécessaires ?
   ↓
alternative moins intrusive ?
   ↓
proportionnalité globale ?
```

Une réponse positive aux deux premières étapes ne répond donc pas automatiquement aux suivantes.

Questions permettant de tester concrètement la proportionnalité

L'analyse permet désormais de poser des questions beaucoup plus précises :

> **1. Quelles catégories exactes de données personnelles issues des factures sont exploitées dans la PSD pour chaque modèle ou requête ?**

> **2. Quelle analyse démontre la nécessité de chacune de ces catégories ?**

> **3. Quels tests ont été réalisés avec un jeu de données moins étendu ou moins granulaire ?**

> **4. L'administration a-t-elle comparé l'efficacité de l'exploitation massive avec celle d'une collecte ou sélection préalable fondée sur des critères de risque ?**

> **5. Quelles données sont supprimées avant exploitation parce qu'elles ne sont pas nécessaires ?**

> **6. Quelles données sont agrégées, pseudonymisées ou anonymisées avant leur rapprochement ?**

> **7. Pour chaque catégorie de données, quelle durée de conservation est effectivement appliquée et pourquoi cette durée est-elle nécessaire ?**

> **8. Quelle analyse porte sur l'effet cumulé des différentes sources utilisées dans CFVR ?**

> **9. L'AIPD examine-t-elle des architectures alternatives moins intrusives ?**

> **10. Quelle démonstration permet d'établir que le changement d'échelle introduit par plusieurs milliards de factures demeure proportionné aux gains obtenus pour les finalités poursuivies ?**

Ces questions ne demandent pas à l'administration de démontrer que le traitement présente un risque nul.

Elles demandent la démonstration de sa nécessité et de sa proportionnalité.

Conclusion de 6.5

AVÉRÉ :

> Le principe de minimisation impose que les données personnelles soient adéquates, pertinentes et limitées à ce qui est nécessaire aux finalités poursuivies S36-S43.

PRINCIPE JURISPRUDENTIEL :

> Une administration fiscale ne peut pas procéder de manière générale et indifférenciée à la collecte de données personnelles et doit s'abstenir de collecter celles qui ne sont pas strictement nécessaires S53.

PRINCIPE JURISPRUDENTIEL :

> Le responsable du traitement doit pouvoir démontrer qu'il a cherché à minimiser autant que possible la quantité de données collectées et la période concernée S53.

GARANTIE CONSTITUTIONNELLE :

> La collecte, l'enregistrement, la conservation, la consultation et la communication de données personnelles doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif S44.

AVÉRÉ :

> L'intégration de la facturation électronique entraîne une augmentation substantielle du volume de données de CFVR, estimée à plusieurs milliards de factures par an, nécessitant le recours à une infrastructure de calcul renforcée S37.

AVÉRÉ :

> La CNIL demande déjà, concernant certains échanges inter-administrations, que les durées de conservation soient précisées catégorie de données par catégorie de données S37.

VULNÉRABILITÉ JURIDIQUE :

> La légitimité de la lutte contre la fraude ne dispense pas de démontrer la nécessité de la quantité, de la granularité, de la durée et des rapprochements de données effectivement utilisés.

VULNÉRABILITÉ STRUCTURELLE :

> La nécessité individuelle de données provenant de plusieurs systèmes ne démontre pas automatiquement la nécessité de leur combinaison.

VULNÉRABILITÉ DOCUMENTAIRE :

> Les sources publiques étudiées expliquent pourquoi une infrastructure de calcul renforcée est nécessaire pour exploiter le volume envisagé, mais ne suffisent pas à démontrer pourquoi l'exploitation de cette volumétrie précise constitue elle-même le moyen minimal nécessaire à chaque finalité poursuivie.

ANGLE MORT DOCUMENTAIRE :

> Nous n'avons pas identifié dans les sources publiques étudiées une comparaison permettant de déterminer si certaines finalités de CFVR pourraient être atteintes avec une quantité moindre de données, une granularité inférieure ou un ciblage préalable plus restrictif.

À ÉTABLIR :

> L'administration peut-elle démontrer, conformément au principe de responsabilité, la nécessité de chaque catégorie de données personnelles exploitée et l'absence d'une solution raisonnablement moins intrusive permettant d'atteindre les mêmes finalités ?

À ÉTABLIR :

> L'effet cumulé des extensions successives de CFVR fait-il l'objet d'une appréciation globale et régulièrement réévaluée de nécessité et de proportionnalité ?

DÉDUCTIBLE JURIDIQUEMENT :

> Toute future interconnexion de données personnelles provenant de la facturation, de l'identité, des produits, du DPP, de données environnementales ou d'infrastructures de paiement devrait justifier la nécessité du rapprochement lui-même et non seulement la légalité séparée de chaque source.

NON ÉTABLI :

> Les sources étudiées ne permettent pas de conclure que l'intégration actuelle des données de facturation électronique dans CFVR est disproportionnée ou contraire au RGPD.

6.6 Droits des personnes et contrôle par la CNIL

Statut : DROITS ÉTABLIS / RESTRICTIONS EXPRESSÉMENT PRÉVUES / CONTRÔLE INDÉPENDANT / EFFECTIVITÉ À EXAMINER

Les sections précédentes ont établi qu'une quantité importante de données personnelles peut être collectée, rapprochée et analysée dans le cadre de CFVR.

Elles ont également établi que :

- les données de facturation électronique doivent rejoindre cette architecture ;
- certains résultats sont produits par des traitements algorithmiques ;
- ces résultats peuvent contribuer à la sélection de dossiers ;
- des échanges existent avec d'autres administrations ;
- les données et résultats peuvent circuler entre plusieurs environnements et catégories de destinataires S37-S45.

Une question devient alors centrale :

> **Quels moyens une personne possède-t-elle pour savoir quelles données la concernant sont utilisées, vérifier leur exactitude, obtenir leur correction et contester un traitement qui porterait atteinte à ses droits ?**

Cette question concerne l'effectivité des garanties.

Un droit inscrit dans un texte et un droit effectivement exerçable ne constituent pas nécessairement la même chose.

Le RGPD reconnaît des droits importants aux personnes

Le RGPD prévoit notamment :

- un droit à l'information ;
- un droit d'accès ;
- un droit de rectification ;
- dans certaines conditions, un droit à l'effacement ;
- un droit à la limitation du traitement ;
- dans certaines conditions, un droit d'opposition ;
- des garanties relatives à certaines décisions automatisées ;
- un droit de saisir une autorité de contrôle ;

- un droit à un recours juridictionnel effectif S43.

Le droit d'accès prévu à l'article 15 permet notamment de connaître :

- les finalités du traitement ;
- les catégories de données personnelles concernées ;
- les destinataires ou catégories de destinataires ;
- la durée de conservation ou ses critères de détermination ;
- l'existence de certains autres droits ;
- l'origine des données lorsqu'elles n'ont pas été collectées auprès de la personne ;
- dans les situations prévues par le RGPD, certaines informations relatives à la logique d'une décision automatisée S43.

GARANTIE JURIDIQUE :

> Une personne n'est donc pas juridiquement dépourvue de moyens de contrôle sur l'utilisation de ses données par une administration.

CFVR prévoit explicitement l'exercice de certains de ces droits

L'article 6 de l'arrêté instituant CFVR prévoit expressément que les droits d'accès et de rectification des articles 15 et 16 du RGPD peuvent être exercés S45.

Selon l'origine des données, ces droits s'exercent :

- auprès du bureau SJCF-1D ;
- ou auprès du centre des finances publiques dont relève la personne S45.

Le droit à la limitation prévu à l'article 18 du RGPD s'exerce également auprès du bureau SJCF-1D S45.

AVÉRÉ :

> CFVR n'est pas un traitement placé en dehors des droits d'accès, de rectification et de limitation.

Mais l'arrêté prévoit immédiatement plusieurs restrictions.

Première restriction majeure : le droit d'opposition ne s'applique pas à CFVR

L'article 6 de l'arrêté CFVR dispose explicitement que :

> **le droit d'opposition prévu à l'article 21 du RGPD ne s'applique pas au traitement** S45.

Depuis la modification de juillet 2026, cette exclusion est expressément rattachée aux objectifs mentionnés aux e et h du paragraphe 1 de l'article 23 du RGPD S45.

Ces dispositions concernent notamment :

- des objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment en matière fiscale ;
- des missions de contrôle, d'inspection ou de réglementation liées notamment à ces objectifs S43.

La conséquence pratique est importante.

Une personne ne peut pas simplement décider :

```
« je refuse que mes données
soient utilisées dans CFVR »
   ↓
arrêt du traitement
```

Le droit d'opposition est expressément écarté pour ce traitement.

LATITUDE JURIDIQUE :

> Le droit européen permet, sous conditions, que certains droits soient restreints pour protéger notamment des intérêts fiscaux importants et les missions de contrôle associées.

RESTRICTION AVÉRÉE :

> Dans CFVR, le droit d'opposition prévu à l'article 21 du RGPD n'est pas applicable S45.

Cette restriction ne constitue donc pas en elle-même une violation du RGPD.

Elle constitue néanmoins une limitation concrète du contrôle individuel exercé par la personne sur l'utilisation de ses données.

Deuxième restriction : accès et rectification peuvent eux-mêmes être limités

L'arrêté CFVR prévoit également que les droits d'accès et de rectification peuvent faire l'objet de restrictions dans les conditions prévues par l'article 52 de la loi Informatique et Libertés S45-S54.

Cette disposition concerne précisément certains traitements utilisés par les administrations pour contrôler ou recouvrer des impositions S54.

La logique est compréhensible :

```
droit d'accès
   ↓
mais
   ↓
ne pas révéler une information
qui compromettrait
le contrôle fiscal
```

Une personne faisant l'objet d'une analyse de risque ne peut donc pas nécessairement obtenir immédiatement l'intégralité des informations qui permettraient de révéler les méthodes de contrôle ou de compromettre leur finalité.

LATITUDE JURIDIQUE :

> Le droit prévoit expressément la possibilité de restreindre certains droits afin de préserver l'efficacité de certaines missions fiscales.

Mais cette possibilité crée une tension évidente :

```
pour contester efficacement
   ↓
il faut comprendre
ce qui est fait

   mais

pour préserver le contrôle
   ↓
certaines informations
peuvent être restreintes
```

La CNIL devient alors un intermédiaire essentiel

Lorsque les restrictions prévues pour CFVR s'appliquent, la personne exerce ses droits par l'intermédiaire de la CNIL dans les conditions prévues par l'article 118 de la loi Informatique et Libertés S45-S54.

La CNIL procède alors aux vérifications nécessaires.

Elle peut faire procéder aux modifications nécessaires.

Elle informe ensuite la personne qu'il a été procédé aux vérifications et lui indique l'existence d'un recours juridictionnel S54.

Lorsque certaines informations peuvent être communiquées sans compromettre les finalités protégées, leur communication peut intervenir dans les conditions prévues par la loi S54.

GARANTIE JURIDIQUE :

> La restriction de l'accès direct n'entraîne donc pas nécessairement l'absence de contrôle.

Un tiers institutionnel indépendant peut vérifier le traitement.

Mais une différence fondamentale apparaît entre vérification et compréhension personnelle

Cette architecture protège simultanément deux intérêts :

```
efficacité du contrôle fiscal
   ↕
droits de la personne
```

Mais elle peut produire une situation particulière :

```
la personne soupçonne
une donnée ou analyse erronée
   ↓
elle demande accès / rectification
   ↓
certaines informations sont restreintes
   ↓
la CNIL effectue des vérifications
   ↓
la personne peut être informée
que les vérifications ont été réalisées
   ↓
sans nécessairement connaître
l'intégralité des informations protégées
```

VULNÉRABILITÉ JURIDIQUE STRUCTURELLE :

> Plus les informations nécessaires pour comprendre l'origine d'un signalement sont protégées contre leur divulgation, plus l'effectivité de la contestation individuelle dépend du contrôle exercé par la CNIL et, le cas échéant, par le juge.

Cela ne signifie pas que le recours devient fictif.

Cela signifie que le contrôle individuel peut devenir en partie **médiatisé par une autorité indépendante** plutôt que directement exercé par la personne.

La rectification devient particulièrement importante dans une architecture interconnectée

Le droit de rectification permet d'obtenir la correction de données personnelles inexactes S43.

Mais l'architecture étudiée ne se limite plus nécessairement à une donnée stockée dans une seule base.

Une donnée peut suivre une chaîne :

```
donnée source
   ↓
transmission
   ↓
rapprochement
   ↓
analyse
   ↓
indicateur
   ↓
résultat algorithmique
   ↓
dossier proposé
```

Le RGPD prévoit également que lorsqu'une rectification, un effacement ou une limitation intervient, le responsable du traitement doit en principe la communiquer aux destinataires auxquels les données ont été transmises, sauf impossibilité ou effort disproportionné S43.

Cette garantie devient particulièrement importante dans une architecture multi-sources.

Première question difficile : corriger la donnée corrige-t-il ses conséquences ?

Prenons une situation hypothétique :

```
donnée A incorrecte
   ↓
croisement avec B et C
   ↓
indicateur D
   ↓
score / classification E
   ↓
signalement F
```

La correction de A est juridiquement encadrée.

Mais plusieurs questions supplémentaires apparaissent :

> **D est-il automatiquement recalculé ?**

> **E est-il supprimé ou réévalué ?**

> **F est-il retiré s'il reposait sur l'information incorrecte ?**

> **Les destinataires de F sont-ils informés ?**

> **Les données dérivées demeurent-elles dans d'autres environnements ?**

Le RGPD contient des mécanismes de rectification, de limitation et de notification aux destinataires S43.

Mais leur application à des chaînes complexes de données dérivées doit être examinée concrètement.

ANGLE MORT DOCUMENTAIRE :

> Les sources publiques étudiées ne permettent pas de déterminer précisément le mécanisme technique par lequel une rectification effectuée dans une donnée source est propagée aux résultats, indicateurs, classifications ou signalements déjà produits à partir de cette donnée dans CFVR et la PSD.

Cette question n'est pas théorique pour CFVR

La CNIL demande que les agents vérifient notamment que les dernières déclarations déposées ont bien été prises en compte avant de décider de l'ouverture d'un contrôle S37.

Cette exigence constitue une garantie importante.

Mais elle confirme également qu'un résultat algorithmique peut être affecté par l'état des données utilisées au moment de sa production.

La chaîne suivante est donc juridiquement pertinente :

```
donnée ancienne / inexacte / incomplète
   ↓
analyse algorithmique
   ↓
anomalie apparente
   ↓
signalement
   ↓
vérification humaine
```

La vérification humaine constitue ici une barrière essentielle.

GARANTIE DOCUMENTÉE :

> L'agent ne doit pas traiter le signal algorithmique comme une vérité autonome et doit analyser le dossier à partir des informations pertinentes et actualisées S37.

Le droit à la limitation offre une protection supplémentaire

L'article 18 du RGPD prévoit notamment qu'une personne peut demander la limitation du traitement lorsqu'elle conteste l'exactitude de données, pendant la période permettant au responsable de vérifier leur exactitude S43.

CFVR prévoit expressément l'exercice de ce droit auprès du bureau SJCF-1D S45.

La limitation peut donc constituer une protection particulièrement importante lorsqu'une information susceptible d'influencer un traitement est contestée.

GARANTIE JURIDIQUE :

> La contestation de l'exactitude d'une donnée peut, dans les conditions prévues par le RGPD, conduire à limiter temporairement son traitement pendant sa vérification S43-S45.

À ÉTABLIR :

> Comment cette limitation est-elle techniquement propagée lorsque la donnée contestée a déjà contribué à produire des résultats dans plusieurs environnements ?

Le problème devient plus complexe avec les données dérivées

Une infrastructure algorithmique ne se contente pas nécessairement de recopier les données sources.

Elle peut produire :

- des indicateurs ;
- des catégories ;
- des relations ;
- des anomalies ;
- des scores ;
- des résultats de requêtes ;
- des propositions de contrôle.

CFVR alimente notamment GALAXIE concernant certains liens entre individus et entités et PILOT CF concernant les dossiers proposés pour contrôle S45.

La question de rectification doit donc potentiellement être envisagée à plusieurs niveaux :

```
niveau 1
donnée source

niveau 2
donnée rapprochée

niveau 3
inférence / indicateur

niveau 4
résultat algorithmique

niveau 5
conséquence opérationnelle
```

VULNÉRABILITÉ STRUCTURELLE :

> Plus une architecture produit de données dérivées à partir de plusieurs sources, plus la correction effective d'une information erronée nécessite de maîtriser non seulement la donnée initiale, mais également les résultats qui en ont été tirés.

Deuxième question difficile : peut-on savoir pourquoi son dossier a été sélectionné ?

Le droit d'accès permet d'obtenir de nombreuses informations relatives au traitement S43.

Mais CFVR est précisément un dispositif de détection et de programmation du contrôle fiscal.

Une divulgation trop détaillée des règles de détection pourrait compromettre certaines de ses finalités.

D'où la possibilité de restreindre certains droits S45-S54.

La personne peut donc se trouver face à une difficulté structurelle :

```
pour contester un signalement
   ↓
comprendre pourquoi
le système l'a produit

   mais

expliquer précisément
la méthode de détection
   ↓
peut compromettre
l'efficacité du contrôle
```

VULNÉRABILITÉ JURIDIQUE :

> L'effectivité du droit de contestation dépend de l'équilibre entre le niveau d'information accessible à la personne et le niveau de secret nécessaire à la protection des méthodes de contrôle.

Cette tension rejoint directement l'explicabilité étudiée en 6.4

La jurisprudence étudiée en 6.4 montre que, lorsque le régime des décisions automatisées est applicable, la complexité d'un système ne dispense pas le responsable de fournir les explications juridiquement requises S52.

CFVR ne constitue pas, selon les sources actuelles, un système décidant automatiquement de l'ouverture d'un contrôle.

Mais la question de l'explicabilité reste importante parce que la CNIL demande elle-même au ministère de mener des travaux sur l'explicabilité et les biais S37.

On obtient donc une frontière :

```
secret nécessaire
des méthodes de contrôle

   ↕

compréhension nécessaire
pour exercer les droits
```

À ÉTABLIR :

> Quel niveau d'explication peut être fourni à une personne concernant le rôle d'un résultat CFVR dans la sélection de son dossier sans compromettre les méthodes de contrôle ?

L'information des personnes reste néanmoins obligatoire

Concernant les nouveaux échanges entre la DGFiP et les organismes de sécurité sociale, la CNIL rappelle expressément que chacune des administrations concernées doit informer les personnes conformément aux articles 12 à 14 du RGPD S37.

Le ministère a indiqué que les conventions organisant ces échanges rappelleront cette obligation S37.

C'est un point important.

L'existence d'échanges légalement autorisés ne supprime donc pas automatiquement l'obligation d'information.

GARANTIE DOCUMENTÉE :

> La CNIL exige que les personnes concernées soient informées des échanges de données entre la DGFiP et les organismes de sécurité sociale dans les conditions prévues par le RGPD S37.

Mais l'information générale ne signifie pas connaissance individuelle de chaque utilisation

Il faut distinguer :

```
être informé
de l'existence d'un traitement
   ≠
savoir qu'une donnée précise
a été utilisée dans une analyse précise

   ≠

connaître le résultat
de cette analyse
   ≠
savoir que ce résultat
a contribué à une décision
```

Ces quatre niveaux d'information n'ont ni le même objet ni nécessairement le même régime juridique.

VULNÉRABILITÉ DOCUMENTAIRE :

> L'information générale sur l'existence et les finalités de CFVR ne permet pas, à elle seule, de déterminer dans quelle mesure une personne peut retracer concrètement l'utilisation de ses données dans une analyse particulière.

La CNIL dispose de pouvoirs de contrôle importants

La CNIL ne se limite pas à rendre des avis lors de la création ou de la modification des traitements.

Le RGPD lui confère notamment des pouvoirs permettant :

- d'exiger les informations nécessaires ;
- de mener des enquêtes et audits ;
- d'accéder aux données personnelles nécessaires à sa mission ;
- d'accéder aux installations et moyens de traitement ;
- d'ordonner certaines mises en conformité ;
- de limiter ou interdire certains traitements dans les conditions prévues par le droit S43.

Une personne peut également introduire une réclamation auprès d'une autorité de contrôle lorsqu'elle estime qu'un traitement la concernant viole le RGPD S43.

GARANTIE INSTITUTIONNELLE :

> Le contrôle de la légalité du traitement ne dépend donc pas uniquement de l'administration qui exploite les données.

L'avis préalable de la CNIL ne constitue cependant pas une validation définitive du système

CFVR existe depuis 2014.

Depuis, son périmètre a connu de nombreuses évolutions S37-S45.

Il a notamment été étendu :

- aux professionnels ;
- aux personnes physiques liées aux entreprises ;
- aux particuliers ;
- à de nouvelles sources ;
- à de nouvelles méthodes algorithmiques ;
- à des données issues de plateformes ;
- à de nouveaux échanges administratifs ;
- à une nouvelle infrastructure de calcul ;
- et désormais aux données issues de la facturation électronique S37-S45.

La CNIL a rendu plusieurs avis successifs sur ces évolutions S37.

Mais un avis rendu à un instant donné porte sur le dispositif qui lui est présenté à cet instant.

GARANTIE :

> Les modifications importantes du dispositif font l'objet d'un encadrement juridique et certaines ont donné lieu à de nouveaux avis de la CNIL.

VULNÉRABILITÉ STRUCTURELLE :

> La conformité d'une architecture évolutive ne peut être considérée comme définitivement acquise du seul fait qu'une version antérieure ou une modification particulière a fait l'objet d'un avis de la CNIL.

Le respect du RGPD constitue une obligation continue.

Le contrôle ex post devient donc essentiel

La CNIL peut contrôler un organisme :

- à la suite d'une plainte ;
- à la suite d'un signalement ;
- ou de sa propre initiative S43.

Elle peut procéder à des contrôles sur place, sur pièces, sur audition ou en ligne.

En cas de manquement, différentes mesures correctrices peuvent être mises en œuvre.

Cette distinction est fondamentale :

```
avis sur un projet
   ≠
contrôle du fonctionnement réel
   ≠
constat de conformité permanent
```

GARANTIE INSTITUTIONNELLE :

> L'existence d'un avis favorable ou comportant des observations ne prive pas la CNIL de ses pouvoirs ultérieurs de contrôle.

Une vulnérabilité particulière apparaît avec l'évolution permanente des systèmes

Les sections 6.3 à 6.5 ont montré que plusieurs caractéristiques peuvent évoluer simultanément :

```
plus de données
   +
plus de sources
   +
plus de croisements
   +
nouveaux algorithmes
   +
nouveaux destinataires
   +
nouvelle infrastructure
```

Or chacune de ces évolutions peut modifier le niveau de risque pour les droits et libertés.

Une garantie conçue pour une architecture donnée peut donc devenir insuffisante si l'architecture change profondément.

VULNÉRABILITÉ JURIDIQUE :

> Dans un traitement évolutif, l'effectivité des garanties dépend de leur réévaluation lorsque la nature, l'ampleur ou les risques du traitement changent.

Cette question rejoint directement l'obligation de réexaminer l'analyse d'impact lorsque l'évolution du risque le justifie S48.

Le recours juridictionnel constitue la dernière garantie

Le RGPD reconnaît :

- le droit d'introduire une réclamation auprès d'une autorité de contrôle ;
- le droit à un recours juridictionnel effectif contre certaines décisions de cette autorité ;
- le droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant lorsque la personne estime que ses droits ont été violés S43.

La procédure particulière prévue par l'article 118 de la loi Informatique et Libertés rappelle également l'existence d'un recours juridictionnel S54.

GARANTIE JURIDIQUE :

> Même lorsqu'une personne ne peut pas obtenir directement certaines informations protégées, le traitement n'échappe pas à tout contrôle extérieur.

Mais un recours effectif suppose de pouvoir identifier suffisamment le problème

Une difficulté demeure néanmoins.

Pour contester efficacement un traitement, une personne doit généralement pouvoir identifier au moins l'existence d'un problème.

Dans une architecture complexe :

```
collecte
   ↓
croisement
   ↓
inférence
   ↓
signalement
   ↓
transmission
   ↓
conséquence
```

une erreur peut apparaître loin de la donnée initiale.

La personne peut connaître la conséquence sans nécessairement connaître immédiatement :

- la donnée qui l'a provoquée ;

- la source de cette donnée ;
- le rapprochement effectué ;
- l'inférence produite ;
- le système ayant généré le signal ;
- les destinataires qui l'ont reçu.

VULNÉRABILITÉ STRUCTURELLE :

> Plus la chaîne de traitement comporte d'étapes, de responsables et de données dérivées, plus l'exercice effectif des droits dépend de la traçabilité interne du traitement et de la capacité des autorités de contrôle à reconstruire cette chaîne.

Cette question dépasse CFVR et rejoint les autres infrastructures de l'enquête

Les chapitres précédents ont identifié séparément plusieurs infrastructures capables de traiter des informations concernant :

- l'identité ;
- les transactions ;
- la facturation ;
- les produits ;
- le DPP ;
- les caractéristiques environnementales ;
- les paiements.

Aucune source étudiée ne démontre aujourd'hui l'existence d'un système unique exploitant l'ensemble de ces informations afin de prendre une décision individuelle.

Mais si plusieurs de ces infrastructures étaient un jour rapprochées, la question des droits deviendrait plus complexe.

```
système A
identité
       ↓
système B
transaction
       ↓
système C
produit / DPP
       ↓
système D
information environnementale
       ↓
système E
paiement
```

La question ne serait plus uniquement :

> **« ai-je un droit d'accès dans chacun de ces systèmes ? »**

Elle deviendrait :

> **« puis-je reconstruire la chaîne qui a conduit à la conséquence qui me concerne ? »**

Le droit d'accès à chaque composant ne garantit pas automatiquement la compréhension du système résultant

Cette distinction est essentielle.

Supposons que chaque infrastructure fournisse séparément :

```
A → accès possible
B → accès possible
C → accès possible
D → accès possible
E → accès possible
```

Il ne s'ensuit pas automatiquement :

```
A + B + C + D + E
   ↓
compréhension possible
de la décision résultante
```

VULNÉRABILITÉ JURIDIQUE STRUCTURELLE :

> Dans une architecture interconnectée, l'effectivité des droits doit être appréciée non seulement traitement par traitement, mais également au regard de la capacité de la personne à comprendre et contester la chaîne de traitement qui produit une conséquence à son égard.

Cette conclusion constitue un nouveau pont juridique avec les chapitres précédents.

Le rapprochement avec les libertés fondamentales doit cependant rester rigoureux

Le droit à la protection des données personnelles n'est pas seulement une exigence technique.

Il participe à la protection des droits et libertés des personnes.

Mais toute collecte de données ou tout traitement administratif ne constitue pas automatiquement une violation d'une liberté fondamentale.

La question juridiquement pertinente est :

```
ingérence / traitement
   ↓
base juridique
   ↓
finalité légitime
   ↓
nécessité
   ↓
proportionnalité
   ↓
garanties
   ↓
droits effectifs
   ↓
contrôle indépendant
   ↓
recours effectif
```

Une atteinte juridiquement problématique peut apparaître lorsque cet équilibre n'est plus respecté.

Le véritable point de fragilité est donc l'effectivité

Après les sections précédentes, une ligne commune apparaît.

La protection ne repose pas sur une impossibilité technique d'utiliser les données.

Elle repose sur une succession de garanties juridiques et organisationnelles :

```
limitation des finalités
   ↓
minimisation
   ↓
proportionnalité
   ↓
sécurité
   ↓
intervention humaine
   ↓
information
   ↓
accès
   ↓
rectification
   ↓
limitation
   ↓
contrôle CNIL
   ↓
recours juridictionnel
```

Plus les infrastructures deviennent capables de collecter, rapprocher et analyser des données, plus l'effectivité de chacune de ces garanties devient importante.

VULNÉRABILITÉ STRUCTURELLE :

> La protection des libertés ne repose donc pas uniquement sur l'existence formelle de droits, mais sur la possibilité concrète de les exercer et sur l'existence d'autorités capables de contrôler les traitements lorsque l'accès individuel doit être restreint.

Questions permettant de tester cette effectivité

L'enquête peut désormais poser des questions beaucoup plus précises :

> **1. Une personne peut-elle obtenir la liste des données la concernant effectivement utilisées dans CFVR et leur origine ?**

> **2. Peut-elle connaître les destinataires auxquels les résultats la concernant ont été transmis ?**

> **3. Lorsqu'une donnée est rectifiée, quels mécanismes garantissent la correction ou le recalcul des résultats dérivés de cette donnée ?**

> **4. Une limitation demandée au titre de l'article 18 est-elle propagée aux environnements et résultats dans lesquels la donnée a déjà été utilisée ?**

> **5. Peut-on connaître le rôle joué par CFVR dans la sélection d'un dossier sans révéler les méthodes dont la confidentialité est nécessaire au contrôle fiscal ?**

> **6. Quelles informations sont effectivement communiquées à une personne lorsque son droit d'accès est exercé par l'intermédiaire de la CNIL ?**

> **7. Quels mécanismes permettent à la CNIL de reconstruire la chaîne complète lorsqu'une donnée a circulé entre plusieurs traitements ou administrations ?**

> **8. Les personnes sont-elles informées de manière suffisamment précise des nouveaux échanges DGFiP / organismes sociaux ?**

> **9. Comment les droits sont-ils exercés lorsque plusieurs responsables de traitement interviennent successivement dans une même chaîne ?**

> **10. Les évolutions de CFVR entraînent-elles une réévaluation régulière de l'effectivité des droits et des restrictions qui leur sont apportées ?**

Ces questions ne présument aucune violation.

Elles permettent de tester si les garanties sont réellement opérationnelles.

Conclusion de 6.6

AVÉRÉ :

> CFVR prévoit l'exercice des droits d'accès, de rectification et de limitation S45.

RESTRICTION AVÉRÉE :

> Le droit d'opposition prévu à l'article 21 du RGPD ne s'applique pas à CFVR S45.

RESTRICTION AVÉRÉE :

> Les droits d'accès et de rectification peuvent faire l'objet de restrictions dans les conditions prévues par la loi Informatique et Libertés S45-S54.

GARANTIE JURIDIQUE :

> Lorsqu'une restriction s'applique, une procédure d'exercice des droits par l'intermédiaire de la CNIL est prévue et un recours juridictionnel demeure possible S54.

GARANTIE JURIDIQUE :

> Le RGPD prévoit des mécanismes permettant notamment la rectification de données inexactes, la limitation de certains traitements et la notification de certaines rectifications ou limitations aux destinataires S43.

GARANTIE DOCUMENTÉE :

> La CNIL rappelle que la DGFiP et les organismes de sécurité sociale doivent informer les personnes concernées des échanges de données prévus entre eux S37.

GARANTIE INSTITUTIONNELLE :

> La CNIL dispose de pouvoirs d'enquête et de contrôle indépendants de ses avis préalables et une personne peut introduire une réclamation lorsqu'elle estime que le traitement de ses données viole le RGPD S43.

VULNÉRABILITÉ JURIDIQUE :

> La protection individuelle devient plus dépendante du contrôle de la CNIL et du juge lorsque les informations nécessaires à la compréhension directe du traitement peuvent légalement être restreintes.

VULNÉRABILITÉ STRUCTURELLE :

> Dans une architecture multi-sources, la rectification effective d'une donnée suppose de maîtriser les résultats, inférences et transmissions déjà produits à partir de cette donnée.

ANGLE MORT DOCUMENTAIRE :

> Les sources publiques étudiées ne permettent pas de déterminer précisément comment une rectification ou une limitation est propagée aux résultats algorithmiques et aux données dérivées déjà produits dans CFVR, la PSD ou les applications alimentées par leurs résultats.

ANGLE MORT DOCUMENTAIRE :

> Les sources publiques étudiées ne permettent pas de mesurer précisément le niveau d'information effectivement obtenu par une personne lorsque certaines informations relatives à CFVR sont soumises aux restrictions prévues par le droit fiscal.

À ÉTABLIR :

> Une personne peut-elle reconstruire suffisamment la chaîne ayant conduit d'une donnée source à un signalement ou à une proposition de contrôle pour exercer effectivement ses droits lorsque plusieurs traitements ont participé au résultat ?

À ÉTABLIR :

> Les mécanismes de traçabilité permettent-ils à la CNIL de reconstruire cette chaîne complète lorsque la personne elle-même ne peut accéder directement à certaines informations ?

DÉDUCTIBLE JURIDIQUEMENT :

> Si plusieurs infrastructures relatives à l'identité, aux transactions, à la facturation, aux produits, aux données environnementales ou au paiement étaient un jour interconnectées pour produire une conséquence individuelle, l'existence de droits séparés dans chaque infrastructure ne suffirait pas nécessairement à garantir un recours effectif contre le résultat produit par leur combinaison.

NON ÉTABLI :

> Les sources étudiées ne permettent pas de conclure que les restrictions actuellement prévues dans CFVR privent les personnes d'un recours effectif ou sont contraires au RGPD.

6.7 Garanties propres aux infrastructures étudiées

Statut : GARANTIES SPÉCIFIQUES ÉTABLIES / INTERFACES DOCUMENTÉES / FRONTIÈRES JURIDIQUES IDENTIFIÉES

Les sections précédentes ont étudié les garanties générales applicables aux traitements de données :

- finalité ;
- base juridique ;
- minimisation ;
- proportionnalité ;
- sécurité ;
- profilage ;
- décisions automatisées ;
- droits des personnes ;
- contrôle par les autorités indépendantes.

Mais les infrastructures étudiées dans les chapitres précédents disposent également de garanties qui leur sont propres.

Cette section examine donc séparément :

```
facturation électronique
   +
identité numérique
   +
passeport numérique de produit
   +
données environnementales
   +
paiement / euro numérique
```

L'objectif est ensuite de déterminer ce que deviennent ces garanties lorsque plusieurs infrastructures sont susceptibles d'interagir.

Première constatation : les infrastructures ne sont pas juridiquement conçues comme une base de données unique

Les chapitres précédents ont identifié plusieurs possibilités techniques d'interconnexion.

Mais les textes juridiques étudiés organisent au contraire plusieurs séparations.

On retrouve notamment :

```
données fiscales
→ finalités fiscales déterminées

identité numérique
→ contrôle de l'utilisateur
→ divulgation sélective
→ cloisonnement

DPP
→ information produit
→ droits d'accès déterminés
→ protection des données clients

paiement
→ finalités propres
→ protection des données
→ garanties spécifiques
```

GARANTIE STRUCTURELLE :

> Aucun des textes étudiés n'établit un droit général permettant de fusionner librement l'ensemble des données issues de ces infrastructures.

L'interopérabilité technique ne constitue donc pas une autorisation générale d'interconnexion juridique.

L'identité numérique européenne comporte des garanties particulièrement fortes

Le règlement eIDAS 2 prévoit que le portefeuille européen d'identité numérique fonctionne sous le contrôle de l'utilisateur S55.

L'utilisateur doit notamment pouvoir :

- sélectionner les données qu'il souhaite présenter ;
- combiner différents attributs ;
- utiliser la divulgation sélective ;
- consulter les parties utilisatrices avec lesquelles il a interagi ;
- connaître, le cas échéant, les données échangées ;
- demander l'effacement de certaines données ;
- signaler une demande suspecte à l'autorité de protection des données S55.

Le portefeuille peut également générer et stocker localement des pseudonymes.

Le règlement envisage même des technologies permettant de démontrer qu'une condition est satisfaite sans révéler les données sous-jacentes.

Exemple :

```
attribut complet
« date de naissance : ... »
   ↓
preuve minimale
« plus de 18 ans : OUI »
```

plutôt que :

```
transmission de
l'identité complète
   +
date de naissance
   +
autres attributs inutiles
```

GARANTIE JURIDIQUE ET TECHNIQUE :

> L'architecture de l'identité numérique européenne intègre explicitement des mécanismes destinés à réduire la quantité d'informations révélées lors de l'accès à un service S55.

Le fournisseur du portefeuille ne doit pas devenir un observateur général de son utilisateur

Une garantie particulièrement importante apparaît dans le règlement.

Le fournisseur du portefeuille ne doit pas collecter d'informations sur son utilisation qui ne soient pas nécessaires à la fourniture du service S55.

Il doit assurer une forme d'« inobservabilité » lui empêchant d'obtenir une visibilité générale sur les transactions réalisées par l'utilisateur.

Il lui est également interdit de combiner les données d'identification ou autres données personnelles liées au portefeuille avec les données provenant d'autres services lorsque cette combinaison n'est pas nécessaire au service du portefeuille, sauf demande expresse de l'utilisateur S55.

Les services d'attestation d'attributs font également l'objet d'obligations de séparation.

GARANTIE MAJEURE :

> Le portefeuille européen d'identité numérique n'est juridiquement pas conçu pour permettre à son fournisseur de reconstruire librement l'ensemble des activités numériques de son utilisateur.

Cette garantie répond directement à l'un des risques identifiés dans les chapitres précédents.

Le refus d'utiliser le portefeuille ne doit pas devenir un motif général d'exclusion

Le règlement prévoit également que l'accès aux services publics et privés, au marché du travail et à la liberté d'entreprendre ne doit pas être restreint ou rendu désavantageux du seul fait qu'une personne n'utilise pas le

portefeuille européen d'identité numérique S55.

Des moyens alternatifs doivent rester disponibles.

La conséquence est importante.

```
utilisation du wallet
   ↓
possible

   mais

refus du wallet
   ↓
ne doit pas, par lui-même,
entraîner une exclusion
```

GARANTIE DE LIBERTÉ DE CHOIX :

> Le cadre actuel cherche explicitement à empêcher que le portefeuille européen d'identité numérique devienne une condition générale et obligatoire d'accès aux services.

Cette garantie sera particulièrement importante à surveiller lors du déploiement pratique du dispositif.

Mais le portefeuille est également conçu pour combiner des attributs

La même infrastructure possède une autre caractéristique.

Le portefeuille doit permettre à son utilisateur de :

> demander, obtenir, sélectionner, combiner, stocker, supprimer, partager et présenter des données d'identification et des attestations électroniques d'attributs S55.

Il est donc conçu pour pouvoir présenter à une partie utilisatrice plusieurs attributs provenant de sources distinctes.

```
identité
   +
attribut A
   +
attribut B
   +
attestation C
   ↓
présentation à un service
```

Cette capacité n'est pas en elle-même une vulnérabilité.

Elle constitue précisément l'une des fonctions du portefeuille.

Mais elle crée une frontière importante.

FRONTIÈRE JURIDIQUE :

> La protection ne repose pas sur une impossibilité technique de combiner des attributs. Elle repose sur le contrôle de l'utilisateur, la limitation des données demandées, la finalité du service et les règles applicables à la partie utilisatrice.

Les parties utilisatrices doivent déclarer les données qu'elles demandent

Une partie souhaitant utiliser le portefeuille européen d'identité numérique doit s'enregistrer et déclarer notamment l'usage prévu ainsi que les données qu'elle prévoit de demander S55.

Elle ne doit ensuite pas demander à l'utilisateur d'autres données que celles déclarées.

Elle doit également s'identifier auprès de l'utilisateur.

GARANTIE JURIDIQUE :

> Une partie utilisatrice ne dispose donc pas d'un accès indifférencié aux attributs présents dans le portefeuille.

L'architecture fonctionne selon une logique d'accès déterminé :

```
service
   ↓
finalité déclarée
   ↓
attributs déclarés
   ↓
demande
   ↓
présentation sélective
```

et non :

```
service
   ↓
accès à tout le wallet
```

Le DPP contient lui aussi une séparation fondamentale

Le passeport numérique de produit est conçu comme une infrastructure de données relatives au produit S56.

Il peut contenir notamment des informations relatives :

- aux caractéristiques du produit ;

- à sa conformité ;
- à son cycle de vie ;
- à sa durabilité ;
- à certaines caractéristiques environnementales ;
- à sa traçabilité.

Le DPP doit être associé à un identifiant unique de produit et fonctionner dans un environnement de données ouvert et interopérable S56.

Selon les exigences applicables, il peut être établi au niveau :

```
modèle
   ou
lot
   ou
article
```

Cette dernière possibilité augmente fortement la granularité potentielle de la traçabilité du produit.

Mais le règlement introduit immédiatement une garantie importante.

Le DPP n'est pas juridiquement un dossier environnemental du consommateur

Le règlement ESPR prévoit explicitement :

> les données personnelles relatives aux clients ne doivent pas être stockées dans le passeport numérique de produit sans leur consentement explicite S56.

Cette règle casse une association qui pourrait sinon sembler évidente :

```
produit identifiable
   ↓
acheteur identifiable
```

Le premier élément ne produit pas juridiquement le second.

Un DPP peut identifier précisément un produit ou un article sans identifier son propriétaire ou son utilisateur.

GARANTIE JURIDIQUE MAJEURE :

> Le cadre actuel du DPP sépare explicitement l'identification du produit de l'identification personnelle du client.

NON ÉTABLI :

> Le DPP européen ne constitue pas, dans les textes étudiés, un « passeport environnemental individuel » enregistrant les achats ou l'empreinte environnementale personnelle d'un citoyen.

Cette distinction doit impérativement être conservée.

Mais l'identifiant unique et l'interopérabilité rendent techniquement possible une autre opération

La garantie précédente ne signifie pas qu'un produit ne puisse jamais être relié à une personne dans un autre système.

Une transaction commerciale peut déjà contenir :

```
acheteur
   +
vendeur
   +
produit
   +
date
   +
montant
```

Le DPP peut de son côté contenir :

```
identifiant produit
   +
caractéristiques produit
   +
données environnementales
```

Une association externe pourrait donc théoriquement produire :

```
transaction
   ↓
produit identifié
   ↓
DPP
   ↓
caractéristiques environnementales
```

Cette possibilité technique a déjà été identifiée dans les chapitres précédents.

Mais juridiquement :

FRONTIÈRE JURIDIQUE :

> La protection du DPP contre le stockage de données personnelles du client ne constitue pas une interdiction générale de tout rapprochement externe entre un produit et une transaction.

Un tel rapprochement constituerait cependant un traitement distinct devant disposer de sa propre finalité, de sa propre base juridique et respecter les exigences de nécessité, de proportionnalité et de minimisation lorsqu'il implique des données personnelles S43-S44-S53-S56.

Une première asymétrie apparaît donc

Le DPP protège son propre contenu :

```
DPP
   ↓
pas de données personnelles client
sans consentement explicite
```

Mais cette garantie porte sur :

> **ce qui est stocké dans le DPP.**

Elle ne signifie pas nécessairement :

> **qu'aucun autre système ne peut utiliser l'identifiant du produit pour effectuer un rapprochement autorisé par un autre fondement juridique.**

VULNÉRABILITÉ STRUCTURELLE :

> Une garantie empêchant la centralisation d'une donnée personnelle dans une infrastructure ne constitue pas nécessairement une interdiction de reconstruire la relation entre plusieurs données au moyen d'un traitement externe.

C'est une distinction importante pour l'ensemble de cette enquête.

L'euro numérique comporte lui aussi une garantie particulièrement forte

Le cadre proposé pour l'euro numérique contient une interdiction explicite :

> **l'euro numérique ne doit pas être de la monnaie programmable** S57.

Une unité d'euro numérique ne doit donc pas comporter une logique intrinsèque imposant :

```
utilisable seulement
pour produit X
   ou
interdit pour produit Y
   ou
utilisable seulement
avant telle date
   ou
utilisable seulement
auprès de tel bénéficiaire
```

La BCE rappelle également que de telles limitations seraient incompatibles avec la conception retenue de l'euro numérique S57.

GARANTIE MONÉTAIRE MAJEURE :

> Le cadre proposé interdit que l'euro numérique devienne intrinsèquement une monnaie dont l'utilisation serait limitée selon les biens, services, dates ou bénéficiaires.

Cette garantie répond directement à l'une des préoccupations les plus fortes pouvant apparaître autour d'une monnaie numérique de banque centrale.

Mais « monnaie non programmable » ne signifie pas « paiement non conditionnable »

C'est ici qu'apparaît une frontière beaucoup plus subtile.

La proposition distingue explicitement :

```
**MONNAIE PROGRAMMABLE**
logique inscrite dans la monnaie
qui limite sa fongibilité
   ↓
INTERDITE
```

de :

```
**PAIEMENT CONDITIONNEL**
logiciel
   +
condition prédéfinie
   +
accord payeur / bénéficiaire
   +
déclenchement automatique
   ↓
PRÉVU
```

S57

Une opération conditionnelle est définie comme une opération déclenchée automatiquement lorsque des conditions prédéfinies convenues par le payeur et le bénéficiaire sont satisfaites.

La proposition permet même à la BCE de fournir les standards et fonctionnalités nécessaires à ces paiements, notamment la réservation de fonds S57.

LATITUDE JURIDIQUE EXPLICITE :

> Le cadre proposé interdit la programmation intrinsèque de la monnaie mais autorise la programmation de certaines conditions d'exécution du paiement.

Cette distinction est fondamentale.

La protection porte donc sur la monnaie, pas sur l'existence de toute logique conditionnelle autour du paiement

On peut représenter la frontière ainsi :

```
« cet euro ne peut acheter
que certaines catégories de produits »
   ↓
monnaie programmable
   ↓
INTERDITE
```

mais :

```
« exécute ce paiement
si la condition convenue X
est satisfaite »
   ↓
paiement conditionnel
   ↓
PRÉVU
```

POINT DE FRICTION JURIDIQUE :

> L'interdiction de la monnaie programmable ne constitue donc pas une interdiction générale de toute infrastructure capable de conditionner automatiquement l'exécution d'un paiement.

C'est probablement l'une des distinctions les plus importantes identifiées dans cette enquête.

Cela ne signifie toujours pas qu'une condition environnementale soit prévue

Il faut immédiatement conserver la frontière documentaire.

Les exemples officiels de paiements conditionnels concernent notamment :

- le paiement à la livraison ;
- le paiement à l'usage ;
- des paiements liés à certaines étapes ;
- certains paiements automatisés entre machines S57.

Aucune source étudiée ne démontre qu'un paiement en euro numérique serait destiné à être conditionné :

- à un score environnemental individuel ;
- à une empreinte carbone personnelle ;
- à un DPP ;
- à un historique d'achats ;
- ou à une classification environnementale d'une personne.

NON ÉTABLI :

> Aucun mécanisme officiel étudié ne relie actuellement une donnée environnementale ou un DPP à l'autorisation ou au refus d'un paiement en euro numérique.

Mais la condition peut provenir d'une information extérieure au paiement

Un paiement conditionnel suppose nécessairement qu'un système puisse déterminer si :

```
condition X
   =
satisfaite
   ou
non satisfaite
```

Les travaux étudiés dans les chapitres précédents ont déjà établi expérimentalement la possibilité pour un système externe de vérifier une condition utilisée pour déclencher un paiement.

La structure technique générale est donc :

```
source externe
   ↓
vérification de condition
   ↓
condition satisfaite ?
   ↓
OUI / NON
   ↓
exécution du paiement
```

La nature de la source externe dépend du service concerné.

FRONTIÈRE JURIDIQUE :

> Le cadre proposé autorise l'existence d'une condition externe au paiement, mais la légalité de la condition elle-même dépendrait de sa finalité, du mécanisme utilisé, des données traitées, de l'accord des parties et des autres règles applicables.

Autrement dit :

> **la capacité de conditionner existe ; la liberté juridique de choisir n'importe quelle condition n'est pas établie.**

L'identité numérique et l'euro numérique possèdent une interface explicitement prévue

Un autre élément est particulièrement important.

La proposition de règlement sur l'euro numérique prévoit que les services front-end soient :

> **interopérables ou intégrés aux portefeuilles européens d'identité numérique** S57.

Le portefeuille européen d'identité numérique permet de son côté la présentation d'identité et d'attestations d'attributs à des services publics ou privés S55.

On dispose donc ici d'une interconnexion qui n'est plus seulement déduite techniquement :

```
portefeuille européen
d'identité numérique
   ↕
services euro numérique
```

INTERFACE DOCUMENTÉE :

> Le cadre proposé pour l'euro numérique prévoit explicitement une interopérabilité ou une intégration avec le portefeuille européen d'identité numérique.

Cette interface ne signifie pas que l'ensemble des attributs du portefeuille deviennent accessibles au système de paiement.

Les garanties du règlement eIDAS 2 continuent de s'appliquer.

Mais l'existence de l'interface elle-même est documentée.

Le pont identité → paiement est donc établi, mais strictement limité dans sa portée

La conclusion doit être précise.

On peut désormais établir :

```
identité numérique
   ↕
interface prévue
   ↕
euro numérique
```

Mais pas :

```
tous les attributs d'identité
   ↓
tous les paiements
```

et encore moins :

```
identité
   +
environnement
   ↓
autorisation de paiement
```

AVÉRÉ AU NIVEAU DU CADRE PROPOSÉ :

> Une interface entre le portefeuille européen d'identité numérique et les services de paiement en euro numérique est explicitement prévue S57.

NON ÉTABLI :

> Cette interface ne démontre aucune utilisation d'attributs environnementaux ou de DPP pour autoriser, refuser ou limiter un paiement.

Le cadre de l'euro numérique prévoit également des protections fortes de la vie privée

Le projet distingue notamment les paiements en ligne et hors ligne S57.

Pour les paiements hors ligne, le niveau de confidentialité recherché doit se rapprocher de celui des espèces.

Les détails des transactions hors ligne ne doivent pas être accessibles à la BCE ou aux banques centrales nationales dans les mêmes conditions que les paiements en ligne.

Pour les paiements en ligne, la proposition prévoit des mesures techniques et organisationnelles destinées à empêcher que les données transmises à l'Eurosystème permettent d'identifier directement les utilisateurs individuels S57.

GARANTIE DE CONFIDENTIALITÉ :

> L'architecture proposée ne repose pas sur l'idée que la BCE devrait disposer d'un historique nominatif général des paiements individuels.

Les autorités européennes de protection des données ont néanmoins demandé des garanties supplémentaires

L'EDPB et l'EDPS ont examiné la proposition d'euro numérique.

Ils reconnaissent les efforts réalisés en matière de protection de la vie privée, notamment :

- la modalité hors ligne ;
- la protection des données dès la conception ;
- la minimisation ;
- le maintien du choix entre espèces et euro numérique.

Mais ils ont également demandé que la conception évite une centralisation excessive des données personnelles par la BCE ou les banques centrales nationales.

POINT DE VIGILANCE INSTITUTIONNEL :

> Même une architecture explicitement conçue pour offrir un haut niveau de confidentialité doit être examinée au regard de la quantité de données centralisées et de la répartition des responsabilités entre les différents acteurs.

La possibilité de payer en espèces constitue elle-même une garantie importante

Le cadre proposé pour l'euro numérique ne vise pas à supprimer les espèces.

L'euro numérique doit constituer un moyen de paiement supplémentaire.

Les autorités européennes de protection des données ont expressément salué le maintien du choix entre euro numérique et espèces.

La BCE affirme également que l'euro numérique doit compléter les billets et pièces.

GARANTIE DE LIBERTÉ DE CHOIX :

> Dans le cadre actuellement proposé, l'euro numérique ne doit pas constituer l'unique moyen de paiement disponible.

Cette garantie réduit fortement le risque qu'une restriction propre à l'euro numérique devienne automatiquement une impossibilité générale de payer.

Une architecture intéressante apparaît lorsqu'on assemble uniquement les interfaces documentées

À ce stade, il faut distinguer ce qui est réellement établi de ce qui reste hypothétique.

Les éléments documentés permettent déjà d'écrire :

```
IDENTITÉ NUMÉRIQUE
   ↓
interface prévue
   ↓
EURO NUMÉRIQUE

EURO NUMÉRIQUE
   ↓
paiements conditionnels possibles
   ↓
condition externe vérifiée

PRODUIT
   ↓
identifiant unique
   ↓
DPP
   ↓
données produit / environnementales

TRANSACTION
   ↓
peut identifier un produit
```

En revanche, le lien suivant reste absent :

```
DPP / environnement
   ↓
condition de paiement
```

FRONTIÈRE DOCUMENTAIRE :

> Plusieurs segments de la chaîne existent séparément ou disposent d'interfaces documentées, mais la jonction permettant à une donnée environnementale issue du DPP de déterminer une condition de paiement n'est pas établie.

Le véritable point faible potentiel n'est donc pas l'absence de garanties

Les garanties sont nombreuses.

On trouve notamment :

```
IDENTITÉ
→ contrôle utilisateur
→ divulgation sélective
→ inobservabilité
→ séparation des données
→ alternatives au wallet

DPP
→ droits d'accès
→ architecture décentralisée
→ pas de données personnelles client
  sans consentement explicite

EURO NUMÉRIQUE
→ confidentialité
→ espèces maintenues
→ monnaie programmable interdite
```

Mais chacune de ces garanties protège principalement **son propre périmètre**.

La question transversale devient :

> **Que se passe-t-il lorsqu'une information quitte son infrastructure d'origine et devient une entrée juridiquement autorisée d'un autre traitement ?**

C'est là que se situe le point de friction le plus intéressant de 6.7.

Une garantie locale ne constitue pas nécessairement une interdiction globale de rapprochement

Trois exemples permettent de comprendre cette distinction.

DPP

```
pas de données personnelles client
dans le DPP sans consentement
```

ne signifie pas automatiquement :

```
impossibilité de rapprocher ailleurs
une transaction et l'identifiant produit
```

Identité numérique

```
fournisseur du wallet
ne doit pas observer
toutes les transactions
```

ne signifie pas :

```
aucun service autorisé
ne peut recevoir un attribut
présenté par l'utilisateur
```

Euro numérique

```
monnaie programmable interdite
```

ne signifie pas :

```
paiement conditionnel interdit
```

VULNÉRABILITÉ STRUCTURELLE :

> Plusieurs garanties fortes identifiées dans les textes sont des garanties de périmètre : elles limitent ce qu'une infrastructure ou un acteur peut faire directement, sans nécessairement constituer une interdiction générale de tout traitement ultérieur ou de toute interface autorisée avec une autre infrastructure.

C'est ici que les sections 6.2 à 6.6 reprennent toute leur importance

Une information quittant son silo ne tombe pas dans un vide juridique.

Son traitement ultérieur devrait toujours satisfaire les exigences précédemment étudiées :

```
base juridique
   ↓
finalité
   ↓
compatibilité / nouveau fondement
   ↓
nécessité
   ↓
minimisation
   ↓
proportionnalité
   ↓
sécurité
   ↓
droits
   ↓
contrôle
```

Ainsi, l'existence d'interfaces techniques ne supprime pas les garanties générales.

Mais inversement :

> **les garanties propres à chaque infrastructure ne suffisent pas nécessairement à elles seules à empêcher toute interconnexion future.**

Une frontière particulièrement importante apparaît autour du consentement

Plusieurs protections identifiées reposent sur une action ou une demande de l'utilisateur.

Par exemple :

- présentation volontaire d'attributs dans le portefeuille ;
- consentement explicite pour certaines données personnelles dans le DPP ;
- conditions de paiement convenues entre payeur et bénéficiaire.

Cela constitue une protection importante.

Mais le consentement n'est juridiquement valable que lorsqu'il répond aux exigences applicables, notamment lorsqu'il doit être libre.

Une question apparaîtrait donc si l'accès à un bien, un service ou un moyen de paiement devenait pratiquement conditionné à l'acceptation d'un rapprochement de données.

FRONTIÈRE JURIDIQUE :

> L'existence formelle d'un consentement ou d'un accord ne suffirait pas nécessairement si les conditions juridiques permettant de le considérer comme libre et valable n'étaient plus réunies.

NON ÉTABLI :

> Les sources étudiées ne démontrent pas l'existence actuelle d'un dispositif imposant à une personne de partager des données environnementales pour accéder à un paiement ou à un service essentiel.

La liberté de choix constitue donc une garantie transversale à surveiller

Deux infrastructures comportent des protections particulièrement intéressantes sur ce point.

Pour l'identité numérique :

```
wallet
   ↓
ne doit pas devenir
l'unique moyen d'accès
```

Pour l'euro numérique :

```
euro numérique
   ↓
complément des espèces
   ↓
pas remplacement obligatoire
```

Cette redondance constitue une protection forte.

Elle signifie que le cadre actuel conserve des voies alternatives.

GARANTIE TRANSVERSALE :

> Tant que des alternatives réelles demeurent accessibles sans désavantage injustifié, la capacité d'une infrastructure numérique à imposer seule une condition à l'ensemble de la vie économique ou administrative reste juridiquement et pratiquement limitée.

Le mot important est cependant :

> **réelles.**

Une alternative existant uniquement en droit mais devenant impraticable en pratique poserait une question différente.

À ce stade, la frontière la plus importante est identifiable

L'enquête ne permet pas d'établir :

```
identité
   +
facturation
   +
DPP
   +
environnement
   +
paiement
   ↓
contrôle individuel
```

Mais elle permet désormais d'établir quelque chose de plus précis :

```
chaque infrastructure
dispose de garanties propres
   ↓
certaines interfaces
entre infrastructures
sont explicitement prévues
   ↓
certaines capacités externes
peuvent fournir des conditions
   ↓
les garanties locales
ne valent pas nécessairement
interdiction globale
d'un rapprochement futur
   ↓
tout nouveau rapprochement
devrait alors franchir
les garanties générales
étudiées en 6.1 à 6.6
```

C'est cette frontière qu'il faudra conserver pour la suite.

Questions désormais ouvertes

> **1. Quelles catégories d'attributs pourront effectivement être utilisées dans l'intégration entre portefeuille européen d'identité numérique et services en euro numérique ?**

> **2. Les données présentées lors de cette interaction pourront-elles être techniquement et juridiquement réutilisées pour d'autres finalités que l'authentification ou l'exécution du service demandé ?**

> **3. Comment l'inobservabilité du portefeuille sera-t-elle auditée dans les interactions avec des services de paiement ?**

> **4. Quelles garanties empêchent qu'un identifiant produit ou transactionnel soit utilisé pour reconstruire indirectement une relation entre une personne et un DPP sans stocker cette relation dans le DPP lui-même ?**

> **5. Quelles catégories de sources externes pourront alimenter les conditions utilisées par les futurs services de paiement conditionnels ?**

> **6. Jusqu'où une condition de paiement peut-elle porter sur un attribut concernant le payeur sans devenir incompatible avec les règles de protection des données, de proportionnalité ou de non-discrimination ?**

> **7. Comment sera garantie l'existence d'alternatives réelles lorsque le portefeuille européen d'identité numérique ou l'euro numérique seront intégrés à des services publics ou privés ?**

> **8. Une architecture juridiquement conforme silo par silo peut-elle devenir disproportionnée lorsque ses interfaces permettent de reconstruire des informations que chaque silo avait précisément été conçu pour ne pas centraliser ?**

La dernière question constitue probablement le principal point de recherche transversal issu de cette section.

Conclusion de 6.7

GARANTIE ÉTABLIE :

> Le portefeuille européen d'identité numérique prévoit le contrôle de l'utilisateur, la divulgation sélective, l'inobservabilité de son utilisation par le fournisseur et des limitations à la combinaison des données S55.

GARANTIE ÉTABLIE :

> Le refus d'utiliser le portefeuille européen d'identité numérique ne doit pas, à lui seul, restreindre ou désavantager l'accès aux services publics ou privés ; des alternatives doivent demeurer disponibles S55.

GARANTIE ÉTABLIE :

> Le DPP ne doit pas stocker de données personnelles relatives aux clients sans leur consentement explicite S56.

GARANTIE ÉTABLIE :

> L'identification d'un produit ou d'un article dans un DPP ne constitue pas juridiquement, par elle-même, l'identification de son acheteur S56.

GARANTIE PROPOSÉE :

> Le cadre proposé pour l'euro numérique interdit la monnaie programmable et maintient le principe d'une monnaie pleinement fongible S57.

LATITUDE JURIDIQUE EXPLICITE DANS LA PROPOSITION :

> Cette interdiction ne s'étend pas aux paiements conditionnels : le cadre proposé prévoit expressément des paiements déclenchés automatiquement lorsque des conditions prédéfinies et convenues sont satisfaites S57.

INTERFACE DOCUMENTÉE DANS LA PROPOSITION :

> Les services front-end de l'euro numérique doivent être interopérables ou intégrés aux portefeuilles européens d'identité numérique S57.

FRONTIÈRE JURIDIQUE :

> L'interdiction de la monnaie programmable protège la fongibilité de la monnaie, mais ne constitue pas une interdiction générale de toute logique conditionnelle appliquée à l'exécution d'un paiement.

VULNÉRABILITÉ STRUCTURELLE :

> Les garanties propres aux infrastructures étudiées protègent principalement leur périmètre respectif. Elles ne constituent pas nécessairement une interdiction générale de toute association externe de données lorsqu'un autre traitement dispose d'un fondement juridique valable.

VULNÉRABILITÉ STRUCTURELLE :

> Une architecture peut éviter de centraliser une relation dans chacun de ses composants tout en permettant techniquement que cette relation soit reconstruite dans un traitement distinct par rapprochement de leurs identifiants ou données.

À ÉTABLIR :

> Les garanties de cloisonnement prévues séparément pour l'identité, les produits et les paiements suffisent-elles à empêcher qu'une interconnexion future reconstitue, dans un autre traitement, des relations que chaque infrastructure prise isolément ne conserve pas ?

À ÉTABLIR :

> Quelles limites juridiques s'appliqueraient au choix d'une condition externe utilisée pour déclencher un paiement conditionnel lorsque cette condition concerne des données ou attributs relatifs à une personne ?

NON ÉTABLI :

> Aucun élément étudié ne démontre qu'une donnée environnementale, un DPP, un historique de consommation ou un score environnemental individuel soit actuellement destiné à autoriser, refuser ou limiter un paiement en euro numérique.

NON ÉTABLI :

> L'euro numérique n'est pas encore adopté ni émis au 3 septembre 2026. Les dispositions étudiées relatives à son architecture juridique restent celles du cadre législatif en cours de négociation.

6.8 Évolution des finalités et du cadre juridique

Statut : ÉVOLUTION JURIDIQUE AVÉRÉE / GARANTIES NON IMMUTABLES / FRONTIÈRES FUTURES À ÉTABLIR

Les sections précédentes ont établi un ensemble important de garanties.

Elles montrent notamment que le droit actuel :

- limite les finalités des traitements ;
- impose une base juridique ;
- encadre les réutilisations ;
- impose nécessité, proportionnalité et minimisation ;
- protège certaines décisions individuelles contre une automatisation excessive ;
- organise des droits et des voies de recours ;
- impose des garanties particulières à certaines infrastructures ;
- interdit actuellement certains usages, comme la monnaie programmable dans le cadre proposé pour l'euro numérique.

Une question reste cependant essentielle :

> **ces garanties figent-elles définitivement les finalités et les usages juridiquement autorisés ?**

La réponse est négative.

Une protection juridique applicable aujourd'hui ne constitue pas nécessairement une impossibilité juridique permanente.

Il faut distinguer trois situations différentes

L'évolution d'une infrastructure peut résulter de mécanismes juridiquement très différents.

```
1. même finalité
   +
   évolution technique

2. nouvelle utilisation
   compatible avec la finalité initiale

3. nouvelle finalité
   +
   nouveau fondement juridique
```

Ces trois situations ne doivent pas être confondues.

Le RGPD encadre les traitements ultérieurs et prévoit notamment l'examen de la compatibilité d'une nouvelle finalité avec celle ayant initialement justifié la collecte S43-S46.

Mais lorsqu'un nouveau traitement repose sur une disposition du droit de l'Union ou du droit national satisfaisant aux exigences applicables, le droit peut également créer ou modifier le fondement juridique permettant ce traitement S43-S46-S47.

GARANTIE JURIDIQUE :

> Une administration ne peut pas simplement décider qu'une donnée collectée pour une finalité déterminée peut désormais être utilisée pour n'importe quelle autre finalité.

LATITUDE JURIDIQUE :

> Le législateur ou l'autorité réglementaire compétente peut néanmoins faire évoluer le périmètre juridiquement autorisé d'un traitement lorsque les conditions prévues par le droit supérieur sont respectées.

La différence est fondamentale.

La limitation des finalités n'est donc pas une garantie d'immuabilité

Une lecture trop simple du principe de limitation des finalités conduirait à penser :

```
donnée collectée pour X
   ↓
utilisable uniquement pour X
pour toujours
```

Le droit fonctionne de manière plus complexe.

Selon les circonstances, une évolution peut résulter :

```
finalité initiale
   ↓
traitement ultérieur compatible
```

ou :

```
finalité initiale
   ↓
nouveau texte juridique
   ↓
nouveau traitement autorisé
sous nouvelles conditions
```

S43-S46

VULNÉRABILITÉ JURIDIQUE :

> Une garantie fondée sur la finalité actuelle d'un traitement limite les usages présents, mais ne garantit pas que le périmètre légal de ce traitement ne pourra jamais évoluer.

Cela ne signifie pas que toute évolution serait autorisée.

Cela signifie que la frontière est juridique et non techniquement immuable.

CFVR fournit un exemple concret d'évolution progressive d'une même infrastructure

Cette possibilité n'est pas seulement théorique.

CFVR existe depuis 2014 S58.

Depuis sa création, son cadre a été modifié à plusieurs reprises.

```
2014
création de CFVR
   ↓
2017
modification du traitement
   +
extension expérimentale
aux fraudes relatives aux particuliers
   ↓
2021
nouvelle modification
   +
articulation avec la collecte
de certaines données publiques
issues des plateformes en ligne
   ↓
2024
nouvelle modification
   ↓
2026
nouvelle modification
   +
facturation électronique
   +
nouvelles sources
   +
échanges avec organismes sociaux
   +
exploitation dans la PSD
```

S37-S45-S58

AVÉRÉ :

> Le périmètre juridique de CFVR a évolué par étapes successives depuis sa création.

Le traitement conserve pourtant la même identité générale :

> **« ciblage de la fraude et valorisation des requêtes ».**

Une infrastructure peut donc conserver son nom tout en changeant profondément d'échelle

Cette observation est importante.

L'évolution d'un système public ne suppose pas nécessairement :

```
ancien système
   ↓
suppression
   ↓
nouveau système
```

Elle peut prendre la forme :

```
même infrastructure
   ↓
nouvelle source
   ↓
nouvelle catégorie de données
   ↓
nouveau destinataire
   ↓
nouvelle capacité
   ↓
nouvelle modification juridique
```

CFVR fournit précisément un exemple documenté de cette évolution S58.

AVÉRÉ :

> La continuité institutionnelle d'un traitement ne signifie pas la stabilité de son périmètre de données, de sources, de destinataires ou de modalités d'exploitation.

Le passage de 2017 est particulièrement révélateur

En 2017, le cadre CFVR distinguait explicitement :

```
fraudes relatives
aux professionnels
   ↓
traitement pérenne
```

et :

```
fraudes relatives
aux particuliers
   ↓
expérimentation
de deux ans
```

S58

Le traitement pouvait ainsi utiliser, à titre expérimental, des données concernant des particuliers sans lien avec une entreprise.

Le cadre actuel concerne désormais les fraudes relatives aux professionnels **et aux particuliers** S45-S58.

Cette évolution fournit un exemple particulièrement clair :

```
capacité limitée / expérimentale
   ↓
évaluation et évolution juridique
   ↓
intégration dans un périmètre
plus large
```

VULNÉRABILITÉ JURIDIQUE :

> Le caractère expérimental ou limité d'un traitement à une date donnée ne garantit pas que ce périmètre restera expérimental ou limité.

Cela ne signifie pas que toute expérimentation devient nécessairement permanente.

Cela démontre seulement que la pérennisation constitue une évolution juridiquement possible lorsqu'un nouveau cadre l'autorise.

L'intégration de la facturation électronique fournit un second exemple

Avant la réforme étudiée dans ce dossier, CFVR existait déjà.

La facturation électronique constitue une infrastructure distincte, développée pour répondre notamment à des obligations fiscales et économiques propres.

En 2026, les données issues de cette infrastructure sont expressément intégrées parmi les catégories de données utilisées par CFVR S37-S45.

La séquence est donc documentée :

```
infrastructure A
facturation électronique
   +
infrastructure B
CFVR
   ↓
modification juridique
   ↓
données de A
utilisées dans B
```

AVÉRÉ :

> Une infrastructure de données existante peut ultérieurement devenir une nouvelle source juridiquement autorisée d'un traitement préexistant.

Cette observation est centrale pour l'ensemble de l'enquête.

La question n'est donc plus seulement de savoir si deux infrastructures sont reliées aujourd'hui

Il faut distinguer :

```
INTERCONNEXION ACTUELLE
   ↓
question factuelle
```

de :

```
INTERCONNEXION FUTURE
   ↓
question juridique
   +
évolution éventuelle du droit
```

L'absence actuelle d'une interconnexion constitue une information importante.

Mais elle ne permet pas d'affirmer :

> **« cette interconnexion ne pourra juridiquement jamais exister ».**

Inversement, la possibilité de modifier le droit ne permet absolument pas d'affirmer :

> **« cette interconnexion sera créée ».**

GARANTIE JURIDIQUE :

> Toute nouvelle interconnexion impliquant des données personnelles devrait respecter le cadre juridique applicable au moment de sa mise en œuvre.

NON ÉTABLI :

> La possibilité juridique abstraite de faire évoluer un traitement ne démontre aucune intention institutionnelle de créer une interconnexion déterminée.

Cette distinction est essentielle pour le DPP

Le cadre actuel du DPP prévoit des garanties fortes S56.

Mais le règlement ESPR prévoit lui-même que les actes délégués applicables aux différents groupes de produits préciseront notamment :

```
données du DPP
   +
niveau modèle / lot / article
   +
acteurs disposant d'un accès
   +
données accessibles à chacun
   +
durée de disponibilité
```

S56

Le règlement prévoit également que lorsque d'autres dispositions du droit de l'Union exigent ou autorisent l'inclusion de données spécifiques dans le DPP, ces données peuvent y être intégrées conformément à l'acte délégué applicable.

AVÉRÉ :

> Le contenu concret et les droits d'accès au DPP ne sont pas entièrement figés dans le règlement-cadre : ils doivent être précisés pour les différents groupes de produits par des actes délégués S56.

Mais certaines limites du DPP demeurent inscrites dans le règlement lui-même

Cette capacité d'évolution n'efface pas les garanties supérieures.

Le règlement prévoit notamment que les données personnelles relatives aux clients ne doivent pas être stockées dans le DPP sans leur consentement explicite S56.

Une évolution par acte délégué ne signifie donc pas :

```
Commission
   ↓
liberté illimitée
   ↓
n'importe quelle donnée
dans le DPP
```

Les actes délégués doivent rester dans le cadre de l'habilitation et respecter le droit supérieur applicable.

GARANTIE JURIDIQUE :

> La capacité de préciser ou de faire évoluer le contenu d'une infrastructure par des actes ultérieurs ne supprime pas les limites prévues par le règlement qui l'encadre.

Le portefeuille européen d'identité numérique possède lui aussi une architecture évolutive

Le règlement eIDAS 2 fixe les garanties fondamentales du portefeuille S55.

Mais son fonctionnement concret repose également sur des actes d'exécution déterminant des standards, spécifications et procédures techniques.

Cela concerne notamment :

- les interfaces du portefeuille ;
- l'émission et la présentation des attributs ;
- l'identification des parties utilisatrices ;
- les procédures d'enregistrement ;
- certaines modalités de certification ;
- l'interopérabilité S55.

Le règlement permet en outre la combinaison de plusieurs attestations d'attributs sous le contrôle de l'utilisateur.

AVÉRÉ :

> Le cadre juridique fondamental du portefeuille est fixé par le règlement, tandis qu'une partie importante de son fonctionnement concret est précisée par des actes d'exécution et des spécifications techniques S55.

Une évolution technique peut donc modifier fortement les capacités pratiques sans supprimer les garanties juridiques

C'est une distinction supplémentaire.

```
règle juridique stable
   ↓
nouvelle spécification
   ↓
nouvelle capacité technique
```

n'est pas nécessairement :

```
nouvelle finalité juridique
```

Mais l'évolution des standards peut augmenter :

- l'interopérabilité ;
- le nombre d'attributs disponibles ;
- le nombre de services compatibles ;
- la facilité avec laquelle certaines preuves peuvent être présentées ;
- le nombre d'interactions possibles entre infrastructures.

VULNÉRABILITÉ JURIDIQUE :

> L'évolution des capacités pratiques d'une infrastructure peut précéder ou accompagner l'évolution de ses usages, ce qui rend nécessaire de réexaminer régulièrement si les garanties juridiques initiales restent adaptées aux capacités réellement déployées.

La frontière est encore plus évidente pour l'euro numérique

Contrairement à eIDAS 2 et au règlement ESPR, le règlement établissant l'euro numérique n'est pas encore définitivement adopté au moment de cette enquête S57.

Les garanties étudiées en 6.7 concernant notamment :

- l'interdiction de la monnaie programmable ;
- les paiements conditionnels ;
- la confidentialité ;
- l'intégration avec le portefeuille européen d'identité numérique ;

doivent donc être qualifiées selon leur statut dans le processus législatif.

GARANTIE JURIDIQUE :

> Tant que le texte n'est pas adopté, il ne faut pas présenter les dispositions de la proposition comme un cadre définitif et immuable.

À ÉTABLIR :

> Quelles garanties, définitions et possibilités techniques relatives aux paiements conditionnels et à l'interopérabilité avec le portefeuille européen d'identité numérique figureront dans le texte finalement adopté ?

Le point central apparaît maintenant : la protection juridique est dynamique

Les chapitres précédents pourraient donner l'impression d'une architecture statique :

```
système
   +
finalité
   +
garanties
   =
équilibre définitif
```

L'historique de CFVR montre une réalité différente.

L'équilibre ressemble davantage à :

```
infrastructure
   ↓
premier cadre juridique
   ↓
nouvelle capacité
   ↓
nouvelle source
   ↓
modification du cadre
   ↓
nouvelles garanties
   ↓
nouvelle capacité
   ↓
nouvelle modification
   ↓
etc.
```

S58

VULNÉRABILITÉ JURIDIQUE :

> La conformité d'une infrastructure à une date donnée ne garantit pas que son périmètre futur restera identique ; elle impose au contraire de réexaminer la conformité lorsque les finalités, données, sources, destinataires ou capacités évoluent.

Cela change la manière d'interpréter les garanties identifiées en 6.7

En 6.7, nous avons établi notamment :

```
DPP
→ pas de données personnelles client
  sans consentement explicite

WALLET
→ contrôle utilisateur
→ divulgation sélective
→ limitation des demandes
→ alternatives

EURO NUMÉRIQUE
→ monnaie programmable interdite
→ paiements conditionnels prévus
  dans le cadre proposé
```

Ces garanties sont réelles.

Mais elles doivent être lues comme :

> **garanties du cadre juridique applicable.**

Pas comme :

> **impossibilités techniques éternelles.**

La distinction est fondamentale.

Une évolution peut également intervenir sans fusionner physiquement les bases

C'est probablement le point le plus important pour l'architecture étudiée.

Une évolution juridique n'a pas nécessairement besoin de créer :

```
MEGA BASE CENTRALE
identité
   +
factures
   +
produits
   +
environnement
   +
paiements
```

Elle pourrait théoriquement autoriser :

```
système A
   ↓
résultat / attribut

système B
   ↓
résultat / attribut

   ↓
traitement C
```

Autrement dit, la question des libertés ne dépend pas uniquement de l'existence d'une base centralisée.

Elle dépend aussi :

- des données accessibles ;
- des identifiants permettant les rapprochements ;
- des attributs pouvant être présentés ;
- des résultats pouvant être transmis ;
- des conditions pouvant être vérifiées ;
- des conséquences attachées à ces résultats.

VULNÉRABILITÉ JURIDIQUE :

> Une évolution du cadre peut augmenter les possibilités de rapprochement sans nécessiter la fusion physique des infrastructures concernées.

C'est précisément pourquoi les interfaces identifiées dans le Chapitre 5 et en 6.7 sont importantes

Nous avons documenté séparément :

```
transaction
⇔ produit

produit
⇔ DPP

DPP
⇔ données environnementales

wallet
⇔ attributs vérifiés

wallet
⇔ services euro numérique
   dans le cadre proposé

condition externe
⇔ paiement conditionnel
```

La chaîne complète :

```
identité
   +
historique économique
   +
produit
   +
environnement
   ↓
condition
   ↓
autorisation / refus / limitation
d'un paiement
```

n'est **pas établie**.

Mais la question juridique pertinente n'est plus seulement :

> **« cette chaîne existe-t-elle aujourd'hui ? »**

Elle devient également :

> **« quelles modifications juridiques seraient nécessaires pour permettre chacune de ses jonctions, et quelles garanties s'y opposeraient ? »**

C'est une question beaucoup plus précise et vérifiable.

Une frontière juridique importante apparaît autour des droits et libertés

Le droit de l'Union et le droit constitutionnel ne permettent pas au législateur de supprimer librement toute protection simplement en adoptant un nouveau texte.

Une évolution demeure notamment confrontée :

```
droits fondamentaux
   ↓
vie privée
   +
protection des données
   +
nécessité
   +
proportionnalité
   +
garanties effectives
```

S39-S44-S53

Lorsqu'une restriction aux droits protégés par le RGPD entre dans le champ de l'article 23, elle doit notamment respecter l'essence des libertés et droits fondamentaux et constituer une mesure nécessaire et proportionnée dans une société démocratique S47.

GARANTIE JURIDIQUE :

> Le fait que le législateur puisse faire évoluer le droit ne signifie pas qu'il puisse juridiquement autoriser n'importe quelle surveillance, n'importe quel profilage ou n'importe quelle restriction.

La vraie vulnérabilité se situe donc entre deux affirmations fausses

Première affirmation excessive :

```
« c'est interdit aujourd'hui,
donc ce sera impossible demain »
```

Faux.

Deuxième affirmation excessive :

```
« le droit peut changer,
donc ils pourront tout faire »
```

Faux également.

La position juridiquement défendable est :

```
architecture techniquement capable
   +
usage non autorisé aujourd'hui
   ↓
évolution juridique possible
   ↓
mais soumise aux normes supérieures
   ↓
contrôle de nécessité
   +
proportionnalité
   +
droits fondamentaux
   +
garanties
   +
contrôle juridictionnel
```

L'historique de CFVR montre néanmoins pourquoi cette distinction n'est pas théorique

Entre 2014 et 2026, le même traitement a connu plusieurs modifications successives S58.

Au fil de ces évolutions apparaissent notamment :

```
plus de catégories de personnes
   +
plus de sources
   +
plus de données
   +
plus de possibilités d'analyse
   +
plus d'échanges
   +
nouvelle infrastructure de calcul
   +
facturation électronique
```

S37-S45-S58

Chaque évolution prise isolément peut disposer de sa justification et de ses garanties.

La question transversale devient cependant :

> **à quel moment faut-il réexaminer non seulement chaque extension séparément, mais également l'effet cumulé de toutes les extensions précédentes ?**

Cette question rejoint directement 6.5.

À ÉTABLIR :

> Existe-t-il une appréciation globale et périodique permettant de mesurer l'effet cumulé des modifications successives d'un traitement sur la vie privée et les libertés, au-delà de l'examen juridique de chaque modification prise séparément ?

Le risque documentaire est celui d'une normalisation progressive

Il faut ici rester particulièrement prudent.

Les sources ne démontrent aucune stratégie visant à introduire progressivement un système de contrôle généralisé.

Une telle intention ne peut pas être déduite de la seule succession des textes.

Mais une propriété objective peut être étudiée :

```
extension A
→ juridiquement autorisée

extension B
→ juridiquement autorisée

extension C
→ juridiquement autorisée

extension D
→ juridiquement autorisée
```

n'implique pas automatiquement que :

```
A + B + C + D
```

ait fait l'objet d'une appréciation publique globale distincte.

ANGLE MORT DOCUMENTAIRE :

> Les sources publiques étudiées ne permettent pas d'établir systématiquement comment l'effet cumulé de toutes les extensions successives d'une infrastructure est évalué lorsqu'une nouvelle modification est adoptée.

Cette formulation est beaucoup plus solide que d'affirmer l'existence d'une dérive.

Une garantie peut aussi changer de nature lorsque l'écosystème change

Une garantie efficace dans une infrastructure isolée peut devenir moins protectrice si l'environnement technique évolue.

Exemple abstrait :

```
identifiant produit
seul
   ↓
faible capacité
d'identification personnelle
```

puis :

```
identifiant produit
   +
transaction identifiable
   +
attribut d'identité
   ↓
capacité de rapprochement
beaucoup plus importante
```

La règle propre au DPP peut rester exactement la même.

Mais l'écosystème autour du DPP a changé.

Même raisonnement pour :

```
attribut wallet
   +
service de paiement
   +
condition externe
```

VULNÉRABILITÉ JURIDIQUE :

> L'efficacité réelle d'une garantie de cloisonnement doit être appréciée dans l'écosystème technique et juridique dans lequel l'infrastructure fonctionne, et pas seulement à partir du contenu de son propre texte fondateur.

La question ultime devient celle du changement de conséquence

Un système peut initialement servir uniquement à :

```
informer
```

puis éventuellement :

```
recommander
```

puis :

```
classer
```

puis :

```
orienter
```

puis, si le droit le permettait :

```
conditionner une décision
```

Ce dernier passage change profondément l'analyse juridique.

Les sections 6.4 et 6.5 ont montré que plus un résultat automatisé devient déterminant dans une décision produisant un effet juridique ou significatif, plus les garanties relatives aux décisions automatisées, à la nécessité et à la proportionnalité deviennent centrales S43-S51-S53.

GARANTIE JURIDIQUE :

> Le fait qu'une donnée puisse juridiquement être utilisée pour informer ou orienter ne signifie pas automatiquement qu'elle puisse être utilisée pour produire une restriction individuelle.

Appliqué à l'environnement, ce point devient déterminant

Le DPP et les infrastructures environnementales peuvent produire des informations concernant les caractéristiques d'un produit.

Une utilisation informative pourrait prendre la forme :

```
produit
   ↓
information environnementale
   ↓
information du consommateur
```

Une architecture beaucoup plus intrusive serait :

```
produit
   +
historique de consommation
   +
identité
   ↓
profil environnemental individuel
   ↓
conséquence sur
paiement / droit / service
```

Ces deux architectures ne sont juridiquement pas équivalentes.

NON ÉTABLI :

> Aucun élément étudié ne démontre actuellement l'existence ou la préparation d'un dispositif européen attribuant aux personnes un score environnemental individuel utilisé pour limiter leurs paiements, leurs achats ou leurs droits.

GARANTIE JURIDIQUE :

> Le passage d'une information environnementale relative au produit à une restriction individuelle fondée sur un profil personnel constituerait un changement substantiel de traitement et devrait être examiné au regard des bases juridiques et des garanties applicables.

L'absence actuelle de la chaîne complète reste donc une conclusion importante

À ce stade :

```
DPP
   ↓
information produit / environnement

wallet
   ↓
identité / attributs

paiement conditionnel
   ↓
condition externe possible
```

sont documentés séparément.

Mais :

```
DPP environnemental
   ↓
profil individuel
   ↓
condition imposée
   ↓
paiement refusé
```

reste :

> **NON ÉTABLI.**

Cette frontière ne doit pas être affaiblie.

Elle rend au contraire l'enquête plus solide.

Ce qu'il faut désormais surveiller n'est donc pas une intention, mais des modifications vérifiables

Les indicateurs pertinents seraient notamment :

```
nouvelle catégorie de données
   ↓
nouvel identifiant
   ↓
nouvelle catégorie d'accédants
   ↓
nouvelle interface
   ↓
nouvelle finalité
   ↓
nouvelle possibilité de croisement
   ↓
nouvelle conséquence individuelle
```

Une évolution de l'un de ces éléments peut être documentée objectivement.

Il n'est pas nécessaire de spéculer sur les intentions.

Questions ouvertes après 6.8

> **1. Quelles modifications successives ont précisément augmenté le périmètre de chaque infrastructure étudiée depuis sa création ?**

> **2. Lorsqu'une nouvelle source est ajoutée à un traitement existant, l'effet cumulé avec l'ensemble des sources déjà présentes fait-il l'objet d'une analyse distincte ?**

> **3. Comment les futures évolutions des actes délégués du DPP modifieront-elles les données disponibles, leur granularité et les catégories d'acteurs pouvant y accéder ?**

> **4. Quelles nouvelles catégories d'attestations seront progressivement utilisables dans le portefeuille européen d'identité numérique ?**

> **5. Quelles données seront réellement échangées entre le portefeuille européen d'identité numérique et les futurs services en euro numérique ?**

> **6. Quelles sources externes pourront être utilisées par les services proposant des paiements conditionnels ?**

> **7. Une nouvelle base juridique serait-elle nécessaire si une donnée environnementale relative à un produit devait être transformée en attribut relatif à une personne ?**

> **8. Quelle base juridique et quelles garanties seraient nécessaires si un tel attribut devait ensuite influencer l'accès à un paiement, un service ou un droit ?**

> **9. Existe-t-il un mécanisme permettant d'identifier le moment où plusieurs extensions juridiquement admissibles séparément produisent ensemble une architecture nécessitant une nouvelle appréciation globale de proportionnalité ?**

Conclusion de 6.8

AVÉRÉ :

> Le périmètre juridique d'une infrastructure publique de données peut évoluer dans le temps. CFVR en fournit un exemple documenté depuis 2014 S58.

AVÉRÉ :

> CFVR a connu plusieurs modifications successives concernant notamment les personnes concernées, les sources de données, les traitements associés et, en 2026, l'intégration des données issues de la facturation électronique S37-S45-S58.

AVÉRÉ :

> Le règlement ESPR prévoit que le contenu concret, la granularité et les droits d'accès au DPP soient précisés pour les différents groupes de produits par des actes délégués S56.

AVÉRÉ :

> Le fonctionnement concret du portefeuille européen d'identité numérique repose également sur des actes d'exécution et des spécifications techniques, dans les limites fixées par le règlement eIDAS 2 S55.

GARANTIE JURIDIQUE :

> Une modification du droit ne permet pas d'écarter librement les exigences supérieures relatives aux droits fondamentaux, à la protection des données, à la nécessité et à la proportionnalité.

LATITUDE JURIDIQUE :

> Une finalité, une source de données, un destinataire ou une interconnexion qui ne sont pas juridiquement autorisés aujourd'hui peuvent, selon les circonstances, faire ultérieurement l'objet d'un nouveau fondement juridique, sous réserve du respect des normes supérieures applicables.

VULNÉRABILITÉ JURIDIQUE :

> Une garantie reposant sur le périmètre actuel d'un traitement constitue une protection présente, mais non une garantie d'immuabilité de ce périmètre.

VULNÉRABILITÉ JURIDIQUE :

> Une évolution peut augmenter les possibilités de rapprochement entre infrastructures sans nécessiter leur fusion physique dans une base de données unique.

ANGLE MORT DOCUMENTAIRE :

> Les sources publiques étudiées ne permettent pas d'établir systématiquement comment l'effet cumulé de toutes les extensions successives d'une infrastructure est réévalué lorsqu'une nouvelle extension est adoptée.

À ÉTABLIR :

> Jusqu'où plusieurs extensions successives, chacune juridiquement encadrée séparément, peuvent-elles modifier l'équilibre global d'une infrastructure avant qu'une nouvelle appréciation d'ensemble de nécessité et de proportionnalité devienne indispensable ?

NON ÉTABLI :

> Aucun élément étudié ne démontre qu'une évolution juridique soit actuellement engagée afin de créer un profil environnemental individuel relié à l'identité numérique et utilisé pour autoriser, refuser ou limiter un paiement, un achat, un service ou un droit.

NON ÉTABLI :

> La possibilité juridique de modifier ultérieurement les finalités ou les interfaces d'une infrastructure ne constitue pas la preuve qu'une telle modification est envisagée.

6.9 Vulnérabilités juridiques et limites de l'analyse

Statut : VULNÉRABILITÉS IDENTIFIÉES / GARANTIES SUPÉRIEURES / LIMITES FACTUELLES DE L'ENQUÊTE

L'enquête permet désormais de répondre à une question plus importante que celle de savoir si chaque infrastructure étudiée est, prise isolément, juridiquement encadrée.

La question finale est :

> **que se passe-t-il lorsque plusieurs infrastructures juridiquement distinctes augmentent simultanément leurs capacités de collecte, d'identification, de rapprochement, d'analyse et d'action ?**

Les sections précédentes ont établi que le droit contient de nombreuses protections.

Elles ont également montré que ces protections ne constituent pas toutes des impossibilités techniques et que le périmètre juridique des infrastructures peut évoluer.

La vulnérabilité principale identifiée par cette enquête se situe précisément dans cet écart.

```
CAPACITÉ TECHNIQUE
   ↓
plus large que
   ↓
USAGE JURIDIQUEMENT AUTORISÉ
AUJOURD'HUI
```

Cette différence protège actuellement contre certains usages.

Mais elle signifie également que l'évolution du droit devient une variable essentielle de l'architecture.

Première vulnérabilité : la centralisation fonctionnelle peut exister sans base centrale unique

L'enquête n'a pas identifié une base européenne unique réunissant :

```
identité
   +
factures
   +
transactions
   +
produits
   +
données environnementales
   +
paiements
```

Une telle affirmation serait incorrecte.

Les chapitres précédents ont en revanche documenté plusieurs infrastructures spécialisées disposant d'identifiants, d'interfaces, de registres, de mécanismes de vérification ou de capacités de rapprochement.

La facturation électronique française fournit un exemple particulièrement concret.

Les données issues des factures électroniques constituent désormais une source de CFVR et doivent alimenter la plateforme sécurisée des données de la DGFiP afin d'être exploitées à grande échelle S37-S45.

CFVR rapproche déjà de nombreuses autres sources fiscales, économiques, administratives et sociales.

AVÉRÉ :

> Une centralisation physique dans une base unique n'est pas nécessaire pour permettre des rapprochements entre informations provenant de systèmes distincts.

VULNÉRABILITÉ JURIDIQUE :

> L'encadrement séparé de plusieurs infrastructures ne suffit pas nécessairement à apprécier les conséquences résultant de leur combinaison lorsqu'elles deviennent interopérables ou lorsque les résultats produits par l'une peuvent être utilisés par une autre.

La question déterminante n'est donc pas seulement :

> **« où sont stockées les données ? »**

mais également :

> **« quelles informations peuvent être reliées, vérifiées, transmises ou utilisées pour produire une conséquence ? »**

Deuxième vulnérabilité : une finalité légalement limitée aujourd'hui peut évoluer demain

La section 6.8 a établi que CFVR fournit déjà un exemple historique de modifications successives d'un même traitement S58.

Une infrastructure peut conserver son existence institutionnelle tout en voyant évoluer :

- ses sources ;
- ses catégories de données ;
- les personnes concernées ;
- ses destinataires ;
- ses capacités techniques ;
- ses modalités d'exploitation.

GARANTIE JURIDIQUE :

> Une administration ne peut pas modifier librement une finalité ou réutiliser librement des données en dehors du cadre juridique applicable.

VULNÉRABILITÉ JURIDIQUE :

> L'absence actuelle d'un usage ne constitue pas nécessairement une interdiction juridique définitive : un nouveau texte peut modifier le périmètre autorisé, sous réserve du respect du droit supérieur.

Cette distinction interdit deux conclusions opposées.

```
« ce n'est pas autorisé aujourd'hui
donc ce sera toujours impossible »
```

n'est pas démontré.

Mais :

```
« le droit peut évoluer
donc cet usage sera autorisé demain »
```

ne l'est pas davantage.

Troisième vulnérabilité : l'accumulation peut devenir plus importante que chaque extension prise isolément

L'analyse de CFVR révèle une difficulté transversale.

Une succession peut prendre la forme :

```
extension A
   +
extension B
   +
nouvelle source C
   +
nouvel échange D
   +
nouvelle capacité E
```

Chacune peut être examinée juridiquement lors de son introduction.

Mais l'enjeu final devient :

```
A + B + C + D + E
   ↓
CAPACITÉ GLOBALE
```

ANGLE MORT DOCUMENTAIRE :

> Les sources publiques étudiées ne permettent pas d'établir systématiquement comment l'effet cumulé de toutes les extensions successives d'une infrastructure est réévalué indépendamment de l'examen de chaque nouvelle modification.

Cette question devient particulièrement importante lorsque progressent simultanément :

```
volume
   +
nombre de sources
   +
précision
   +
interopérabilité
   +
capacité algorithmique
   +
nombre de destinataires
```

Quatrième vulnérabilité : l'interopérabilité peut produire une capacité nouvelle sans fusion des systèmes

Les infrastructures étudiées sont de plus en plus conçues autour :

- d'identifiants ;
- d'interfaces ;
- de registres ;

- d'attestations vérifiables ;
- de mécanismes de présentation d'attributs ;
- de services capables de vérifier des conditions ;
- de standards communs.

Cela permet une architecture dans laquelle une infrastructure n'a pas nécessairement besoin de recevoir toutes les données brutes d'une autre.

```
SYSTÈME A
   ↓
attribut / preuve / résultat

SYSTÈME B
   ↓
vérification

SYSTÈME C
   ↓
conséquence
```

VULNÉRABILITÉ JURIDIQUE :

> Une infrastructure distribuée peut produire des conséquences comparables à celles d'un système centralisé sans nécessiter la constitution d'une base contenant physiquement l'intégralité des données concernées.

Cette propriété rend l'analyse des seules bases de données insuffisante.

Il faut également examiner les interfaces.

Cinquième vulnérabilité : le passage de l'information à la conséquence

Cette frontière constitue probablement la plus importante de l'ensemble du chapitre.

Une donnée peut être utilisée pour :

```
INFORMER
```

puis :

```
VÉRIFIER
```

puis :

```
CLASSER
```

puis :

```
ORIENTER
```

et éventuellement :

```
CONDITIONNER
```

Ces fonctions ne produisent pas les mêmes conséquences juridiques.

CFVR fournit déjà un exemple de cette distinction.

Les résultats algorithmiques peuvent orienter les agents, mais la CNIL exige qu'ils ne remplacent pas leur analyse et que la décision humaine demeure effective S37-S51.

GARANTIE JURIDIQUE :

> L'autorisation d'utiliser une donnée pour informer, détecter ou vérifier ne constitue pas automatiquement une autorisation de l'utiliser pour produire une restriction individuelle.

VULNÉRABILITÉ JURIDIQUE :

> Plus une donnée ou un résultat algorithmique devient déterminant pour l'accès à un paiement, un service, un droit ou une autre possibilité importante, plus les exigences relatives à la base juridique, à la proportionnalité, à l'exactitude, à la transparence, à la contestation et aux décisions automatisées deviennent déterminantes.

Sixième vulnérabilité : une erreur peut changer de nature lorsqu'elle traverse plusieurs infrastructures

Les sections précédentes ont identifié les droits d'accès et de rectification.

Mais une architecture interconnectée pose une difficulté supplémentaire.

```
donnée A erronée
   ↓
traitement B
   ↓
classification C
   ↓
attribut D
   ↓
décision E
```

Corriger A ne garantit pas techniquement, à lui seul, que :

```
B
C
D
E
```

aient tous été recalculés, corrigés ou neutralisés.

Le droit prévoit différentes obligations de rectification, de limitation et de communication aux destinataires lorsque les conditions correspondantes sont réunies S43.

VULNÉRABILITÉ JURIDIQUE :

> Dans une architecture distribuée, l'effectivité du droit de rectification dépend non seulement de la correction de la donnée source, mais également de la capacité à identifier et corriger les conséquences dérivées encore associées à cette donnée.

ANGLE MORT DOCUMENTAIRE :

> Les sources publiques étudiées ne permettent pas d'établir l'existence d'un mécanisme transversal permettant à une personne de connaître puis de faire corriger automatiquement toutes les données dérivées ou conséquences propagées à travers plusieurs infrastructures juridiquement distinctes.

Septième vulnérabilité : la protection dépend parfois du maintien d'une séparation fonctionnelle

Plusieurs garanties identifiées reposent sur des frontières.

Pour CFVR :

```
algorithme
   ↓
signalement
   ↓
analyse humaine
   ↓
décision
```

Pour le DPP :

```
information produit
   ≠
profil personnel du consommateur
```

Pour l'euro numérique dans le cadre proposé :

```
paiement conditionnel
   ≠
monnaie programmable
```

Pour le portefeuille européen :

```
présentation d'un attribut nécessaire
   ≠
divulgation systématique
de l'ensemble de l'identité
```

Ces séparations constituent de véritables garanties.

Mais leur efficacité dépend de leur maintien.

VULNÉRABILITÉ JURIDIQUE :

> Lorsqu'une protection repose sur une séparation entre deux fonctions techniquement rapprochables, toute évolution réduisant cette séparation doit faire l'objet d'une nouvelle analyse juridique.

Huitième vulnérabilité : l'euro numérique pourrait être créé sans consentement individuel de chaque citoyen

Il faut ici distinguer création d'une monnaie et obligation individuelle de l'utiliser.

Le cadre européen proposé prévoit une procédure législative permettant d'établir l'euro numérique.

Une fois ce cadre adopté, la décision d'émettre ou non l'euro numérique appartiendrait à la BCE S57.

Il ne s'agit donc pas d'un mécanisme reposant sur le consentement individuel de chaque citoyen à la création de cette nouvelle forme de monnaie.

AVÉRÉ :

> La création éventuelle de l'euro numérique relève du processus institutionnel et législatif européen puis, dans le cadre envisagé, d'une décision d'émission de la BCE ; elle n'est pas conditionnée à l'accord individuel de chaque utilisateur.

Mais cette constatation ne signifie pas :

```
euro numérique créé
   =
obligation pour chaque citoyen
d'abandonner les espèces
```

Le cadre actuellement négocié prévoit au contraire la coexistence de l'euro numérique avec les espèces et des mesures destinées à préserver l'accès et l'acceptation du cash S57.

NON ÉTABLI :

> Aucun élément étudié ne permet d'affirmer que le cadre actuel prévoit la suppression des espèces ou l'obligation générale pour chaque citoyen d'utiliser exclusivement l'euro numérique.

Neuvième vulnérabilité : le contrôle d'une monnaie numérique et le contrôle de l'usage de chaque unité ne sont pas juridiquement équivalents

Une infrastructure de monnaie numérique de banque centrale implique nécessairement des règles concernant notamment :

- son émission ;
- sa distribution ;
- son fonctionnement ;
- ses intermédiaires ;
- ses limites éventuelles de détention ;
- ses mécanismes de paiement.

Le cadre actuellement proposé envisage effectivement des limites de détention S57.

Mais une autre frontière existe.

La BCE considère que limiter intrinsèquement :

```
où
 +
quand
 +
à qui
```

une unité d'euro numérique peut être dépensée reviendrait à créer une monnaie programmable incompatible avec son caractère de monnaie pleinement fongible et avec son cours légal S57.

GARANTIE JURIDIQUE :

> Le cadre proposé exclut la transformation de l'euro numérique en monnaie programmable dont les unités imposeraient intrinsèquement des restrictions concernant les biens, services, lieux, moments ou bénéficiaires auxquels elles pourraient être utilisées.

Cette garantie est importante.

Elle ne doit pas être confondue avec les paiements conditionnels.

Dixième vulnérabilité : les paiements conditionnels créent néanmoins une interface avec des conditions externes

Les chapitres précédents ont documenté la possibilité technique et expérimentale d'utiliser une condition vérifiée extérieurement afin de déclencher un paiement.

Le cadre proposé pour l'euro numérique distingue précisément :

```
MONNAIE PROGRAMMABLE
   ↓
restriction intrinsèque
de la monnaie
   ≠
PAIEMENT CONDITIONNEL
   ↓
paiement déclenché
selon une condition convenue
```

S22-S27-S28-S57

AVÉRÉ :

> Le cadre proposé interdit la monnaie programmable tout en permettant le développement de services de paiement conditionnel.

Cette distinction constitue simultanément :

```
une GARANTIE
   +
une INTERFACE À SURVEILLER
```

La garantie est que la monnaie elle-même ne peut pas être limitée à certains usages.

L'interface à surveiller concerne la nature des conditions utilisées par les services de paiement.

C'est ici que la question environnementale doit être formulée avec une précision maximale

Les chapitres précédents ont établi :

```
produit
   ↓
DPP
   ↓
données environnementales
```

et séparément :

```
condition externe
   ↓
vérification
   ↓
paiement conditionnel
```

Mais ils n'ont pas établi :

```
identité
   ↓
historique d'achats
   ↓
score environnemental personnel
   ↓
quota
   ↓
autorisation / refus de paiement
```

NON ÉTABLI :

> Aucun élément étudié ne démontre actuellement l'existence, le déploiement ou l'adoption juridique d'un « pass environnemental » individuel utilisant les données du DPP pour déterminer si une personne peut ou non effectuer un paiement.

Cette conclusion doit rester explicite.

Mais elle n'épuise pas la question juridique.

La vraie question devient : quelles protections s'activeraient si cette frontière était franchie ?

Une architecture hypothétique :

```
IDENTITÉ
   +
TRANSACTIONS
   +
PRODUITS
   +
DONNÉES ENVIRONNEMENTALES
   ↓
PROFIL INDIVIDUEL
   ↓
CONDITION
   ↓
PAIEMENT / SERVICE / DROIT
```

ne pourrait pas être analysée comme une simple extension technique.

Elle devrait notamment être examinée au regard :

- de sa base juridique ;
- de sa finalité ;
- de la nécessité ;
- de la proportionnalité ;
- de la minimisation ;
- des droits d'accès et de rectification ;
- des règles relatives au profilage ;
- des décisions automatisées lorsque leurs conditions sont réunies ;
- des droits fondamentaux affectés ;
- des voies de recours.

S43-S44-S47-S51-S53

GARANTIE JURIDIQUE :

> Une infrastructure techniquement capable de produire une restriction n'est pas juridiquement autorisée à la produire du seul fait que cette capacité existe.

Et même une nouvelle loi ne constitue pas un pouvoir sans limite

C'est probablement la frontière juridique la plus importante de ce chapitre.

Une nouvelle loi ou un nouveau règlement peut faire évoluer les usages autorisés.

Mais :

```
NOUVELLE LOI
   ≠
POUVOIR JURIDIQUE ILLIMITÉ
```

Lorsqu'une mesure limite des droits fondamentaux protégés par le droit de l'Union, cette limitation doit notamment :

```
être prévue par la loi
   +
respecter le contenu essentiel du droit
   +
être nécessaire
   +
être proportionnée
   +
répondre effectivement
à un objectif d'intérêt général
ou protéger les droits d'autrui
```

S39-S44

GARANTIE JURIDIQUE :

> L'évolution du droit peut déplacer certaines frontières, mais elle reste elle-même soumise aux normes juridiques supérieures et au contrôle juridictionnel.

Cette garantie constitue la limite à l'idée selon laquelle :

> **« il suffirait de changer la loi pour pouvoir tout faire ».**

La réforme de la facturation électronique constitue néanmoins un changement d'échelle majeur

Il faut ici revenir au point de départ de l'enquête.

Une facture électronique structurée n'est pas seulement un PDF envoyé autrement.

Elle transforme des informations économiques auparavant dispersées en données :

```
structurées
   +
standardisées
   +
exploitables automatiquement
   +
transmissibles
   +
rapprochables
   +
analysables à grande échelle
```

Les chapitres 1 et 2 ont établi la nature et le cycle de ces données.

Le Chapitre 5 a étudié les possibilités d'interconnexion.

Le présent chapitre a montré que certaines données de facturation électronique sont désormais intégrées à CFVR et exploitées dans une infrastructure algorithmique capable de traiter une volumétrie de plusieurs milliards de factures annuelles S37-S45.

AVÉRÉ :

> La réforme augmente fortement la quantité de données économiques structurées susceptibles d'être traitées automatiquement par l'administration fiscale.

Mais « centraliser tout » serait une conclusion excessive

Le dossier ne démontre pas :

```
FACTURATION ÉLECTRONIQUE
   ↓
BASE UNIQUE
   ↓
toute l'identité
   +
tous les produits
   +
tout l'environnement
   +
tous les paiements
```

NON ÉTABLI :

> La réforme française de la facturation électronique ne constitue pas, sur la base des sources étudiées, une base centrale réunissant l'ensemble des infrastructures analysées dans cette enquête.

La conclusion exacte est différente :

> **elle crée une nouvelle couche massive de données économiques structurées qui peut devenir une source pour d'autres traitements lorsque le droit l'autorise.**

CFVR en fournit désormais un exemple concret.

C'est précisément ce qui fait de la facturation électronique une infrastructure structurante

Le point critique n'est donc pas :

> **« la facture électronique contrôle déjà tout ».**

Le point documenté est :

```
ACTIVITÉ ÉCONOMIQUE
   ↓
DONNÉES STRUCTURÉES
   ↓
TRANSMISSION
   ↓
TRAITEMENT À GRANDE ÉCHELLE
   ↓
CROISEMENT
   ↓
ANALYSE ALGORITHMIQUE
```

Cette chaîne existe désormais dans le domaine fiscal étudié S37-S45.

VULNÉRABILITÉ JURIDIQUE :

> Plus une infrastructure transforme une activité économique diffuse en données structurées, standardisées et interopérables, plus l'évolution de ses finalités, de ses destinataires et de ses possibilités de rapprochement devient déterminante pour les libertés.

La vulnérabilité fondamentale n'est donc pas une fonction cachée

Au terme de l'enquête, aucune source n'a révélé :

```
bouton secret
« contrôle total »
```

La vulnérabilité identifiée est plus structurelle.

```
NUMÉRISATION
   ↓
STRUCTURATION
   ↓
IDENTIFICATION
   ↓
INTEROPÉRABILITÉ
   ↓
CROISEMENT
   ↓
ANALYSE
   ↓
CONDITION / DÉCISION POSSIBLE
```

À chaque étape existent des garanties.

Mais chaque étape augmente également la capacité potentielle de l'étape suivante.

La protection des libertés dépend donc moins de l'existence des capacités que des frontières imposées à leur usage

Cette enquête montre finalement que deux réalités peuvent être vraies simultanément.

Première réalité :

> **les infrastructures étudiées ne constituent pas aujourd'hui un système juridiquement autorisé de contrôle général des achats, de l'identité, de l'environnement et de la monnaie.**

Deuxième réalité :

> **elles augmentent objectivement les capacités techniques d'identification, de structuration, de rapprochement, de vérification et d'automatisation disponibles dans l'écosystème numérique européen.**

Il n'y a aucune contradiction entre ces deux constats.

C'est précisément l'espace situé entre eux que le droit doit protéger.

Les lignes rouges deviennent alors identifiables

L'enquête permet désormais de définir des changements qui nécessiteraient une réévaluation particulièrement rigoureuse :

> **1. utilisation d'un identifiant commun permettant de relier systématiquement identité, achats, produits et paiements ;**

> **2. transformation des informations environnementales relatives aux produits en profil environnemental individuel ;**

> **3. utilisation de ce profil pour produire une conséquence sur un paiement, un service ou un droit ;**

> **4. transformation d'une aide algorithmique en mécanisme déterminant pratiquement la décision humaine ;**

> **5. disparition ou réduction substantielle de la possibilité d'utiliser un moyen de paiement non associé au même niveau de traçabilité ;**

> **6. extension des finalités permettant l'utilisation croisée de données initialement collectées dans des infrastructures distinctes ;**

> **7. impossibilité pratique pour une personne de connaître, corriger ou contester les données et résultats dérivés utilisés à son égard ;**

> **8. multiplication d'extensions séparément justifiées sans évaluation publique suffisante de leur effet cumulé.**

Aucun de ces points ne doit être présenté comme réalisé lorsqu'il ne l'est pas.

Ils constituent des critères de surveillance vérifiables.

Ce que l'enquête ne permet pas d'affirmer

NON ÉTABLI :

> Il n'est pas établi que l'Union européenne ou la France mettent actuellement en place un système destiné à attribuer un score environnemental individuel aux citoyens.

NON ÉTABLI :

> Il n'est pas établi que les données du DPP seront utilisées pour déterminer l'autorisation ou le refus des achats d'une personne.

NON ÉTABLI :

> Il n'est pas établi que l'euro numérique permettra à la BCE d'autoriser ou d'interdire les achats d'une personne en fonction des produits qu'elle souhaite acheter.

NON ÉTABLI :

> Il n'est pas établi que la facturation électronique, le DPP, le portefeuille européen d'identité numérique et l'euro numérique seront réunis dans une infrastructure unique de contrôle.

NON ÉTABLI :

> Il n'est pas établi que les espèces seront supprimées lors de l'introduction éventuelle de l'euro numérique.

Ces limites ne diminuent pas l'enquête.

Elles en définissent la solidité.

Ce qu'elle permet en revanche d'établir

AVÉRÉ :

> La facturation électronique transforme une partie importante de l'activité économique en données structurées pouvant être exploitées automatiquement.

AVÉRÉ :

> Certaines de ces données sont désormais destinées à alimenter CFVR et la plateforme sécurisée des données de la DGFiP S37-S45.

AVÉRÉ :

> CFVR combine déjà de nombreuses sources et utilise des méthodes algorithmiques pour détecter des anomalies et orienter le contrôle fiscal S37.

AVÉRÉ :

> Le DPP permet d'associer à des produits des informations structurées pouvant notamment inclure des informations environnementales S56.

AVÉRÉ :

> Le portefeuille européen d'identité numérique permet la présentation et la vérification d'attributs électroniques selon le cadre étudié S55.

AVÉRÉ :

> Le cadre proposé pour l'euro numérique distingue et interdit la monnaie programmable tout en permettant des services de paiement conditionnel S57.

AVÉRÉ :

> Les finalités, sources et périmètres de certaines infrastructures publiques peuvent évoluer juridiquement dans le temps, comme l'historique de CFVR le démontre S58.

GARANTIE JURIDIQUE :

> Ces capacités techniques ne peuvent pas être librement combinées pour produire n'importe quelle conséquence individuelle : leur utilisation demeure soumise aux bases juridiques, aux finalités autorisées, aux droits fondamentaux et aux exigences de nécessité et de proportionnalité.

Conclusion de 6.9

Le résultat de l'enquête n'est donc ni :

```
« tout est déjà connecté »
```

ni :

```
« les garanties actuelles rendent
toute évolution impossible »
```

Le résultat est plus précis.

```
INFRASTRUCTURES DISTINCTES
   ↓
CAPACITÉS CROISSANTES
   ↓
INTEROPÉRABILITÉ CROISSANTE
   ↓
POSSIBILITÉS DE RAPPROCHEMENT
   ↓
USAGES LIMITÉS PAR
LE DROIT ACTUEL
   ↓
MAIS CADRE JURIDIQUE
SUSCEPTIBLE D'ÉVOLUER
   ↓
SOUS CONTRÔLE DES
DROITS FONDAMENTAUX
```

VULNÉRABILITÉ JURIDIQUE :

> Le principal risque identifié n'est pas l'existence démontrée d'un système unique de contrôle, mais la possibilité que des extensions successives de finalités, d'accès, d'interfaces ou de conséquences rapprochent progressivement des infrastructures initialement séparées.

ANGLE MORT DOCUMENTAIRE :

> Les sources publiques permettent généralement d'étudier chaque infrastructure et chaque modification juridique séparément, mais beaucoup moins facilement d'évaluer l'effet cumulé de l'ensemble de l'écosystème sur les capacités d'identification, de rapprochement et de décision.

GARANTIE JURIDIQUE :

> Même lorsqu'une évolution est décidée par le législateur, les limitations apportées aux droits fondamentaux demeurent soumises aux exigences de légalité, de respect du contenu essentiel des droits, de nécessité et de proportionnalité.

NON ÉTABLI :

> L'enquête ne démontre actuellement ni l'existence d'un « pass environnemental » individuel, ni l'utilisation d'un profil environnemental pour contrôler les paiements, ni une architecture unique reliant automatiquement facturation électronique, identité numérique, DPP et euro numérique afin de restreindre les droits ou achats des citoyens.

CONCLUSION :

> **La question déterminante n'est donc pas de savoir si l'infrastructure permet déjà un contrôle généralisé. Elle est de savoir si les frontières juridiques qui séparent aujourd'hui collecte, information, identification, rapprochement, profilage et décision continueront à évoluer au même rythme que les capacités techniques qui permettent de les franchir.**

Et c'est précisément pour cette raison que l'analyse doit rester évolutive :

> **chaque nouvelle source de données, chaque nouvel identifiant, chaque nouvelle interface, chaque nouvelle finalité et chaque nouvelle conséquence attachée à ces infrastructures doit être examinée non seulement isolément, mais également pour ce qu'elle permet lorsqu'elle est combinée avec ce qui existe déjà.**

Chapitre 7 — Synthèse générale

> **Navigation :** ← Retour au sommaire

Ce chapitre rassemble les principaux éléments établis au cours de l'enquête et met en perspective les résultats des différents chapitres.

L'objectif est de distinguer clairement :

- ce qui est **AVÉRÉ** par les sources étudiées ;
- ce qui a été **EXPÉRIMENTÉ** dans des projets ou pilotes documentés ;
- ce qui est **DÉDUCTIBLE TECHNIQUEMENT** à partir des architectures et raccords identifiés ;
- ce qui demeure **NON ÉTABLI** ou **À ÉTABLIR**.

La synthèse ne cherche pas à transformer une possibilité technique en fait établi. Elle vise au contraire à déterminer jusqu'où les sources permettent de remonter la chaîne étudiée et à identifier précisément les points où la démonstration s'arrête.

Sommaire

- Chapitre 1 — Données de facturation transmises à l'administration
- Chapitre 2 — Conservation, accès et finalités des données
- Chapitre 3 — Données environnementales
- Chapitre 4 — Euro numérique et infrastructures de paiement
- Chapitre 5 — Interconnexions
- Chapitre 6 — Garanties juridiques
- Conclusion générale

Chapitre 1 — Données de facturation transmises à l'administration

Statut : AVÉRÉ

La réforme française de la facturation électronique met en place une infrastructure permettant la transmission automatisée à l'administration fiscale de données économiques structurées.

Ces données comprennent notamment l'identification des entreprises participant à une transaction, les dates et numéros de facture, les montants hors taxe, les taux et montants de TVA ainsi que certaines informations relatives aux livraisons et aux paiements.

À compter du 1er septembre 2027, pour les opérations B2B concernées, les données transmises comprennent également des informations au niveau des lignes de facture :

- la dénomination précise du bien ou du service ;
- la quantité ;
- le prix unitaire hors taxe.

Le dispositif permet donc, dans ces situations, de transmettre à l'administration des données structurées décrivant précisément le contenu économique d'une transaction B2B.

Pour les opérations B2C relevant du e-reporting, les données actuellement prévues sont en revanche agrégées par jour. Les éléments documentés ne permettent donc pas d'affirmer que le détail de chaque achat réalisé par un particulier est individuellement transmis à l'administration.

Chapitre 2 — Conservation, accès et finalités des données

Statut : AVÉRÉ / À ÉTABLIR

Les textes étudiés établissent que la réforme ne se limite pas à la transmission technique des factures. Les données structurées issues des factures, des transactions et, dans les situations prévues, des paiements sont transmises à l'administration dans un cadre organisé faisant intervenir les plateformes agréées.

Les entreprises restent soumises à des obligations propres de conservation des documents fiscaux. Ces obligations ne permettent toutefois pas de déduire que l'administration conserve les données reçues pendant une durée identique.

La lutte contre la fraude à la TVA, le pré-remplissage des déclarations de TVA, la connaissance en temps réel de l'activité des entreprises et le pilotage des politiques publiques figurent parmi les objectifs officiellement annoncés de la réforme.

La documentation de la DGFiP indique également que la disponibilité et l'exploitation de données obtenues de façon automatique et continue doivent faciliter la connaissance de la conjoncture économique, notamment par secteur d'activité, ainsi que le pilotage de l'économie par la puissance publique.

Les travaux préparatoires de la réforme mentionnent en outre la possibilité d'enrichir des modèles d'analyse avec les données recueillies afin de faciliter notamment la détection et l'accompagnement des entreprises en difficulté.

Il est donc établi que les données recueillies ne répondent pas uniquement à une fonction de transmission des factures ou de détermination de la TVA : leur exploitation doit également contribuer à l'observation de l'activité économique et au pilotage des politiques publiques.

Plusieurs éléments restent cependant à établir, notamment la durée précise de conservation des différentes catégories de données par l'administration, les règles d'accès et d'habilitation, les traitements automatisés effectivement appliqués, les éventuels croisements avec d'autres bases de données et les conditions juridiques permettant leur réutilisation pour d'autres politiques publiques.

Les sources étudiées ne permettent pas d'établir l'existence d'une interconnexion avec des données environnementales, une infrastructure monétaire numérique ou des mécanismes permettant de conditionner certaines transactions. Ces possibilités doivent être étudiées séparément dans les chapitres suivants.

Chapitre 3 — Données environnementales

Statut : AVÉRÉ / DÉDUCTIBLE TECHNIQUEMENT / À ÉTABLIR

L'Union européenne a établi un cadre juridique et technique pour le passeport numérique de produit, ou Digital Product Passport (DPP), permettant d'associer des données numériques structurées, lisibles par machine et interopérables à des produits identifiables.

Selon les exigences applicables aux différentes catégories de produits, le passeport peut être défini au niveau du modèle, du lot ou de l'article individuel.

Les informations susceptibles d'être associées à certains produits comprennent notamment des données relatives à leur composition, leur durabilité, leur réparabilité, leur recyclabilité ainsi qu'à leur empreinte carbone ou environnementale.

L'Union européenne dispose également de méthodes permettant de quantifier certains impacts environnementaux des produits sur leur cycle de vie. Le règlement relatif aux batteries fournit déjà un exemple concret dans lequel une empreinte carbone quantitative est réglementairement associée à certaines catégories de produits.

Le DPP repose sur des identifiants structurés et peut notamment comporter un GTIN ou un identifiant équivalent. Les standards utilisés dans les échanges commerciaux électroniques permettent également de transporter des identifiants standardisés au niveau des articles.

Il est donc techniquement possible, lorsqu'un identifiant commun ou un mécanisme de correspondance existe et que les droits d'accès nécessaires sont réunis, de rapprocher une transaction commerciale des informations environnementales associées au produit correspondant.

La donnée environnementale n'a pas besoin d'être directement inscrite dans la facture pour qu'un tel rapprochement soit techniquement réalisable : l'identifiant du produit peut permettre de retrouver cette information dans un système distinct.

De même, l'identité de l'acheteur n'a pas besoin d'être stockée dans le DPP pour qu'un rapprochement soit techniquement possible si un autre système dispose séparément des informations permettant d'identifier la partie à la transaction et le produit concerné.

Lorsque plusieurs transactions comportent des produits identifiables auxquels sont associées des valeurs environnementales quantitatives, ces valeurs peuvent également, sur le plan technique, être rapprochées et agrégées par un système disposant des données et droits d'accès nécessaires.

L'architecture réglementaire du DPP prévoit par ailleurs des mécanismes d'interopérabilité, des échanges automatisés, une API, un registre européen et une interconnexion avec les systèmes douaniers. Des projets européens associent également traçabilité numérique, preuves de transactions commerciales et acteurs administratifs chargés notamment de la TVA et des douanes.

Ces éléments ne permettent cependant pas d'établir qu'une empreinte environnementale individuelle des achats est actuellement calculée par l'administration, que les données environnementales des produits sont automatiquement rapprochées des données françaises de facturation ou de e-reporting, ni qu'elles sont utilisées pour autoriser, refuser ou conditionner un paiement.

Chapitre 4 — Euro numérique et infrastructures de paiement

Statut : AVÉRÉ / DÉDUCTIBLE TECHNIQUEMENT / À ÉTABLIR

Le projet d'euro numérique repose sur une infrastructure centralisée de règlement exploitée par l'Eurosystème et distribuée aux utilisateurs par l'intermédiaire de prestataires de services de paiement.

Cette infrastructure ne repose pas sur une blockchain comme fondement du système. Les utilisateurs conserveraient principalement une relation avec leur banque ou leur prestataire de services de paiement, tandis que l'Eurosystème assurerait les fonctions centrales nécessaires au règlement et au fonctionnement de l'infrastructure.

Pour les paiements en ligne, le modèle technique publié prévoit le traitement de données structurées relatives aux utilisateurs, comptes, appareils, prestataires, payeurs, bénéficiaires et transactions.

Les transactions disposent notamment d'identifiants, d'un montant, d'une date et d'une heure, d'un type, d'un environnement et d'un statut. Le modèle comprend également différentes informations permettant l'identification ou la catégorisation des acteurs intervenant dans une transaction.

Certaines informations relatives au commerçant peuvent également intervenir dans le processus. Le Merchant Category Code, ou MCC, permet notamment de catégoriser le type d'activité commerciale du bénéficiaire et fait partie des informations transmises dans certaines étapes du processus de paiement documenté.

L'architecture distingue cependant les données présentes dans le modèle, les données effectivement transmises lors d'une transaction et les données auxquelles chaque acteur peut réellement accéder. L'existence d'une donnée dans le modèle technique ne signifie donc pas que tous les participants au système peuvent la consulter.

Le projet prévoit également un fonctionnement hors ligne permettant d'effectuer certains paiements directement entre appareils sans connexion à Internet. Dans ce mode, les détails personnels de la transaction ne sont pas transmis aux prestataires de services de paiement ni à l'Eurosystème pendant ou après le paiement. Cette architecture constitue une limitation importante aux possibilités de centralisation systématique des informations relatives aux transactions.

La proposition relative à l'euro numérique exclut explicitement la création d'une monnaie programmable au sens d'unités monétaires auxquelles seraient intrinsèquement attachées des restrictions déterminant les biens, services, lieux, personnes ou périodes pour lesquels elles pourraient être utilisées.

Cette interdiction ne signifie cependant pas l'absence de mécanismes automatisés autour des paiements.

La documentation de la Banque centrale européenne prévoit explicitement des paiements conditionnels dans lesquels l'exécution d'une transaction peut dépendre de la vérification préalable d'une condition.

L'Eurosystème peut fournir les fonctions monétaires fondamentales nécessaires à ces mécanismes, notamment la réservation des fonds, tandis que la logique permettant de déterminer si une condition est

satisfaite peut être gérée par les prestataires de services de paiement ou d'autres acteurs du marché.

Les travaux techniques de la BCE indiquent également qu'un monitoring externe peut participer au déclenchement de ces conditions.

Ce mécanisme général ne constitue plus uniquement une possibilité théorique. Des acteurs du marché ont connecté leurs propres plateformes, au moyen d'API, à un environnement simulant le back-end de l'euro numérique afin d'expérimenter différents scénarios de paiements conditionnels.

Les scénarios étudiés comprennent notamment le paiement à la livraison, le paiement à l'usage, les paiements par étapes, certains remboursements automatisés et des paiements machine-to-machine.

Il est donc établi dans son principe qu'une information ou un événement provenant d'un système externe à la couche monétaire peut être vérifié par un service afin de participer à la décision d'exécuter, de libérer, de maintenir ou de restituer des fonds associés à une transaction déterminée.

L'information externe utilisée pour vérifier une condition n'a pas nécessairement besoin d'être intégralement stockée dans l'infrastructure monétaire : un système externe peut effectuer la vérification et transmettre uniquement le résultat nécessaire au processus conditionnel.

L'identité numérique européenne possède par ailleurs un raccord explicitement documenté avec les infrastructures de paiement.

L'European Digital Identity Wallet, ou EUDI Wallet, peut être utilisé dans des processus d'authentification de paiement. La BCE prévoit également son utilisation comme méthode d'authentification forte par les prestataires participant au pilote de l'euro numérique pour certaines transactions en ligne.

L'EUDI Wallet repose notamment sur des mécanismes d'attestations vérifiables, de minimisation des données et de divulgation sélective. L'existence de ce raccord ne signifie donc pas que l'ensemble des informations détenues dans le wallet soit communiqué au commerçant, au prestataire de paiement ou à l'Eurosystème.

Les éléments étudiés permettent ainsi d'établir séparément l'existence de transactions structurées et identifiables, de paiements conditionnels, d'une couche de conditionnalité pouvant utiliser des informations provenant de systèmes externes, d'interfaces permettant à des plateformes d'acteurs du marché d'interagir avec l'environnement de paiement et d'un raccord explicite entre identité numérique et paiement.

Ces éléments rendent techniquement possible la construction de services dans lesquels une information provenant d'une infrastructure externe participe à une décision automatisée concernant une transaction déterminée sans que la monnaie elle-même devienne programmable.

Ils ne permettent cependant pas d'établir qu'un passeport numérique de produit, un GTIN, une empreinte carbone, une donnée issue de la facturation électronique ou un profil environnemental individuel soit actuellement utilisé pour déclencher, empêcher ou modifier un paiement en euros numériques.

Le raccord générique entre système externe et paiement conditionnel est donc documenté. Le raccord spécifique entre données environnementales ou fiscales et exécution d'un paiement reste à établir.

Chapitre 5 — Interconnexions

Statut : AVÉRÉ / EXPÉRIMENTÉ / DÉDUCTIBLE TECHNIQUEMENT / NON ÉTABLI

Le Chapitre 5 a recherché les raccords existants, prévus, expérimentés ou techniquement possibles entre les infrastructures étudiées séparément dans les chapitres précédents.

Les recherches montrent que ces infrastructures ne constituent pas un système unique et centralisé, mais qu'elles ne sont pas non plus totalement indépendantes les unes des autres.

La Commission européenne inscrit explicitement plusieurs de ces dispositifs dans un même objectif d'interopérabilité et de création de synergies. Le Digital Product Passport, l'eInvoicing, les European Business Wallets et d'autres infrastructures européennes sont notamment présentés comme participant à un écosystème cohérent de solutions numériques.

La réutilisation des données de facturation électronique dépasse par ailleurs le seul traitement de la facture. Des travaux européens prévoient notamment leur réutilisation pour le reporting de durabilité et leur rapprochement avec certaines données douanières.

Les European Business Wallets constituent un autre point de convergence documenté. Le projet prévoit leur utilisation pour l'identification des opérateurs économiques, les attestations vérifiables, certaines informations fiscales et transactionnelles ainsi que des interactions avec le Digital Product Passport et les données relatives aux produits.

Les travaux de standardisation apportent également un raccord direct entre transaction et produit. Le modèle européen relatif aux eReceipts prévoit qu'un justificatif puisse contenir un identifiant permettant de relier le produit acheté à son Digital Product Passport et aux informations vérifiées correspondantes, comprenant notamment certaines informations relatives à sa durabilité et à ses impacts environnementaux.

La chaîne suivante dispose donc désormais de raccords documentés :

```
transaction
   ↓
eReceipt
   ↓
identifiant DPP
   ↓
Digital Product Passport
   ↓
informations produit / durabilité / environnement
```

Parallèlement, les expérimentations européennes étudiées ont permis de documenter une chaîne reliant identité d'entreprise, paiement, justificatif électronique détaillé, Business Wallet et traitement comptable ou fiscal expérimental.

```
identité / autorisation
   ↓
wallet
   ↓
paiement
   ↓
eReceipt détaillé
   ↓
Business Wallet
   ↓
comptabilité / traitement fiscal expérimental
```

Le raccord entre identité numérique et paiement est également documenté : l'EUDI Wallet peut intervenir dans l'authentification de paiements et son utilisation est prévue dans les travaux relatifs au pilote de l'euro numérique.

Enfin, les travaux de la BCE établissent qu'un système extérieur peut participer à la vérification d'une condition utilisée par un service de paiement conditionnel.

```
système externe
   ↓
vérification d'une condition
  ↓
couche de conditionnalité
   ↓
paiement
```

Ces différents éléments permettent techniquement de reconstruire une architecture dans laquelle une donnée relative à un produit pourrait être récupérée depuis une infrastructure externe, évaluée par un service et transformée en résultat utilisable par une logique automatisée entourant une transaction.

Il demeure cependant **NON ÉTABLI** qu'une donnée environnementale provenant du Digital Product Passport ou d'une infrastructure équivalente soit actuellement utilisée comme condition afin d'autoriser, refuser ou limiter un paiement.

Il demeure également **NON ÉTABLI** qu'un système centralisé réunisse identité individuelle, historique exhaustif des achats, données fiscales, données environnementales et données de paiement, ou qu'un profil carbone individuel généralisé soit calculé à partir de ces infrastructures.

Les travaux relatifs à l'euro numérique maintiennent en outre une distinction essentielle : la monnaie programmable, dont les unités comporteraient intrinsèquement des restrictions sur les biens ou services pouvant être achetés, est explicitement exclue, tandis que des services de paiement conditionnel distincts de la monnaie elle-même sont prévus et expérimentés.

Le résultat du Chapitre 5 est donc précis : **une part importante des infrastructures et des raccords permettant techniquement d'associer transaction, produit, environnement, identité et paiement est désormais documentée ; certains de ces raccords sont explicitement prévus, standardisés ou**

expérimentés ; mais le raccord transformant effectivement une donnée environnementale en règle imposée d'autorisation ou de refus d'un paiement n'a pas été établi.

Chapitre 6 — Garanties juridiques

Statut : AVÉRÉ / GARANTIES JURIDIQUES / VULNÉRABILITÉS JURIDIQUES / ANGLES MORTS DOCUMENTAIRES

Le Chapitre 6 a recherché si les capacités techniques et les interconnexions identifiées dans les chapitres précédents pouvaient être librement exploitées et combinées.

La réponse est négative.

L'existence d'une donnée, d'un identifiant, d'une interface ou d'une possibilité technique de rapprochement ne constitue pas en elle-même une autorisation juridique de l'utiliser pour une nouvelle finalité.

Le RGPD, le droit de l'Union européenne, le droit national et les garanties propres aux différentes infrastructures imposent notamment des exigences relatives :

- à la base juridique des traitements ;
- à la détermination et à la compatibilité des finalités ;
- à la nécessité et à la proportionnalité ;
- à la minimisation des données ;
- à la sécurité et au contrôle des accès ;
- aux droits des personnes ;
- au profilage et aux décisions automatisées ;
- au contrôle par les autorités indépendantes et les juridictions.

L'enquête a néanmoins établi que ces protections ne constituent pas toutes des impossibilités techniques ou des garanties d'immuabilité.

L'exemple de CFVR est particulièrement important.

Ce traitement a vu son périmètre évoluer juridiquement à plusieurs reprises depuis sa création. En 2026, les données issues de la facturation électronique ont été intégrées parmi ses nouvelles sources, dans une architecture permettant leur exploitation algorithmique à grande échelle et leur rapprochement avec d'autres informations utilisées pour la détection d'anomalies et le ciblage du contrôle fiscal.

Cette évolution démontre concrètement qu'une infrastructure de données créée pour une fonction déterminée peut ultérieurement devenir une source juridiquement autorisée d'un autre traitement.

Elle ne démontre pas que toute interconnexion future sera autorisée.

Elle démontre que le périmètre juridique actuel des traitements ne doit pas être confondu avec une impossibilité permanente de faire évoluer leurs usages.

Le Chapitre 6 a également identifié une distinction essentielle entre centralisation physique et centralisation fonctionnelle.

Une architecture n'a pas besoin de réunir toutes les informations dans une base unique pour permettre leur rapprochement.

Des systèmes distincts peuvent échanger :

```
identifiant
   +
attribut
   +
preuve
   +
résultat
   +
condition vérifiée
```

sans nécessairement transférer l'intégralité de leurs données brutes.

Cette propriété est particulièrement importante pour l'analyse des infrastructures étudiées dans ce dossier, qui reposent largement sur des identifiants structurés, des registres, des interfaces, des attestations vérifiables et des mécanismes d'interopérabilité.

Le Chapitre 6 a également établi que certaines garanties importantes sont explicitement inscrites dans les cadres étudiés.

Le DPP prévoit notamment des restrictions concernant les données personnelles des clients.

Le portefeuille européen d'identité numérique prévoit des mécanismes de minimisation, de contrôle utilisateur et de divulgation sélective.

Le cadre actuellement proposé pour l'euro numérique exclut la monnaie programmable, c'est-à-dire une monnaie dont les unités comporteraient intrinsèquement des restrictions déterminant les biens, services, personnes, lieux ou périodes pour lesquels elles peuvent être utilisées.

Cette interdiction coexiste cependant avec la possibilité de développer des services de paiement conditionnel reposant sur des conditions vérifiées extérieurement.

La distinction est fondamentale :

```
monnaie programmable
   ≠
paiement conditionnel
```

Le premier mécanisme est exclu dans le cadre étudié.

Le second est prévu et a fait l'objet d'expérimentations.

Le Chapitre 6 n'a identifié aucun fondement permettant d'affirmer qu'une donnée environnementale relative à un produit est actuellement transformée en restriction individuelle de paiement.

Mais il confirme l'importance juridique de la frontière située entre :

```
information
   ↓
vérification
   ↓
profilage
   ↓
condition
   ↓
conséquence individuelle
```

Plus une donnée ou un résultat devient déterminant pour l'accès à un paiement, un service, un droit ou une autre possibilité importante, plus les exigences relatives à la base juridique, à la nécessité, à la proportionnalité, à l'exactitude, à la transparence, à la contestation et aux droits fondamentaux deviennent centrales.

AVÉRÉ :

> Les capacités techniques documentées dans les chapitres précédents sont juridiquement encadrées et ne peuvent pas être librement combinées pour n'importe quelle finalité.

AVÉRÉ :

> Les données issues de la facturation électronique ont rejoint en 2026 un traitement fiscal préexistant, CFVR, dont le périmètre avait déjà connu plusieurs évolutions successives.

GARANTIE JURIDIQUE :

> Une nouvelle capacité technique ou une nouvelle interconnexion ne constitue pas à elle seule une autorisation juridique de produire une conséquence individuelle.

VULNÉRABILITÉ JURIDIQUE :

> Le périmètre juridiquement autorisé d'une infrastructure peut évoluer, sous réserve du respect des normes supérieures applicables.

VULNÉRABILITÉ JURIDIQUE :

> Une augmentation des possibilités de rapprochement ne nécessite pas nécessairement la création d'une base centralisée réunissant physiquement toutes les données.

ANGLE MORT DOCUMENTAIRE :

> Les sources publiques étudiées permettent plus facilement d'évaluer chaque infrastructure et chaque extension séparément que l'effet cumulé de l'ensemble de leurs évolutions et interconnexions.

NON ÉTABLI :

> Aucun élément étudié ne démontre actuellement l'existence d'un dispositif utilisant un profil environnemental individuel afin d'autoriser, refuser ou limiter les paiements, les achats, les services ou les droits d'une personne.

NON ÉTABLI :

> Aucun élément étudié ne démontre l'existence d'une infrastructure unique réunissant automatiquement facturation électronique, identité numérique, données environnementales, Digital Product Passport et euro numérique afin de contrôler les transactions individuelles.

Conclusion générale

Les six chapitres permettent désormais de suivre une chaîne qui n'était, au début de l'enquête, qu'une hypothèse à vérifier.

La réforme française de la facturation électronique transforme une partie importante de l'activité économique en données structurées, standardisées, transmissibles et exploitables automatiquement.

Ces données ne servent pas uniquement à transporter une facture.

Les sources étudiées établissent leur utilisation ou leur destination pour différentes finalités fiscales et économiques, notamment la lutte contre la fraude, le pré-remplissage de la TVA, la connaissance de l'activité économique et le pilotage des politiques publiques.

Depuis 2026, certaines données issues de la facturation électronique constituent également une source du traitement CFVR et de son infrastructure de traitement à grande échelle.

Parallèlement, l'Union européenne développe plusieurs autres infrastructures numériques.

Le Digital Product Passport permet d'associer à des produits identifiables des données structurées pouvant comprendre des informations relatives à leur durabilité et à leurs impacts environnementaux.

Les standards européens relatifs aux justificatifs électroniques permettent de relier une transaction et un produit à son Digital Product Passport.

Les infrastructures d'identité numérique permettent la présentation et la vérification d'attributs.

Le raccord entre identité numérique et paiement est documenté.

Des expérimentations ont relié identité, paiement, justificatif transactionnel et Business Wallet.

Enfin, les travaux relatifs à l'euro numérique ont établi qu'un système externe peut participer à la vérification d'une condition utilisée par un service de paiement conditionnel.

Le pont recherché au début de l'enquête a donc bien été partiellement construit

L'enquête ne se termine pas au même point qu'elle a commencé.

Au départ, la question était de savoir si des infrastructures concernant :

```
facturation
   +
transaction
   +
produit
   +
environnement
   +
identité
   +
paiement
```

pouvaient réellement disposer de points de raccordement.

Plusieurs de ces raccords sont désormais **AVÉRÉS**, **STANDARDISÉS** ou **EXPÉRIMENTÉS**.

La chaîne documentaire obtenue peut être représentée ainsi :

```
FACTURATION / TRANSACTION
   ↓
DONNÉES STRUCTURÉES
   ↓
TRAITEMENTS ET RAPPROCHEMENTS

TRANSACTION
   ↓
eRECEIPT
   ↓
PRODUIT IDENTIFIABLE
   ↓
DIGITAL PRODUCT PASSPORT
   ↓
INFORMATIONS PRODUIT
   ↓
DURABILITÉ / ENVIRONNEMENT
```

Parallèlement :

```
IDENTITÉ / ATTRIBUTS
   ↓
WALLET
   ↓
AUTHENTIFICATION
   ↓
PAIEMENT
```

et :

```
SYSTÈME EXTERNE
   ↓
VÉRIFICATION
D'UNE CONDITION
  ↓
SERVICE DE
PAIEMENT CONDITIONNEL
   ↓
PAIEMENT
```

Une autre chaîne a en outre été expérimentée :

```
IDENTITÉ / AUTORISATION
   ↓
WALLET
   ↓
PAIEMENT
   ↓
eRECEIPT DÉTAILLÉ
   ↓
BUSINESS WALLET
   ↓
COMPTABILITÉ /
TRAITEMENT FISCAL
```

Le résultat est donc différent d'une simple juxtaposition d'infrastructures indépendantes.

> **Des ponts existent.**

Mais tous les segments ne possèdent ni le même statut ni le même niveau de preuve.

Le dernier raccord déterminant n'est pas établi

L'enquête permet techniquement de reconstruire :

```
transaction
   ↓
produit identifiable
   ↓
DPP
   ↓
information environnementale
```

Elle permet également de reconstruire séparément :

```
système externe
   ↓
condition vérifiée
   ↓
paiement conditionnel
```

Elle documente encore :

```
identité numérique
   ↓
paiement
```

Mais elle n'a pas établi le raccord final :

```
IDENTITÉ
   +
HISTORIQUE DE TRANSACTIONS
   +
PRODUITS
   +
DONNÉES ENVIRONNEMENTALES
   ↓
PROFIL ENVIRONNEMENTAL
INDIVIDUEL
   ↓
CONDITION IMPOSÉE
   ↓
AUTORISATION / REFUS /
LIMITATION D'UN PAIEMENT
```

NON ÉTABLI :

> Aucun élément étudié ne démontre actuellement que cette chaîne complète soit déployée ou juridiquement organisée afin de contrôler les possibilités de paiement d'une personne.

Cette limite est fondamentale.

Elle empêche de présenter comme un fait ce qui demeure une possibilité construite à partir de capacités séparément documentées.

Mais il serait également incorrect de conclure que le pont n'existe pas

L'absence du dernier raccord ne remet pas à zéro les résultats de l'enquête.

Les sources ont permis de passer de :

```
HYPOTHÈSE
« ces systèmes pourraient peut-être
un jour être reliés »
```

à :

```
CONSTAT
plusieurs raccords existent déjà,
sont standardisés,
prévus
ou ont été expérimentés
```

La frontière documentaire se situe désormais beaucoup plus loin dans la chaîne.

Ce qui reste **NON ÉTABLI** n'est plus la possibilité générale de relier transaction, produit, données environnementales, identité et paiement.

Ce qui reste **NON ÉTABLI** est leur utilisation combinée dans une finalité unique produisant une restriction individuelle.

Cette distinction constitue l'un des principaux résultats de l'enquête.

Le Chapitre 6 apporte cependant une seconde frontière : la possibilité technique n'est pas l'autorisation juridique

Même lorsqu'un raccord est techniquement possible, il ne peut pas être librement exploité.

Les traitements demeurent soumis notamment :

```
base juridique
   +
finalité
   +
nécessité
   +
proportionnalité
   +
minimisation
   +
droits des personnes
   +
contrôle
   +
droits fondamentaux
```

Une infrastructure capable de rapprocher deux informations n'est donc pas automatiquement autorisée à le faire.

Et une infrastructure capable de produire une condition n'est pas automatiquement autorisée à utiliser cette condition pour restreindre un paiement, un service ou un droit.

Cette distinction constitue une véritable garantie.

Mais le cadre juridique n'est pas immuable

L'enquête a également établi que les finalités, sources, catégories de données et destinataires d'un traitement peuvent évoluer juridiquement.

CFVR en fournit un exemple concret.

Depuis sa création, son périmètre a été modifié à plusieurs reprises.

En 2026, les données issues de la facturation électronique sont devenues une nouvelle source de ce traitement préexistant.

La frontière entre :

```
« techniquement possible
mais non utilisé »
```

et :

```
« juridiquement autorisé
et effectivement utilisé »
```

peut donc évoluer.

Cette constatation ne démontre aucune évolution future particulière.

Elle démontre que l'état juridique observé aujourd'hui ne doit pas être présenté comme une garantie d'immuabilité.

La réforme de la facturation électronique doit donc être replacée dans un changement d'échelle plus large

L'enquête ne démontre pas que la facturation électronique constitue une base centrale réunissant l'ensemble des informations étudiées.

Une telle affirmation serait excessive.

Elle établit en revanche que cette réforme transforme une part importante de l'activité économique en données structurées pouvant être transmises et exploitées automatiquement.

Dans le domaine fiscal, leur intégration à CFVR fournit désormais un exemple concret de réutilisation dans une infrastructure algorithmique plus large.

La réforme constitue donc une **infrastructure structurante de données économiques**.

Son importance ne vient pas du fait qu'elle centraliserait déjà « tout ».

Elle vient du fait qu'elle rend une partie croissante de l'activité économique :

```
STRUCTURÉE
   ↓
STANDARDISÉE
   ↓
LISIBLE PAR MACHINE
   ↓
TRANSMISSIBLE
   ↓
CROISABLE
   ↓
ANALYSABLE
```

La question de ses interconnexions futures devient dès lors aussi importante que celle de ses finalités présentes.

Le résultat final doit donc être formulé avec deux vérités simultanées

Première vérité :

> **l'enquête n'a pas démontré l'existence actuelle d'un système généralisé utilisant identité, achats, données environnementales et monnaie numérique pour contrôler les possibilités économiques individuelles.**

Deuxième vérité :

> **l'enquête a démontré qu'une partie importante des briques et des raccords techniques permettant de relier transaction, produit, informations environnementales, identité et paiement existe déjà, est prévue par des standards, intégrée à des architectures européennes ou a fait l'objet d'expérimentations.**

Ces deux affirmations ne sont pas contradictoires.

Elles définissent précisément le niveau de preuve atteint.

Ce qui est établi

AVÉRÉ :

> La facturation électronique crée une infrastructure massive de données économiques structurées et exploitables automatiquement.

AVÉRÉ :

> Certaines données issues de cette infrastructure alimentent désormais CFVR, où elles peuvent être rapprochées d'autres informations dans le cadre de traitements algorithmiques destinés notamment à la détection d'anomalies et au ciblage fiscal.

AVÉRÉ :

> Des standards permettent de relier transaction, produit identifiable, Digital Product Passport et informations vérifiées relatives au produit, notamment certaines informations environnementales.

AVÉRÉ / EXPÉRIMENTÉ :

> L'identité numérique peut intervenir dans des processus de paiement et des expérimentations ont relié identité, paiement, justificatif électronique détaillé et Business Wallet.

AVÉRÉ / EXPÉRIMENTÉ :

> Un système externe peut vérifier une condition dont le résultat intervient dans un service de paiement conditionnel.

DÉDUCTIBLE TECHNIQUEMENT :

> Les raccords documentés permettent de construire techniquement une chaîne reliant une transaction identifiable à des informations relatives au produit et à son impact environnemental, puis de faire intervenir le résultat d'une vérification externe dans une logique conditionnelle entourant un paiement.

Ce qui n'est pas établi

NON ÉTABLI :

> Il n'est pas démontré qu'un profil environnemental individuel généralisé soit actuellement calculé à partir des achats des citoyens.

NON ÉTABLI :

> Il n'est pas démontré que les informations environnementales du DPP soient actuellement utilisées comme condition pour autoriser, refuser ou limiter les paiements d'une personne.

NON ÉTABLI :

> Il n'est pas démontré que la facturation électronique, le DPP, l'identité numérique et l'euro numérique soient réunis dans une infrastructure unique destinée au contrôle des comportements individuels.

NON ÉTABLI :

> Il n'est pas démontré que l'euro numérique permettra de programmer intrinsèquement la monnaie afin d'interdire l'achat de certaines catégories de biens ; le cadre étudié exclut au contraire explicitement la monnaie programmable.

La conclusion de l'enquête n'est donc ni une validation ni une accusation

Elle est une cartographie.

Elle montre :

```
ce qui existe
   +
ce qui communique
   +
ce qui a été expérimenté
   +
ce qui est techniquement possible
   +
ce que le droit autorise
   +
ce qu'il interdit ou encadre
   +
ce qui reste à démontrer
```

Le résultat essentiel est que **le pont a bien été construit sur une partie substantielle de son parcours**.

Il ne repose plus uniquement sur une succession d'hypothèses.

Plusieurs de ses piliers sont documentés par des règlements, des standards, des architectures techniques, des projets européens et des expérimentations.

Mais le dernier passage :

```
DONNÉE ENVIRONNEMENTALE
   ↓
PROFIL INDIVIDUEL
   ↓
RÈGLE IMPOSÉE
   ↓
RESTRICTION ÉCONOMIQUE
OU MONÉTAIRE
```

reste **NON ÉTABLI**.

C'est exactement là que les preuves disponibles s'arrêtent aujourd'hui.

Conclusion finale

> **Cette enquête n'établit pas l'existence actuelle d'un système de contrôle environnemental des paiements ou des comportements économiques individuels.**

> **Elle établit en revanche qu'une partie substantielle de l'architecture technique qui rendrait certains rapprochements possibles existe déjà : données économiques structurées, identification des transactions et des produits, Digital Product Passport, données environnementales associées aux produits, identité numérique, infrastructures de paiement, vérification de conditions externes et paiements conditionnels.**

> **Plusieurs raccords entre ces briques sont avérés, standardisés ou expérimentés. Le pont technique n'est donc plus une hypothèse abstraite.**

> **Ce qui n'est pas établi est son activation intégrale dans une finalité unique permettant d'établir un profil environnemental individuel et d'en tirer une conséquence imposée sur un paiement, un achat, un service ou un droit.**

> **Le droit actuel oppose en outre plusieurs garanties à une telle évolution. Mais l'étude de CFVR démontre que le périmètre juridique des traitements peut évoluer dans le temps.**

> **La frontière à surveiller n'est donc plus seulement l'apparition de nouvelles bases de données. Elle se situe dans les nouveaux raccords, les nouvelles finalités, les nouveaux attributs, les nouvelles conditions et surtout les nouvelles conséquences que le droit pourrait progressivement autoriser à partir d'infrastructures déjà existantes.**

> **Le dossier s'arrête ainsi exactement à la limite des preuves disponibles : suffisamment loin pour établir que les briques et plusieurs ponts existent ; pas assez loin pour affirmer qu'elles constituent aujourd'hui le système intégré de contrôle que leur combinaison rendrait techniquement possible.**

Sources officielles

> **Navigation :** ← Retour au sommaire

Ce fichier constitue le registre central des sources utilisées dans l'ensemble du dossier.

Chaque source reçoit un identifiant unique `[S1](#s1)`, `[S2](#s2)`, `[S3](#s3)`, etc. Cet identifiant est conservé dans tous les chapitres afin de permettre la vérification des affirmations et de retrouver précisément leur origine.

Les sources primaires et officielles sont privilégiées.

S1 DGFiP — Données de facture transmises à l'administration

Organisme : Direction générale des Finances publiques

Document : Tableau récapitulatif des données de facture à transmettre à l'administration — opérations domestiques B2B

Mise à jour : août 2026

Utilisé dans : Chapitre 1

Éléments établis : nature et granularité des données de facturation B2B transmises à l'administration, notamment les données de ligne applicables à compter du 1er septembre 2027 : dénomination précise du bien ou service, quantité et prix unitaire hors taxe.

Lien :

- https://www.impots.gouv.fr/sites/default/files/media/1_metier/2_professionnel/EV/2_gestion/290_facturation_electronique/japprof_donnees-de-facture-a-transmettre-a-ladministration-correspondance-flux_vf.pdf

---

S2 DGFiP — Données de transaction transmises à l'administration

Organisme : Direction générale des Finances publiques

Document : Données de transaction — e-reporting de transaction — à transmettre à l'administration en application de l'article 290 du CGI

Mise à jour : août 2026

Utilisé dans : Chapitre 1

Éléments établis : données transmises pour les opérations B2C et B2B internationales ; caractère agrégé par jour du e-reporting B2C ; données détaillées applicables aux opérations B2B internationales.

Lien :

- https://www.impots.gouv.fr/sites/default/files/media/1_metier/2_professionnel/EV/2_gestion/290_facturation_electronique/japprof_donnees-de-transactions-a-transmettre_vf.pdf

---

S3 DGFiP — Données de paiement transmises à l'administration

Organisme : Direction générale des Finances publiques

Document : Données de paiement à transmettre à l'administration

Mise à jour : août 2026

Utilisé dans : Chapitre 1

Éléments établis : transmission des dates d'encaissement et des montants encaissés par taux de TVA ; modalités applicables aux factures électroniques, au B2B international et au B2C.

Lien :

- https://www.impots.gouv.fr/sites/default/files/media/1_metier/2_professionnel/EV/2_gestion/290_facturation_electronique/japprof_donnees-de-paiement-a-transmettre_vf.pdf

---

S4 DGFiP — Spécifications externes de la facturation électronique

Organisme : Direction générale des Finances publiques

Document : Spécifications externes B2B

Version applicable étudiée : 3.2 — 30 avril 2026

Utilisé dans : Chapitres 1 et 2

Éléments établis : architecture fonctionnelle du dispositif, formats et modalités d'échange avec l'administration, concentration des données de facturation, de transaction et de paiement.

Lien :

- https://www.impots.gouv.fr/specifications-externes-b2b

S5 DGFiP — Objectifs de la réforme

Organisme : Direction générale des Finances publiques

Document : Je découvre la facturation électronique

Utilisé dans : Chapitre 2

Éléments établis : objectifs officiels de la réforme, notamment lutte contre la fraude à la TVA, pré-remplissage des déclarations, connaissance en temps réel de l'activité des entreprises et pilotage des politiques publiques.

Lien :

- https://www.impots.gouv.fr/professionnel/je-decouvre-la-facturation-electronique

---

S6 DGFiP — Fiche pédagogique sur les objectifs de la réforme

Organisme : Direction générale des Finances publiques

Document : Fiche pédagogique sur la facturation électronique

Mise à jour : septembre 2025

Utilisé dans : Chapitre 2

Éléments établis : exploitation automatique et continue des données, connaissance de la conjoncture économique et pilotage de l'économie par la puissance publique.

Lien :

- https://www.impots.gouv.fr/sites/default/files/media/1_metier/2_professionnel/EV/2_gestion/290_facturation_electronique/fiche-0_tpe_preambule_2025.pdf

---

S7 Code général des impôts — Transmission des données

Organisme : République française — Légifrance

Document : Code général des impôts — dispositions relatives à la facturation électronique et au e-reporting

Version étudiée : dispositions applicables au 1er septembre 2026

Utilisé dans : Chapitre 2

Éléments établis : fondement légal de la transmission à l'administration des données de facturation, de transaction et de paiement.

Lien :

- https://www.legifrance.gouv.fr/codes/id/LEGISCTA000006162565/

S8 Livre des procédures fiscales — Article L. 102 B

Organisme : République française — Légifrance

Document : Livre des procédures fiscales — article L. 102 B

Versions étudiées : version applicable au 1er septembre 2026 et version applicable à compter du 1er janvier 2027

Utilisé dans : Chapitre 2

Éléments établis : durée de conservation des livres, registres, documents et pièces sur lesquels peuvent s'exercer les droits de communication, d'enquête et de contrôle de l'administration ; délai de six ans dans la version applicable en 2026 et évolution du délai général à dix ans à compter du 1er janvier 2027.

Lien — version applicable en 2026 :

- https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000046869194/2026-07-27

Lien — version applicable à compter du 1er janvier 2027 :

- https://www.legifrance.gouv.fr/codes/id/LEGIARTI000053189500/2027-01-01

S9 Livre des procédures fiscales — Article L. 102 B bis

Organisme : République française — Légifrance

Document : Livre des procédures fiscales — article L. 102 B bis

Version étudiée : dispositions applicables à compter du 1er janvier 2027

Utilisé dans : Chapitre 2

Éléments établis : obligation de conservation des factures dans des conditions garantissant l'authenticité de leur origine, l'intégrité de leur contenu et leur lisibilité pendant leur période de conservation.

Lien :

- https://www.legifrance.gouv.fr/codes/id/LEGIARTI000053189500/2027-01-01

S10 CGI, annexe II — Articles 242 nonies E et 242 nonies E bis

Organisme : République française — Légifrance

Document : Code général des impôts, annexe II — obligations des plateformes agréées

Version étudiée : en vigueur depuis le 29 juillet 2026

Utilisé dans : Chapitre 2

Éléments établis : services obligatoires des plateformes agréées ; garanties d'authenticité de l'origine, d'intégrité du contenu et de lisibilité des factures ; traitement et transmission des informations nécessaires au dispositif ; conservation pendant trois ans après la cessation de ses effets de l'accord formel permettant à une plateforme d'actualiser certaines informations dans l'annuaire central.

Lien :

- https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006069569/LEGISCTA000046385430/

S11 CGI, annexe II — Article 242 nonies L

Organisme : République française — Légifrance

Document : Code général des impôts, annexe II — article 242 nonies L

Version étudiée : en vigueur depuis le 29 juillet 2026

Utilisé dans : Chapitre 2

Éléments établis : transmission à l'administration des données de facturation par la plateforme agréée de l'émetteur dans un délai de vingt-quatre heures à compter du dépôt de la facture électronique sur la plateforme.

Lien :

- https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000054552554/2026-09-01

S12 CGI, annexe II — Articles 242 nonies G et 242 nonies H

Organisme : République française — Légifrance

Document : Code général des impôts, annexe II — annuaire central et transmission des données à l'administration

Version étudiée : en vigueur depuis le 29 juillet 2026

Utilisé dans : Chapitre 2

Éléments établis : recueil au moyen d'une solution dédiée des données de facturation, de transaction et de paiement ainsi que des informations relatives aux statuts de traitement ; contenu et fonctionnement de l'annuaire central ; identification des assujettis, personnes morales de droit public et plateformes agréées ; consultation de l'annuaire par les plateformes agréées aux fins d'adressage des factures.

Lien :

- https://www.legifrance.gouv.fr/codes/id/LEGISCTA000054552483/2026-07-29

S13 DGFiP — Facturation électronique et plateformes agréées

Organisme : Direction générale des Finances publiques

Document : Facturation électronique et plateformes agréées

Utilisé dans : Chapitre 2

Éléments établis : rôle du service d'immatriculation des plateformes agréées ; surveillance des obligations de transmission pesant sur les plateformes et leurs utilisateurs ; mise en œuvre éventuelle de sanctions pécuniaires ; retrait éventuel de l'immatriculation en cas de manquements répétés.

Lien :

- https://www.impots.gouv.fr/facturation-electronique-et-plateformes-agreees

---

S14 Gouvernement — Évaluation préalable de la réforme de la facturation électronique

Organisme : Gouvernement — document annexé au projet de loi de finances rectificative pour 2022, publié par l'Assemblée nationale

Document : Évaluation préalable de l'article relatif à la généralisation de la facturation électronique et à la transmission des données de transaction

Année : 2022

Utilisé dans : Chapitre 2

Éléments établis : objectif d'amélioration de la connaissance en temps réel de l'activité des entreprises afin de permettre un pilotage de la politique économique au plus près de la réalité économique des acteurs ; exemple d'utilisation envisagée des données recueillies pour enrichir les modèles d'analyse et faciliter la détection et l'accompagnement des entreprises en difficulté.

Lien :

- https://www.assemblee-nationale.fr/dyn/docs/PRJLANR5L16B0017.raw

---

S15 Union européenne — Règlement sur l'écoconception des produits durables et le passeport numérique de produit

Organisme : Parlement européen et Conseil de l'Union européenne

Document : Règlement (UE) 2024/1781 du 13 juin 2024 établissant un cadre pour la fixation d'exigences en matière d'écoconception pour des produits durables

Utilisé dans : Chapitre 3

Éléments établis : cadre juridique du passeport numérique de produit ; possibilité d'établir le passeport au niveau du modèle, du lot ou de l'article ; association du passeport à un identifiant unique persistant du produit ; données structurées, lisibles par machine, recherchables et transférables selon des standards ouverts et interopérables ; mise en place d'un registre numérique géré par la Commission européenne contenant au minimum les identifiants uniques ; accès au registre par la Commission, les autorités nationales compétentes et les autorités douanières dans le cadre de leurs missions ; interconnexion prévue entre le registre et le système EU CSW-CERTEX permettant des échanges automatisés avec les systèmes douaniers nationaux.

Lien :

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32024R1781

S16 Commission européenne — Données accessibles dans le passeport numérique de produit

Organisme : Commission européenne — Direction générale du marché intérieur, de l'industrie, de l'entrepreneuriat et des PME

Document : The Digital Product Passport (DPP) for Consumers

Utilisé dans : Chapitre 3

Éléments établis : selon le groupe de produits et la législation applicable, le passeport numérique de produit peut fournir des informations relatives à la durabilité, la réparabilité et la recyclabilité ; aux impacts environnementaux, notamment l'empreinte carbone et l'empreinte environnementale ; aux matériaux et composants du produit ; à son utilisation et sa maintenance ; aux substances dangereuses ; ainsi qu'à son démontage, son réemploi ou son recyclage.

Lien :

- https://single-market-economy.ec.europa.eu/single-market/digital-product-passport/consumers_en

---

S17 OpenPeppol — Identification standard des articles dans la facturation électronique

Organisme : OpenPeppol

Document : Peppol BIS Billing 3.0 — structure et règles relatives à l'identification standard des articles

Utilisé dans : Chapitre 3

Éléments établis : les lignes de facture peuvent contenir un identifiant standard de l'article correspondant au terme métier BT-157 ; cet identifiant repose sur un schéma d'identification enregistré ; Peppol prévoit également l'utilisation d'identifiants standardisés de produits dans ses flux commerciaux, notamment le GTIN pour l'identification des articles dans les commandes.

Lien :

- https://docs.peppol.eu/poacc/billing/3.0/bis/

S18 Commission européenne — Méthode Product Environmental Footprint

Organisme : Commission européenne

Document : Recommandation (UE) 2021/2279 de la Commission du 15 décembre 2021 relative à l'utilisation des méthodes de l'empreinte environnementale pour mesurer et communiquer la performance environnementale des produits et des organisations tout au long de leur cycle de vie

Utilisé dans : Chapitre 3

Éléments établis : existence d'une méthode européenne harmonisée Product Environmental Footprint (PEF) permettant de mesurer et de communiquer les impacts environnementaux potentiels d'un produit sur l'ensemble de son cycle de vie ; utilisation de données et de modèles relatifs notamment aux matériaux, aux procédés de fabrication, à l'énergie, au transport et à la fin de vie ; possibilité de définir des règles spécifiques par catégorie de produits au moyen des Product Environmental Footprint Category Rules (PEFCR).

Lien :

- https://environment.ec.europa.eu/document/download/cb899bd7-bb06-491d-9989-c856a401fcd0_en

---

S19 Union européenne — Empreinte carbone et passeport numérique des batteries

Organisme : Parlement européen et Conseil de l'Union européenne

Document : Règlement (UE) 2023/1542 du 12 juillet 2023 relatif aux batteries et aux déchets de batteries

Utilisé dans : Chapitre 3

Éléments établis : obligation progressive de déclaration de l'empreinte carbone pour certaines catégories de batteries ; expression de l'empreinte en kilogrammes de CO_2 équivalent par kWh fourni sur la durée de vie prévue ; distinction de l'empreinte selon différentes étapes du cycle de vie ; calcul reposant notamment sur des données spécifiques au modèle de batterie et au site de production ; prise en compte de l'acquisition et du prétraitement des matières premières, de la production, de la distribution et de la fin de vie ; utilisation de la méthode d'évaluation climatique issue du Product Environmental Footprint ; association progressive de ces informations au dispositif numérique prévu pour les batteries.

Lien :

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32023R1542

S20 Union européenne — Architecture et fonctionnement du registre des passeports numériques de produits

Organisme : Commission européenne

Document : Règlement d'exécution (UE) 2026/1778 relatif aux modalités de mise en œuvre du registre des passeports numériques de produits

Utilisé dans : Chapitre 3

Éléments établis : architecture opérationnelle du registre européen des passeports numériques de produits ; interface sécurisée ; API permettant l'enregistrement des passeports et la réception d'informations du registre ; plateforme de vérification ; mécanismes d'identification et d'autorisation des utilisateurs ; génération d'identifiants uniques d'enregistrement ; référentiel sémantique ; journalisation des opérations ; vérification des opérateurs économiques et des autres acteurs de la chaîne de valeur ; possibilité de déléguer des droits d'accès ; communication automatisée de l'identifiant unique d'enregistrement par interface ou réponse API ; conservation et versionnement de certaines données d'enregistrement ; possibilité d'intégration avec d'autres systèmes d'information de l'Union disposant d'un processus équivalent ou identique de vérification d'identité.

Lien :

- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32026R1778

S21 Commission européenne — EBSI / e-Origin : transactions commerciales, traçabilité et Digital Product Passport

Organisme : Commission européenne — European Blockchain Services Infrastructure (EBSI)

Document : e-Origin

Utilisé dans : Chapitre 3

Éléments établis : existence d'un pilote européen réunissant notamment administration de la TVA, marketplaces, vendeurs en ligne, courtiers en douane et autorités douanières ; stockage et partage de preuves de transactions commerciales ; reconnaissance de ces preuves par les autorités douanières afin de faciliter le dédouanement ; partage sécurisé de données entre vendeurs, marketplaces et autorités ; développement, dans le cadre du projet EBSI-ELSA, de capacités de traçabilité utilisant le Digital Product Passport.

Lien :

- https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/e-Origin

---

S22 Commission européenne — Proposition de règlement établissant l'euro numérique

Organisme : Commission européenne

Document : Proposition de règlement du Parlement européen et du Conseil établissant l'euro numérique — COM(2023) 369 final

Date : 28 juin 2023

Utilisé dans : Chapitre 4

Éléments établis : cadre juridique proposé pour l'euro numérique ; statut de monnaie de banque centrale ; distribution par l'intermédiaire de prestataires de services de paiement ; comptes et instruments de paiement en euros numériques ; opérations de chargement et de déchargement ; possibilité pour la BCE de fixer certaines limites de détention ; organisation des services de paiement en euros numériques.

Lien :

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52023PC0369

S23 Banque centrale européenne — Architecture et état d'avancement de l'euro numérique

Organisme : Banque centrale européenne

Document : FAQ sur l'euro numérique

Dernière mise à jour étudiée : 17 août 2026

Utilisé dans : Chapitre 4

Éléments établis : architecture technique envisagée reposant sur une plateforme centralisée de règlement ; traitement et vérification des règlements et des avoirs par l'Eurosystème ; absence de recours à une infrastructure DLT ou blockchain comme fondement du système ; architecture reposant sur plusieurs régions et plusieurs serveurs afin d'assurer la résilience ; accès des utilisateurs par l'intermédiaire d'une banque ou d'un intermédiaire public ; possibilité de paiements en ligne et hors ligne ; projet encore en développement et absence, à ce stade, de décision définitive d'émission.

Lien :

- https://www.ecb.europa.eu/euro/digital_euro/faqs/html/ecb.faq_digital_euro.fr.html

---

S24 Banque centrale européenne — Rulebook de l'euro numérique et architecture des participants

Organisme : Banque centrale européenne

Document : Digital euro scheme rulebook v0.91 et annexes techniques

Date : 2 juillet 2026

Utilisé dans : Chapitre 4

Éléments établis : organisation fonctionnelle et technique du dispositif envisagé pour l'euro numérique ; définition des acteurs et des flux de bout en bout ; exigences applicables aux prestataires de services de paiement distributeurs et acquéreurs ; dispositifs d'acceptation ; services communs ; gestion et échange des données ; gestion du risque et de la fraude ; règlement des transactions ; interfaces et standards techniques permettant la communication entre les différents composants du système.

Lien :

- https://www.ecb.europa.eu/euro/digital_euro/timeline/rulebook/html/index.fr.html

S25 Banque centrale européenne — Modèle, dictionnaire et échanges de données de l'euro numérique

Organisme : Banque centrale européenne

Document : Digital euro scheme rulebook v0.91 — Annex D1 Front-end implementation specification #7 « Data management » ; Annex D2 Back-end implementation specification #6 « Data exchange » ; Annex D2 Back-end implementation specification #8 « Data dictionary »

Date : 2 juillet 2026

Utilisé dans : Chapitre 4

Éléments établis : modèle de données envisagé pour les utilisateurs individuels et professionnels, les comptes, les appareils et les transactions ; identifiants de transaction et identifiant de bout en bout ; montant, date et heure, devise, direction, type, environnement et informations complémentaires de transaction ; identifiants du payeur et du bénéficiaire ; méthodes d'initiation ; identification et catégorisation des commerçants ; Merchant Category Code ; points d'interaction et certaines données de localisation ; gestion de scores de risque et de fraude ; utilisation d'identifiants pseudonymes ; service d'échange de données permettant au DESP de fournir aux PSP des rapports et requêtes selon leurs rôles, notamment à des fins opérationnelles, analytiques et statistiques.

Lien :

- https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/html/index.en.html

---

S26 Banque centrale européenne — Fonctionnement et confidentialité des paiements hors ligne en euros numériques

Organisme : Banque centrale européenne

Document : Preparation phase of a digital euro — Closing report ; documentation relative à la confidentialité de l'euro numérique et aux travaux techniques sur le mode hors ligne

Date des éléments étudiés : octobre 2025 à août 2026

Utilisé dans : Chapitre 4

Éléments établis : architecture distincte pour les paiements en ligne et hors ligne ; possibilité de paiements hors ligne sans connexion à Internet ; transfert direct entre appareils au moyen de valeurs cryptographiquement sécurisées ; conservation locale de la valeur et des informations sensibles dans un élément matériel sécurisé ; absence de transmission des détails de la transaction aux PSP et à l'Eurosystème pendant ou après le paiement hors ligne ; connaissance des détails personnels de la transaction limitée au payeur et au bénéficiaire ; contrôles liés à la lutte contre le blanchiment effectués par le PSP lors des opérations de chargement et de déchargement ; travaux techniques portant notamment sur les Secure Elements intégrés et les eSIM ; préparation d'un pilote incluant des paiements hors ligne.

Lien :

- https://www.ecb.europa.eu/euro/digital_euro/progress/html/ecb.deprp202510.en.html

S27 Banque centrale européenne — Paiements conditionnels et distinction avec la monnaie programmable

Organisme : Banque centrale européenne

Documents : Preparation phase of a digital euro — Closing report ; Digital Euro Innovation Platform — Outcome report ; documentation et communications de la BCE relatives aux paiements conditionnels

Date des éléments étudiés : septembre 2025 à juillet 2026

Utilisé dans : Chapitre 4

Éléments établis : exclusion explicite de la monnaie programmable ; distinction entre programmabilité de la monnaie et paiements conditionnels ; fonctionnalité de réservation des fonds fournie par l'infrastructure de l'Eurosystème ; séparation entre une couche de règlement fournie par l'Eurosystème et une couche de conditionnalité développée par les acteurs du marché ; possibilité d'une vérification externe déclenchant la condition ; transfert des fonds lorsque la condition est vérifiée ; annulation ou expiration de la réservation lorsque la condition n'est pas remplie ; expérimentation de paiements conditionnels dans un environnement simulé ; exemples comprenant paiement à la livraison, paiement à l'usage, paiements par étapes, remboursements automatiques et paiements machine-to-machine ; possibilité pour les banques et autres prestataires de développer des services à valeur ajoutée reposant sur les données dont ils disposent.

Liens :

- https://www.ecb.europa.eu/euro/digital_euro/progress/html/ecb.deprp202510.en.html
- https://www.ecb.europa.eu/euro/digital_euro/innovation-platform/html/index.en.html

---

S28 Banque centrale européenne — Expérimentation des conditions externes et intégration avec les plateformes des acteurs du marché

Organisme : Banque centrale européenne

Document : Digital euro innovation platform — Outcome report: pioneers and visionaries workstreams

Date : 26 septembre 2025

Utilisé dans : Chapitre 4

Éléments établis : expérimentation technique des paiements conditionnels dans un environnement simulant le back-end de l'euro numérique ; connexion des plateformes des participants aux interfaces simulées au moyen d'API ; fourniture par l'Eurosystème des fonctions techniques fondamentales et notamment de la réservation des fonds ; définition et gestion de la logique conditionnelle par les PSP et autres acteurs du marché ; possibilité d'un monitoring externe déclenchant les conditions ; expérimentation de scénarios dans le commerce électronique, les services financiers, les transports et l'Industrie 4.0 ; paiements à la livraison, à l'usage ou par étapes ; paiements machine-to-machine ; automatisation de certains remboursements et règlements ; exploration de reçus électroniques et d'autres services à valeur ajoutée associés aux paiements.

Lien :

- https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.deprep250926_innovationplatform.en.pdf

---

S29 Commission européenne et Banque centrale européenne — EUDI Wallet, authentification des paiements et euro numérique

Organismes : Commission européenne ; Banque centrale européenne

Documents : EU Digital Identity Wallet — Payment Authentication Manual ; EU Digital Identity Wallet Pilot implementation ; FAQs on the digital euro pilot

Dernières mises à jour étudiées : juillet-août 2026

Utilisé dans : Chapitre 4

Éléments établis : utilisation de l'European Digital Identity Wallet pour l'authentification de paiements en ligne et en magasin ; intégration avec les infrastructures de paiement existantes ; utilisation d'attestations vérifiables permettant de relier le wallet à un payeur et à un compte de paiement ; possibilité de présenter certains attributs tels que l'âge ou la résidence avec divulgation sélective ; présentation des attestations à une banque, un acquéreur ou un commerçant ; obligation progressive d'accepter l'EUDI Wallet pour certaines authentifications fortes lorsque l'utilisateur le demande ; possibilité explicitement prévue pour les PSP participant au pilote de l'euro numérique d'utiliser l'EUDI Wallet comme méthode d'authentification forte pour les paiements en ligne.

Liens :

- https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/935397429/Payment%2BAuthentication
- https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation
- https://www.ecb.europa.eu/euro/digital_euro/pilot/html/ecb.faq-digital-euro-pilot.en.html

---

S30 Commission européenne — European Business Wallets et interopérabilité avec les infrastructures numériques européennes

Organisme : Commission européenne

Document : Proposition de règlement établissant les European Business Wallets — COM(2025) 838 final ; Staff Working Document SWD(2025) 837 final

Date : 19 novembre 2025

Utilisé dans : Chapitre 5

Éléments établis : création proposée d'une infrastructure harmonisée permettant aux opérateurs économiques de s'identifier, s'authentifier, stocker, gérer et échanger des données et attestations vérifiables avec les administrations et d'autres acteurs économiques ; architecture construite en cohérence avec le cadre européen d'identité numérique et l'EUDI Wallet ; recherche explicite d'interopérabilité avec les infrastructures numériques européennes existantes ; possibilité de stocker et d'échanger de manière vérifiable des attestations relatives à la TVA et des données de transaction dans le cadre de VAT in the Digital Age afin de

soutenir le reporting en temps réel et la facturation de confiance ; possibilité d'intégration avec les systèmes informatiques existants des entreprises et administrations.

Liens :

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52025PC0838
- https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-establishment-european-business-wallets

---

S31 Commission européenne — Stratégie pour le marché unique : DPP, eInvoicing, Business Wallet et réutilisation des données

Organisme : Commission européenne

Document : The Single Market: our European home market in an uncertain world — A Strategy for making the Single Market simple, seamless and strong — COM(2025) 500 final

Date : 21 mai 2025

Utilisé dans : Chapitre 5

Éléments établis : présentation du Digital Product Passport, de l'eInvoicing, du futur European Business Wallet, du Single Digital Gateway, du Once-Only Technical System, du Business Register Interconnection System et d'autres initiatives comme les composants d'un écosystème cohérent de solutions numériques destiné à créer des synergies et faciliter l'échange de données ; volonté d'accroître la réutilisation des données issues de la facturation électronique ; projet pilote de réutilisation des données d'eInvoicing pour le reporting de durabilité ; projet de rapprochement des données d'eInvoicing avec les données douanières en lien avec le développement de l'EU Customs Data Hub.

Liens :

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52025DC0500
- https://single-market-economy.ec.europa.eu/single-market/public-procurement/digital-procurement/einvoicing_en

---

S32 Union européenne — Standards, identifiants, API et mécanismes d'interopérabilité

Organismes : Commission européenne ; Union européenne

Documents : documentation européenne relative à l'interopérabilité de l'eInvoicing et au standard EN 16931 ; règlement (UE) 2024/1781 relatif à l'écoconception des produits durables ; règlement d'exécution (UE) 2026/1778 relatif au registre du Digital Product Passport ; proposition de règlement relative aux European Business Wallets

Dates des éléments étudiés : 2024 à 2026

Utilisé dans : Chapitre 5

Éléments établis : utilisation de données structurées et de modèles sémantiques communs dans l'eInvoicing ; exigences d'identifiants uniques persistants et de formats ouverts, structurés, lisibles par machine et interopérables dans le Digital Product Passport ; mise en place d'une API du registre DPP, d'un référentiel sémantique, de mécanismes d'identification et d'autorisation et d'identifiants uniques de produit et d'opérateur ; utilisation d'API, d'attestations électroniques vérifiables, de mécanismes de contrôle d'accès et de standards d'interopérabilité dans l'architecture proposée des European Business Wallets ; stratégie européenne visant plus largement l'interopérabilité entre les infrastructures numériques publiques.

Liens :

- https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/467108973/Interoperability%2Bof%2BeInvoicing
- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32024R1781
- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32026R1778
- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52025PC0838

S33 BCE / Commission européenne — Acteurs, consortiums et expérimentations communes

Organismes : Banque centrale européenne ; Commission européenne ; WE BUILD Large Scale Pilot

Documents : Digital euro innovation platform — Outcome report ; documentation officielle relative aux Large Scale Pilots de l'EUDI Wallet ; documentation et Architecture & Integration Blueprint du consortium WE BUILD

Dates des éléments étudiés : septembre 2025 à août 2026

Utilisé dans : Chapitre 5

Éléments établis : participation d'environ 70 acteurs du marché à la Digital Euro Innovation Platform de la BCE, comprenant banques, prestataires de paiement, fintechs, entreprises technologiques, commerçants et autres acteurs privés ; expérimentation par ces participants de fonctionnalités et services reposant sur l'infrastructure simulée de l'euro numérique ; existence du consortium européen WE BUILD réunissant plus de 200 organisations publiques et privées autour de cas d'usage relatifs aux entreprises, aux chaînes d'approvisionnement et aux paiements ; expérimentation dans une même architecture de processus comprenant notamment identité numérique, Business Wallet, données d'entreprise, facturation électronique, services bancaires et paiements ; participation d'acteurs financiers et technologiques à plusieurs initiatives européennes relatives à l'identité et au paiement.

Liens :

- https://www.ecb.europa.eu/euro/digital_euro/innovation-platform/html/index.en.html
- https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.deprep250926_innovationplatform.en.pdf
- https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/694487808/What+are+the+Large+Scale+Pilot+Projects
- https://www.webuildconsortium.eu/
- https://webuild-consortium.github.io/wp4-architecture/blueprint/blueprint.html

---

S34 WE BUILD — Chaînes expérimentales reliant identité, paiement, justificatif numérique et fiscalité

Organismes et sources : WE BUILD Consortium ; documentation technique publiée par iGrant.io en qualité de participant au consortium WE BUILD

Documents : documentation WE BUILD relative aux Business Payments et à l'European Business Wallet ; présentation des cas d'usage WE BUILD ; documentation du cas PA4 « Trusted eReceipts for B2B Payments »

Dates des éléments étudiés : mars à septembre 2026

Utilisé dans : Chapitre 5

Éléments établis : expérimentation au sein de WE BUILD de chaînes B2B associant identité d'entreprise, EUDI Wallet, European Business Wallet, ouverture ou utilisation d'un compte bancaire, attestation d'IBAN, paiement et émission d'un justificatif électronique ; présence, dans le même programme, de cas d'usage relatifs aux paiements professionnels, à l'eInvoicing et aux déclarations fiscales transfrontalières ; démonstration par un participant du consortium d'un cas PA4 dans lequel un paiement par compte ou carte authentifié au moyen de l'EUDI Wallet entraîne l'émission d'un eReceipt vérifiable vers le European Business Wallet de l'entreprise acheteuse ; le justificatif comporte notamment des lignes d'achat, montants, informations de TVA et référence de paiement ; connexion du justificatif à un système comptable et démonstration d'un rapprochement de TVA avec un service fiscal de démonstration.

Précaution méthodologique : la chaîne générale identité d'entreprise → compte/IBAN → paiement → eReceipt est documentée par le consortium WE BUILD. Le détail du cas PA4 jusqu'au rapprochement automatisé de TVA est documenté par iGrant.io, participant ayant développé le pilote avec d'autres partenaires WE BUILD. Ce second niveau constitue une preuve d'expérimentation technique par un participant du projet et ne doit pas être présenté comme la preuve du déploiement opérationnel d'un tel système par une administration fiscale nationale réelle.

Liens :

- https://www.webuildconsortium.eu/news/we-build-joins-global-digital-collaboration-2026-discover-our-sessions
- https://igrant.io/articles/trusted-ereceipts-for-b2b-payments-taking-eudi-wallet-payments-from-the-consumer-to-the-company

---

S35 CEN/TS 16931-8:2024 — eReceipts, identifiant DPP et informations environnementales du produit

Organisme : Comité européen de normalisation (CEN)

Document : CEN/TS 16931-8:2024 — Electronic invoicing — Part 8: Semantic data model of the elements of an e-receipt

Date : 2024

Utilisé dans : Chapitre 5

Éléments établis : modèle sémantique européen relatif aux justificatifs électroniques ; description d'un processus dans lequel l'acheteur sélectionne un moyen de paiement, effectue ou initie le paiement puis reçoit un eReceipt généré par le vendeur ; possibilité d'inclure dans certains environnements des informations spécifiques relatives au produit ; mention explicite du Digital Product Passport pour les catégories de produits concernées ; utilisation d'un identifiant DPP permettant de relier le justificatif aux informations vérifiées relatives au produit ; mention parmi ces informations de la durabilité des matériaux ainsi que des impacts sociaux et environnementaux liés aux matériaux, à la production, à l'utilisation et à la fin de vie du produit.

Précaution méthodologique : l'existence d'un champ ou mécanisme permettant de relier un eReceipt au DPP démontre la possibilité normalisée d'établir ce raccord. Elle ne démontre pas que chaque eReceipt contiendra un identifiant DPP, ni que les données environnementales correspondantes seront systématiquement récupérées, ni qu'elles seront utilisées par un système de paiement.

Lien :

- https://norminfo.afnor.org/norme/cents-16931-82024/facturation-electronique-partie-8-modele-semantique-de-donnees-des-elements-dun-recu-electronique-ou-dune-facture/307488

S36 Règlement général sur la protection des données — principes applicables aux traitements

Organisme : Union européenne

Document : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 — Règlement général sur la protection des données (RGPD)

Utilisé dans : Chapitre 6

Éléments établis : principes de licéité, loyauté et transparence ; limitation des finalités ; minimisation des données ; base juridique du traitement ; garanties applicables aux traitements réalisés dans le cadre d'une mission d'intérêt public ; encadrement des décisions individuelles automatisées et du profilage ; obligation de collecter les données pour des finalités déterminées, explicites et légitimes et de ne pas les traiter ultérieurement d'une manière incompatible avec ces finalités ; obligation de limiter les données à ce qui est nécessaire au regard des finalités poursuivies.

Lien :

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679

S37 CNIL — intégration des données de facturation électronique au traitement algorithmique CFVR

Organisme : Commission nationale de l'informatique et des libertés (CNIL)

Document : Délibération n° 2026-068 du 18 juin 2026 portant avis sur un projet d'arrêté modifiant le traitement automatisé de lutte contre la fraude « ciblage de la fraude et valorisation des requêtes » (CFVR)

Publication : 24 juillet 2026

Utilisé dans : Chapitre 6

Éléments établis : intégration des données issues de la facturation électronique aux catégories de données personnelles utilisées par CFVR ; augmentation substantielle du volume de données traité, estimé par la DGFiP à environ 2 à 3 milliards de factures électroniques par an ; alimentation de la plateforme sécurisée des données de la DGFiP ; exploitation possible de ces données afin d'identifier des anomalies et des entreprises présentant certains risques fiscaux ; croisement possible des résultats des requêtes avec d'autres données du traitement ; vocation, à terme, de l'ensemble des données du traitement CFVR à alimenter cette plateforme ; utilisation de méthodes algorithmiques et d'apprentissage, notamment non supervisé ; identification par la CNIL de risques de biais et d'amplification de ces biais ; nécessité de maintenir une analyse humaine préalable à l'ouverture d'un contrôle fiscal ; exigences relatives à la minimisation, aux accès, aux durées de conservation, à l'information des personnes et à la sécurité des données.

Précaution méthodologique : cet avis ne conclut pas à l'illégalité du traitement. Il confirme cependant que les données issues de la facturation électronique sont effectivement destinées à alimenter une infrastructure d'analyse et de ciblage fiscal utilisant notamment des traitements algorithmiques.

Lien :

- https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000054466005

S38 Décret relatif à la généralisation de la facturation électronique — prise en compte du RGPD et avis de la CNIL

Organisme : République française

Document : Décret n° 2022-1299 du 7 octobre 2022 relatif à la généralisation de la facturation électronique dans les transactions entre assujettis à la TVA et à la transmission des données de transaction

Date : 7 octobre 2022

Utilisé dans : Chapitre 6

Éléments établis : référence explicite au règlement général sur la protection des données dans le décret organisant la réforme ; adoption du décret après avis de la Commission nationale de l'informatique et des libertés du 23 juin 2022 ; intégration de la problématique de protection des données au processus réglementaire. Cette consultation et cette référence ne permettent toutefois pas de conclure que toute évolution ultérieure des traitements ou toute nouvelle réutilisation des données serait automatiquement compatible avec le RGPD.

Lien :

- https://www.legifrance.gouv.fr/loda/id/JORFTEXT000046383394

S39 Contrôle de proportionnalité des traitements de données par les pouvoirs publics

Organismes : Cour de justice de l'Union européenne ; Conseil constitutionnel

Documents : jurisprudence de la Cour de justice de l'Union européenne relative aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne ; jurisprudence du Conseil constitutionnel relative au

contrôle de nécessité et de proportionnalité des dispositifs de collecte et de traitement de données à caractère personnel

Utilisé dans : Chapitre 6

Éléments établis : la protection des données personnelles et de la vie privée n'interdit pas aux autorités publiques de mettre en œuvre des traitements poursuivant un objectif d'intérêt général ; ces traitements restent soumis à un contrôle de nécessité et de proportionnalité ; les limitations apportées à la protection des données doivent rester limitées à ce qui est strictement nécessaire et l'objectif d'intérêt général doit être mis en balance avec la gravité de l'ingérence dans les droits concernés ; le contrôle constitutionnel tient notamment compte des finalités poursuivies, de la nature et de l'étendue des données collectées ainsi que des garanties entourant leur utilisation.

Références officielles :

- CJUE : jurisprudence relative aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.
- Conseil constitutionnel : contrôle de nécessité et de proportionnalité des dispositifs de collecte et de traitement de données à caractère personnel.
- https://curia.europa.eu/juris/liste.jsf?num=C-175/20
- https://www.conseil-constitutionnel.fr/decision/2012/2012652DC.html

---

S40 Union européenne — CE-RISE : DPP, réemploi, réparation et recyclage

Organisme : Commission européenne — CORDIS / Horizon Europe

Projet : Circular Economy Resource Information System (CE-RISE)

Utilisé dans : Chapitre 3

Éléments établis : développement et expérimentation d'un système d'information destiné à favoriser le réemploi, la récupération et le recyclage des matériaux ; définition de critères permettant d'évaluer les possibilités de réemploi, réparation, reconditionnement et recyclage ; intégration de ces informations et de la composition des produits dans le Digital Product Passport afin d'assurer la traçabilité des matériaux dans la chaîne de valeur ; intégration du DPP avec des informations relatives à l'empreinte environnementale des produits ; expérimentation du dispositif sur quatre cas d'usage.

Lien :

- https://cordis.europa.eu/project/id/101092281

S41 Union européenne — QUASAR : DPP et traçabilité en fin de vie

Organisme : Commission européenne — CORDIS / Horizon Europe

Projet : QUASAR — 70%plus eco-efficiency gains in the PV EOL supply chain by closed loop systems with enhanced recycling rates, systematic collection and management utilising digital twins

Utilisé dans : Chapitre 3

Éléments établis : utilisation d'un Digital Product Passport pour contribuer au suivi de modules photovoltaïques en fin de vie ; utilisation du DPP et de méthodes d'évaluation afin d'orienter les décisions entre réemploi, réparation et recyclage ; expérimentation de solutions de réparation et de seconde vie ; utilisation d'outils numériques de traçabilité dans une chaîne de valeur circulaire.

Lien :

- https://cordis.europa.eu/project/id/101122298

S42 Commission européenne — Mise en service du registre des passeports numériques de produits

Organisme : Commission européenne — Direction générale du marché intérieur, de l'industrie, de l'entrepreneuriat et des PME

Document : The Digital Product Passport Registry is now live

Date : 20 juillet 2026

Utilisé dans : Chapitre 3

Éléments établis : mise en service du registre européen des passeports numériques de produits le 20 juillet 2026 ; lancement simultané d'un environnement de test ; possibilité d'enregistrer les passeports au moyen d'une interface sécurisée ou d'une API ; stockage des identifiants uniques et des métadonnées d'enregistrement ; mise à disposition d'un référentiel sémantique et d'API documentées ; présence de mécanismes de vérification et de journalisation ; accès à une documentation technique et à des ressources destinées à accompagner la mise en œuvre du dispositif.

Lien :

- https://single-market-economy.ec.europa.eu/news/digital-product-passport-registry-now-live-2026-07-20_en

---

S43 Règlement général sur la protection des données — principes, bases juridiques et garanties applicables aux traitements

Organisme : Union européenne

Document : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 — Règlement général sur la protection des données (RGPD)

Utilisé dans : Chapitre 6

Éléments établis :

- l'article 5 impose notamment les principes de licéité, loyauté et transparence, de limitation des finalités, de minimisation des données, d'exactitude, de limitation de la conservation, d'intégrité, de confidentialité et de responsabilité du responsable du traitement ;
- les données personnelles doivent être collectées pour des finalités déterminées, explicites et légitimes et ne pas être réutilisées ultérieurement d'une manière incompatible avec ces finalités ;

- les données traitées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités poursuivies ;
- l'article 6 prévoit plusieurs bases permettant de rendre un traitement licite, notamment le respect d'une obligation légale et l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique ;
- lorsqu'un traitement fondé sur une obligation légale ou une mission d'intérêt public repose sur le droit de l'Union ou le droit d'un État membre, ce droit doit déterminer la finalité du traitement ou encadrer son exercice conformément au RGPD ;
- l'article 22 encadre les décisions fondées exclusivement sur un traitement automatisé, y compris le profilage, lorsqu'elles produisent des effets juridiques ou affectent significativement une personne de façon similaire ;
- l'article 23 permet au droit de l'Union ou au droit national de limiter certains droits et obligations prévus par le RGPD, notamment pour certains objectifs d'intérêt public, mais exige que cette limitation respecte l'essence des libertés et droits fondamentaux et constitue une mesure nécessaire et proportionnée dans une société démocratique ;
- l'article 25 impose la protection des données dès la conception et par défaut et prévoit notamment que seules les données nécessaires à chaque finalité spécifique soient traitées par défaut, cette exigence concernant notamment leur quantité, l'étendue du traitement, leur durée de conservation et leur accessibilité ;
- l'article 32 impose des mesures techniques et organisationnelles appropriées au niveau de risque présenté par le traitement ;
- l'article 35 impose une analyse d'impact relative à la protection des données lorsqu'un type de traitement, notamment par le recours à de nouvelles technologies et compte tenu de sa nature, de sa portée, de son contexte et de ses finalités, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

Portée pour l'enquête : L'existence d'une base juridique permettant la collecte de données ne constitue pas, à elle seule, une autorisation générale permettant n'importe quelle réutilisation, n'importe quel croisement ou n'importe quelle extension de finalité.
Inversement, le RGPD n'interdit pas par principe les traitements réalisés par une administration sans consentement lorsque ceux-ci reposent sur une autre base juridique prévue par son article 6.
L'analyse juridique doit donc porter sur chaque traitement concerné, sa finalité, sa base juridique, les données effectivement nécessaires, leur durée de conservation, leurs destinataires, leurs modalités d'accès et les garanties applicables.

Lien :

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679

S44 CJUE et Conseil constitutionnel — nécessité, minimisation et proportionnalité des traitements de données

Organismes : Cour de justice de l'Union européenne / Conseil constitutionnel

Utilisé dans : Chapitre 6

Éléments établis : La Cour de justice de l'Union européenne rappelle que tout traitement de données personnelles doit respecter les principes de l'article 5 du RGPD et satisfaire à l'une des conditions de licéité

prévues à son article 6.
Elle rappelle également que les finalités d'un traitement doivent être déterminées, explicites et légitimes et que le responsable du traitement doit être en mesure de démontrer le respect de ces principes.
Dans sa jurisprudence relative aux articles 5 et 6 du RGPD, la Cour rattache le principe de minimisation au contrôle de proportionnalité. L'appréciation de la nécessité d'un traitement peut notamment conduire à rechercher si l'objectif poursuivi peut être atteint par des moyens aussi efficaces mais moins attentatoires à la protection des données personnelles.
Dans l'affaire C-175/20, Valsts ieņēmumu dienests, concernant précisément un traitement de données à des fins fiscales, la Cour rappelle l'application des principes de finalité et de minimisation aux demandes et traitements de données réalisés par une administration fiscale.
Dans l'affaire C-268/21, Norra Stockholm Bygg, la Cour rappelle que le principe de minimisation exprime le principe de proportionnalité et que l'autorité compétente doit notamment examiner si l'objectif poursuivi peut être atteint par des moyens moins intrusifs pour la protection des données personnelles.
Le Conseil constitutionnel considère pour sa part que le droit au respect de la vie privée implique que la collecte, l'enregistrement, la conservation, la consultation et la communication de données personnelles soient justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif.

Portée pour l'enquête : L'existence d'un objectif d'intérêt général, notamment la lutte contre la fraude fiscale, ne suffit donc pas à rendre automatiquement proportionnées toutes les modalités possibles de collecte, de conservation, de croisement ou d'exploitation des données.
Le contrôle juridique peut porter notamment sur l'étendue des données traitées, leur nécessité au regard de la finalité poursuivie, leur durée de conservation, leurs destinataires, les rapprochements effectués et l'existence éventuelle de moyens moins attentatoires permettant d'atteindre efficacement le même objectif.

Liens :

- https://curia.europa.eu/juris/liste.jsf?num=C-175/20
- https://curia.europa.eu/juris/liste.jsf?num=C-268/21

S45 France — Intégration des données de facturation électronique au traitement CFVR

Organisme : République française — ministère de l'Économie et des Finances

Document : Arrêté du 10 juillet 2026 modifiant l'arrêté du 21 février 2014 portant création par la direction générale des finances publiques d'un traitement automatisé de lutte contre la fraude dénommé « ciblage de la fraude et valorisation des requêtes » (CFVR)

Utilisé dans : Chapitre 6

Éléments établis :

- modification du cadre réglementaire applicable au traitement CFVR ;
- ajout des données issues de la facturation électronique aux données susceptibles d'être traitées dans le dispositif ;
- évolution du traitement en lien avec les échanges de données entre administrations et l'organisation du dispositif d'analyse des données ;

- inscription réglementaire de l'intégration des données de facturation électronique dans le traitement automatisé de lutte contre la fraude de la DGFiP.

Portée pour l'enquête : L'intégration des données issues de la facturation électronique dans CFVR n'est plus seulement décrite dans un projet soumis pour avis à la CNIL.
Elle est désormais prévue par un texte réglementaire adopté en juillet 2026.
La légalité de l'existence de ce traitement ne dispense cependant pas d'examiner séparément les garanties applicables à ses modalités concrètes : finalités, catégories de données, conservation, croisements, accès, sécurité, minimisation, proportionnalité et traitements algorithmiques.

Lien :

- https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000054450882

S46 RGPD — traitement ultérieur et compatibilité des finalités

Organisme : Union européenne

Document : Règlement (UE) 2016/679 — article 6, paragraphe 4

Utilisé dans : Chapitre 6

Éléments établis : Le RGPD n'interdit pas par principe tout traitement ultérieur poursuivant une finalité différente de celle ayant justifié la collecte initiale.
Lorsque le traitement ultérieur ne repose ni sur le consentement de la personne concernée ni sur le droit de l'Union ou d'un État membre constituant une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23, paragraphe 1, le responsable du traitement doit déterminer si la nouvelle finalité est compatible avec la finalité initiale.

L'article 6, paragraphe 4 prévoit notamment de prendre en compte :

- l'existence éventuelle d'un lien entre les finalités initiales et la finalité ultérieure ;
- le contexte dans lequel les données ont été collectées, notamment la relation entre les personnes concernées et le responsable du traitement ;
- la nature des données personnelles concernées ;
- les conséquences possibles du traitement ultérieur pour les personnes concernées ;
- l'existence de garanties appropriées, notamment le chiffrement ou la pseudonymisation.

Portée pour l'enquête : Une nouvelle utilisation de données personnelles n'est donc pas automatiquement interdite au seul motif qu'elle diffère de l'utilisation initiale.

Deux situations doivent notamment être distinguées :

1. le traitement ultérieur repose sur une finalité compatible avec la finalité initiale, après application du test de compatibilité prévu par le RGPD ;
2. le traitement ultérieur repose sur le droit de l'Union ou d'un État membre répondant aux conditions prévues par le RGPD.

Le principe de limitation des finalités constitue donc une garantie juridique réelle, mais il ne constitue pas une interdiction absolue de toute évolution des usages.

Lien :

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679

S47 RGPD — restrictions pour objectifs fiscaux et missions de contrôle

Organismes : Union européenne / République française

Documents : Règlement (UE) 2016/679, article 23 ; arrêté du 10 juillet 2026 modifiant le traitement CFVR

Utilisé dans : Chapitre 6

Éléments établis : L'article 23 du RGPD permet au droit de l'Union ou au droit d'un État membre de limiter, par voie législative et sous certaines conditions, la portée de plusieurs obligations et droits prévus par le RGPD.

Une telle limitation doit :

- respecter l'essence des libertés et droits fondamentaux ;
- constituer une mesure nécessaire et proportionnée dans une société démocratique ;
- poursuivre l'un des objectifs prévus par l'article 23.

Parmi ces objectifs figurent notamment, au point e) :

- des objectifs importants d'intérêt public général ;
- un intérêt économique ou financier important de l'Union ou d'un État membre ;
- les domaines monétaire, budgétaire et fiscal ;
- la sécurité sociale.

Le point h) prévoit également :

- une mission de contrôle, d'inspection ou de réglementation liée à l'exercice de l'autorité publique dans les domaines concernés.
  L'arrêté du 10 juillet 2026 modifiant CFVR fait explicitement référence aux points e) et h) du paragraphe 1 de l'article 23 du RGPD dans les dispositions relatives au traitement.

Portée pour l'enquête : Le RGPD prévoit donc lui-même une latitude permettant au législateur d'aménager ou de limiter certains droits et obligations lorsqu'un objectif fiscal ou une mission de contrôle le justifie.
Cette latitude n'est toutefois pas générale ou inconditionnelle.
Elle demeure soumise notamment au respect de l'essence des droits fondamentaux ainsi qu'à un contrôle de nécessité et de proportionnalité.
Le cadre juridique applicable à CFVR mobilise explicitement cette possibilité.

Liens :

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679
- https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000054450882

S48 RGPD — sécurité des traitements, analyse d'impact et réévaluation du risque

Organisme : Union européenne

Document : Règlement (UE) 2016/679 — articles 32 et 35

Utilisé dans : Chapitre 6

Éléments établis : L'article 32 du RGPD impose au responsable du traitement et au sous-traitant de mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

L'appréciation doit notamment prendre en compte :

- l'état des connaissances ;
- la nature du traitement ;
- sa portée ;
- son contexte ;
- ses finalités ;
- la probabilité et la gravité des risques pour les droits et libertés des personnes.

Les mesures envisageables comprennent notamment :

- la pseudonymisation et le chiffrement ;
- la capacité de garantir de façon constante la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes ;
- la capacité de rétablir la disponibilité et l'accès aux données après un incident ;
- des procédures régulières de test, d'analyse et d'évaluation de l'efficacité des mesures de sécurité.

L'évaluation doit notamment prendre en compte les risques de destruction, perte, altération, divulgation non autorisée ou accès non autorisé aux données.
L'article 35 prévoit qu'une analyse d'impact relative à la protection des données doit être réalisée lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, compte tenu notamment de sa nature, de sa portée, de son contexte, de ses finalités et du recours à de nouvelles technologies.
L'article 35 prévoit également qu'un examen doit être réalisé, lorsque nécessaire, afin de vérifier que le traitement demeure conforme à l'analyse d'impact, au moins lorsqu'une modification du risque présenté par les opérations de traitement intervient.

Portée pour l'enquête : La sécurité d'un traitement n'est pas une appréciation figée réalisée une seule fois lors de sa création.
Une augmentation substantielle des volumes, l'ajout de nouvelles sources, de nouveaux croisements, de nouveaux accédants ou de nouvelles infrastructures peut modifier le risque présenté par le traitement et rendre pertinente une réévaluation des garanties mises en œuvre.

Lien :

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679

S49 CNIL — grande échelle, croisement de données et critères de risque élevé

Organisme : Commission nationale de l'informatique et des libertés

Document : Documentation CNIL relative aux analyses d'impact sur la protection des données (AIPD)

Utilisé dans : Chapitre 6

Éléments établis : La CNIL rappelle qu'une analyse d'impact relative à la protection des données est obligatoire lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

Parmi les critères utilisés pour apprécier l'existence d'un risque élevé figurent notamment :

- l'évaluation ou le scoring, y compris le profilage ;
- la prise de décision automatisée produisant un effet juridique ou similaire significatif ;
- la surveillance systématique ;
- le traitement de données sensibles ou hautement personnelles ;
- le traitement de données personnelles à grande échelle ;
- le croisement ou la combinaison d'ensembles de données ;
- le traitement de données concernant des personnes vulnérables ;
- l'utilisation innovante de technologies ou de solutions organisationnelles ;
- l'exclusion du bénéfice d'un droit, d'un service ou d'un contrat.

La CNIL indique qu'en présence d'au moins deux de ces critères, une AIPD doit en principe être réalisée, sous réserve de l'analyse concrète du risque.

L'AIPD doit notamment comporter :

- une description des opérations de traitement ;
- une évaluation de leur nécessité et de leur proportionnalité ;
- une évaluation des risques pour les personnes ;
- les mesures envisagées pour traiter ces risques et assurer la sécurité des données.

Portée pour l'enquête : Le traitement à grande échelle et le croisement d'ensembles de données ne sont pas juridiquement neutres en matière d'évaluation des risques.
Lorsqu'une infrastructure combine plusieurs de ces critères, l'existence, le périmètre et l'actualisation de l'analyse d'impact deviennent des éléments importants pour apprécier la conformité du traitement.

Lien :

- https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd

---

S50 CNIL — état de l'art en matière de sécurité des données personnelles

Organisme : Commission nationale de l'informatique et des libertés

Document : Guide de la sécurité des données personnelles — édition 2024

Utilisé dans : Chapitre 6

Éléments établis : La CNIL rappelle que l'article 32 du RGPD impose un niveau de sécurité adapté au risque et présente son guide de sécurité comme une référence utilisée pour apprécier la sécurité des traitements de données personnelles.

Les mesures recommandées comprennent notamment :

- l'utilisation de comptes nominatifs ;
- la limitation et la gestion des habilitations ;
- l'authentification des utilisateurs ;
- la sécurisation des serveurs et des réseaux ;
- le chiffrement des échanges ;
- la journalisation des opérations ;
- l'analyse des risques ;
- la gestion des incidents et violations de données ;
- la sauvegarde et la capacité de restauration ;
- le maintien d'un plan de continuité et de reprise ;
- des examens réguliers de l'efficacité des mesures de sécurité.

La CNIL recommande également de revoir régulièrement les analyses de risques afin de tenir compte de l'évolution du traitement et des menaces.

Portée pour l'enquête : L'obligation de sécurité ne se limite pas à empêcher l'accès direct à une base de données.
Elle implique une défense organisée dans la durée portant notamment sur les identités, les habilitations, les échanges, la journalisation, la détection des incidents, la résilience et l'évolution des menaces.

Lien :

- https://www.cnil.fr/fr/guide-de-la-securite-des-donnees-personnelles

---

S51 CJUE — SCHUFA : un score automatisé peut lui-même constituer une décision automatisée lorsqu'il joue un rôle déterminant

Organisme : Cour de justice de l'Union européenne

Document : Arrêt du 7 décembre 2023, SCHUFA Holding (Scoring), C-634/21

Utilisé dans : Chapitre 6

Éléments établis : La Cour de justice a interprété l'article 22, paragraphe 1 du RGPD concernant l'établissement automatisé d'un score utilisé ensuite par un tiers pour prendre une décision concernant une personne.
La Cour juge que l'établissement automatisé d'une valeur de probabilité fondée sur des données personnelles peut constituer lui-même une « décision individuelle automatisée » au sens de l'article 22 lorsque la décision prise ultérieurement par un tiers dépend de manière déterminante de cette valeur.
Cette jurisprudence montre que l'existence formelle d'une intervention humaine ou d'une décision ultérieure prise par un tiers ne suffit pas nécessairement à exclure l'application de l'article 22.
L'influence concrète du résultat automatisé sur la décision finale doit être examinée.

Portée pour l'enquête : La présence d'un agent humain à la fin d'une chaîne algorithmique ne permet pas, à elle seule, de conclure que la décision finale échappe nécessairement au régime applicable aux décisions automatisées.
Il faut notamment déterminer si l'agent dispose d'une capacité réelle d'analyse et de remise en cause du résultat produit par l'algorithme ou si ce résultat joue, en pratique, un rôle déterminant dans la décision finale.
Cette jurisprudence ne démontre pas que CFVR relève actuellement de l'article 22.
Elle fournit en revanche un critère juridique permettant d'examiner l'influence réelle des signalements, scores, classifications ou listes produits par un traitement algorithmique sur une décision ultérieure.

Lien :

- https://curia.europa.eu/juris/liste.jsf?num=C-634/21

S52 CJUE — droit à une explication compréhensible de la logique d'une décision automatisée

Organisme : Cour de justice de l'Union européenne

Document : Arrêt du 27 février 2025, Dun & Bradstreet Austria, C-203/22

Utilisé dans : Chapitre 6

Éléments établis : La Cour de justice précise la portée du droit d'accès aux « informations utiles concernant la logique sous-jacente » prévu par l'article 15, paragraphe 1, point h) du RGPD dans le cadre d'une prise de décision automatisée.
La personne concernée doit pouvoir obtenir des informations pertinentes lui permettant de comprendre la procédure et les principes effectivement appliqués à ses données personnelles afin d'obtenir le résultat automatisé.
La Cour précise que la complexité des opérations réalisées ne peut pas dispenser le responsable du traitement de son obligation de fournir une explication compréhensible.
La simple communication d'une formule mathématique complexe ou, à l'inverse, une description exhaustive et technique de toutes les étapes de l'algorithme ne constitue pas nécessairement une explication suffisamment intelligible.
Dans le contexte d'un profilage, la Cour indique notamment qu'une explication peut permettre de comprendre dans quelle mesure une variation des données utilisées aurait conduit à un résultat différent.

Portée pour l'enquête : Lorsqu'un traitement relève du régime des décisions automatisées prévu par le RGPD, la transparence ne peut pas être satisfaite par la seule affirmation qu'un algorithme ou un modèle est utilisé.
La personne concernée doit pouvoir comprendre de manière intelligible comment ses données ont contribué au résultat qui la concerne.
Cette jurisprudence devient particulièrement pertinente pour des systèmes utilisant des modèles complexes, y compris lorsque leur fonctionnement interne rend l'explication plus difficile.

Lien :

- https://curia.europa.eu/juris/liste.jsf?num=C-203/22

S53 CJUE — traitement de données à des fins fiscales : nécessité, minimisation et interdiction d'une collecte générale et indifférenciée

Organisme : Cour de justice de l'Union européenne

Document : Arrêt du 24 février 2022, Valsts ieņēmumu dienests (Traitement des données personnelles à des fins fiscales), C-175/20

Utilisé dans : Chapitre 6

Éléments établis : La Cour de justice examine directement l'application du RGPD à une collecte de données personnelles réalisée par une administration fiscale dans le cadre de ses missions.
Elle juge qu'une administration fiscale reste soumise aux principes de l'article 5 du RGPD lorsqu'elle collecte auprès d'un opérateur économique une quantité importante de données personnelles.
La Cour rappelle que les dérogations et limitations au principe de protection des données doivent rester limitées à ce qui est strictement nécessaire.

Elle en déduit que le responsable du traitement, y compris lorsqu'il agit dans le cadre d'une mission d'intérêt public :

- ne peut pas procéder de manière générale et indifférenciée à la collecte de données personnelles ;
- doit s'abstenir de collecter les données qui ne sont pas strictement nécessaires aux finalités poursuivies ;
- doit rechercher une minimisation aussi importante que possible de la quantité de données collectées ;
- doit limiter la période de collecte à ce qui est strictement nécessaire à l'objectif d'intérêt général poursuivi.

La Cour précise également que le responsable du traitement doit être en mesure de démontrer le respect de ces principes.
Elle indique enfin que la réglementation servant de base au traitement doit prévoir des règles claires et précises concernant la portée et l'application de la mesure ainsi que des garanties minimales permettant de protéger les personnes contre les risques d'abus.

Portée pour l'enquête : L'existence d'une mission fiscale d'intérêt général ne suffit donc pas à justifier n'importe quelle quantité de données ou n'importe quelle durée de traitement.
L'administration doit pouvoir justifier la nécessité des données au regard des finalités précises poursuivies et démontrer la minimisation du traitement.
Cette jurisprudence fournit un critère particulièrement pertinent pour examiner l'intégration massive de données issues de la facturation électronique et leur rapprochement avec d'autres sources dans CFVR.

Lien :

- https://curia.europa.eu/juris/liste.jsf?num=C-175/20

S54 Loi Informatique et Libertés — restrictions des droits en matière fiscale et exercice par l'intermédiaire de la CNIL

Organisme : République française

Document : Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés — articles 52 et 118

Utilisé dans : Chapitre 6

Éléments établis : Pour les traitements mis en œuvre par les administrations publiques ou les personnes chargées d'une mission de service public ayant pour mission de contrôler ou recouvrer des impositions, l'article 52 permet que les droits d'accès, de rectification et d'effacement soient exercés selon la procédure particulière prévue à l'article 118 lorsque l'acte instituant le traitement prévoit de telles restrictions.
Dans cette procédure, la demande est adressée à la CNIL.
La Commission désigne un membre appartenant ou ayant appartenu au Conseil d'État, à la Cour de cassation ou à la Cour des comptes afin de mener les investigations utiles et de faire procéder, lorsque cela est nécessaire, aux modifications appropriées.
La CNIL informe la personne qu'il a été procédé aux vérifications nécessaires et de son droit de former un recours juridictionnel.
Lorsque la Commission constate, en accord avec le responsable du traitement, que la communication des données ne met pas en cause les finalités protégées par le dispositif, certaines informations peuvent être communiquées à la personne.

Portée pour l'enquête : Le droit français prévoit donc qu'en matière fiscale certains droits reconnus aux personnes puissent être restreints afin de ne pas compromettre les finalités du traitement.
Ces restrictions ne suppriment pas tout contrôle : une procédure particulière d'exercice des droits par l'intermédiaire de la CNIL et un recours juridictionnel sont prévus.
Cette architecture crée cependant une différence importante entre l'existence juridique d'un droit et la quantité d'informations que la personne concernée peut effectivement obtenir directement sur le traitement dont elle fait l'objet.

Lien :

- https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460

S55 Règlement eIDAS 2 — portefeuille européen d'identité numérique et garanties de cloisonnement

Organisme : Union européenne

Document : Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique

Utilisé dans : Chapitre 6

Éléments établis : Le portefeuille européen d'identité numérique doit permettre à l'utilisateur de demander, obtenir, sélectionner, combiner, stocker, supprimer, partager et présenter des données d'identification et des attestations électroniques d'attributs.

Le règlement impose notamment :

- le contrôle de l'utilisateur sur les données présentées ;
- la divulgation sélective des attributs ;

- la possibilité d'utiliser des pseudonymes lorsque l'identification n'est pas juridiquement requise ;
- un historique permettant à l'utilisateur de consulter les parties utilisatrices avec lesquelles il a établi une connexion et, le cas échéant, les données échangées ;
- l'identification et l'authentification des parties utilisatrices ;
- l'enregistrement préalable de la nature des données qu'une partie utilisatrice prévoit de demander ;
- l'interdiction pour cette partie de demander d'autres données que celles déclarées ;
- des mécanismes permettant de signaler des demandes suspectes ou potentiellement illicites aux autorités de protection des données.

Le règlement prévoit également une garantie d'« inobservabilité » : le fournisseur du portefeuille ne doit pas collecter des informations non nécessaires sur son utilisation ni disposer d'une visibilité générale sur les transactions de l'utilisateur.
Le fournisseur ne doit pas combiner les données d'identification ou autres données personnelles liées au portefeuille avec les données provenant d'autres services qu'il fournit ou de services tiers lorsqu'elles ne sont pas nécessaires au service du portefeuille, sauf demande expresse de l'utilisateur.
Les fournisseurs d'attestations électroniques d'attributs sont également soumis à des obligations de séparation des données.
Enfin, l'accès aux services publics ou privés ne doit pas être restreint ou rendu désavantageux du seul fait qu'une personne n'utilise pas le portefeuille européen d'identité numérique. Des moyens alternatifs d'identification et d'authentification doivent rester disponibles.

Portée pour l'enquête : Le cadre européen de l'identité numérique prévoit donc expressément plusieurs protections destinées à empêcher que le portefeuille devienne, par lui-même, un outil général d'observation et de centralisation des activités de son utilisateur.
Mais le portefeuille est également conçu pour présenter, sous le contrôle de l'utilisateur, plusieurs attestations et attributs à des parties utilisatrices et pour interagir avec des services publics et privés.
La protection repose donc largement sur le contrôle des finalités, des accès, des demandes d'attributs, du consentement ou de la demande de l'utilisateur et du cloisonnement entre services.

Lien :

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32024R1183

S56 Règlement ESPR — passeport numérique de produit, interopérabilité et protection des données clients

Organisme : Union européenne

Document : Règlement (UE) 2024/1781 du Parlement européen et du Conseil du 13 juin 2024 établissant un cadre pour la fixation d'exigences en matière d'écoconception pour des produits durables

Utilisé dans : Chapitre 6

Éléments établis : Le règlement établit le cadre du passeport numérique de produit.
Le DPP est associé à un identifiant unique de produit et ses données doivent notamment être structurées, lisibles par machine, consultables et transférables au moyen d'un réseau d'échange de données ouvert et interopérable.
Le système est conçu pour améliorer la traçabilité des produits tout au long de la chaîne de valeur.

Les droits d'accès aux données doivent être définis en fonction des catégories d'acteurs et des groupes de produits concernés.
Le règlement prévoit explicitement que les données personnelles relatives aux clients ne doivent pas être stockées dans le passeport numérique de produit sans leur consentement explicite conformément au RGPD.
Le DPP doit pouvoir fonctionner au niveau du modèle, du lot ou de l'article selon les exigences applicables au groupe de produits.
Le système est conçu comme un système de données décentralisé, tandis que la Commission doit maintenir un registre des identifiants uniques associés aux produits mis sur le marché ou mis en service.
Les autorités compétentes disposent d'accès destinés notamment au contrôle de la conformité.

Portée pour l'enquête : Le DPP est donc conçu comme une infrastructure interopérable de données relatives au produit et à son cycle de vie, mais il comporte une séparation juridiquement importante entre l'information relative au produit et les données personnelles relatives au client.
Le règlement ne crée pas, par lui-même, un « passeport environnemental individuel » du consommateur.
La présence d'un identifiant unique au niveau du produit ou de l'article ne signifie pas que cet identifiant est juridiquement rattaché à l'identité de son acheteur.
Une telle association devrait résulter d'un autre traitement disposant de sa propre finalité et de sa propre base juridique.

Lien :

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32024R1781

S57 Proposition de règlement sur l'euro numérique — identité, confidentialité, paiements conditionnels et interdiction de la monnaie programmable

Organismes : Commission européenne / Banque centrale européenne

Document principal : COM(2023) 369 final — Proposition de règlement établissant l'euro numérique

Statut au 3 septembre 2026 : procédure législative en cours ; règlement non encore adopté.

Utilisé dans : Chapitre 6

Éléments établis :

La proposition établit une distinction explicite entre :

- la monnaie programmable ;
- et les paiements conditionnels.

La monnaie programmable, entendue comme une monnaie dont les unités comporteraient intrinsèquement des limitations de pleine fongibilité, doit être interdite.
L'euro numérique ne doit donc pas être limité intrinsèquement à certains biens, certains services, certaines périodes ou certains bénéficiaires.
En revanche, la proposition autorise les paiements conditionnels.
Une opération conditionnelle est une opération dont l'instruction est déclenchée automatiquement lorsque des conditions prédéfinies et convenues entre le payeur et le bénéficiaire sont remplies.
La proposition permet à la BCE de fournir des règles, standards et fonctionnalités techniques nécessaires à

l'exécution de telles opérations, notamment la réservation de fonds.
La proposition prévoit également que les services front-end de l'euro numérique soient interopérables ou intégrés aux portefeuilles européens d'identité numérique.
Elle prévoit plusieurs garanties relatives à la vie privée et à la protection des données.
Pour les paiements hors ligne, l'architecture proposée vise un niveau de confidentialité proche de celui des espèces.
Pour les paiements en ligne, les données transmises à la BCE, aux banques centrales nationales ou aux prestataires de services d'appui doivent faire l'objet de mesures empêchant l'identification directe des utilisateurs individuels dans les conditions prévues par le texte.
La proposition prévoit également des traitements nécessaires notamment à l'application des limites de détention, à l'exécution des paiements, à la prévention de la fraude, aux obligations de lutte contre le blanchiment et le financement du terrorisme et à certaines obligations fiscales.

Portée pour l'enquête : L'interdiction de la monnaie programmable constitue une garantie substantielle : l'euro numérique ne doit pas devenir une monnaie dont la valeur ou l'utilisabilité dépend intrinsèquement de la nature des biens ou services achetés.
Cette interdiction ne doit cependant pas être confondue avec une interdiction générale des paiements conditionnels.
Le cadre proposé prévoit au contraire explicitement une infrastructure capable d'exécuter des paiements déclenchés automatiquement lorsque des conditions convenues sont satisfaites.
Il prévoit également une interface juridique et technique entre l'euro numérique et le portefeuille européen d'identité numérique.
Ces capacités ne démontrent pas qu'une donnée environnementale, un DPP ou un attribut d'identité soit destiné à conditionner un paiement.
Elles établissent en revanche que certaines des interfaces techniques nécessaires à des services de paiement conditionnels et à l'utilisation d'une identité numérique sont explicitement envisagées dans l'architecture proposée.

Liens :

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52023PC0369
- https://eur-lex.europa.eu/legal-content/FR/HIS/?uri=CELEX:52023PC0369

S58 Évolution successive du périmètre juridique du traitement CFVR depuis 2014

Organisme : Direction générale des finances publiques / Légifrance

Documents :

- arrêté du 21 février 2014 portant création du traitement « ciblage de la fraude et valorisation des requêtes » (CFVR) ;
- arrêté du 28 août 2017 modifiant le traitement CFVR ;
- arrêté du 8 mars 2021 modifiant le traitement CFVR ;
- arrêté du 21 octobre 2024 modifiant le traitement CFVR ;
- arrêté du 10 juillet 2026 modifiant le traitement CFVR.

Utilisé dans : Chapitre 6

Éléments établis : Le traitement CFVR n'est pas demeuré juridiquement identique depuis sa création en 2014.

Son cadre réglementaire a fait l'objet de plusieurs modifications successives portant notamment sur :

- les catégories de personnes concernées ;
- les catégories de données traitées ;
- les sources alimentant le traitement ;
- les finalités ou modalités d'exploitation ;
- les destinataires ;
- les échanges avec d'autres traitements ou administrations ;
- les durées de conservation ;
- les modalités d'exercice de certains droits.

En 2017, le traitement a notamment été étendu, à titre expérimental, aux fraudes relatives aux particuliers et a été autorisé à utiliser des données concernant des particuliers sans lien avec une entreprise.
En 2021, son articulation avec les traitements permettant la collecte et l'exploitation de certaines données rendues publiques sur les plateformes en ligne a été intégrée à son cadre.
Une nouvelle modification est intervenue en 2024.
En juillet 2026, le cadre a de nouveau été modifié afin notamment d'intégrer les données issues de la facturation électronique, de nouvelles sources de données et certaines transmissions aux organismes de sécurité sociale.

Portée pour l'enquête : L'historique de CFVR démontre qu'un traitement public peut conserver sa continuité institutionnelle tout en voyant évoluer, par modifications juridiques successives, son périmètre de données, de personnes concernées, de sources, de destinataires et d'usages.
Cette évolution n'est pas en elle-même irrégulière : chaque modification demeure soumise au cadre juridique applicable.
Elle montre néanmoins qu'une garantie fondée sur le périmètre juridique actuel d'une infrastructure ne constitue pas une garantie d'immuabilité de ce périmètre.

Liens :

- 2014 : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000028684963
- 2017 : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000036012682
- 2021 : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043426791
- 2024 : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000050771533
- 2026 : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000054450882