Dossier Peppol / ViDA / Facturation électronique obligatoire

Enquête probatoire sur l’infrastructure obligatoire de traçabilité économique

Table des matières

1. Thèse centrale du dossier

La réforme de la facturation électronique ne doit pas être analysée comme une simple modernisation comptable.

Elle organise une infrastructure obligatoire de circulation de données économiques : factures, transactions, données de paiement, plateformes agréées, annuaire, concentrateur fiscal, interopérabilité Peppol, reporting fiscal et trajectoire européenne ViDA.

Le cœur du dossier est le suivant :

> Plus le dispositif avance, plus ses décideurs et opérateurs s’exposent.
> Mais ils ne s’exposent juridiquement que si la preuve est créée : demandes écrites, mises en connaissance, questions précises, archivage des réponses, exploitation des silences.

La méthode du dossier est donc :

> STOP • PAUSE • ÉCRITS • TRACE.

On ne se contente pas d’alerter.
On met en connaissance.
On demande les bases légales.
On exige les études.
On archive les réponses.
On exploite les silences.
On prépare les recours.

2. Faits pivots établis et contexte d’antériorité

2.1. Faits pivots établis

Les éléments suivants constituent, à ce stade, les faits structurants du dossier. Ils doivent être conservés comme base probatoire, chacun devant être accompagné de sa source archivée, datée et, si possible, sauvegardée en PDF.

Fait établi	Source à archiver	Usage probatoire
Le Portail Public de Facturation a été recentré autour de l’annuaire et du concentrateur de données, après le communiqué du 16 octobre 2024.	AIFE / ministère de l’Économie	Établir que la solution publique initialement envisagée comme outil complet a été réduite ou recentrée. L’AIFE indique que le recentrage porte sur la fonction d’annuaire et celle de concentrateur pour la transmission des données de facturation et de transaction à l’administration fiscale.
Les entreprises devront recourir à des plateformes agréées pour saisir, déposer ou transmettre leurs factures électroniques et les données obligatoires de e-reporting.	impots.gouv.fr	Établir l’obligation de passage par des plateformes agréées à compter du calendrier officiel de déploiement.
Le Code général des impôts prévoit que l’émission, la transmission et la réception des factures électroniques s’effectuent en recourant à une plateforme agréée.	CGI, article 289 bis	Identifier la base légale française principale à encadrer, questionner ou contester.
Les données des factures électroniques émises en application de l’article 289 bis sont transmises à	CGI, article 289 E	Point central : la réforme ne vise pas seulement l’échange de factures entre entreprises, mais aussi la transmission de données à l’administration.

Fait établi	Source à archiver	Usage probatoire
l’administration par la plateforme agréée choisie par l’assujetti.		
Les données relatives au paiement de certaines opérations doivent être communiquées à l’administration sous forme électronique, selon les normes définies.	CGI, article 290 A	Montrer que le dispositif ne concerne pas seulement la facture, mais aussi certaines données de paiement.
La DGFiP est devenue France Peppol Authority le 8 juillet 2025.	OpenPeppol / DGFiP	Établir l’arrimage officiel de la France au cadre Peppol.
OpenPeppol est une AISBL de droit belge, structurée comme une organisation pilotée par ses membres.	OpenPeppol	Identifier un enjeu de gouvernance privée ou hybride d’un standard devenu structurant.
OpenPeppol indique que des volontaires issus d’organisations membres jouent un rôle de direction dans ses activités de gestion et de développement.	OpenPeppol	Établir la nécessité d’instruire les risques de conflits d’intérêts, d’autorégulation et de capture normative.
Le paquet ViDA a été adopté le 11 mars 2025 et doit être déployé progressivement jusqu’en janvier 2035.	Commission européenne	Situer la réforme française dans une trajectoire européenne plus large.
Le Parlement européen a approuvé les règles ViDA par 589 voix pour, 42 contre et 10 abstentions.	Parlement européen / votes nominaux	Permettre la traçabilité politique des votes et des responsabilités démocratiques.
La France a déjà été exposée à plusieurs fuites ou incidents de données significatifs.	Sources cyber / CNIL / ANSSI / presse spécialisée / autorités publiques	Justifier une exigence renforcée d’audit cyber, de cartographie des flux, de sécurité, d’hébergement et de responsabilité. Cybernews classe la France comme le pays européen le plus touché par les fuites de données au premier semestre 2025, et l’ANTS a signalé en 2026 un incident pouvant impliquer une divulgation de données issues de comptes particuliers et professionnels.

Ces faits ne suffisent pas, pris isolément, à établir une faute ou une infraction. En revanche, leur combinaison fait apparaître un enjeu juridique majeur : une fonction économique essentielle — facturer, transmettre, recevoir, déclarer — devient dépendante d’une infrastructure technique obligatoire, impliquant des plateformes agréées, des flux de données structurées, des données de paiement, une gouvernance technique complexe et des risques de dépendance à des acteurs privés ou étrangers.

Le point central du dossier est donc le suivant :

> La réforme ne peut pas être analysée uniquement comme une modernisation administrative. Elle doit être examinée comme une infrastructure obligatoire de traçabilité économique, dont la nécessité, la proportionnalité, la souveraineté, la sécurité, la gouvernance, les coûts, les alternatives et les recours doivent être démontrés par écrit.

2.2. Niveaux de preuve à distinguer

Pour éviter toute fragilisation du dossier, il convient de distinguer quatre niveaux.

Niveau	Qualification	Usage dans le dossier
Niveau 1	Fait officiel établi	Peut être affirmé fermement, avec source archivée.
Niveau 2	Risque juridique sérieux	Doit être formulé comme un risque à instruire par demandes écrites.
Niveau 3	Hypothèse pénale à instruire	Ne doit pas être affirmée comme constituée ; elle sert à orienter la collecte de preuves.
Niveau 4	Contexte d'antériorité	Ne prouve pas l'illégalité, mais justifie un audit renforcé et une exigence accrue de transparence.

Cette distinction est indispensable. Elle permet de conserver une ligne offensive sans surqualification prématurée.

2.3. Antériorité institutionnelle et numérique : pourquoi Peppol/ViDA doit faire l'objet d'un audit renforcé

La réforme Peppol/ViDA ne doit pas être examinée comme un objet technique isolé. Elle intervient dans un contexte déjà marqué par plusieurs précédents de fragilisation de la souveraineté, de centralisation de données sensibles, d'externalisation de fonctions stratégiques, de dépendance à des infrastructures privées ou étrangères, et de défiance croissante envers la capacité des institutions à garantir un contrôle effectif, indépendant et contradictoire.

Cette antériorité ne sert pas à affirmer, à elle seule, une illégalité constituée. Elle sert à poser une exigence renforcée de justification.

Lorsqu'un dispositif obligatoire organise la circulation structurée de données économiques, de données de facturation, de données de transaction et de données de paiement, les autorités doivent pouvoir démontrer :

- le besoin réel ;
- la nécessité ;
- la proportionnalité ;
- la sécurité effective ;
- la souveraineté des flux ;
- l'indépendance des audits ;
- l'absence ou la prévention des conflits d'intérêts ;
- les alternatives disponibles ;
- les voies de recours effectives ;
- les responsabilités en cas de fuite, blocage, usurpation, erreur ou préjudice.

Le point de vigilance n’est donc pas seulement la facturation électronique. Le point de vigilance est la transformation progressive d’une obligation fiscale en infrastructure obligatoire de traçabilité économique, alors même que plusieurs précédents ont déjà montré la fragilité des garanties publiques dans des domaines sensibles.

A. Précédents de rupture ou de fragilisation à prendre en compte

Terrain d’antériorité	Enseignement utile	Usage probatoire dans le dossier Peppol/ViDA
Affaiblissement du consentement démocratique sur des choix structurants	Un dispositif peut être juridiquement habillé tout en demeurant politiquement ou démocratiquement contestable.	Exiger la traçabilité des décisions, votes, arbitrages, consultations et débats.
Normalisation des régimes d’exception	Ce qui est présenté comme temporaire, technique ou nécessaire peut devenir durable et structurant.	Vérifier que le reporting fiscal ne devienne pas une surveillance économique permanente.
Externalisation de fonctions sensibles	Des missions proches de la souveraineté peuvent être transférées à des acteurs privés ou hybrides.	Questionner le recentrage du Portail Public de Facturation et le rôle des plateformes privées.
Centralisation massive de données sensibles	Toute centralisation augmente les enjeux de sécurité, d’accès, d’hébergement, de contrôle et de responsabilité.	Exiger AIPD, audits cyber, cartographie des flux, sous-traitants et pays d’accès.
Dépendance à des acteurs privés ou étrangers	Les risques ne sont pas seulement techniques : ils peuvent être économiques, stratégiques, juridiques et géopolitiques.	Instruire les risques liés aux acteurs étrangers, aux lois extraterritoriales et à la gouvernance Peppol.
Fuites de données répétées	L’argument de modernisation ne suffit pas si la sécurité effective n’est pas démontrée.	Demander les garanties en cas de fuite, d’usurpation, de fraude, de blocage ou d’accès non autorisé.
Influence des lobbies et conflits d’intérêts	La participation d’acteurs privés à la fabrication ou à la gouvernance de standards devenus obligatoires impose un contrôle renforcé.	Demander qui décide, qui audite, qui profite, qui contrôle et comment les conflits d’intérêts sont prévenus.

B. Utilité juridique de cette antériorité

Cette antériorité permet d’éviter une lecture naïve du dossier. Elle ne prouve pas automatiquement une infraction, mais elle justifie de poser les questions avec un niveau d’exigence renforcé.

Les questions prioritaires sont les suivantes :

1. Quel besoin réel et chiffré justifie la réforme ?
2. Pourquoi une solution publique complète n’a-t-elle pas été maintenue ?
3. Quelles alternatives moins intrusives ont été étudiées ?
4. Qui a décidé le recentrage du Portail Public de Facturation ?
5. Quels acteurs privés bénéficient économiquement du dispositif ?
6. Quels acteurs participent à la gouvernance technique ou normative ?
7. Quels mécanismes empêchent les conflits d’intérêts ?
8. Quels flux de données sont créés ?

9. Quelles données de paiement sont transmises ?
10. Quels sous-traitants interviennent ?
11. Quels pays d'hébergement ou d'accès sont possibles ?
12. Quels risques extraterritoriaux ont été évalués ?
13. Quelles garanties existent contre l'accès par des entités étrangères ou sous contrôle étranger ?
14. Quels recours existent en cas de fuite, blocage, erreur, usurpation ou impossibilité de facturer ?
15. Quelle responsabilité est prévue en cas de préjudice économique ?

C. Formule probatoire centrale

L'antériorité ne remplace pas la preuve. Elle fonde l'exigence de preuve.

Dans un contexte déjà marqué par des précédents de centralisation, d'externalisation, de dépendance privée, de fuites de données et de fragilisation du contrôle démocratique, les autorités ne peuvent pas se contenter d'invoquer la modernisation ou la lutte contre la fraude.

Elles doivent démontrer, pièces à l'appui :

- le besoin réel ;
- la nécessité ;
- la proportionnalité ;
- l'absence d'alternative moins intrusive ;
- la sécurité effective ;
- la souveraineté des flux ;
- l'indépendance des audits ;
- la prévention des conflits d'intérêts ;
- les garanties RGPD ;
- la protection du secret des affaires ;
- les recours effectifs ;
- les responsabilités en cas de préjudice.

À défaut, leur silence, leur refus ou leurs réponses insuffisantes pourront être conservés, annexés et produits dans le cadre des démarches, signalements ou recours légalement ouverts.

D. Transition vers la qualification juridique

Cette antériorité permet de renforcer, sans la remplacer, la qualification juridique propre du dossier.

Le sujet n'est donc pas seulement de savoir si la facturation électronique est utile. Le sujet est de savoir si l'État peut transformer une obligation fiscale en infrastructure privée ou semi-privée de traçabilité économique sans démonstration complète de nécessité, proportionnalité, souveraineté, sécurité, alternative publique et recours effectif.

3. Qualification juridique propre

À ce stade, les qualifications immédiatement solides sont :

- infrastructure obligatoire de traçabilité économique ;

- marché captif de conformité obligatoire ;
- dépendance réglementaire à des plateformes privées agréées ;
- privatisation partielle d’une infrastructure fiscale obligatoire ;
- abandon ou recentrage d’une alternative publique souveraine ;
- risque structurel de conflits d’intérêts ;
- risque d’atteinte au secret des affaires ;
- risque d’atteinte à la souveraineté économique ;
- risque de défaut de proportionnalité ;
- risque de défaut de recours effectif ;
- risque de transfert ou d’accessibilité indirecte de données économiques sensibles.

La formule centrale :

> Nous ne contestons pas par principe la modernisation administrative.
> Nous contestons la transformation d’une obligation fiscale en infrastructure privée obligatoire de traçabilité économique, sans démonstration suffisante de nécessité, de proportionnalité, de souveraineté, d’indépendance, de cybersécurité, d’alternative publique et de recours effectif.

4. Question du besoin réel

Le besoin officiel est la lutte contre la fraude à la TVA, notamment les fraudes transfrontalières et carrousel, avec un reporting numérique en temps réel. La Commission présente ViDA comme un dispositif visant notamment à adapter la TVA à l’ère numérique et à améliorer la capacité des administrations fiscales à lutter contre la fraude.

Mais juridiquement, il faut exiger :

1. le montant exact de fraude TVA visé en France ;
2. la part imputable aux factures B2B ;
3. la démonstration que le passage obligatoire par plateformes privées est nécessaire ;
4. la comparaison avec une solution publique gratuite ;
5. l’analyse du coût pour TPE, indépendants, associations et petites structures ;
6. l’analyse des risques cyber ;
7. l’analyse d’impact RGPD ;
8. l’analyse de souveraineté ;
9. les garanties en cas de fuite, blocage, usurpation ou erreur.

La faille à chercher est ici :

> Si le besoin est réel mais que la solution choisie est disproportionnée, non souveraine, coûteuse, risquée ou insuffisamment auditée, alors le dispositif devient juridiquement contestable.

5. Droits fondamentaux et textes à mobiliser

Texte	Droit protégé	Atteinte potentielle	Preuve à obtenir
DDHC art. 14	Consentement à l’impôt / contrôle de la contribution publique	Obligation fiscale transformée en dépendance technique privée	Études, débat, coût, justification

Texte	Droit protégé	Atteinte potentielle	Preuve à obtenir
DDHC art. 15	Droit de demander compte à tout agent public	Refus de transparence sur arbitrage PPF / Peppol / plateformes	Décisions, notes, audits, avis
DDHC art. 16	Garantie des droits / recours effectif	Infrastructure obligatoire sans recours clair en cas de blocage/fuite	Procédures de recours, responsabilités
DDHC art. 17	Propriété	Impossibilité de facturer = atteinte possible à créances/revenus	Cas de blocage, sanctions, refus
Constitution art. 34	Garanties fondamentales des libertés publiques	Délégation excessive à infrastructure technique privée	Textes d'application, rôle plateformes
Constitution art. 55	Supériorité des traités	Contrôle au regard CEDH / Charte UE / RGPD	Analyse conformité
Charte UE art. 7 et 8	Vie privée / données personnelles	Données clients, fournisseurs, dirigeants, paiements	Cartographie données
Charte UE art. 16	Liberté d'entreprise	Obligation de passer par tiers agréé	Coût, absence alternative
Charte UE art. 17	Propriété	Blocage économique en cas d'impossibilité de facturer	Scénarios de blocage
Charte UE art. 47	Recours effectif	Absence de recours rapide contre plateforme ou État	Procédure de contestation
Charte UE art. 52	Nécessité / proportionnalité	Mesure générale sans alternatives moins intrusives	Étude de proportionnalité
RGPD art. 5, 6, 25, 32, 35, 44 s.	Licéité, minimisation, sécurité, AIPD, transferts hors UE	Données massives, sous-traitants, accès hors UE	AIPD, registre, transferts
Code de commerce L.151-1 s.	Secret des affaires	Factures = clients, prix, volumes, stratégie commerciale	Clauses, garanties, accès
Code pénal 410-1	Intérêts fondamentaux de la Nation	Potentiel économique, données économiques sensibles	Cartographie de sensibilité économique

Le Code pénal inclut dans les intérêts fondamentaux de la Nation les éléments essentiels du potentiel scientifique et économique, notamment agricole. C'est un levier sérieux pour instruire la question des données économiques massives.

6. Qualifications pénales potentielles à instruire

Point de méthode essentiel :

> À ce stade, il ne s'agit pas d'affirmer une trahison constituée. Il s'agit d'instruire si la mise en place d'une infrastructure obligatoire de circulation de données économiques sensibles peut, selon ses flux, sous-traitants, accès, transferts, acteurs et garanties, exposer les décideurs ou opérateurs à des qualifications liées aux atteintes aux intérêts fondamentaux de la Nation.

Qualification potentielle	Conditions juridiques	Ce qui manque aujourd’hui	Action probatoire
Code pénal art. 411-1	Les faits définis aux articles 411-2 à 411-11 constituent la trahison lorsqu’ils sont commis par un Français ou un militaire au service de la France, et l’espionnage lorsqu’ils sont commis par toute autre personne.	Faits précis qualifiables.	Ne pas accuser ; instruire.
Code pénal art. 411-5	Intelligences avec puissance étrangère, entreprise ou organisation étrangère ou sous contrôle étranger, de nature à porter atteinte aux intérêts fondamentaux.	Preuve d’intelligences + atteinte potentielle caractérisée.	Demander contrats, échanges, décisions, rôles.
Code pénal art. 411-6	Livraison ou accessibilité de données, fichiers ou documents à une puissance étrangère, entreprise ou organisation étrangère ou sous contrôle étranger, si leur exploitation est de nature à porter atteinte aux intérêts fondamentaux.	Preuve d’accessibilité effective et sensibilité stratégique.	Cartographier accès, sous-traitants, hébergement, AP/SMP, certificats.
Code pénal art. 411-7	Recueil ou rassemblement de données en vue de les livrer.	Intention, destination, acteur étranger.	Demander finalités, flux, destinataires, transferts.
Secret des affaires	Information non généralement connue, ayant une valeur commerciale et faisant l’objet de mesures raisonnables de protection.	Qualification des données de facturation comme secrets selon contexte.	Demander garanties plateformes.
RGPD	Licéité, minimisation, sécurité, transferts encadrés, AIPD si risque élevé.	AIPD, flux, pays, sous-traitants, garanties.	Saisine CNIL / demandes DPO.

7. Cartographie des acteurs

Acteur	Rôle	Risque à instruire
DGFiP	Autorité fiscale, France Peppol Authority	Arbitrage, contrôle, garanties, rôle dans certificats/exigences
AIFE	PPF, annuaire, concentrateur	Pourquoi recentrage/abandon du PPF complet
Ministère de l’Économie	Décision politique et réglementaire	Arbitrage public/privé, coût, souveraineté
OpenPeppol AISBL	Gouvernance / spécifications Peppol	Gouvernance par membres, conflits d’intérêts
Plateformes agréées	Passage obligatoire des factures/données	Coûts, accès, blocages, sous-traitants
Cabinets de conseil / auditeurs	Conseil, conformité, audits	Risque de juge-partie, revenus de conformité
Fournisseurs ERP / cloud	Solutions techniques	Dépendance technique, extraterritorialité
CNIL	Données personnelles	AIPD, transferts, minimisation

Acteur	Rôle	Risque à instruire
ANSSI	Cybersécurité	Audit sécurité et souveraineté
Parlementaires / eurodéputés	Vote / contrôle politique	Traçabilité des votes et explications
CADA	Accès documents administratifs	En cas de refus de communication

8. Stratégie probatoire

Phase 1 — Mise en connaissance

Objectif : créer une trace datée.

Destinataires prioritaires :

- DGFiP ;
- AIFE ;
- ministère de l'Économie ;
- CNIL ;
- ANSSI ;
- CADA si refus ;
- plateformes agréées ;
- experts-comptables / organisations professionnelles ;
- députés, sénateurs, eurodéputés français.

Phase 2 — Questions écrites

Objectif : forcer les réponses exploitables.

Trois issues utiles :

- réponse complète : pièces obtenues ;
- réponse vague : preuve d'insuffisance ;
- silence : preuve de carence ;
- refus : ouverture CADA / CNIL / recours.

Phase 3 — Recours

- CADA pour documents publics refusés ;
- CNIL pour données personnelles, AIPD, transferts, sous-traitants ;
- recours pour excès de pouvoir contre textes d'application ;
- QPC à l'occasion d'un litige ;
- action indemnitaire en cas de préjudice ;
- signalement parquet uniquement si éléments précis d'accessibilité ou de livraison de données sensibles.

8 bis. Scénarios de préjudice à anticiper

Scénario	Préjudice possible	Question probatoire à poser
Plateforme indisponible	Impossibilité de facturer, retard de paiement, perte de chiffre d'affaires	Quelle procédure de secours ? Quelle indemnisation ?
Facture frauduleuse via le réseau	Paiement détourné, litige client, perte financière	Qui authentifie l'émetteur ? Qui indemnise ?
Fuite de données clients/fournisseurs	Atteinte au secret des affaires, perte concurrentielle	Quelle responsabilité ? Quelle notification ?
Blocage ou suspension d'accès à une plateforme	Impossibilité d'exister commercialement	Quel recours urgent ? Quelle alternative immédiate ?
Erreur de routage	Facture non reçue ou envoyée au mauvais destinataire	Qui prouve la réception ? Qui corrige ?
Sous-traitant hors UE ou accès extraterritorial	Risque RGPD, souveraineté, accès par autorité étrangère	Quelles garanties ? Quels pays ? Quels contrats ?
Croisement futur avec scoring fiscal, identité numérique, euro numérique ou gel administratif	Profilage économique, restriction de droits, dépendance numérique	Quelle interdiction de réutilisation ? Quelle base légale ?
Panne longue ou cyberattaque	Paralysie administrative et économique	Quel plan de continuité ? Quel audit ANSSI ?
Plateforme en conflit d'intérêts	Dépendance économique et absence d'indépendance	Qui audite l'auditeur ? Qui contrôle les liens d'intérêts ?

8 ter. Demandes minimales non négociables

Les demandes minimales à obtenir sont les suivantes :

1. Communication de la décision de recentrage du Portail Public de Facturation.
2. Communication des études d'impact.
3. Communication des avis CNIL / ANSSI, s'ils existent.
4. Cartographie complète des flux.
5. Liste des sous-traitants.
6. Pays d'hébergement et pays d'accès.
7. Procédure de secours en cas de panne.
8. Procédure de recours en cas de blocage.
9. Responsabilité en cas de fuite.
10. Garantie contre les conflits d'intérêts.
11. Garantie contre l'accès par entités étrangères ou sous contrôle étranger.
12. Garantie contre le croisement futur avec identité numérique, euro numérique, scoring fiscal ou gel administratif.
13. Identification des responsables fonctionnels compétents.
14. Définition des délais de réponse et d'indemnisation en cas de préjudice.
15. Liste des audits réalisés et identité des auditeurs.

9. Liste des documents à demander

À la DGFiP / AIFE / ministère :

1. décision de recentrage ou d'abandon du PPF complet ;
2. notes préparatoires ;
3. études de coût ;
4. études de risques ;
5. étude de proportionnalité ;
6. analyse de souveraineté ;
7. analyse d'impact RGPD ;
8. avis CNIL ;
9. avis ANSSI ;
10. cartographie des flux ;
11. liste des plateformes agréées ;
12. critères d'agrément ;
13. audits de conformité ;
14. gestion des conflits d'intérêts ;
15. garanties contre transferts hors UE ;
16. procédures en cas de fuite ;
17. procédures en cas de blocage de facturation ;
18. alternative gratuite ou publique pour TPE, indépendants et associations ;
19. modalités de recours ;
20. responsabilités en cas de préjudice.

10. Questionnaire DGFiP / AIFE

Objet : Demande de communication et de justification — Facturation électronique, PPF, Peppol, plateformes agréées, souveraineté et données économiques

Questions essentielles :

1. Qui a décidé le recentrage du PPF ?
2. À quelle date exacte ?
3. Sur quelle base juridique ?
4. Quels documents ont motivé cette décision ?
5. Quel était le coût estimé du PPF complet ?
6. Quel coût est désormais transféré aux entreprises ?
7. Pourquoi une solution publique gratuite complète n'a-t-elle pas été maintenue ?
8. Quelles alternatives moins intrusives ont été étudiées ?
9. Quelle analyse de proportionnalité a été réalisée ?
10. Quelle AIPD RGPD a été menée ?
11. Quels avis CNIL / ANSSI existent ?
12. Quelles données de facturation sont transmises à l'administration ?
13. Quelles données de transaction sont transmises ?
14. Quelles données de paiement sont transmises ?
15. Quels sous-traitants peuvent intervenir ?
16. Les données ou métadonnées peuvent-elles sortir de l'Union européenne ?

17. Quels recours existent en cas de blocage, fuite, erreur ou refus de plateforme ?
18. Quelles garanties contre les conflits d'intérêts ?
19. Quelles plateformes agréées sont aussi membres OpenPeppol ?
20. Qui contrôle l'indépendance des audits ?
21. Les auditeurs sont-ils eux-mêmes membres de l'écosystème Peppol ou prestataires de plateformes agréées ?
22. Des cabinets de conseil ont-ils conseillé à la fois l'État, des plateformes ou des entreprises bénéficiaires du dispositif ?
23. Existe-t-il une déclaration de conflits d'intérêts ?
24. Qui audite les auditeurs ?
25. Quelle responsabilité en cas d'impossibilité de facturer ?
26. Quelle garantie contre un croisement futur avec identité numérique, euro numérique, scoring fiscal ou gel administratif ?

11. Questionnaire CNIL / ANSSI

Objet : Demande d'examen RGPD et cybersécurité — Facturation électronique obligatoire, données de transaction, données de paiement, plateformes agréées et transferts

Questions :

1. Une analyse d'impact RGPD globale a-t-elle été réalisée ?
2. Par qui ?
3. Sur quels périmètres ?
4. Quelles données personnelles sont concernées ?
5. Quelles données de paiement sont concernées ?
6. Quels responsables de traitement ?
7. Quels sous-traitants ?
8. Quels transferts hors UE ?
9. Quels accès extraterritoriaux possibles ?
10. Quelles garanties appropriées ?
11. Quelle minimisation des données ?
12. Quelle durée de conservation ?
13. Quels droits pour les personnes physiques concernées ?
14. Quelle procédure en cas de fuite ?
15. Quelle procédure en cas d'usurpation ?
16. Quelle information des entreprises clientes ?
17. Quelle sanction en cas de manquement de plateforme ?
18. Quels audits cyber sont exigés ?
19. Quels critères ANSSI sont applicables ou recommandés ?
20. Quels plans de continuité sont imposés en cas de cyberattaque, panne ou indisponibilité ?

La CNIL rappelle que les transferts hors UE doivent assurer un niveau de protection suffisant et être encadrés par les outils du chapitre V du RGPD.

12. Questionnaire plateformes agréées

1. Où sont hébergées les données ?

2. Quels sous-traitants interviennent ?
3. Quels pays d’accès sont possibles ?
4. Êtes-vous membre OpenPeppol ?
5. Êtes-vous Access Point / SMP ?
6. Quels certificats utilisez-vous ?
7. Qui peut accéder aux métadonnées ?
8. Quels logs sont conservés ?
9. Quelle durée de conservation ?
10. Quels transferts hors UE ?
11. Quelle AIPD avez-vous réalisée ?
12. Quelle certification sécurité détenez-vous ?
13. Quelle responsabilité en cas de fuite ?
14. Quelle responsabilité en cas de facture frauduleuse ?
15. Quelle responsabilité en cas de blocage ?
16. Quelle indemnisation en cas de préjudice ?
17. Comment contester une erreur ?
18. Comment récupérer ses données ?
19. Comment changer de plateforme ?
20. Quelle garantie contre croisement avec scoring, identité numérique, euro numérique ou gel administratif ?
21. Quels cabinets ont audité votre conformité ?
22. Ces cabinets ont-ils des liens avec OpenPeppol, la DGFiP, des ERP, des plateformes agréées ou des fournisseurs concurrents ?
23. Quelle procédure d’urgence existe si votre plateforme devient indisponible ?
24. Quelle garantie contractuelle donnez-vous contre l’accès par une entité étrangère ou sous contrôle étranger ?

13. Mise en connaissance juridique préalable

Objet : Mise en connaissance juridique préalable — Facturation électronique obligatoire, plateformes agréées, Peppol, souveraineté économique, données sensibles et responsabilités

Madame, Monsieur,

Je vous adresse la présente afin de vous mettre formellement en connaissance des interrogations juridiques, économiques, numériques, fiscales, probatoires et constitutionnelles soulevées par la réforme de la facturation électronique obligatoire.

Cette réforme ne se limite pas à la dématérialisation de factures. Elle organise une infrastructure obligatoire de circulation de données économiques structurées : factures, transactions, données de paiement, plateformes agréées, annuaire, concentrateur fiscal, interopérabilité, certificats, routage et reporting.

Elle intervient, en outre, dans un contexte de défiance légitime lié à la multiplication des dispositifs numériques obligatoires, aux précédents de centralisation de données sensibles, aux risques de fuites de données, aux enjeux de souveraineté économique, ainsi qu’aux risques de conflits d’intérêts dans la fabrication ou la gouvernance de standards techniques devenus obligatoires.

Cette antériorité ne vaut pas accusation. Elle justifie en revanche une exigence renforcée de transparence, d'audit, de proportionnalité et de responsabilité.

Plusieurs points appellent donc une justification écrite :

- le besoin réel et chiffré justifiant la réforme ;
- les montants de fraude visés ;
- les alternatives moins intrusives étudiées ;
- les raisons du recentrage du Portail Public de Facturation ;
- l'absence ou le maintien d'une alternative publique complète, gratuite et souveraine ;
- l'obligation de passage par plateformes agréées ;
- l'arrimage au cadre Peppol ;
- la gouvernance de l'écosystème ;
- les données collectées ;
- les données de facturation transmises à l'administration ;
- les données de transaction et de paiement transmises ;
- les sous-traitants ;
- l'hébergement ;
- les flux et métadonnées ;
- les transferts éventuels hors Union européenne ;
- les risques extraterritoriaux ;
- les conflits d'intérêts ;
- les audits de cybersécurité ;
- l'indépendance des auditeurs ;
- les analyses d'impact RGPD ;
- les garanties de souveraineté ;
- les recours effectifs ;
- les responsabilités en cas de fuite, erreur, fraude, usurpation, blocage ou impossibilité de facturer.

Je vous demande en conséquence de me communiquer les bases légales, études d'impact, audits, analyses de proportionnalité, avis, cartographies de flux, garanties de souveraineté, procédures de recours et mécanismes de responsabilité relatifs à ce dispositif.

Je rappelle que les données économiques structurées peuvent relever, selon les cas, de la protection des données personnelles, du secret des affaires, de la liberté d'entreprendre, du droit de propriété, du recours effectif et, selon leur nature, leur destination ou leur accessibilité, des intérêts fondamentaux de la Nation.

À ce stade, il ne s'agit pas d'affirmer une infraction constituée. Il s'agit d'obtenir les garanties nécessaires permettant d'écarter tout risque d'atteinte à la souveraineté économique, à la sécurité des données, au secret des affaires, aux droits fondamentaux et aux intérêts essentiels protégés par le droit français et européen.

La présente constitue donc :

1. une mise en connaissance préalable ;
2. une demande de justification écrite ;
3. une demande de traçabilité ;

4. une demande de communication des garanties ;
5. une réserve expresse de droits ;
6. une préparation loyale des démarches et recours légalement ouverts.

À défaut de réponse précise, complète et documentée, tout silence, refus ou réponse insuffisante pourra être conservé, annexé et produit dans le cadre des démarches, signalements ou recours légalement ouverts.

Veuillez agréer, Madame, Monsieur, l’expression de mes salutations distinguées.

14. Mise en demeure renforcée

Objet : Mise en demeure de transparence et de garanties — Facturation électronique obligatoire, plateformes agréées, Peppol et données économiques sensibles

Madame, Monsieur,

Je fais suite à ma mise en connaissance du [date], reçue le [date], demeurée sans réponse complète / ayant reçu une réponse insuffisante.

Je vous mets en demeure de répondre précisément, sous quinze jours, aux demandes relatives :

- à la base légale du dispositif ;
- au recentrage du Portail Public de Facturation ;
- aux raisons de l’abandon ou du recentrage d’une solution publique complète ;
- aux données exactes collectées ;
- aux données de facturation transmises à l’administration ;
- aux données de transaction et de paiement transmises ;
- aux plateformes agréées ;
- aux sous-traitants ;
- aux flux et métadonnées ;
- aux garanties RGPD ;
- aux transferts éventuels hors Union européenne ;
- aux risques extraterritoriaux ;
- aux audits de cybersécurité ;
- à l’indépendance des auditeurs ;
- aux conflits d’intérêts ;
- aux recours en cas de blocage, fuite, usurpation, erreur ou préjudice ;
- aux responsabilités prévues en cas d’impossibilité de facturer.

Je rappelle qu’une infrastructure obligatoire de facturation ne peut pas être contrôlée uniquement par les acteurs qui en tirent directement un intérêt économique. L’indépendance des audits, des certifications et des contrôles doit être démontrée.

Je rappelle également que les données économiques structurées d’entreprises peuvent relever du secret des affaires, de la protection des données personnelles, de la liberté d’entreprendre, du droit de propriété et, selon leur nature, leur destination ou leur accessibilité, des intérêts fondamentaux de la Nation.

À ce stade, il ne s’agit pas d’affirmer une infraction constituée. Il s’agit d’obtenir les garanties nécessaires permettant d’écarter tout risque d’atteinte à la souveraineté économique, à la sécurité des données, au secret des affaires et aux droits fondamentaux.

À défaut de réponse complète, je me réserve toute démarche utile auprès de la CADA, de la CNIL, de l’ANSSI, des autorités compétentes, des juridictions administratives et, le cas échéant, de toute autorité judiciaire si des faits précis devaient justifier un examen pénal.

Veuillez agréer, Madame, Monsieur, l’expression de mes salutations distinguées.

15. Version courte publique

La facturation électronique obligatoire n’est pas seulement une réforme comptable.

C’est une infrastructure obligatoire de traçabilité économique : factures, transactions, paiements, plateformes agréées, reporting fiscal, interopérabilité Peppol.

La France avait prévu un Portail Public de Facturation. Il a été recentré. Les entreprises devront passer par des plateformes agréées.

La question est simple :

Qui contrôle les flux ?
Qui héberge les données ?
Qui audite ?
Qui profite ?
Qui répond en cas de fuite ou de blocage ?
Quelle alternative publique reste disponible ?
Quels recours existent en cas d’impossibilité de facturer ?

Dans un pays déjà exposé à des fuites de données, on ne peut pas imposer une infrastructure obligatoire de circulation de données économiques sans transparence totale.

Plus ce dispositif avance, plus ses décideurs et opérateurs s’exposent.

Mais ils ne s’exposent que si nous créons la preuve :

- demandes écrites ;
- mises en connaissance ;
- archives ;
- réponses ;
- silences ;
- recours.

STOP • PAUSE • ÉCRITS • TRACE.

16. Plan d’archivage probatoire

À conserver :

- captures des pages officielles ;
- PDF des sources ;

- date et heure de consultation ;
- hash SHA-256 des PDF ;
- copie des courriers envoyés ;
- preuves LRAR ;
- réponses automatiques ;
- réponses reçues ;
- silences documentés ;
- tableau de suivi ;
- relances ;
- refus ;
- saisines CNIL / CADA / ANSSI ;
- versions successives du dossier ;
- liste des plateformes agréées à date ;
- preuves de modifications de pages officielles ;
- éléments relatifs aux votes européens ;
- éléments relatifs au recentrage du PPF ;
- éléments relatifs à la gouvernance OpenPeppol ;
- preuves d'incidents cyber ou de fuites de données utilisés comme antériorité.

Nom d'archive conseillé :

Dossier Peppol-ViDA — Enquête probatoire sur l'infrastructure obligatoire de traçabilité économique

17. Conclusion stratégique

Le dossier est sérieux parce qu'il ne repose pas sur une seule accusation. Il repose sur une chaîne :

1. obligation légale ;
2. passage par plateformes agréées ;
3. données de facture, transaction et paiement ;
4. transmission de données à l'administration ;
5. PPF recentré ;
6. DGFiP Peppol Authority ;
7. OpenPeppol member-driven ;
8. écosystème privé/international ;
9. risques cyber déjà documentés ;
10. droits fondamentaux concernés ;
11. secret des affaires ;
12. liberté d'entreprendre ;
13. droit de propriété ;
14. recours effectif ;
15. questions pénales à instruire si des données économiques sensibles deviennent accessibles à des entités étrangères ou sous contrôle étranger.

La stratégie gagnante :

> On ne crie pas seulement au scandale.
> On met en connaissance.

On exige les études.
On demande les bases légales.
On exige les audits.
On demande qui décide.
On demande qui profite.
On demande qui audite les auditeurs.
On archive les réponses.
On exploite les silences.
On prépare les recours.

Formule finale :

Sans mise en connaissance, il n’y a pas d’archive.
Sans archive, il n’y a pas de responsabilité.
Sans responsabilité, le mensonge devient droit positif.

STOP • PAUSE • ÉCRITS • TRACE.

Ressources, sources à archiver et utilité probatoire

Cette section a pour objet de centraliser les sources utiles au dossier, de distinguer les sources officielles des sources d’enquête, et de préciser l’usage probatoire de chacune.

Pour un usage contentieux, les sources doivent être archivées en PDF, datées, accompagnées de captures d’écran, avec date et heure de consultation. Les sources officielles doivent être prioritaires. Les sources journalistiques, militantes ou d’enquête doivent être utilisées comme pistes de vérification, indices ou supports d’orientation, puis corroborées par des sources primaires lorsque cela est possible.

A. Sources officielles françaises

Source	Nature	Utilité probatoire
AIFE — Facturation électronique interentreprises	Source publique officielle.	Prouver les objectifs de la réforme, le rôle DGFiP/AIFE, le calendrier 2026/2027, le recentrage du Portail Public de Facturation autour de l’annuaire et du concentrateur, ainsi que l’ouverture de l’annuaire et le rôle des plateformes agréées. L’AIFE indique notamment que le PPF a été recentré après le communiqué du 16 octobre 2024 et que ce recentrage a été entériné par la loi de finances 2025.
impots.gouv.fr — Facturation électronique et plateformes agréées	Source fiscale officielle.	Prouver que les entreprises assujetties devront recourir à une plateforme agréée pour transmettre et recevoir les factures électroniques et adresser des données de transaction et de paiement à l’administration à compter du 1er septembre 2026. Cette source est centrale pour démontrer le caractère obligatoire du passage par plateforme agréée.

Source	Nature	Utilité probatoire
URSSAF — Facturation électronique obligatoire	Source institutionnelle d’information professionnelle.	Prouver que l’obligation de facturation électronique est diffusée aux entreprises comme une échéance générale à compter du 1er septembre 2026. Utile comme source de vulgarisation institutionnelle à destination des professionnels.
Légifrance — CGI article 289 bis	Source légale primaire.	Prouver que l’émission, la transmission et la réception des factures électroniques s’effectuent en recourant à une plateforme agréée. C’est la base légale principale à encadrer, questionner ou contester.
Légifrance — CGI article 289 E	Source légale primaire.	Prouver que les données des factures électroniques émises en application de l’article 289 bis sont transmises à l’administration par la plateforme agréée choisie par l’assujetti. C’est une pièce centrale pour démontrer que la réforme ne porte pas seulement sur l’échange de factures, mais sur la transmission de données à l’administration.
Légifrance — CGI article 290 A	Source légale primaire.	Prouver que certaines données relatives au paiement sont également communiquées à l’administration sous forme électronique. Cette source renforce l’axe “données de paiement” et justifie les demandes de cartographie des flux, finalités, sous-traitants et garanties RGPD.
Légifrance — CGI article 1737	Source légale primaire.	À archiver pour étudier le régime de sanction applicable aux plateformes agréées en cas d’omission ou de manquement aux obligations de transmission de données mentionnées à l’article 289 E. Utile pour interroger l’équilibre responsabilité plateforme / responsabilité entreprise.

B. Sources européennes et Peppol

Source	Nature	Utilité probatoire
Commission européenne — VAT in the Digital Age, ViDA	Source européenne officielle.	Situer la réforme française dans la trajectoire européenne ViDA, notamment le reporting numérique et l’harmonisation de la TVA à l’ère numérique. La Commission indique que ViDA a été adopté le 11 mars 2025 et se déploie progressivement jusqu’en 2035.
Parlement européen — vote ViDA	Source parlementaire européenne.	Prouver la traçabilité politique du vote européen. Le Parlement indique que les règles ViDA ont été approuvées par 589 voix pour, 42 contre et 10 abstentions. Utile pour identifier les votes et responsabilités politiques.
OpenPeppol — profil France	Source officielle OpenPeppol.	Prouver l’arrimage de la France au cadre Peppol et la désignation de la DGFiP comme France Peppol Authority.
OpenPeppol — organisation	Source officielle OpenPeppol.	Prouver qu’OpenPeppol est une organisation pilotée par ses membres et que sa gouvernance repose sur des structures internes, communautés et fonctions techniques. Utile pour l’axe “gouvernance privée / hybride / member-driven”.

Source	Nature	Utilité probatoire
OpenPeppol — liste complète des membres	Source officielle OpenPeppol.	Identifier les membres du réseau, les Access Points, les SMP, les autorités Peppol et les acteurs privés ou publics impliqués. Cette source doit être archivée régulièrement car elle peut évoluer.
OpenPeppol — membres certifiés / service providers	Source officielle OpenPeppol.	Identifier les prestataires certifiés, leur pays, leur rôle AP/SMP et leur rattachement éventuel à une Peppol Authority. Utile pour cartographier les acteurs opérationnels et les risques d'accès technique.
Registre de transparence UE / Parlement européen	Source institutionnelle sur le lobbying.	Prouver que les institutions européennes reconnaissent l'existence d'organisations cherchant à influencer la formulation ou la mise en œuvre des politiques européennes. Utile pour cadrer juridiquement l'axe "influence / lobbying / conflits d'intérêts" sans surqualification.
Commission européenne — registre de transparence	Source institutionnelle.	Prouver que le registre de transparence vise à rendre visibles les intérêts représentés, par qui, et avec quels budgets. Utile pour demander l'identification des acteurs ayant participé à la fabrique de la norme.
LobbyFacts — OpenPeppol AISBL	Source de veille issue du registre de transparence.	À utiliser comme outil d'exploitation du registre officiel, pour documenter les données déclarées par OpenPeppol et orienter les demandes de vérification. Cette source doit être corroborée par le registre officiel UE quand c'est possible.

C. Sources sur les acteurs, membres, risques d'intérêts et acteurs étrangers

Source	Nature	Utilité probatoire
OpenPeppol — présence de Baiwangyun Singapore dans la liste des membres	Source officielle OpenPeppol.	Prouver que Baiwangyun (Singapore) Technology Pte. Ltd. apparaît dans la liste des membres OpenPeppol avec les mentions AP et SMP. Ce fait doit être archivé en capture datée.
OpenPeppol — présence de Deloitte dans la liste des membres	Source officielle OpenPeppol.	Prouver que plusieurs entités Deloitte apparaissent dans la liste des membres OpenPeppol. Utile pour l'axe "cabinets de conseil / audit / conformité / qui audite les auditeurs ?".
OpenPeppol — présence de KPMG dans la liste des membres	Source officielle OpenPeppol.	Prouver que KPMG Advisory SRL apparaît dans la liste des membres OpenPeppol. Utile pour l'analyse des liens entre cabinets de conseil, audit et écosystème de conformité.
OpenPeppol — présence de PwC dans la liste des membres	Source officielle OpenPeppol.	Prouver que plusieurs entités PwC apparaissent dans la liste des membres OpenPeppol. Utile pour étayer les questions sur l'indépendance des audits et conflits d'intérêts.
OpenPeppol — présence de SAP SE	Source officielle OpenPeppol.	Prouver que SAP SE apparaît dans la liste des membres OpenPeppol. Utile pour questionner le rôle des grands fournisseurs ERP dans un écosystème devenu obligatoire pour les entreprises.
Baiwang — profil officiel de l'entreprise	Source primaire entreprise.	Prouver que Baiwang se présente comme plateforme numérique d'affaires, fournisseur de solutions de gestion

Source	Nature	Utilité probatoire
		de factures, fiscalité, transactions, finance supply chain et data-driven analytics. Utile pour cartographier son objet social et ses capacités déclarées.
Simply Wall St — structure actionnariale Baiwang	Source financière secondaire.	Source à utiliser avec prudence et à corroborer par documents financiers primaires si possible. Elle indique notamment Alibaba Group Holding Limited à 11,4 % et Beijing Watertek Information Technology Co., Ltd. à 9,5 % parmi les actionnaires principaux. Utile comme piste d'enquête sur l'actionnariat.

D. Sources cybersécurité, données personnelles et transferts hors UE

Source	Nature	Utilité probatoire
Cybernews — fuites de données en France au premier semestre 2025	Source de presse cyber / étude spécialisée.	Appuyer l'argument d'un terrain cyber déjà fragilisé. Cybernews présente la France comme le pays européen le plus touché par les fuites de données au premier semestre 2025. Source utile pour justifier la demande d'audit cyber renforcé, mais à compléter par CNIL, ANSSI ou rapports officiels.
CNIL — transferts de données hors UE	Source officielle autorité indépendante.	Encadrer juridiquement les demandes relatives aux transferts hors UE, sous-traitants, garanties appropriées, pays d'accès, clauses contractuelles, décision d'adéquation ou autres mécanismes du chapitre V du RGPD.
Innovate Tax — risques de fraude d'identité via Peppol	Source technique / professionnelle.	Source à utiliser comme alerte technique, non comme preuve définitive. Elle sert à justifier les questions sur l'usurpation, les identifiants Peppol, la réception effective, les factures frauduleuses, les procédures de secours et l'indemnisation.

E. Sources presse, professionnelles et enquêtes à utiliser comme pistes

Source	Nature	Utilité probatoire
ChannelNews — abandon/recentrage du Portail Public de Facturation	Presse professionnelle numérique.	Utile pour documenter la lecture professionnelle de l'abandon ou du recentrage du PPF, l'impact sur l'écosystème et la bascule vers les plateformes privées. À corroborer avec AIFE, ministère de l'Économie et textes financiers.
The Paypers — partenariat Commission européenne / OpenPeppol	Presse spécialisée fintech / paiement.	Utile comme élément historique sur les liens anciens entre Commission européenne et OpenPeppol dans les infrastructures d'échange numérique. À corroborer avec les documents de la Commission et d'OpenPeppol.
Giak — "Le réseau qui nous facture"	Enquête citoyenne / Substack.	Source à classer comme piste d'enquête et document d'alerte. Elle rassemble plusieurs liens utiles sur Peppol, Baiwang, lobbying, PPF, Belgique, risques de fraude et gouvernance. Elle ne doit pas être utilisée seule comme preuve contentieuse, mais comme carte d'orientation vers des sources primaires à archiver.
Aurélie Soldai — ViDA a été voté	Analyse professionnelle /	Source utile pour comprendre les changements pratiques de ViDA et vulgariser les étapes européennes.

Source	Nature	Utilité probatoire
	vulgarisation fiscale.	À utiliser comme support pédagogique, à corroborer avec la Commission européenne, le Parlement européen et les textes officiels.

F. Sources à rechercher ou compléter

Les sources suivantes doivent encore être recherchées, téléchargées ou demandées officiellement pour renforcer le dossier :

Source ou document à obtenir	Pourquoi c’est important
Communiqué de presse Bercy du 15 ou 16 octobre 2024 sur le recentrage du PPF	Pièce centrale sur la décision politique de recentrage.
Décision formelle de recentrage du PPF	Permet d’identifier l’autorité décisionnaire, la date, la base juridique et les motifs.
Études de coût du PPF complet	Permet de comparer coût public / coût transféré aux entreprises.
Études de risques et d’impact	Permet d’évaluer proportionnalité, cybersécurité, souveraineté et alternatives.
Analyse d’impact RGPD nationale	Pièce centrale pour CNIL, données personnelles, flux, sous-traitants et transferts.
Avis CNIL, s’ils existent	Permet de vérifier les réserves ou recommandations sur le dispositif.
Avis ANSSI, s’ils existent	Permet de vérifier le niveau d’évaluation cyber de l’infrastructure.
Liste officielle actualisée des plateformes agréées	Permet de cartographier les opérateurs, pays, membres Peppol, liens d’intérêts.
Critères d’agrément et contrôles des plateformes	Permet d’évaluer indépendance, sécurité, responsabilités et sanctions.
Cartographie officielle des flux	Pièce centrale : qui envoie quoi, à qui, où, par quel canal, avec quels accès.
Liste des sous-traitants autorisés	Permet d’instruire hébergement, maintenance, support, accès indirects et transferts.
Procédure de secours en cas de panne ou cyberattaque	Permet d’éviter l’impossibilité de facturer et de documenter les recours urgents.
Procédures d’indemnisation	Permet d’identifier la responsabilité en cas de fuite, erreur, fraude, blocage ou impossibilité de facturer.
Déclarations d’intérêts / conflits d’intérêts des auditeurs	Permet de traiter l’axe “qui audite les auditeurs ?”.
Historique des versions des pages OpenPeppol et listes de membres	Permet de prouver les évolutions du réseau dans le temps.

G. Méthode d’archivage des sources

Chaque source doit être conservée selon la même méthode :

1. sauvegarde PDF de la page ;
2. capture d’écran de la partie utile ;
3. date et heure de consultation ;
4. adresse URL complète ;

5. hash SHA-256 du PDF si possible ;
6. résumé en une ligne de l’utilité probatoire ;
7. classement par catégorie : officiel, légal, européen, OpenPeppol, cyber, presse, enquête, hypothèse à instruire ;
8. tableau de suivi indiquant si la source est primaire, secondaire ou à corroborer.

H. Formule à intégrer dans le dossier

Les sources officielles établissent le socle factuel : obligation de plateforme agréée, transmission de données de facturation, transmission de données de transaction et de paiement, recentrage du Portail Public de Facturation, calendrier, rôle DGFiP/AIFE et arrimage au cadre Peppol.

Les sources professionnelles, cyber, journalistiques et citoyennes ne doivent pas être utilisées comme preuves uniques d’illégalité. Elles servent à orienter l’enquête, identifier les angles de risque, préparer les demandes écrites, et justifier la nécessité d’obtenir des documents primaires auprès des autorités compétentes.

La stratégie probatoire reste donc :

> Source officielle pour établir.
> Source technique pour comprendre.
> Source d’enquête pour orienter.
> Demande écrite pour prouver.
> Silence ou réponse insuffisante pour engager la suite.