CONSEIL D'ETAT

SECTION DU CONTENTIEUX

REQUÊTE EN RÉFÉRÉ-SUSPENSION

CJA, art. L. 521-1

Pour :

1. La société par actions simplifiée **Paymium**, dont le siège est situé 73 rue du Château à Boulogne-Billancourt (92100), prise en la personne de son représentant légal, dûment domicilié en cette qualité audit siège, représentant unique,

2. La société à responsabilité limitée **Leonod,** dont le siège est situé 15 Place Jules Ferry à Lyon (69006), prise en la personne de son représentant légal, dûment domicilié en cette qualité audit siège,

3. La société de droit canadien **Satoshi Portal Inc**., dont le siège est situé 4004 4 St SE à Calgary (AB T2G 2W3) au Canada, prise en la personne de son représentant légal, dûment domicilié en cette qualité audit siège.

Ayant pour avocat :

ORWL Avocats SELAS

Contre :

Le décret n° 2025-1276 du 19 décembre 2025, publié au JORF le 24 décembre 2025, relatif à l'obligation déclarative et de diligences incombant aux prestataires de services sur crypto-actifs en application des articles 1649 AC *bis* à 1649 AC *sexies* du code général des impôts (***cf. Pièce n° 1***).

Connexité avec la requête n° 513141

ORWL Avocats SELAS — 54 bis, rue de Clichy 75009 Paris
+33 1 88 80 36 33 — contact@orwl.fr
Barreau de Paris – Toque D1496 — 839 527 785 RCS Paris

ORWL

Sommaire

1. FAITS

1. Les sociétés Paymium SAS et Leonod SARL fournissent, depuis 2011 et 2013, des services sur crypto-actifs tels que définis par le règlement (UE) 2023/1114 du Parlement européen et du Conseil sur les marchés de crypto-actifs (ci-après, le « **Règlement MiCA** »)[1] sous les noms commerciaux, respectivement, « Paymium » et « Bull Bitcoin ». Elles sont à cet effet agréées en qualité de prestataires de services sur crypto-actifs (ci-après, « **PSCA** ») auprès de l'Autorité des marchés financiers sous les numéros, respectivement, A2026-018 et A2026-019. La société Satoshi Portal Inc., société de droit canadien, détient à 100 % la société de droit français Leonod SARL.

2. Les exposantes sont par ailleurs utilisatrices des services sur crypto-actifs fournis par leurs différents fournisseurs de solution de conservation de crypto-actifs ou de liquidité.

3. Aussi sont-elles, depuis le 1er janvier 2026, directement concernées par les nouvelles obligations déclaratives instaurées par la directive (UE) 2023/2226 dite « DAC 8 » adoptée le 17 octobre 2023 (ci-après, la « **Directive DAC 8** »), transposée par l'article 54 de la loi n° 2025-127 du 14 février 2025 de finances pour 2025 pour l'application de laquelle a été pris le décret attaqué n° 2025-1276 du 19 décembre 2025, d'une part, en qualité d'entités soumises aux obligations déclaratives et, d'autre part, en qualité d'utilisatrices de services sur crypto-actifs.

4. La nature des crypto-actifs, leur cadre réglementaire et fiscal ainsi que le dispositif instauré par la Directive DAC 8 et ses textes de transposition et d'application sont exposés de manière exhaustive dans la requête au fond et le mémoire complémentaire produits à l'appui de la présente requête (***cf. Pièces n° 2 et 3***), auxquels il est renvoyé.

5. En substance, la Directive DAC 8 insère dans la directive 2011/16/UE relative à la coopération administrative dans le domaine fiscal un article 8 bis quinquies instituant un mécanisme d'échange automatique et obligatoire, entre les administrations fiscales des États membres, d'informations portant sur les transactions en crypto-actifs.

6. Le décret attaqué n° 2025-1276 du 19 décembre 2025, publié au Journal officiel le 24 décembre 2025 et entré en vigueur le 1er janvier 2026, précise l'ensemble des modalités d'application de la loi de transposition. Il n'a pas été pris après consultation de la la Commission nationale de l'informatique et des libertés (ci-après « **CNIL** »), alors même qu'il institue des traitements automatisés de données à caractère personnel à grande échelle.

7. Le dispositif impose aux PSCA — quelle que soit leur taille — les obligations suivantes :

    i) identifier chaque utilisateur au moyen d'une auto-certification signée comportant ses prénom et nom, adresse de résidence, État ou territoire de résidence fiscale, numéro d'identification fiscale et date de naissance, obtenue lors de l'entrée en relation et, pour l'intégralité du stock d'utilisateurs préexistants au 31 décembre 2025, avant le 1er janvier 2027 ;

[1] Règlement (UE) 2023/1114 du Parlement européen et du Conseil du 31 mai 2023 sur les marchés de crypto-actifs, et modifiant les règlements (UE) n° 1093/2010 et (UE) n° 1095/2010 et les directives 2013/36/UE et (UE) 2019/1937.

ii) collecter, vérifier et déclarer annuellement à l'administration fiscale **la totalité des transactions réalisées** par chacun de leurs utilisateurs — opérations d'échange (achats, ventes, échanges de crypto-actifs), mais également simples transferts (dépôts, retraits, transferts vers des adresses auto-hébergées) —, agrégées par type et valorisées en monnaie légale, indépendamment de tout fait générateur d'imposition et de tout risque de fraude ;

iii) interdire toute nouvelle transaction à l'utilisateur qui refuse de fournir les informations d'auto-certification requises après deux rappels demeurés sans réponse dans un délai de soixante jours ;

iv) conserver l'ensemble des données ainsi collectées pendant une durée de dix ans.

8. Les informations collectées au titre de l'année 2026 (première année d'application) :

- devront être déclarées par les PSCA à l'administration fiscale française **au plus tard le 15 juin 2027** (Décret n° 2025-1276 du 19 décembre 2025, art. 19) ;
- seront ensuite mises à la disposition de l'État de résidence de chaque utilisateur **au plus tard le 30 septembre 2027** par l'intermédiaire d'un répertoire centralisé hébergé par la Commission européenne, dont la création est prescrite **avant le 31 décembre 2026**.

9. Les données collectées, conservées puis échangées révèlent de manière précise l'identité, l'adresse et l'état du patrimoine en crypto-actifs des utilisateurs. Or, compte tenu des particularités techniques des crypto-actifs (transactions irréversibles, réalisables de pair à pair, de manière quasi instantanée), détenir des crypto-actifs équivaut à détenir de l'or ou des espèces dans un coffre-fort à son domicile : l'association de l'identité et de l'adresse d'une personne à son patrimoine en crypto-actifs constitue ainsi une information d'une sensibilité toute particulière.

10. C'est la raison pour laquelle ces données suscitent la convoitise d'une criminalité organisée qui cible les détenteurs de crypto-actifs selon des modes opératoires d'une violence extrême (enlèvements avec mutilations, *home jacking*). La France connaît une recrudescence inégalée de ces faits : la procureure nationale anti-criminalité organisée (Pnaco) recensait, au 24 avril 2026, **135 faits de ce type depuis 2023 — 18 en 2024, 67 en 2025 et déjà 47 en 2026**[2].

11. **Le 30 juin 2026, le ministère de l'Intérieur recensait 77 faits de séquestration, enlèvement, extorsion ou tentatives liés au secteur des cryptomonnaies, soit, en 2026, un fait tous les deux jours et demi sur le seul territoire français[3].**

12. Les victimes sont généralement ciblées grâce aux fuites de données révélant leur lieu de résidence et leur patrimoine, réel ou supposé, en crypto-actifs. À la suite de la fuite de données d'une société spécialisée dans l'analyse du patrimoine en crypto-actifs de ses utilisateurs, le Parquet de Paris a publié, le 22 janvier 2026, un communiqué alertant le public sur les risques d'hameçonnage, d'escroqueries et d'appels de faux représentants de l'ordre visant à obtenir des informations sur les détenteurs de crypto-actifs, et précisant que « *dans les situations les plus graves, des malfaiteurs peuvent aller jusqu'à* ***menacer et agresser physiquement les victimes ou leur entourage***

[2] Le Monde avec AFP, Enlèvements dans le secteur des cryptomonnaies : 88 mises en examen dans les enquêtes en cours, selon le Pnaco, 24 avr. 2026.

[3] La Tribune, Enlèvements liés aux cryptomonnaies : le secteur veut aller plus loin que le plan Nuñez, 2 juill. 2026.

*proche pour les extorquer. Des **enlèvements et séquestrations** ont encore été signalés aux forces de l'ordre en janvier 2026 »*[4].

13. Les administrations publiques, destinataires des données collectées, ne sont pas épargnées par ces fuites et n'apparaissent pas en mesure d'assurer la sécurité de ces données :

i) le 13 mars 2024, France Travail a subi une attaque concernant les données personnelles de 43 millions de personnes (noms, dates de naissance, numéros de sécurité sociale, coordonnées)[5] ;

ii) le 18 février 2026, la DGFIP a subi une attaque sur le fichier national des comptes bancaires (FICOBA), par usurpation des identifiants d'un fonctionnaire, ayant permis la consultation, s'agissant de 1,2 million de comptes, des coordonnées bancaires, de l'identité du titulaire, de son adresse et, parfois, de son identifiant fiscal[6] ;

iii) le 15 avril 2026, l'Agence nationale des titres sécurisés a subi une attaque concernant les données personnelles de 11 à 19 millions de comptes[7].

iv) très récemment, le ministère de l'action et des comptes publics a rendu publiques, après qu'elle ont été revendiquées par l'attaquant, des intrusions, à trois reprises, dans les systèmes d'information de la DGFIP ayant permis la consultation et l'extraction de très nombreuses données personnelles :

a) le 12 août 2026, le ministre a communiqué sur une intrusion ayant eu lieu fin juin 2026 et ayant conduit à la fuite de « *données concernant un total de 678 000 particuliers et professionnels* » notamment, en ce qui concerne les particuliers, des données fiscales telles que le revenu fiscal de référence, le quotient familial ou le taux de prélèvement à la source, l'état civil, l'adresse postale et la situation de famille et, concernant les entreprises, des données telles que leur raison sociale ou leur SIREN[8] ;

b) le 13 août 2026, le ministre a communiqué sur une deuxième intrusion ayant eu lieu fin juillet 2026 et ayant conduit à la fuite de données professionnelles cadastrales concernant 433 485 particuliers et 1 082 professionnels ;

c) le 18 août 2026, le ministre a communiqué sur une troisième intrusion ayant conduit à la fuite de données relatives aux successions dans des proportions qui n'ont pas été dévoilées.

d) enfin, le 18 août 2026, lors d'une conférence de presse qui s'est tenue au ministère de l'Économie, la directrice générale de la DGFiP a annoncé avoir identifié une nouvelle intrusion dans la journée du 17 août 2026.

[4] Parquet de Paris, Violation de données personnelles dans le secteur des crypto-actifs : situation, risques et recommandations, 22 janv. 2026.

[5] CNIL, France Travail : la CNIL enquête sur la fuite de données et donne des conseils pour se protéger, 13 mars 2024.

[6] DGFIP, FICOBA : tout savoir à l'accès illégitime au fichier national des comptes bancaires, 3 mars 2026.

[7] ANTS, Incident de sécurité relatif au portail ants.gouv.fr, 20 avr. 2026.

[8] DGFIP, 953 - CP - Accès illégitimes au système d'information de la Direction générale des Finances publiques, 14 août 2026.

La combinaison de ces données permet de reconstituer un profil particulièrement précis d'un contribuable et de son foyer, avec des informations rarement réunies dans une seule fuite de données.

Le ministre, M. David Amiel, a déclaré, lors d'une conférence de presse en date du 18 août 2026, après avoir présenté ses excuses aux contribuables concernés : **« *Nos systèmes d'information comportent des faiblesses* »**.

14. De manière plus générale, la CNIL recensait 5 629 violations de données personnelles en 2024, en hausse de 20 % par rapport à l'année précédente, et une nouvelle augmentation de 10 % en 2025, le secteur le plus touché étant celui des administrations publiques, qui concentre à lui seul 19 % des violations[9].

15. Le risque n'est pas seulement externe : la presse a révélé, en janvier 2026, la mise en examen d'agents de l'administration fiscale pour avoir consulté et communiqué des informations relatives à la situation de fortune de personnes spécialisées dans le secteur des crypto-actifs[10].

16. La DGFIP a elle-même déclaré, en février 2026, dans le cadre des discussions parlementaires relatives à la création d'une déclaration des portefeuilles de crypto-actifs (dites « adresses auto-hébergées »), qu' « ***une déclaration généralisée de ces portefeuilles [de crypto-actifs] conduirait à centraliser des données très sensibles, comme l'identité des détenteurs et la valeur de leurs actifs*** » et que « ***dans un contexte de cyberattaques fréquentes contre les grandes bases de données, ces informations deviendraient une cible privilégiée pour les pirates, avec des risques accrus d'escroquerie*** »[11].

17. La sensibilité de ces données relevée par la DGFIP s'explique par les caractéristiques techniques de crypto-actifs qui reposent sur des *blockchains* publiques. Ainsi, les transactions réalisées entre différents portefeuilles peuvent être consultées par tous (par exemple, via des site dédiés tels que etherscan.com pour la blockchain Ethereum ou btcscan.org pour la blockchain Bitcoin). En mettant un nom derrière une adresse auto-hébergée, il est donc possible à tout un chacun de connaître l'ensemble du patrimoine détenu par un contribuable mais également l'ensemble des transactions qu'il a réalisées.

18. C'est dans ce contexte que les requérantes, par une requête sommaire enregistrée le 24 février 2026 (***cf. Pièce n° 2***) sous le numéro 513141, complétée par un mémoire complémentaire enregistré le 22 mai 2026 (***cf. Pièce n° 3***), ont déféré à la censure du Conseil d'État, juge de l'excès de pouvoir, le décret n° 2025-1276 du 19 décembre 2025, après avoir procédé à un renvoi préjudiciel en appréciation de validité.

19. **Au regard de l'urgence, les exposantes n'ont d'autre choix que de solliciter, par une requête distincte de la requête principale à fin d'annulation, la suspension du décret n° 2025-1276 du 19 décembre 2025.**

---

[9] CNIL, Violations massives de données en 2024, 28 janv. 2025. – CNIL, Protéger les données de chacun pour sécuriser l'avenir numérique de tous, 19 mai 2026, p. 51.

[10] J. Constant, L'agente du fisc ciblait gardiens de prison et investisseurs en cryptomonnaies pour un mystérieux commanditaire, Le Parisien, 6 janv. 2026.

[11] Ass. nat., Séance du 26 févr. 2026, article 3 quater, examen des amendements n° 483 et 995, selon les propos rapportés par M. Daniel Labaronne, rapporteur.

2. DISCUSSION

20. Aux termes de l'article L. 521-1 du code de justice administrative :

> *« Quand une décision administrative, même de rejet, fait l'objet d'une requête en annulation ou en réformation, le juge des référés, saisi d'une demande en ce sens, peut ordonner la suspension de l'exécution de cette décision, ou de certains de ses effets, lorsque l'urgence le justifie et qu'il est fait état d'un moyen propre à créer, en l'état de l'instruction, un doute sérieux quant à la légalité de la décision.*
>
> *Lorsque la suspension est prononcée, il est statué sur la requête en annulation ou en réformation de la décision dans les meilleurs délais. La suspension prend fin au plus tard lorsqu'il est statué sur la requête en annulation ou en réformation de la décision. »*

21. Il s'ensuit que la suspension d'une décision est subordonnée à la réunion de deux conditions cumulatives et autonomes : l'urgence à suspendre (2.1) et l'existence d'un doute sérieux quant à la légalité de la décision (2.2).

2.1. Sur l'urgence à suspendre l'acte litigieux

22. Après avoir rappelé les dispositions pertinentes applicables (2.1.1), l'urgence sera établie en l'espèce à plusieurs titres (2.1.2).

2.1.1. En droit

23. **<u>En droit</u>,** il est de jurisprudence constante que « *l'urgence justifie la suspension de l'exécution d'un acte administratif lorsque celui-ci porte* ***atteinte de manière suffisamment grave et immédiate*** *à* ***un intérêt public****, à la* ***situation du requérant*** *ou aux* ***intérêts qu'il entend défendre*** *; qu'il appartient au juge des référés d'apprécier concrètement, compte tenu des justifications fournies par le requérant, si les effets de l'acte contesté sont de nature à caractériser une urgence justifiant que, sans attendre le jugement de la requête au fond, l'exécution de la décision soit suspendue ; que l'urgence doit être appréciée objectivement et compte tenu de l'ensemble des circonstances de l'affaire* » (CE, 1er octobre 2014, n° 384354 ; CE, 12 septembre 2014, n° 383721 ; CE, 5 septembre 2014, n° 384079 ; CE, 19 janvier 2001, n° 228815, *Confédération des radios libres*, Rec. p. 29).

24. Le juge des référés apprécie l'existence d'une situation d'urgence « *objectivement et compte tenu de l'ensemble des circonstances de chaque espèce* » (CE, Sect., 28 février 2001, n° 229563, au Rec.). Le juge des référés doit ainsi tenir compte de manière concrète, globale et objective des circonstances de l'espèce et procéder à une balance des intérêts en cause (CE, 30 novembre 2001, *SA Kerry,* n° 233327).

25. La condition tenant à l'urgence doit être appréciée à la date à laquelle le juge des référés se prononce, et non pas à la date à laquelle le requérant a introduit sa demande de suspension (CE, 31 octobre 2001, n° 239050, au Recueil).

26. Le délai dans lequel le juge du fond sera en mesure de se prononcer sur la légalité de l'acte **peut également être pris en considération** (v. not. CE, ord., 19 septembre 2003, *Société Cora Belgique,* n° 260199, aux tables).

27. Plus généralement, pour qu'il y ait urgence, il faut que l'**écoulement du temps risque de préjudicier gravement aux intérêts du demandeur avant que le juge du fond puisse assurer sa protection** (*Le guide des référés administratifs,* Dalloz, 3e éd., § 222.31).

28. Il est en outre précisé que la condition d'urgence « *s'apprécie au regard des effets de la décision attaquée* » (CE, 31 mars 2014, *Commune de Mios,* n° 368003).

29. **S'agissant d'une atteinte à un intérêt public**, il est acquis que le doute sérieux sur la compatibilité d'une norme française avec le droit de l'Union européenne doit être regardé comme caractérisant **à lui seul** une situation d'urgence.

30. Le juge des référés du Conseil d'État a ainsi affirmé « *que l'intérêt public commande pour les motifs énoncés au point 4* » (point de la décision ayant établi l'existence d'un doute sérieux quant à la compatibilité de l'acte attaqué avec une directive de l'Union européenne) « ***que soient prises les mesures nécessaires pour faire cesser immédiatement l'atteinte aux droits conférés par l'ordre juridique de l'Union européenne*** » (CE, ord., 14 février 2013, *Lallier,* n° 365459, aux tables).

31. Ainsi, en vertu de cette jurisprudence, dans la balance des intérêts à laquelle procède le juge des référés, pour apprécier si la condition d'urgence doit être regardée comme remplie, il est tenu compte, le cas échéant, de ce que l'**intérêt public commande que soient prises les mesures provisoires nécessaires pour faire cesser immédiatement l'atteinte aux droits conférés par l'ordre juridique de l'Union européenne**.

32. Cette solution est une conséquence de la jurisprudence *Simmenthal,* qui confère au juge national le pouvoir d'écarter toute disposition nationale contraire au droit de l'Union « *au moment même* » de l'application de celui-ci (CJCE, 9 mars 1978, *Simmenthal,* aff. 106/77, pt 22). Cette solution ayant été étendue au juge de l'urgence (CJCE, 19 juin 1990, *Factortame,* C-213/89, pt 20).

33. La Cour du justice de l'Union européenne a postérieurement précisé que « *La protection provisoire qui est assurée aux justiciables devant les juridictions nationales par le droit communautaire* ***ne saurait varier, selon qu'ils contestent la compatibilité de dispositions de droit national avec le droit communautaire ou la validité d'actes communautaires de droit dérivé****, dès lors que, dans les deux cas, la contestation est fondée sur le droit communautaire lui-même* » et que **les juges nationaux doivent ainsi être investis du pouvoir de suspendre l'exécution de tout acte administratif, quand bien même cet acte serait pris pour l'application d'un acte de droit dérivé de l'Union européenne, lorsqu'il existe des doutes sérieux sur la validité du texte de droit de l'Union sur lequel est fondé l'acte administratif attaqué** (CJCE, 21 février 1991, *Zuckerfabrik Süderdithmarschen AG*, C-143/88 et C-92/89, pts 20 et 21). Dans ce cas, le juge est par ailleurs investi également du pouvoir de prescrire toute mesure positive qui rend provisoirement inapplicable le texte de droit de l'Union européenne (CJCE, 9 novembre 1995, *Atlanta Fruchthandelsgesellschaft mbH et autres*, C-465/93, pts 27 à 30).

34. **S'agissant d'une atteinte portée aux intérêts défendus par le requérant ou à ceux qu'il entend défendre**, et de manière comparable aux problématiques soulevées par la présente affaire, on peut relever que le juge des référés du Conseil d'État a ordonné la suspension de l'exécution d'un décret n° 2016-567 du 10 mai 2016 relatif aux modalités de consultation du registre des trusts, créé pour lutter contre la fraude fiscale et prévu par l'article 1649 AB, al. 2 du CGI (CE, ord., 22 juillet 2016, n° 400913, aux tables ; v. aussi Cons. const., 21 octobre 2016, n° 2016-591 QPC, déclarant lesdites dispositions inconstitutionnelles comme portant une atteinte manifestement disproportionnée au droit au respect de la vie privée – absence de limitation des personnes pouvant accéder au registre, absence de précision sur leur qualité et les motifs de la consultation).

35. **Cette affaire illustre que lorsque la mise en œuvre d'un dispositif déclaratif et de publicité fiscale entraîne la diffusion ou le traitement de données personnelles sensibles, le Conseil d'État admet l'urgence, même si l'atteinte est encore « *prospective* ».**

36. De même qu'un registre public des trusts, qui touche aux données patrimoniales, et qui répond à une finalité fiscale et de lutte contre la fraude, le dispositif de collecte et de reporting sur crypto-actifs - en application des articles 1649 AC bis à 1649 AC sexies CGI, fondé sur la Directive DAC 8 - qui touche aux données personnelles sensibles pour répondre de manière comparable à des préoccupations de lutte contre la fraude, pose le problème d'une ingérence grave et potentiellement irréversible dans la vie privée et les données des personnes concernées.

2.1.2. En l'espèce

37. **En l'espèce**, **en premier lieu**, l'exécution du décret attaqué, en ce qu'il met en application les dispositions de la loi n° 2025-127 du 14 février 2025 transposant la Directive DAC 8, porte atteinte tout à la fois à un intérêt public, aux intérêts que les requérantes entendent défendre et à leur situation propre.

38. D'abord, s'agissant de l'intérêt public, il sera démontré ci-après (cf. *infra, 2.2.2.1 et 2.2.2.3*) que le doute sérieux affectant la légalité du décret attaqué **procède, notamment, de la méconnaissance du droit de l'Union européenne**, et ce dans les deux configurations envisagées par les jurisprudences rappelées *supra* (*cf. § 30 à 33*) :

i) le décret méconnaît directement une obligation édictée par le droit de l'Union, la consultation préalable de la CNIL exigée par le paragraphe 4 de l'article 36 du RGPD ayant été omise (*cf. infra, 2.2.2.1*) ;

ii) le décret est, en outre, privé de base légale en raison de la contrariété de la Directive DAC 8 elle-même au droit primaire de l'Union (*cf. infra, 2.2.2.3*), dont l'appréciation devrait faire l'objet du renvoi préjudiciel sollicité dans l'instance au fond n° 513141.

39. L'urgence résulte ainsi du fait que l'intérêt public commande que soient prises les mesures nécessaires pour faire cesser immédiatement l'atteinte aux droits conférés par l'ordre juridique de l'Union.

40. L'intérêt public s'attache, en outre et en toute hypothèse, à la protection des données à caractère personnel de l'ensemble des utilisateurs de services sur crypto-actifs et à la prévention des atteintes aux biens et aux personnes qui en résultent. Il est à ce titre rappelé que le ministère de

l'Intérieur recense un fait de séquestration, d'enlèvement ou d'extorsion lié au secteur tous les deux jours et demi en 2026 (*cf. supra, § 11*), le Parquet de Paris alerte publiquement sur les conséquences des fuites de données du secteur (*cf. supra, § 12*) et la DGFIP a elle-même déclaré qu'une centralisation de l'identité des détenteurs de crypto-actifs et de la valeur de leurs actifs constituerait « *une cible privilégiée pour les pirates, avec des risques accrus d'escroquerie* » (*cf. supra, § 16*). Or c'est précisément cette cible que l'exécution du décret permet de constituer, jour après jour, depuis le 1er janvier 2026.

41. À l'inverse, dans la balance des intérêts à laquelle procède le juge des référés, y compris au titre de la prise en compte de l'intérêt de l'Union, aucun intérêt public ne s'oppose à la suspension. L'administration fiscale conserve l'intégralité de l'arsenal déclaratif et de contrôle existant applicable aux crypto-actifs (déclaration des plus-values de l'article 150 VH bis du CGI, déclaration des comptes d'actifs numériques ouverts à l'étranger de l'article 1649 bis C du CGI, droit de communication et assistance administrative internationale), de sorte que la lutte contre la fraude fiscale n'est nullement désarmée par la suspension.

42. Ensuite, s'agissant des intérêts que les requérantes entendent défendre, à savoir ceux de l'ensemble de leurs utilisateurs, le décret impose aux exposantes de collecter, vérifier, conserver pendant dix ans puis déclarer l'identité, l'adresse, la résidence fiscale, le numéro d'identification fiscale et la date de naissance de chacun d'eux, ainsi que l'intégralité de leurs transactions (*cf. supra, § 7*).

43. Cette collecte, mais surtout la communication de ces données à l'administration fiscale, porte une atteinte manifeste au droit au respect de la vie privée et au droit à la protection des données personnelles (*cf. infra, 2.2.2.3*).

44. Par ailleurs, l'association identité-adresse-patrimoine fait des détenteurs de crypto-actifs les cibles d'une criminalité organisée aux modes opératoires d'une violence extrême (*cf. supra, § 9 à 12*), les victimes étant précisément ciblées grâce aux fuites de données révélant leur lieu de résidence et leur patrimoine (*cf. supra, § 12*).

45. Outre la collecte de ces données, leur communication à l'administration fiscale et leur conservation au sein d'un registre centralisant l'ensemble des données de transactions de tous les résidents d'Etats membres de l'Union, accentuera considérablement le risque de fuite de ces données. Il est à cet égard précisé que les requérantes n'ont, depuis leur lancement en 2011 et 2013, subi aucune intrusion dans leurs systèmes d'informations.

46. Il est en effet évident qu'un registre centralisant autant de données constituera une cible nettement plus précieuse pour les cybercriminels que les bases de données détenues individuellement par chacun des PSCA. Les moyens déployés par ces cybercriminels pour pouvoir y avoir accès seront ainsi d'autant plus importants que le prix qu'ils pourront en tirer sera élevé. L'Agence nationale de la sécurité des systèmes d'information relève ainsi, dans ses recommandations pour l'hébergement des systèmes d'information dans le cloud d'août 2024, que « *Les infrastructures sont ciblées en raison de la concentration des données et des traitements qu'elles hébergent, et du fait de l'usage de solutions de virtualisation et d'administration mutualisées* ». La concentration génère un risque considérable en augmentant le retour sur investissement des cybercriminels.

47. Or le risque de compromission de ces données, une fois collectées puis transmises, n'a rien d'hypothétique. Il s'est déjà réalisé, de manière répétée, massive et récente, au sein même des administrations qui en seront destinataires (*cf. supra, § 13 à 15*).

48. A ce titre, les déclarations récentes de la DGFIP, qui s'est opposée à la création d'une déclaration des portefeuilles auto-hébergés précisément pour cette raison (*cf. supra, § 16*), et du ministre qui a indiqué, le 18 août 2026, « *Nos systèmes d'information comportent des faiblesses* », établissent le niveau de criticité de ce risque.

49. Enfin, s'agissant de la situation des requérantes, l'exécution du décret leur impose, sans attendre :

i) de déployer et maintenir, à leurs frais, les systèmes de collecte, de vérification, de conservation décennale et de déclaration requis ;

ii) de solliciter, dès à présent, l'auto-certification de l'intégralité de leur stock de clients ;

iii) d'interdire toute nouvelle transaction aux clients n'ayant pas fourni les informations requises après deux rappels demeurés sans réponse dans un délai de soixante jours ;

iv) de collecter et transmettre, sous peine de sanctions, des données exposant leurs clients aux risques décrits ci-dessus, au prix d'une atteinte directe à la relation de confiance qui fonde leur activité et d'une incitation objective de leurs utilisateurs à se détourner vers des opérateurs de pays tiers ou des protocoles décentralisés échappant à toute obligation équivalente — détournement de clientèle difficilement réversible, au détriment d'acteurs français régulés.

50. Une fuite des données transmises aurait par ailleurs des conséquences réputationnelles très importantes pour les requérantes, d'autant plus si ces fuites sont, comme c'est le cas tous les deux jours et demi en moyenne en France, exploitées à des fins d'extorsion et de vol avec violences.

51. Les exposantes sont au surplus elles-mêmes utilisatrices de services sur crypto-actifs. Leurs propres données patrimoniales sont, à ce titre, collectées, conservées et promises à l'échange dans les conditions critiquées.

52. **En deuxième lieu**, ces atteintes sont graves.

53. Elles le sont par leur ampleur. La collecte porte sur la totalité des transactions, y compris les simples transferts, non susceptibles de constituer des faits générateurs d'imposition, de la totalité des utilisateurs, indépendamment de tout risque de fraude, et les données sont conservées dix ans.

54. Elles le sont surtout par leur nature. L'**association de l'identité et de l'adresse d'une personne à l'état précis de son patrimoine en crypto-actifs** constitue une information dont la compromission expose les personnes concernées, au-delà des escroqueries, à des atteintes à leur intégrité physique (*cf. supra, § 9 à 12*), c'est-à-dire à des dommages par nature irréparables.

55. Elles présentent en outre un caractère largement irréversible. Une fois les données collectées, déclarées à l'administration fiscale, versées au répertoire central de la Commission puis échangées entre États membres, aucune annulation contentieuse ne permettra de restaurer leur confidentialité à l'égard des personnes qui en auront eu connaissance, *a fortiori* en cas de fuite, la divulgation de données patrimoniales et de localisation étant définitive.

56. A la suite de fuites de ce type, dans lesquelles figuraient l'adresse postale ainsi que des informations sur un patrimoine réel ou supposé en crypto-actifs, certains contribuables ont ainsi été contraints de vendre leur résidence pour voir cesser les agressions physiques. Mais la vente d'un bien ne suffit pas puisque, les données circulant toujours librement en ligne, les nouveaux acquéreurs restent également exposés. En juin 2026, un couple ayant récemment acquis une maison dans la Somme a ainsi subi trois intrusions, parfois accompagnées de violences physiques, en moins d'un mois à leur domicile de trois équipes de criminels différentes ; la maison avait été acquise auprès d'un couple disposant d'un important patrimoine de crypto-actifs et dont la fiche d'imposition aurait fuité selon l'avocat des victimes (*N. Fillon, Somme : un couple séquestré chez lui et cible de vols pour un million d'euros en cryptomonnaie... qu'il ne possède pas, ICI Picardie, 10 août 2026*).

57. **En dernier lieu**, ces atteintes sont immédiates.

58. Le décret est entré en vigueur le 1er janvier 2026 et produit des effets immédiats et continus. La collecte et la conservation s'opèrent, à chaque transaction, depuis cette date.

59. Ces effets s'inscrivent, de surcroît, dans un calendrier certain et rapproché d'aggravation et de consolidation de l'atteinte : création du répertoire central de la Commission avant le 31 décembre 2026 ; auto-certification de l'intégralité du stock de clients avant le 1er janvier 2027 ; première déclaration à l'administration fiscale au plus tard **le 15 juin 2027** ; premier échange entre États membres au plus tard le **30 septembre 2027** (*cf. supra, § 7 et 8*). Ainsi qu'exposé *supra*, ces échéances aggraveront considérablement les risques de compromission des données.

60. **Or le juge du fond ne sera pas en mesure d'assurer sa protection avant la consommation de ces échéances. Le renvoi préjudiciel en appréciation de validité sollicité dans l'instance n° 513141, qui s'impose au regard du monopole de la Cour de justice, implique, compte tenu des délais propres à la procédure préjudicielle, que le juge de l'excès de pouvoir ne se prononcera vraisemblablement pas avant que les données collectées aient été déclarées, centralisées et échangées entre Etats membres. Seule la suspension permet, dans cette attente, d'éviter que le recours au fond soit privé de son effet utile.**

61. L'urgence à suspendre est donc acquise.

2.2. Sur le doute sérieux sur la légalité de l'acte litigieux

62. Il résulte de l'article L. 521-1 du code de justice administrative que cette seconde condition exige seulement qu'il existe, en l'état de l'instruction, un moyen propre à créer un doute sérieux quant à la légalité de l'acte attaqué. Après avoir rappelé les dispositions générales applicables (2.2.1), il sera démontré qu'un tel doute est établi compte tenu d'un certain nombre de vices (2.2.2).

2.2.1. En droit

63. **En droit,** l'illégalité nécessaire au prononcé d'une mesure de suspension doit être une illégalité **vraisemblable ou apparente**.

64. Le juge des référés fait droit à la demande de suspension lorsqu'il estime que l'un des moyens invoqués est susceptible d'entraîner l'annulation ou la réformation de l'acte attaqué.

65. On rappellera, en tant que de besoin, la **possibilité de se fonder sur un moyen non développé dans le recours au fond**, dès lors que le Conseil d'État admet « *que le juge des référés, saisi d'une demande de suspension de l'exécution d'une décision administrative, peut retenir un moyen propre à créer un doute sérieux quant à sa légalité qui n'a pas été soulevé à l'appui de la demande à fin d'annulation ou de réformation de cette décision* » (CE, 30 décembre 2002, *Société Cottage Wood*, n° 249860, aux tables p. 867).

66. Sont susceptibles d'être retenus **des moyens de légalité interne, comme de légalité externe**, notamment l'incompétence de l'auteur de l'acte ou un vice de procédure substantiel (v. par ex. CE, 9 février 2009, *Association Réseau Diabète du Val d'Oise,* n° 320288, aux tables : moyen tiré d'une insuffisance de motivation).

67. **S'agissant de la légalité externe**, un défaut de consultation obligatoire et, *a fortiori,* d'avis conforme, qui équivalent à une incompétence, sont des vices d'une particulière gravité en principe regardés comme propres à créer un doute sérieux.

68. Cette solution vaut évidemment pour le défaut de consultation du Conseil d'État, y compris le cas où la décision prise est différente du projet soumis au Conseil d'État (CE, 9 février 1994, *Préfet de Seine-et-Marne,* n° 129243, p. 60). De même, le juge administratif assimile **à l'incompétence le défaut d'un avis exigé par le droit** (CE, 8 juin 1994, *Madame Laurent,* n° 127032, p. 1137).

69. **Quant aux moyens de légalité interne**, ils peuvent notamment être tirés de l'incompatibilité du droit national avec le droit supranational : tel est le cas, en particulier, d'**un recours contre le texte de transposition d'une directive, tiré de la contrariété de cette directive avec les stipulations du traité CE** (CE, ord., 29 octobre 2003, *Société Techna SA,* n° 260768, p. 422).

70. De plus, si la possibilité d'accueillir un moyen tiré de l'inconventionnalité d'un texte législatif servant de base légale à l'acte administratif est en principe encadrée pour le juge des référés, le

Conseil d'État opposant autrefois son inopérance par sa jurisprudence *Carminati*[12], il est bien autorisé à **examiner le moyen tiré de l'incompatibilité de la loi au regard des dispositions de droit de l'Union européenne (**CE, ord., 16 juin 2010, *Diakité,* n° 340250, au Recueil).

2.2.2. En l'espèce

71. **En l'espèce**, plusieurs moyens sont propres, en l'état de l'instruction, à créer un doute sérieux quant à la légalité du décret attaqué : l'absence de consultation de la CNIL sur le projet de décret méconnaît le droit interne et le droit de l'UE (2.2.2.1), le décret est entaché d'incompétence en ce que le pouvoir réglementaire a étendu son champ d'application (2.2.2.2) et le décret est entaché de défaut de base légale en ce qu'il a été pris pour l'application d'une loi transposant une directive méconnaissant le droit primaire de l'UE (2.2.2.3).

2.2.2.1. S'agissant du défaut de consultation de la CNIL

72. **En droit**, la consultation préalable de l'autorité de contrôle sur les textes organisant un traitement de données à caractère personnel constitue une obligation du droit de l'UE et de droit interne.

73. Aux termes de l'article 36, 4 du règlement (UE) 2016/679 du 27 avril 2016 (ci-après « **RGPD** ») :

> « *Les États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, o**u d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement.*** »

74. Le considérant 96 du même règlement en éclaire l'objet :

> « *L'autorité de contrôle devrait également être consultée au stade de la préparation d'une mesure législative ou réglementaire qui prévoit le traitement de données à caractère personnel, afin d'assurer que le traitement prévu respecte le présent règlement et, en particulier, **d'atténuer le risque qu'il comporte pour la personne concernée***. »

75. En droit interne, aux termes du a) du 4° du I de l'article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la CNIL :

> « *est consultée sur tout projet de loi ou de décret ou toute disposition de projet de loi ou de décret relatifs à la protection des données à caractère personnel ou au traitement de telles données* ».

76. Cette consultation obligatoire constitue, pour les personnes dont les données sont traitées, une garantie au sens de la jurisprudence *Danthony* (CE, Ass., 23 décembre 2011, n° 335033, au Recueil). Son omission, qui prive de son effet utile le contrôle préventif confié à une autorité indépendante précisément pour « ***atténuer le risque*** » que le traitement comporte pour les

[12] La jurisprudence *Carminati* (CE, 30 décembre 2002, n° 240430, p. 510), qui interdisait au juge du référé-suspension de contrôler à titre inédit la conventionnalité de la loi, a été assouplie, et a déjà été abandonnée en référé-liberté (CE, 31 mai 2016, *Gonzalez Gomez,* n° 396848, au Recueil). On peut préciser que la doctrine considère que cette jurisprudence « critiquée au sein même du Conseil d'Etat » a également vocation à être abandonnée en référé-suspension (Le guide des référés administratifs, Dalloz, 2023-2024, § 222.821).

personnes concernées (considérant 96 précité), constitue un vice substantiel entachant d'illégalité le texte adopté.

77. Elle constitue, en outre et surtout, la **méconnaissance directe d'une obligation édictée par le droit de l'Union dont le juge national doit assurer la pleine efficacité en écartant ou en privant d'effet l'acte adopté en violation de celle-ci** (CJCE, 9 mars 1978, *Simmenthal*, aff. 106/77 ; CJCE, 19 juin 1990, *Factortame*, aff. C-213/89). Cette méconnaissance caractérisant au demeurant, à elle seule, une situation d'urgence au sens de l'article L. 521-1 du code de justice administrative (*cf. supra, § 29 et s.*).

78. **En l'espèce**, le décret attaqué entre pleinement dans le champ de la double obligation de consultation rappelée ci-dessus.

79. Il constitue, au sens du paragraphe 4 de l'article 36 du RGPD, une « *mesure réglementaire fondée sur une [...] mesure législative* » (l'article 54 de la loi n° 2025-127 du 14 février 2025 de finances pour 2025, qu'il vise et pour l'application duquel il est pris), « *qui se rapporte au traitement* », puisqu'il a précisément pour objet d'organiser la collecte, la vérification, la conservation et la transmission à l'administration fiscale de données à caractère personnel à grande échelle.

80. Il détermine, par lui-même, plusieurs des caractéristiques essentielles du traitement :

- les catégories de données collectées et déclarées : prénom et nom, adresse, État(s) de résidence fiscale, numéro(s) d'identification fiscale, date et lieu de naissance des utilisateurs et des personnes détenant le contrôle des entités, ainsi que l'intégralité de leurs transactions sur crypto-actifs (articles 13 et 18 du décret) ;
- la durée de conservation des données du registre des démarches et informations, fixée à dix ans (article 8), la directive imposant que cette durée soit comprise entre cinq et dix ans ;
- les destinataires et les modalités de transmission : dépôt par voie électronique auprès de la direction générale des finances publiques, sur un support dont elle détermine les caractéristiques (article 19) ;
- la consignation des informations d'enregistrement des opérateurs dans un registre central européen administré par la Commission européenne (article 20, III) ;
- les procédures de diligence gouvernant l'identification des personnes et la vérification de la vraisemblance des informations collectées (articles 7 à 16).

81. **Or, le décret attaqué n'a pas été soumis à l'avis préalable de la CNIL, ses visas ne mentionnant que l'avis du comité consultatif de la législation et de la réglementation financières du 20 novembre 2025.**

82. Il s'ensuit que le décret attaqué a été adopté au terme d'une procédure irrégulière, en méconnaissance tant du a) du 4° du I de l'article 8 de la loi du 6 janvier 1978 que du paragraphe 4 de l'article 36 du RGPD, et que cette omission a privé les personnes concernées, au nombre desquelles figurent les requérantes, en leur qualité d'utilisatrices de services sur crypto-actifs, d'une garantie.

83. Son annulation est encourue de ce seul chef.

84. Cette violation, directe, actuelle et continue, du droit de l'Union appelle une cessation immédiate et, dans le cadre de l'instance de référé, est de nature tant à créer un doute sérieux quant à la légalité du décret qu'à concourir, à elle seule, à la caractérisation de l'urgence (*cf. supra, § 29 et s.*).

2.2.2.2. S'agissant de l'incompétence

85. Le décret attaqué apparaît entaché d'un **vice d'incompétence matérielle** en ce que les dispositions de son article 1er ont ajouté aux dispositions du I de l'article 1649 AC bis du CGI une obligation déclarative incombant aux prestataires fournissant des services de jalonnement et de prêt sur crypto-actifs alors même que la loi de transposition ne l'a pas prévu.

86. **En droit**, l'article 34 de la Constitution du 4 octobre 1958 dans sa rédaction en vigueur prévoit que la loi fixe les règles concernant « *l'assiette, le taux* ***et les modalités de recouvrement*** *des impositions de toutes natures* ».

87. L'article 34 de la Constitution place ainsi dans le domaine de la loi la détermination des modalités de recouvrement des impositions de toutes natures, ce qui inclut, ainsi que le juge le Conseil constitutionnel, les dispositions relatives au contrôle fiscal. Lorsqu'il définit une imposition, *« le législateur doit déterminer ses modalités de recouvrement,* ***lesquelles comprennent les règles régissant le contrôle*** *(...)* » (Cons. const., 30 mars 2012, n° 2012-225 QPC, *Société Unibail-Rodamco*, cons. 3).

88. Il a ainsi été jugé par le Conseil d'État que **les dispositions de l'article 1649 AG du CGI se rattachent au contrôle fiscal dès lors qu'elles font en sorte que, par des moyens contraignants, l'administration fiscale soit informée de l'existence et de la nature d'un dispositif transfrontière** *« critique* », étant tenu compte de ce que l'information devant lui être délivrée par les intermédiaires concernés est détaillée, au regard du contenu obligatoire de la déclaration.

89. Ainsi, à l'occasion de la contestation en excès de pouvoir des commentaires administratifs publiés au BOFIP, pris en application des dispositions de l'article 1649 AG du CGI, qui avaient transposé en droit interne les dispositions de la directive DAC 6, le Conseil d'État a jugé que ces actes réglementaires, ajoutant à la loi les conditions d'organisation d'un délai que celle-ci ne prévoyait pas explicitement, étaient entachés d'incompétence (CE, 25 juin 2021, n° 448486).

90. **En l'espèce**, pour transposer les dispositions de la Directive DAC 8, le législateur a créé par le biais de l'article 54 de la loi n° 2025-127 du 14 février 2025 un article 1649 AC bis au sein du CGI aux termes duquel :

> « *I. - Le* ***prestataire de services qui fournit un service sur crypto-actifs, au sens du 16 du 1 de l'article 3 du règlement (UE) 2023/1114*** *du Parlement européen et du Conseil du 31 mai 2023 sur les marchés de crypto-actifs, et modifiant les règlements (UE) n° 1093/2010 et (UE) n° 1095/2010 et les directives 2013/36/UE et (UE) 2019/1937, souscrit auprès de l'administration fiscale, dans des conditions et délais fixés par décret, une déclaration relative aux transactions réalisées par des utilisateurs de crypto-actifs par son intermédiaire.* »

91. Il résulte de ces dispositions que le CGI ne soumet à l'obligation de déclaration que les prestataires de services sur crypto-actifs au sens du 16 du 1 de l'article 3 du Règlement MiCA.

92. Or, il est constant que lesdits prestataires **sont définis limitativement par ledit règlement**.

93. Les dispositions de l'article 1er du décret attaqué inséré dans le Chapitre 1er relatif aux définitions relatives aux personnes soumises à l'obligation déclarative prévoient pour leur part que :

> « *Pour l'application des articles 1649 AC bis à 1649 AC sexies du code général des impôts :*
>
> *1° Constituent des prestataires qui fournissent un service sur crypto-actifs :*
>
> *a) Un prestataire de services sur crypto-actifs qui est une personne morale ou une autre entreprise dont l'occupation ou l'activité consiste à fournir un ou plusieurs services sur crypto-actifs à des clients à titre professionnel, et qui est autorisée à fournir des services sur crypto-actifs conformément aux articles 59 ou 60 du règlement (UE) 2023/1114 du Parlement européen et du Conseil du 31 mai 2023 susvisé ;*
>
> *(...)*
>
> *2° Un service sur crypto-actifs s'entend des services sur crypto-actifs au sens de l'article 3, paragraphe 1, point 16, du même règlement (UE) 2023/1114 du Parlement européen et du Conseil du 31 mai 2023,* ***y compris le jalonnement et le prêt de crypto-actifs*** *; (...)* »

94. Le 2° de l'article 1er du décret attaqué ajoute ainsi aux services sur crypto-actifs visés par le règlement (UE) 2023/1114 **les services de jalonnement et de prêt de crypto-actifs** dans la liste des services dont la fourniture engendre l'assujettissement à l'obligation déclarative prévue à l'article 1649 AC bis du CGI.

95. Il est pourtant évident que ces deux services ne figurent pas parmi ceux mentionnés au point 16 du paragraphe 1 de l'article 3 du règlement sur les marchés de crypto-actifs.

96. Ce faisant, il est donc clair que le 2° de l'article 1er du décret en litige a ainsi ajouté à la catégorie des prestataires de services sur crypto-actifs au sens du règlement (UE) 2023/1114 les acteurs fournissant des services de jalonnement et de prêt sur crypto-actifs comme étant soumis à l'obligation déclarative, sans habilitation législative.

97. **Or, il ressort de la jurisprudence précitée du Conseil d'État et du Conseil constitutionnel que le pouvoir réglementaire ne pouvait ainsi soumettre à cette obligation relative aux modalités de recouvrement des impositions incluant les règles qui en régissent le contrôle, les personnes fournissant des services de jalonnement et de prêt sur crypto-actifs, alors que la loi ne le prévoyait pas.**

98. Par conséquent, le décret est entaché d'incompétence.

2.2.2.3. S'agissant du défaut de base légale du décret d'application de la loi de transposition de la Directive DAC 8, en raison de la méconnaissance du droit primaire de l'Union européenne

99. Enfin, le décret attaqué est privé de base légale dès lors qu'il a pour objet de mettre en œuvre les articles 1649 AC bis à 1649 AC sexies du CGI, issus de l'article 54 de la loi n° 2025-127 du 14 février 2025, lesquels assurent la transposition des dispositions précises et inconditionnelles de la Directive DAC 8, qui méconnaissent elles-mêmes le droit primaire de l'Union — notamment les articles 7, 8 et 52, § 1, de la charte des droits fondamentaux de l'Union européenne (la « **Charte** ») — ainsi que l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (la « **Convention EDH** »). Est ainsi excipée, par le truchement de la loi de transposition, l'invalidité de la Directive DAC 8 elle-même, dont l'appréciation relève de la Cour de justice sur renvoi préjudiciel.

100. Le renvoi préjudiciel en appréciation de validité de la Directive DAC 8 est expressément sollicité dans le cadre de la requête au fond n° 513141, **auquel il est renvoyé pour l'exposé exhaustif du moyen** (***cf. Pièces n° 2 et 3***).

101. **En droit**, **en premier lieu**, **sur l'office du juge des référés saisi d'une contestation de la validité du droit dérivé de l'Union**, lorsqu'il est soutenu qu'une directive méconnaît les traités, la Charte ou les principes généraux du droit de l'Union, il appartient au juge administratif, en l'absence de difficulté sérieuse, d'écarter le moyen ou, dans le cas contraire, de saisir la CJUE d'une question préjudicielle dans les conditions prévues à l'article 267 du TFUE (CE, 6 mai 2019, n° 416088, aux tables) ; il en va de même lorsqu'est invoquée la méconnaissance de la Convention EDH, dont les garanties font partie du droit de l'Union en tant que principes généraux en vertu de l'article 6, § 3 du TUE (CE, 20 juin 2016, n° 383333, aux tables). Le juge national ne peut en effet constater lui-même l'invalidité d'un acte de droit dérivé, ce contrôle relevant du monopole de la Cour de justice (CJCE, 22 octobre 1987, *Foto-Frost*, aff. 314/85, pt 20).

102. Ce monopole ne prive pas le juge national, et *a fortiori* le juge de l'urgence, du pouvoir de faire provisoirement obstacle, au profit du justiciable, aux effets de l'acte national pris en application du droit dérivé dont la validité est sérieusement contestée. Au contraire, le droit de l'Union lui impose de disposer de ce pouvoir.

103. Par l'arrêt *Zuckerfabrik Süderdithmarschen* (CJCE, 21 février 1991, aff. jtes C-143/88 et C-92/89), la Cour de justice a dit pour droit que le juge national peut accorder un sursis à l'exécution d'un acte administratif national pris sur la base d'un acte de droit dérivé dont la légalité est contestée, et dont seule la Cour peut constater l'invalidité.

104. Il en résulte que l'hypothèse dans laquelle l'acte national est contesté en raison de l'invalidité alléguée de l'acte de droit dérivé qu'il met en œuvre au regard du droit primaire, relève d'un régime de protection provisoire directement exigé par le droit de l'Union, strictement symétrique de celui applicable lorsque c'est l'acte national qui méconnaît le droit de l'Union.

105. **En deuxième lieu,** sur les dispositions litigieuses, la Directive DAC 8 a inséré dans la directive 2011/16/UE un article 8 bis quinquies qui impose aux États membres, d'une part, d'exiger des prestataires de services sur crypto-actifs déclarants qu'ils remplissent les obligations de

déclaration et appliquent les procédures de diligence prévues à son annexe VI et, d'autre part, d'échanger automatiquement les informations ainsi déclarées avec les États membres de résidence des utilisateurs, dans les neuf mois suivant la fin de l'année civile concernée (soit un premier échange au plus tard le 30 septembre 2027 pour l'année 2026).

106. Les informations échangées comprennent, pour chaque utilisateur devant faire l'objet d'une déclaration : son nom, son adresse, son ou ses États de résidence, son ou ses NIF, sa date et son lieu de naissance, ainsi que, **pour chaque type de crypto-actif, le montant brut, le nombre d'unités et le nombre de transactions au titre des acquisitions et cessions contre monnaie fiat ou contre d'autres crypto-actifs, des opérations de paiement de détail et des transferts entrants et sortants, y compris vers des adresses de registres distribués non associées à un prestataire** (DAC 8, art. 8 bis quinquies, § 3).

107. L'annexe VI définit très largement le champ du dispositif : sont visés tous les prestataires au sens du Règlement MiCA ainsi que les « *opérateurs de crypto-actifs* » non agréés, pour l'ensemble des services sur crypto-actifs, « *y compris le jalonnement et le prêt* » ; sont concernés tous les utilisateurs, personnes physiques ou entités, à l'exception d'exclusions limitées (entités cotées, entités publiques, organisations internationales, banques centrales, certaines institutions financières) ; et les prestataires doivent conserver les informations recueillies pendant une durée comprise entre cinq et dix ans[13].

108. L'article 16 de la directive 2011/16/UE, tel que modifié, définit les finalités d'exploitation de ces informations : établissement et application de la législation relative aux impôts, à la TVA et autres taxes indirectes, droits de douane, lutte contre le blanchiment de capitaux et le financement du terrorisme, ainsi que mise en œuvre des mesures restrictives fondées sur l'article 215 TFUE ; **ces finalités ne sont pas limitatives, chaque État membre pouvant prévoir dans son droit national d'autres finalités, moyennant notification ou autorisation de l'État émetteur**[14].

109. L'article 21, § 5, confie enfin à la Commission le soin de mettre au point, au plus tard le 31 décembre 2026, un répertoire central dans lequel les informations communiquées au titre de l'article 8 bis quinquies, § 2 et 3, sont enregistrées, chaque État membre n'ayant accès qu'aux informations relatives à ses propres résidents ; et l'article 25 soumet expressément l'ensemble de ces traitements au RGPD, dont l'article 5, § 1, énonce les principes de limitation des finalités, de minimisation, de limitation de la conservation, d'intégrité et de confidentialité.

110. Ces dispositions ont été transposées, sans marge d'appréciation, par l'article 54 de la loi n° 2025-127 du 14 février 2025 (art. 1649 AC bis à 1649 AC sexies du CGI), dont le décret attaqué fixe les modalités d'application.

111. **En troisième lieu, sur le droit au respect de la vie privée et à la protection des données personnelles**, aux termes de l'article 7 de la Charte, « *toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications* » ; aux termes de son article 8, « *toute personne a droit à la protection des données à caractère personnel la concernant* », lesquelles «

[13] Dir. 2011/16/UE, annexe VI, section V, B, 1, telle qu'insérée par l'annexe III de la directive DAC 8.

[14] Dir. 2011/16/UE, art. 16, 2, al. 1 et 2, tel que modifié par la directive DAC 8.

doivent être traitées loyalement, à des fins déterminées et sur la base [d'un] fondement légitime prévu par la loi », sous le contrôle d'une autorité indépendante.

112. L'article 8 de la Convention EDH garantit des droits correspondants qui constituent, en vertu de l'article 52, § 3, de la Charte, un seuil de protection minimale (CJUE, 8 décembre 2022, *Orde van Vlaamse Balies*, aff. C-694/20, pts 25 et 26).

113. Il est constant que « *la communication de données à caractère personnel à un tiers, tel qu'une autorité publique, constitue une ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, quelle que soit l'utilisation ultérieure des informations communiquées* » (CJUE, 21 juin 2022, *Ligue des droits humains*, aff. C-817/19, pt 96 ; CJUE, 22 novembre 2022, *Luxembourg Business Registers*, aff. C-37/20 et C-601/20, pt 39), *a fortiori* s'agissant de données bancaires et patrimoniales (CEDH, 22 décembre 2015, *G.S.B. c. Suisse*, n° 28601/11, pt 93 ; CEDH, 14 décembre 2021, *Samoylova c. Russie*, n° 49108/11, pt 62).

114. Conformément à l'article 52, § 1, de la Charte, une telle ingérence n'est admissible que si elle est prévue par la loi, respecte le contenu essentiel des droits, répond effectivement à un objectif d'intérêt général reconnu par l'Union et demeure nécessaire et proportionnée.

115. **S'agissant du principe de légalité**, l'acte qui permet l'ingérence doit définir lui-même la portée de la limitation (CJUE, 21 juin 2022, *Ligue des droits humains*, préc., pt 114 ; CJUE, 22 novembre 2022, *Luxembourg Business Registers*, préc., pt 47). La Cour EDH exige quant à elle, au titre de la « *qualité de la loi* », que **la marge d'appréciation des autorités soit suffisamment limitée** — par des critères pertinents conditionnant la décision d'ingérence et par une obligation de motivation — (CEDH, 8 janvier 2026, *Ferrieri et Bonassisa c. Italie*, n° 40607/19 et 34583/20, pts 81 et 82) et, si l'efficacité fiscale peut justifier l'absence de contrôle indépendant *ex ante*, que soient **prévues d'autres garanties effectives contre l'abus et l'arbitraire, notamment un contrôle indépendant ou judiciaire *ex post*** (même arrêt, pt 86), un recours dont l'existence et l'accessibilité sont incertaines et l'intervention indéterminée dans le temps ne constituant pas une garantie suffisante (même arrêt, pts 92 et 93).

116. **S'agissant de l'objectif d'intérêt général**, si la prévention du risque de fraude et d'évasion fiscales constitue un objectif reconnu par l'Union (CJUE, 6 octobre 2020, *État luxembourgeois*, aff. C-245/19 et C-246/19, pts 86 à 88), de même que la lutte contre la planification fiscale agressive (CJUE, *Orde van Vlaamse Balies*, préc., pt 44 ; CJUE, 29 juillet 2024, *Belgian Association of Tax Lawyers*, aff. C-623/22, pt 141), la Cour a toujours exigé, pour reconnaître de tels objectifs, un lien — fût-il ténu — entre la mesure et l'existence d'un réel risque de fraude (montages abusifs : CJUE, 22 novembre 2017, *Cussens*, aff. C-251/16, pt 53 ; sauvegarde de la répartition du pouvoir d'imposition : CJUE, 26 février 2019, *X GmbH c/ Finanzamt Stuttgart*, aff. C-135/17, pt 72) — **sauf à ériger en intérêt général tout dispositif de surveillance généralisée, qui, par définition, accroît la prévention de tous types d'infractions**.

117. **S'agissant de la nécessité et de la proportionnalité**, l'ingérence doit être limitée au strict nécessaire (CJUE, 8 avril 2014, *Digital Rights Ireland*, aff. C-293/12 et C-594/12, pt 56). L'arrêt *Orde van Vlaamse Balies* — rendu précisément à propos d'une disposition de la directive 2011/16/UE, dont il a prononcé l'invalidation au regard de l'article 7 de la Charte — explicite la méthode d'appréciation : il convient de vérifier que la mesure (i) répond à un objectif d'intérêt général

reconnu par l'Union, (ii) est apte à réaliser cet objectif, (iii) est limitée au strict nécessaire, « *en ce sens que l'objectif poursuivi ne pourrait raisonnablement être atteint de manière aussi efficace par d'autres moyens moins attentatoires à ce droit* », et (iv) n'est pas disproportionnée par rapport audit objectif, « *ce qui implique notamment une pondération de l'importance de celui-ci et de la gravité de ladite ingérence* » (pts 41 et 42).

118. Le même arrêt précise que l'aptitude d'une mesure à « *contribuer* » à l'objectif ne suffit pas à la rendre nécessaire si celui-ci peut être atteint par des moyens moins intrusifs (pt 46) ; et la nécessité s'apprécie au regard de l'ensemble des instruments moins attentatoires déjà disponibles permettant d'atteindre le même objectif (pts 47 à 52). Les principes de l'article 5, § 1, du RGPD — limitation des finalités, minimisation, limitation de la conservation, intégrité et sécurité — constituent, dans ce cadre, les critères opératoires du contrôle, la Cour ayant en outre censuré, dans l'arrêt *Digital Rights Ireland* (pt 66), l'absence de protection suffisante contre les risques d'abus et d'accès illicites.

119. **En l'espèce**, les dispositions litigieuses de la Directive DAC 8, dont le décret attaqué constitue la mesure d'exécution, organisent une ingérence particulièrement grave dans les droits garantis par les articles 7 et 8 de la Charte et 8 de la Convention EDH, qui méconnaît le principe de légalité, ne poursuit pas d'objectif d'intérêt général établi et n'est, en tout état de cause, ni apte, ni nécessaire, ni proportionnée.

i) Des ingérences d'une particulière gravité

120. **D'une part,** l'ampleur de la collecte est sans précédent. La directive n'impose pas la seule communication des revenus générés par les contribuables. Elle exige la déclaration de l'intégralité des transactions réalisées par les utilisateurs : transactions d'échange (achat, échange, vente) mais aussi simples transferts, de sorte qu'un dépôt de crypto-actifs sur une plateforme sera déclaré et que la totalité du patrimoine en crypto-actifs, qu'il génère ou non des revenus imposables, sera placée sous la surveillance des autorités. **Rapportée au secteur bancaire, cette obligation équivaudrait à imposer aux banques de déclarer chaque année la somme agrégée de tous les dépôts et retraits réalisés sur les comptes de tous leurs clients** (là où la directive DAC 2, mettant en œuvre la norme commune de déclaration, se limite au solde du compte en fin d'année et aux revenus versés[15]). Ces données révèlent ainsi, avec précision, l'état et la localisation du patrimoine en crypto-actifs des personnes concernées.

121. **D'autre part**, ces données sont d'une sensibilité très particulière au regard des risques pour l'intégrité physique des personnes qu'elles génèrent. Ainsi que mentionné supra (*cf. supra, § 9 à 12*) les données révélant l'identité, l'adresse et le patrimoine de leurs détenteurs suscitent la convoitise d'une criminalité organisée aux modes opératoires d'une violence extrême.

122. Or les administrations destinataires de ces données n'apparaissent pas en mesure d'en assurer la sécurité, ainsi qu'en attestent les compromissions massives et répétées relevées *supra* (*cf. § 13 à 15*).

[15] Directive 2014/107/UE (« DAC 2 »), annexe I, section I, points A 1) à A 7) ; CGI, art. 1649 AC, I ; BOI-INT-AEA-20, 26 février 2020.

123. Les ingérences en cause (collecte, conservation décennale, échange automatique et centralisation à l'échelle de l'Union) sont donc établies et doivent être regardées comme particulièrement graves.

ii) La méconnaissance du principe de légalité

124. Ces ingérences graves ne satisfont pas aux exigences du principe de légalité et de qualité de la loi tirés de l'article 52, § 1, de la Charte, interprété à la lumière de la jurisprudence de la CEDH.

125. **D'une part**, la marge d'appréciation conférée aux autorités nationales n'est pas suffisamment limitée : les finalités d'exploitation des données ne sont pas limitatives, chaque État membre pouvant en ajouter par simple notification[16] ; aucun critère (volume de transactions, niveau de revenus, indices objectifs et préalables de fraude) ne conditionne la consultation et l'exploitation des données par les nombreuses autorités compétentes (en France : DGFIP, douanes, autorité judiciaire, Tracfin, officiers de police judiciaire, ACPR, AMF et divers ordres professionnels (LPF, art. L. 83 A et L. 167 A)) et aucune obligation de motivation ne permet d'en contrôler la légitimité, situation dans laquelle la CEDH voit l'exercice d'un pouvoir discrétionnaire sans limite, incompatible avec l'exigence de qualité de la loi (CEDH, *Ferrieri et Bonassisa*, préc., pts 81 et 82) ; enfin, aucune disposition ne permet à un État membre de s'opposer à la transmission des données à un autre État ne présentant pas de garanties équivalentes.

126. **D'autre part**, la directive ne prévoit aucune garantie procédurale suffisante contre l'abus et l'arbitraire : en l'absence de critères et de motivation, aucun contrôle indépendant, notamment juridictionnel, ne peut être exercé sur la consultation et l'exploitation des données (v. CEDH, *Ferrieri et Bonassisa*, préc., pt 98) ; la seule garantie offerte aux utilisateurs — l'information préalable et l'exercice des droits tirés du RGPD (dir. 2011/16/UE, art. 25, § 4) — demeure théorique, ces droits étant neutralisés par les durées de conservation imposées et dépourvus de tout effet suspensif sur la communication des données ; et le recours juridictionnel éventuel, dans le cadre de la contestation d'impositions ultérieures, présente une existence et une accessibilité incertaines et n'interviendrait qu'à un moment futur indéterminé, ce qui ne satisfait pas aux exigences conventionnelles (CEDH, *Ferrieri et Bonassisa*, préc., pts 92 et 93).

iii) L'absence d'objectif d'intérêt général établi

127. L'exposé des motifs de la Directive DAC 8 rattache le dispositif à la lutte contre la fraude et l'évasion fiscale, dans un contexte de risque tenant aux caractères décentralisé et transfrontière des crypto-actifs, qui compliqueraient la détection des faits générateurs (cons. 1, 6, 7, 11 et 12). Or le dispositif effectivement adopté est sans rapport avec ce risque : **il s'applique aux opérations nationales comme transfrontières** (cons. 13) ; il couvre des **transactions non susceptibles de constituer des faits générateurs d'imposition** (achats, transferts, échanges crypto-crypto neutralisés fiscalement dans plusieurs États dont la France), alors que la Commission proposait initialement de limiter l'obligation aux seuls « *revenus perçus* »[17] ; et **il vise tous les utilisateurs, indépendamment de tout indice de risque**, le particulier ayant acquis une centaine d'euros de crypto-actifs voyant l'ensemble de ses transactions déclarées au même titre que l'entreprise en encaissant des millions.

[16] Dir. 2011/16/UE, art. 16, 2, al. 1 et 2, préc.

[17] Proposition de directive n° COM/2022/707, exposé des motifs.

128. Il s'agit donc, en réalité, d'un objectif de surveillance généralisée d'un type d'actif jugé sensible et non de lutte contre la fraude. Aucune étude produite aux travaux préparatoires n'établit d'ailleurs de lien entre le niveau de fraude et l'utilisation de crypto-actifs, ni que ceux-ci y participeraient davantage que les devises légales, considérablement moins surveillées ; le comité d'examen de la réglementation a lui-même relevé que le rapport de la Commission ne décrivait pas suffisamment le vide juridique qu'il visait à combler. Faute du lien avec un réel risque de fraude qu'exige la jurisprudence de la Cour, l'objectif poursuivi ne saurait être regardé comme un objectif d'intérêt général reconnu par l'Union.

iv) Une ingérence ni apte, ni nécessaire, ni proportionnée

129. À supposer même l'objectif admis, l'ingérence ne satisfait à aucun des trois critères du test de proportionnalité tel qu'explicité par l'arrêt *Orde van Vlaamse Balies*.

130. Elle n'est pas apte à réaliser l'objectif poursuivi : les obligations déclaratives pèsent exclusivement sur des entreprises centralisées, le Règlement MiCA excluant les services « *fournis de manière entièrement décentralisée sans aucun intermédiaire* ». Or les transactions réalisées par l'intermédiaire des prestataires ne sont ni décentralisées (elles se traduisent par de simples inscriptions en compte, sans traduction sur la *blockchain*) ni pseudonymes (les prestataires, assujettis à la lutte contre le blanchiment, tiennent des comptes nominatifs). Le dispositif ne traite donc en rien les risques (décentralisation, pseudonymat) invoqués pour le justifier, et ne prévoit rien au-delà des transactions centralisées et nominatives.

131. Elle n'est pas limitée au strict nécessaire, l'objectif pouvant raisonnablement être atteint de manière aussi efficace par des moyens moins attentatoires :

i) **par une approche par les risques**, limitant la déclaration aux utilisateurs présentant des indices objectifs de risque (les prestataires, déjà tenus de classifier leurs clients par niveaux de risque au titre de la lutte contre le blanchiment et disposant d'une visibilité totale sur les transactions, sont techniquement en mesure de l'appliquer, à l'image des diligences graduées de la directive DAC 2 selon la valeur des comptes) ;

ii) **par une limitation aux utilisateurs non-résidents**, seuls concernés par le risque transfrontière invoqué, les administrations disposant déjà, pour leurs résidents, d'un arsenal déclaratif et de contrôle complet (pour la France : art. 150 VH bis et 1649 bis C du CGI, droit de communication, assistance administrative — cf. mémoire complémentaire, § 28 et s.) ;

iii) **par une limitation aux transactions susceptibles de constituer des faits générateurs d'imposition**, conformément à la proposition initiale de la Commission limitée aux revenus[18], les transferts de compte à compte du même utilisateur (que le prestataire est en mesure d'identifier au titre du règlement TFR) et les opérations neutres fiscalement pouvant en être exclus ;

[18] Proposition de directive n° COM/2022/707, préc.

iv) **par un encadrement de la consultation et de l'exploitation des données** (critères préalables caractérisant un risque réel, obligation de motivation, droit d'opposition à l'échange avec un État ne présentant pas de garanties) ;

v) **par des garanties techniques de sécurité** : en substituant aux échanges bilatéraux cloisonnés un répertoire central agrégeant les données de l'ensemble des utilisateurs de l'Union, le dispositif crée un point de défaillance unique dont la compromission exposerait l'intégralité des données patrimoniales collectées, sans qu'aucune protection cryptographique (chiffrement de bout en bout, chiffrement homomorphe pour les traitements statistiques de la Commission) ne rende techniquement effective la limitation purement logicielle des accès, en méconnaissance de l'exigence de sécurité appropriée de l'article 5, § 1, f), du RGPD, alors même que les compromissions de bases administratives par usurpation d'identifiants se sont déjà réalisées ;

vi) **par une durée de conservation alignée sur le délai de reprise de droit commun**, la fourchette de cinq à dix ans imposée par la directive excédant largement ce qui est nécessaire, la directive DAC 2 s'étant limitée à cinq ans.

132. Elle est ainsi disproportionnée.

133. Au surplus, la collecte généralisée et indifférenciée du patrimoine intégral en crypto-actifs de l'ensemble des utilisateurs, sans distinction selon le risque ni selon la nature imposable des opérations, méconnaît le principe de minimisation (RGPD, art. 5, § 1, c) ; les finalités non limitatives et l'exploitation possible à des fins répressives, douanières ou de politique étrangère, sans information des personnes concernées, méconnaissent le principe de limitation des finalités (art. 5, § 1) ; et l'absence de toute limite à l'exploitation algorithmique des données expose les personnes concernées à des décisions fondées sur des traitements automatisés au sens de l'article 22 du RGPD (v. CJUE, 7 décembre 2023, *OQ c. Land Hessen*, aff. C-634/21, pts 42 à 49).

134. **La gravité de l'ingérence est ainsi sans relation avec l'importance de l'objectif, dont la pondération avec les droits en cause n'a au demeurant jamais été démontrée par le législateur de l'Union.**

135. Ces éléments soulèvent, à tout le moins, une difficulté sérieuse quant à la validité de la Directive DAC 8, justifiant la question préjudicielle en appréciation de validité sollicitée dans l'instance au fond (cf. mémoire complémentaire, § 232).

136. Ce doute sérieux sur la validité de la directive emporte, par voie de conséquence, un doute sérieux sur la légalité du décret attaqué, privé de base légale.

137. À tous égards donc, il existe un doute sérieux quant à la légalité du décret attaqué qui doit conduire à sa suspension, à titre conservatoire, dans l'attente que le juge de l'excès de pouvoir se prononce.

ORWL

PAR CES MOTIFS

Et tous autres à produire, déduire ou suppléer, au besoin d'office, les sociétés Paymium, Leonod et Satoshi Portal Inc. concluent qu'il plaise au Conseil d'État de :

SUSPENDRE l'exécution du décret attaqué ;

METTRE A LA CHARGE de l'État le versement d'une somme de 5 000 euros sur le fondement de l'article L. 761-1 du code de justice administrative.

Avec les conséquences de droit.

ORWL Avocats
Me Romain Chilly
Avocat associé

ORWL Avocats
Me Alexandre Lourimi
Avocat associé