



---

# ASSEMBLÉE NATIONALE

## COMMUNICATION

en conclusion des travaux de la mission d'information flash relative aux dysfonctionnements  
du logiciel Hélios

ET PRÉSENTÉE PAR

M. JACQUES OBERTI  
rapporteur

---



## SOMMAIRE

|  |           |
|--|-----------|
| (I) En premier lieu, l'analyse du déroulement de l'incident révèle un déficit d'anticipation partiellement explicable et des faiblesses certaines de la communication de crise de la DGFIP .....                   | 6         |
| 1. L'application Hélios constitue l'outil comptable du quotidien pour les collectivités locales et les établissements hospitaliers .....   | 6         |
| 2. Le contexte récent est marqué par des dysfonctionnements multiples de systèmes informatiques de la DGFIP et d'autres administrations.....   | 7         |
| 3. Si le dysfonctionnement d'Hélios au mois de février 2026 a pour origine une défaillance unique et improbable, l'absence de mesures de secours a allongé les délais de redémarrage .....                         | 8         |
| 4. Bien que la DGFIP ait mis en œuvre un ensemble de mesures de communication de crise, l'hétérogénéité de la circulation de l'information a conduit à une forte inquiétude pour la majorité des ordonnateurs..... | 10        |
| (II) Si le pire a été évité, les conséquences de l'incident sur les utilisateurs d'Hélios et leurs partenaires financiers demeurent significatives .....   | 12        |
| 1. Le dysfonctionnement a fortement retardé l'ensemble des opérations comptables, affectant tout particulièrement le règlement des fournisseurs et l'approbation des comptes .....                                 | 12        |
| 2. Un même incident, s'il était survenu à un autre moment, aurait pu présenter des conséquences désastreuses .....   | 15        |
| 3. Un incident similaire, concernant une autre application ou résultant d'une cyberattaque, pourrait conduire à de fortes difficultés financières pour les utilisateurs d'Hélios et leurs partenaires.....         | 16        |
| (III) Il importe de renforcer les mesures de prévention de tels dysfonctionnements, et d'améliorer les modalités de gestion de crise en cas d'incident.....  | 17        |
| 1. Afin de prévenir l'émergence d'un incident similaire, certaines vulnérabilités pourraient être réduites .....   | 17        |
| 2. En vue de renforcer les modalités de gestion de crise, il convient d'anticiper la création d'un plan formalisé de communication et des solutions redondantes .....  | 20        |
| <b>LISTE DES PERSONNES AUDITIONNÉES PAR LE RAPPORTEUR .....</b>  | <b>22</b> |



Monsieur le Président,

Chers collègues,

La commission des finances, de l'économie générale et du contrôle budgétaire a créé le mardi 24 mars dernier une mission d'information *flash* chargée d'analyser le déroulement, les conséquences et la gestion du dysfonctionnement survenu au mois de février 2026 de l'application Hélios, fournie par la direction générale des finances publiques (DGFIP) aux collectivités locales et aux établissements hospitaliers, en vue de la réalisation de l'ensemble de leurs opérations comptables. La commission a confié à M. Jacques Oberti, député de la Haute-Garonne (Socialistes et apparentés), le soin de rapporter cette mission d'information.

Cet incident technique, résultant d'une défaillance matérielle sur une baie de stockage, a intégralement suspendu les opérations comptables transitant par Hélios. Entre le 5 et le 17 février, la moitié des utilisateurs d'Hélios ont ainsi été dans l'incapacité de réaliser la bonne transmission des titres et des mandats, de consulter le niveau de leur trésorerie et de compléter le processus de clôture de leurs comptes. Ce dysfonctionnement ne semble pas isolé, à la lumière d'autres incidents récents d'autre nature ayant notamment affecté des services en ligne et fichiers de la DGFIP (dysfonctionnement GMBI et d'OCAPI, accès illicite aux données de FICOBA, etc.), de nombreux hôpitaux, ou encore le groupe La Poste (attaques DDoS) pour faire écho à une autre mission d'information rapportée par M. Jacques Oberti.

Les objectifs poursuivis lors de la création de cette mission *flash* étaient multiples : documenter le déroulement de l'incident, de la réponse technique et de la communication de crise de la DGFIP ; objectiver les conséquences de l'incident en matière de retards et de décalage des opérations comptables et de gestion des ressources humaines des organismes concernés ; et surtout formuler des recommandations en vue de prévenir l'émergence d'incidents similaires, quelle qu'en soit la nature, et d'améliorer leur gestion s'ils surviennent tout de même.

En deux mois, le rapporteur a entendu les associations d'élus locaux, les gestionnaires publics et directeurs d'établissements hospitaliers concernés par l'incident, les organisations syndicales et les autorités administratives de la DGFIP, des éditeurs de logiciels et des agences de l'État compétentes, ainsi que le ministre de l'action et des comptes publics, M. David Amiel. Le rapporteur tient à remercier l'ensemble des personnes qui l'ont averti de l'incident – en particulier en outre-mer –, ainsi que les organismes qui ont répondu à ses invitations et ceux qui lui ont adressé une contribution écrite.

Après une présentation succincte du contexte et du déroulement de la défaillance de l'application Hélios (I), le présent rapport analyse ses conséquences

effectives et potentielles (II) et formule des recommandations constructives afin d'améliorer la prévention et la gestion de ce type d'incidents techniques (III).

**(I) En premier lieu, l'analyse du déroulement de l'incident révèle un déficit d'anticipation partiellement explicable et des faiblesses certaines de la communication de crise de la DGFIP**

## **1. L'application Hélios constitue l'outil comptable du quotidien pour les collectivités locales et les établissements hospitaliers**

L'application Hélios appartient à la suite d'applications développées dans le cadre du programme *Copernic* de refondation des systèmes d'information fiscaux lancé en 2001 par les anciennes administrations fiscales<sup>1</sup>. Elle a progressivement remplacé, entre 2005 et 2012, les solutions disparates utilisées jusqu'alors. L'ensemble des ordonnateurs des collectivités locales et des établissements hospitaliers et médicaux-sociaux utilisent Hélios<sup>2</sup>. Pour les 20 000 agents de la DGFIP et pour les 55 000 ordonnateurs qui y accèdent, Hélios constitue un outil du quotidien, dont l'utilisation est imposée par la loi<sup>3</sup>. Il permet la réalisation de l'intégralité des opérations comptables, à savoir :

- la transmission et la réception de l'ensemble des titres et des mandats de paiement<sup>4</sup> à la DGFIP, à travers le protocole d'échange standard d'Hélios (PES V2) et via un tiers de télétransmission ;
- la consultation du niveau de trésorerie, du statut des paiements et des encaissements passés et à venir, des marchés publics, des régies, des immobilisations, ainsi que l'extraction et le traitement de l'ensemble de ces données ;
- l'ensemble des étapes de préparation de la clôture des comptes : échanges avec les conseillers aux décideurs locaux, rapprochements des comptes administratifs et de gestion, signature des comptes financiers unique (CFU) et des comptes de gestion, dépôt des documents pour transmission à la DGFIP.

---

<sup>1</sup> La direction générale des impôts (DGI) et la direction générale de la comptabilité publique (DGCP) ont fusionné en 2008 pour former la direction générale des finances publiques (DGFIP).

<sup>2</sup> À l'exception de l'Assistance Publique - Hôpitaux de Paris (AP-HP) qui dispose de procédures comptables spécifiques, ainsi que de certaines collectivités d'outre-mer.

<sup>3</sup> En vertu de l'arrêté du 27 juin 2007 portant application de l'article D. 1617-23 du code général des collectivités territoriales relatif à la dématérialisation des opérations en comptabilité publique, le recours à Hélios est exclusif et obligatoire.

<sup>4</sup> Les mandats correspondent aux ordres de virement émis par les ordonnateurs en vue de réaliser un paiement. Les titres correspondent aux opérations de recouvrement des créances.

Les serveurs d'Hélios sont situés à Versailles et à Metz. Ces deux sites se partagent respectivement la moitié des postes comptables, sans aucun lien de proximité géographique. Ils sont par ailleurs spécialisés respectivement dans l'exploitation applicative – c'est-à-dire le traitement final des données – et la gestion et le suivi des flux entrants et sortants. En d'autres termes, les serveurs de Metz sont les seuls à disposer d'un module de réception des flux entrants.

Ces deux serveurs accueillent une quinzaine de sites d'hébergement, dits « sites logiques », assignés à des fonctions distinctes, dont près de la moitié correspondent aux opérations des utilisateurs courants de l'application (ordonnateurs des collectivités locales et des établissements hospitaliers). Un site logique est consacré au module CDG-D SPL, permettant la préparation de la clôture des comptes.

Le dysfonctionnement matériel ayant affecté les serveurs de Metz, le transit des flux entrants et sortants pour l'ensemble des postes comptables a été interrompu, mais n'a pas, pour la moitié des postes qui relèvent du site de Versailles, affecté le traitement du stock des flux déjà transmis. Les sites logiques de Metz ont graduellement redémarré après l'incident, et non simultanément, expliquant la reprise hétérogène des opérations.

## **2. Le contexte récent est marqué par des dysfonctionnements multiples de systèmes informatiques de la DGFIP et d'autres administrations**

La DGFIP opère un catalogue de 800 applicatifs, et emploie à cet effet près de 25 % des informaticiens civils de l'État<sup>5</sup>. Si des incidents peuvent toujours survenir, ils sont le plus souvent gérés avec efficacité, comme l'ont souligné la DGFIP et l'agence pour l'information financière de l'État (AIFE) lors de leurs auditions. Toutefois, certains dysfonctionnements notables ont émaillé l'actualité récente. En ce qui concerne des services relatifs aux impôts fonciers locaux tels que Gérer mes biens immobiliers (GMBI) et Gesloc, un récent rapport d'information de la commission des finances de l'Assemblée nationale analyse ces incidents<sup>6</sup>.

Outre des dysfonctionnements techniques, des intrusions malveillantes ont également été observées comme lors de la consultation illicite de données du fichier des comptes bancaires (FICOBA) fin janvier 2026. Enfin, d'autres dysfonctionnements récents n'ont pas connu d'importante couverture médiatique malgré leur réel impact – c'est notamment le cas de l'application OCAPI de traitement des pensions de retraite.

---

<sup>5</sup> Schéma directeur du numérique, 2025

[https://www.economie.gouv.fr/files/files/directions\\_services/dgfip/Rapport/schema\\_dir\\_num/sdnum.pdf](https://www.economie.gouv.fr/files/files/directions_services/dgfip/Rapport/schema_dir_num/sdnum.pdf).

<sup>6</sup> Assemblée nationale, commission des finances, M. David Amiel et Mme Christine Pirès Beaune, rapport d'information relatif aux dysfonctionnements dans la gestion des impôts locaux et leurs conséquences.

La DGFIP n'est pas la seule administration concernée par ce type d'incidents. L'ANSSI rapporte 2 209 signalements et 1 366 incidents en 2025<sup>7</sup>, qui ont affecté quatre secteurs d'activité en particulier : l'éducation et la recherche (34 %), les ministères et les collectivités territoriales (24 %), la santé<sup>8</sup> (10 %) et les télécommunications (9 %). Concernant ce dernier secteur, la mission d'information de la commission des finances relative aux services publics de la Poste en vue d'une nouvelle loi postale, dont les travaux sont en cours<sup>9</sup>, a pu documenter des attaques par déni de service distribué, dites DDoS, contre les infrastructures du groupe La Poste.

### **3. Si le dysfonctionnement d'Hélios au mois de février 2026 a pour origine une défaillance unique et improbable, l'absence de mesures de secours a allongé les délais de redémarrage**

L'incident qui a affecté Hélios en février 2026 a été causé par une défaillance matérielle du module de déduplication des données de la baie de stockage du site de Metz, qui a pour objectif d'économiser de l'espace de stockage des données en évitant que celles-ci soient dupliquées. Une telle défaillance était improbable : ce matériel de la marque Hitachi (série VSP 5600), qui répond aux standards les plus avancés du marché, a été acquis il y a approximativement deux ans, et n'a connu dans le monde et depuis son déploiement aucun incident de ce type. La DGFIP elle-même détient 11 baies de stockage du même modèle, et 3 000 sont actuellement utilisés dans le monde. Il s'agissait donc, en tout état de cause, d'une anomalie unique et imprévisible, probablement due selon la DGFIP à une interaction entre les modalités spécifiques de traitement des données de l'application Hélios et le fonctionnement du module de déduplication de ces données, fourni par Hitachi. La capacité d'anticipation du fournisseur n'apparaît donc pas non plus en cause. Le module de déduplication, facultatif, a été retiré afin de prévenir une reproduction de l'incident.

Si l'origine précise de l'incident semble difficilement prévisible, un défaut d'anticipation face à la survenance d'un tel incident a entraîné un redémarrage laborieux quand bien même les techniciens d'Hitachi et les intervenants de la DGFIP se sont mobilisés sans compter. Les dispositifs de sauvegarde des données<sup>10</sup>, ainsi que leurs redondances (des disques durs distincts, stockés dans la même baie<sup>11</sup>), étaient en effet logés sur la même machine : dès lors, un incident rare affectant

<sup>7</sup> Agence nationale de la sécurité des systèmes d'information (ANSSI), mars 2026, Panorama de la cybermenace 2025.

<sup>8</sup> Près de 8 % de l'ensemble des établissements de santé ont ainsi été affectés en 2025, selon l'ANSSI.

<sup>9</sup> Assemblée nationale, commission des finances, M. Jean-René Cazeneuve et M. Jacques Oberti, mission d'information relative aux services publics de la Poste en vue d'une nouvelle loi postale.

<sup>10</sup> Les sauvegardes d'Hélios sont réalisées quotidiennement sur des backups du modèle Quantum DXI 9100.

<sup>11</sup> La nature même d'une baie de stockage est d'assurer la redondance des données : le stockage de disques durs distincts permet de reconstituer les données hébergées d'un disque dur défaillant sur un autre disque dur non affecté par cette défaillance.

l'ensemble de la baie – tel qu'un dysfonctionnement du module de déduplication – pouvait conduire à une perte intégrale des données en l'absence d'un site de secours distinct. C'est ce qui s'est produit le 5 février peu avant midi.

Il a donc été nécessaire de restaurer intégralement l'application Hélios. Les étapes de ce redémarrage ont inévitablement excédé le délai de 48 heures définissant le temps de réaction idéal <sup>12</sup> pour ce type d'incidents : formatage complet de la baie (du vendredi 6 février au samedi 7 février), restauration des données à partir de sauvegardes antérieures, recréation des serveurs puis redémarrage progressif des sites logiques de Metz entre le lundi 13 et le vendredi 17 février. Les premiers jours de la reprise d'activité ont été marqués par un ralentissement de la transmission des données en raison de l'accumulation des flux suspendus.

Comme souligné précédemment, les postes comptables hébergés sur les sites logiques de Versailles, ont pu poursuivre le traitement des stocks de flux financiers déjà transmis avant l'incident. *In fine*, seules une partie des données du 5 février ont été définitivement perdues.

L'essentiel des utilisateurs et partenaires d'Hélios ont partagé avec le rapporteur leur étonnement au regard de la lenteur du redémarrage de l'application. Ces délais trouvent leur origine dans l'absence de site de secours et non dans la réponse opérationnelle de la DGFIP, qui semble avoir correctement géré les conséquences techniques de l'arrêt des serveurs.

Pour qu'une telle interruption soit évitée, il aurait fallu prévoir un dispositif de secours, dont l'installation n'avait pas été retenue au moment du déploiement d'Hélios. En effet, au moment de la conception d'Hélios, au début des années 2000, l'analyse des risques qui avait été opérée à la lumière des standards techniques du moment avait conduit à un arbitrage, pouvant être qualifié rétrospectivement de sous-optimal, consistant à prévoir des mesures de sauvegarde et de redondances des données, mais pas de secours. Or, des incidents similaires ont pu être résolus pour d'autres applications grâce à la présence d'un site de secours distinct disposant d'une réplique des données en continu :

- l'interruption en septembre 2012 de l'application REC de mise en recouvrement et paiement de certains impôts fonciers locaux, en raison d'une surcharge électrique affectant un serveur de la marque GCOS ;
- l'interruption de Chorus, utilisé pour la transmission des flux financiers dans les administrations de l'État, en juin 2013 en raison de l'endommagement d'une baie de données ;

---

<sup>12</sup> Ce temps de réaction correspond à un standard du métier, tel que confirmé par les contributions des auditionnés à la mission d'information.

- l'interruption des téléservices des particuliers en juin 2021 (espace personnel, gestion du prélèvement à la source, déclaration en ligne).

Afin de prévenir l'émergence de tels incidents, en particulier en cas de cyberattaques, aux conséquences similaires, le rapporteur considère indispensable le déploiement d'un site de secours pour Hélios, ainsi que pour les autres applications importantes de la DGFIP n'en disposant pas.

#### **4. Bien que la DGFIP ait mis en œuvre un ensemble de mesures de communication de crise, l'hétérogénéité de la circulation de l'information a conduit à une forte inquiétude pour la majorité des ordonnateurs**

Le plan de communication de la DGFIP a été marqué par des messages réguliers et relativement précoces concernant la cause de l'incident technique et le déroulement du redémarrage. Dès le 5 février, une notice sur le portail de la DGFIP avertissait de la défaillance matérielle de la baie de stockage et de ses conséquences. L'ensemble des directions départementales des finances publiques (DDFIP) ont été prévenues le 6 février, et une consigne de communiquer avec les ordonnateurs a été transmise. Le redémarrage progressif d'Hélios entre le 13 et le 17 février a été ponctué de messages concernant l'évolution de la disponibilité de l'application, d'alertes sur des risques de faux ordres de virement, et de conseils relatifs à la reprise de l'envoi des flux urgents et prioritaires.

Ce n'est toutefois que le 10 février que les organisations syndicales et les associations d'élus locaux ont été formellement prévenues du déroulement de l'incident. Il convient de souligner qu'en date du 9 février, il était toujours évoqué avec les DDFIP un redémarrage à compter du 12 février. Quant au redémarrage de l'application CDG-D SPL, il a été annoncé le 24 février pour le lendemain, sans que les utilisateurs en soient directement informés au préalable.

Dans ce contexte, les retours d'expérience de la part des utilisateurs d'Hélios concernant la communication de crise de la DGFIP sont ambivalents.

De manière générale, les grands utilisateurs et leurs associations ont particulièrement apprécié la communication directe régulière avec l'administration centrale ou déconcentrée de la DGFIP. En revanche, les plus petits utilisateurs, bien plus nombreux, et ceux dont la relation de confiance avec les administrations centrales apparaît dégradée, soulignent plusieurs des faiblesses de la communication du ministère.

On peut tout d'abord relever le manque d'information directe de la DGFIP aux collectivités locales elles-mêmes, même après le 10 février. En tout état de cause cette circulation très hétérogène de l'information a laissé de côté certaines

collectivités. Cela a amené près de 15 % des utilisateurs<sup>13</sup>, recevant parfois des informations contradictoires de leurs pairies et du portail de la DGFIP, à poursuivre l'envoi de flux informatiques, que ce soit par méconnaissance, par souci de bien faire et notamment pour éviter ensuite la prise en charge d'intérêts moratoires, ou afin d'attester de leur détermination à se conformer à leurs obligations légales. Ce phénomène a pu complexifier le travail de correction comptable *a posteriori*. Sur ces points, la DGFIP justifie son choix d'avertir principalement les DDFIP et les associations d'utilisateurs par une volonté d'adaptation territoriale de la communication. L'information des associations d'utilisateurs aurait été différée jusqu'au 10 février afin de ne pas les inquiéter outre mesure, alors que la DGFIP entrevoyait une perspective de reprise rapide de l'application. Quant à l'information directe des utilisateurs eux-mêmes, la DGFIP met en avant les notices du portail de la DGFIP – qui se sont avérées, selon plusieurs remontées du terrain, pas toujours exhaustives voire incompréhensibles.

Par ailleurs, l'annonce à plusieurs reprises d'un redémarrage imminent mais maintes fois reporté, qui a certainement été motivée par la volonté de communiquer régulièrement avec les parties prenantes, a pu entraîner la confusion chez certains utilisateurs. Cette situation a conduit à réduire la circulation de l'information et la préparation par les utilisateurs d'Hélios de scénarios de redémarrages tardifs : la sévérité de l'incident étant relativisée par la perspective d'une reprise rapide, certains gestionnaires publics n'ont initialement pas été saisis par un sentiment d'urgence ou d'appréhension.

D'autres informations ont été communiquées tardivement. Ainsi, les conseils de reprise d'activité n'ont été partagés par la DGFIP que la veille du redémarrage (flux à prioriser, risques de lenteurs). Par ailleurs, la lettre de couverture signée par Madame la ministre Amélie de Montchalin, autorisant les comptables publics affectés par l'incident à procéder au paiement sans effectuer les contrôles qui leur incombent, n'a été transmise au réseau local que le 19 février.

Enfin, certaines informations n'ont tout simplement pas été communiquées aux parties prenantes. Les solutions de redondances et scénarios alternatifs de reprise d'activité, en cas de redémarrage très tardif de l'application, n'ont pas été diffusés, ce qui a pu susciter l'inquiétude des collectivités locales. La DGFIP justifie cet arbitrage par la conviction d'une reprise rapide, et par la volonté de ne pas laisser entrevoir une reprise en mode dégradé qui aurait entraîné d'importants correctifs comptables *a posteriori*. Ces raisons peuvent paraître fondées – sans qu'il ne soit pour autant impossible de rassurer les utilisateurs en les informant *a minima* de l'existence de plans alternatifs de reprise d'activité sans les détailler outre mesure.

---

<sup>13</sup> Selon une enquête relativement représentative réalisée par une association d'utilisateurs et fournie au rapporteur.

Surtout, l'absence d'informations concernant l'application éventuelle d'intérêts de retards en raison de l'impossibilité technique de verser certaines prestations sociales a particulièrement inquiété certains utilisateurs. Ce n'est que le 4 mars que la DGFIP a confirmé avec l'URSSAF – sans prévenir directement les utilisateurs – que les pénalités censées s'appliquer en raison du retard de transmission des mandats seraient supprimées (voir II.1 ci-après). A *fortiori*, l'absence d'application d'intérêts de retards par la caisse nationale des allocations familiales (CNAF) a dû être confirmée par le rapporteur lui-même le 1<sup>er</sup> avril : il semblerait que ni la DGFIP, ni les collectivités, n'en étaient informées avant cette date.

## **(II) Si le pire a été évité, les conséquences de l'incident sur les utilisateurs d'Hélios et leurs partenaires financiers demeurent significatives**

### **1. Le dysfonctionnement a fortement retardé l'ensemble des opérations comptables, affectant tout particulièrement le règlement des fournisseurs et l'approbation des comptes**

L'incident technique a suspendu la consultation et la gestion des flux de trésorerie des utilisateurs d'Hélios. La transmission des titres et des mandats, la consultation de la trésorerie et l'avancement de la procédure de clôture des comptes ont ainsi été interrompus.

**La suspension du versement des prestations sociales aux populations vulnérables** a particulièrement suscité l'inquiétude des parties prenantes. Près de 30 % des départements auraient connu des difficultés de versement d'une partie des prestations sociales dont ils assurent la gestion<sup>14</sup>. Les utilisateurs d'Hélios ont également fait part d'inquiétudes concernant les retards de paiement des organismes chargés de la transmission d'autres prestations – telle que la CNAF pour le RSA. Ces appréhensions ne semblent pas avoir été initialement dissipées par la DGFIP, jusqu'à une prise de contact directe du rapporteur avec la CNAF intervenue le 1<sup>er</sup> avril.

**Le règlement des fournisseurs, prestataires et des intérêts bancaires** a également été retardé par l'incident. Jusqu'à 90 % des départements et 95 % des comptables publics ont fait état de retards pour le paiement des fournisseurs. Des réclamations ponctuelles ont pu être observées, ainsi que des menaces de dénonciation des conventions et partenariats. Certains utilisateurs ont reporté des travaux pour prévenir le risque de retard de paiement. Pour mémoire, le délai de paiement maximal des collectivités locales est égal à 30 jours, répartis en 20 jours

---

<sup>14</sup> Selon une enquête relativement représentative de l'assemblée des départements de France transmise au rapporteur.

pour l'ordonnateur et 10 jours pour le comptable public<sup>15</sup>. La panne d'Hélios a allongé de 4 jours le délai global moyen de paiement des collectivités par rapport au mois de février 2025, soit 34,51 jours en février 2026, et de 0,39 jour le délai de paiement du comptable, soit 6,47 jours en février 2026. Le dysfonctionnement d'Hélios a donc légèrement allongé les délais de paiement de l'ensemble des fournisseurs, les conduisant à excéder, en moyenne, le délai réglementaire, et affectant la réputation des utilisateurs auprès de leurs partenaires.

*In fine*, le taux de dépassement du délai réglementaire pour les collectivités locales a augmenté de 1,81 point, à 30,15 %, et de 4,17 points pour les établissements de santé, à 54,33 %. Dans ce contexte, l'imposition d'intérêts moratoires<sup>16</sup> – relativement faibles, mais dont la compilation n'était pas achevée au moment des auditions de la mission – pose la question de la responsabilité financière de la DGFIP à l'égard des utilisateurs d'Hélios aux paiements retardés.

**Les risques de retards de versement des paies des agents publics** ne se sont pas réalisés, mais ont fortement préoccupé les utilisateurs d'Hélios jusqu'à son redémarrage. Au cours de l'incident, des paiements ponctuels ont pu être réalisés par un autre outil, BDF-Directe 2, et des initiatives locales ont également conduit au recours ponctuel à des circuits parallèles, qui est resté toutefois marginal. Globalement, le redémarrage d'Hélios avant la dernière semaine de février a permis de verser l'ensemble des paies des agents publics. Les indicateurs de référence pour février 2026 témoignent de conséquences très limitées : 7,78 milliards d'euros de dépenses de personnel contre 7,82 milliards d'euros en janvier 2026 et 7,68 milliards d'euros en février 2025 ; 4 843 433 paies traitées contre 4 825 062 en janvier 2026 et 4 789 229 en février 2025. Toutefois, d'autres dépenses de personnel ont été retardées, notamment le remboursement des frais de déplacement.

**Les retards pris par la procédure de clôture des comptes** ont affecté certaines collectivités soucieuses de conduire l'approbation de leurs comptes avant la période électorale. Certes, la date limite légale d'approbation des comptes est le 30 juin de l'année suivant l'exercice budgétaire<sup>17</sup> et aucune collectivité n'était tenue juridiquement d'approuver les comptes en février 2026. Toutefois, le contexte électoral a conduit certaines équipes municipales à inscrire l'approbation des comptes à l'ordre du jour du conseil municipal en février, malgré l'incident, entraînant *a posteriori* des recours contentieux de la part d'opposants politiques quant aux irrégularités administratives et comptables observées.

<sup>15</sup> En application de l'article R. 2192-10 du code de la commande publique.

<sup>16</sup> Ces intérêts moratoires sont automatiquement dus en application de l'article L. 2192-13 du code de la commande publique. La renonciation au paiement des intérêts moratoires dans les marchés publics est formellement interdite et considérée comme non écrite, en vertu de l'article L. 2192-14 du même code.

<sup>17</sup> En application de l'article L. 1612-12 du code général des collectivités territoriales (CGCT).

Le dysfonctionnement jusqu'au 25 février de l'application CDG-D, hébergée sur les mêmes serveurs qu'Hélios, a ainsi conduit à limiter le taux de reddition des comptes qui s'établissait à 23 % au 27 février (contre 48 % à la même période en 2025), 58 % au 13 mars (contre 68 % en 2025) et 67 % au 20 mars (contre 77 % en 2025). Par ailleurs, certaines collectivités ont également été préoccupées par le risque – non réalisé – de dépassement du délai maximal de 10 semaines entre le débat d'orientation budgétaire (DOB) et le vote du budget <sup>18</sup>. Certes, l'approbation des comptes est déconnectée juridiquement du DOB et du vote du budget. Toutefois, il est d'usage d'approuver les comptes à la même période : un retard d'approbation des comptes peut ainsi induire un retard du reste de la procédure budgétaire.

**Enfin, le dysfonctionnement de l'application Hélios et de son module CDG-D SPL assurant le processus d'approbation des comptes a complexifié la gestion des ressources humaines.** Les collectivités locales rapportent une augmentation des contrôles redondants, des ressaisies et des réémissions des flux PES V2. Des remontées des postes comptables soulignent une forte surcharge de travail à la reprise. Des informations contradictoires ont été rapportées concernant d'éventuelles annulations forcées de jours de congés, la mise au chômage partiel et l'absence de rémunération d'heures supplémentaires, laissant penser qu'elles ont été extrêmement limitées. En tout état de cause, un sentiment de dégradation des conditions de travail, et parfois d'abandon, a été décrit au rapporteur par des agents réalisant l'interface entre l'application Hélios et les flux comptables.

Concernant la question de l'engagement de la responsabilité des gestionnaires publics au cours de cette situation exceptionnelle, une note de la ministre de l'action et des comptes publics au moment de l'incident, Mme Amélie de Montchalin, datée du 19 février 2026 et valant doctrine administrative, avait été transmise aux directions locales. Ce texte autorise les comptables publics à « payer sans effectuer les contrôles qui leur incombent » un ensemble de dépenses jugées prioritaires (rémunérations, aides sociales, emprunts, dépenses obligatoires) ainsi que d'autres dépenses à « arrêt(er) conjointement par l'ordonnateur et le comptable », de janvier 2026 jusqu'au 28 février 2026. Un bilan de cette couverture ministérielle devra être réalisé. Elle a en effet été communiquée tardivement et a ainsi pu conduire à une appropriation hétérogène : certains comptables ont partagé des inquiétudes concernant l'engagement potentiel de leur responsabilité après avoir expédié des contrôles sans accord préalable avec l'ordonnateur.

---

<sup>18</sup> Article L. 5217-10-4 du CGCT.

## **2. Un même incident, s'il était survenu à un autre moment, aurait pu présenter des conséquences désastreuses**

Deux scénarios fictifs concernant la date et la durée de l'incident technique auraient débouché sur des conséquences plus graves, témoignant du caractère aléatoire d'un dysfonctionnement au milieu du mois de février.

Si l'incident s'était produit à la fin du mois, entre le 23 et le 28 février, l'ensemble des opérations comptables de fin de mois auraient été remises en cause. Certains titres n'auraient pas pu être perçus, en particulier les recettes de l'assurance maladie qui représentent 80 % des ressources des établissements hospitaliers. La procédure de versement des paies aurait été bouleversée, en particulier pour les organismes publics caractérisés par un emploi variable et atypique (permanences, gardes, heures supplémentaires, taux de rotation élevé, missions ponctuelles etc.). En période de renouvellement des mandats municipaux, un tel retard du versement des paies aurait pu affecter indûment les résultats électoraux. Le versement des prestations sociales et le règlement des fournisseurs et des prestataires auraient été davantage impactés. Des intérêts moratoires conséquents auraient potentiellement pu être imposés aux ordonnateurs. Le remboursement des emprunts bancaires aurait également été affecté.

Si en raison d'une durée plus longue, l'incident avait interrompu les flux comptables pendant plus de 20 jours, quelle que soit la date de reprise, le délai global de paiement des fournisseurs, prestataires et marchés publics aurait été significativement affecté, conduisant à des forts risques réputationnels et à des défaillances d'entreprises.

Selon les informations fournies au rapporteur, la DGFIP avait prévu plusieurs solutions en cas de retard du redémarrage de l'application prolongeant son indisponibilité au-delà du 20 février, en particulier l'exécution forcée des flux des ordonnateurs lors de jours non ouvrables (les samedi 21 et dimanche 22 février) pour transmission à l'application bancaire de la DGFIP puis traitement par la Banque de France. Cela aurait permis le déblocage des flux urgents, mais aurait engendré un travail particulièrement important de correction et de contrôle *a posteriori* par les comptables publics, qui n'auraient donc pas eu accès à ces flux avant leur envoi. Cette option aurait eu le mérite de ne pas interrompre intégralement l'ensemble des flux financiers, notamment les plus urgents, ce qui peut rassurer les utilisateurs d'Hélios en cas d'incidents similaires à l'avenir. Une telle exécution forcée n'a toutefois jamais été expérimentée, et aurait très probablement été limitée aux paiements les plus importants, dénotant l'importance d'approfondir les différentes options de redondances en anticipation d'incidents similaires.

### **3. Un incident similaire, concernant une autre application ou résultant d'une cyberattaque, pourrait conduire à de fortes difficultés financières pour les utilisateurs d'Hélios et leurs partenaires**

Le dysfonctionnement d'Hélios interroge les vulnérabilités d'autres applications similaires de l'État. Unanimement, les utilisateurs d'Hélios ont fait part de leurs inquiétudes concernant une interruption d'une durée similaire affectant Chorus ou les services de télédéclaration de la TVA. D'autres applications critiques ont également été mentionnées : TOTEM et Actes (transmission de documents réglementaires et contrôle de légalité), GMBI et PAYFIP (recouvrement de certaines recettes), ainsi que les référentiels de la DGFIP (bases de données des personnes physiques et morales, des occurrences fiscales, des éléments topographiques etc.).

L'essentiel de ces applications ne présente pas de vulnérabilités similaires à celles d'Hélios. En particulier, Chorus dispose de l'ensemble des moyens nécessaires, humains et techniques, pour assurer la continuité du service et un redémarrage rapide en cas d'incident, notamment grâce à son site de secours et à des exercices réguliers pour tester son plan de reprise d'activité et entraîner les exploitants.

En revanche, un incident technique affectant les référentiels de la DGFIP aurait conduit à un délai de reprise supérieur à celui d'Hélios, notamment en raison de la nécessaire synchronisation avec les diverses applications utilisatrices qui y sont connectées.

Plus largement, le rapporteur est préoccupé par la vulnérabilité des systèmes d'information des administrations centrales aux cyberattaques, en particulier concernant les applications s'appuyant sur des données sensibles des particuliers et ceux structurant les relations entre l'État et les autres administrations publiques tel que le vol récent de données ayant affecté l'agence nationale des titres sécurisés (ANTS). Les informations qui lui ont été communiquées semblent indiquer que ces risques sont bien pris en compte dans la stratégie numérique des acteurs publics, avec des moyens parfois insuffisants, *a fortiori* pour les collectivités locales qui devraient bénéficier d'un accompagnement renforcé de l'État.

**(III) Il importe de renforcer les mesures de prévention de tels dysfonctionnements, et d'améliorer les modalités de gestion de crise en cas d'incident**

**1. Afin de prévenir l'émergence d'un incident similaire, certaines vulnérabilités pourraient être réduites**

**Il s'agit tout d'abord d'organiser un bilan exhaustif de l'incident de février 2026 réunissant l'ensemble des acteurs concernés.** La direction de la DGFIP a commencé à organiser un retour d'expérience formalisé pour ce dysfonctionnement. Toutefois, les acteurs et modalités de ce bilan ne sont pas précisés. En tout état de cause, il convient que ce retour d'expérience associe tous les types d'utilisateurs de l'application Hélios, qu'ils soient ordonnateurs (communes, EPCI, départements, régions, établissements hospitaliers et médico-sociaux), comptables publics ou représentants des agents de la DGFIP, ainsi que les membres de l'écosystème des éditeurs et les partenaires financiers des utilisateurs. Il pourra ainsi organiser une compilation des conséquences précises de l'incident.

Certes, la présente communication permet déjà de dresser un premier bilan à vif de l'incident technique. Toutefois, le format d'auditions séparées de chacun des utilisateurs, retenu par le rapporteur, ne permet pas d'interactions entre les parties prenantes avec un croisement des regards sur ce qui s'est passé. Dans ces conditions, la coconstruction des mesures à prendre en conséquence du dysfonctionnement de février 2026, dont certaines orientations sont proposées dans la présente communication, devra reposer sur une association de toutes les parties prenantes dans des formats élargis, pilotés par les autorités de la DGFIP. Selon le rapporteur, une réunion annuelle, en format réduit, pourrait être envisagée, afin de faciliter l'élaboration des plans de continuité et de reprise d'activité, et des simulations de leur mise en œuvre intégrant une chaîne d'information, voire de communication jusqu'à l'utilisateur final ainsi qu'un dispositif spécifique (cellule de crise) pour répondre aux questions.

**Par ailleurs, afin de prévenir la reproduction d'un incident similaire portant à nouveau sur l'application Hélios, la solution la plus robuste, même si sans doute la plus coûteuse, serait de prévoir un plan de continuité d'activité formalisé, dans le cadre du déploiement d'Hélios 2.** L'ensemble des acteurs auditionnés s'accordent sur le principe du développement d'un serveur de secours en cas d'incident technique pour Hélios, sur le modèle de Chorus. Ce serveur de secours serait complémentaire des mesures de redondances et des sauvegardes déjà prévues. Il reposerait sur un site passif, qui serait activé en cas d'incident, disposant d'une puissance équivalente aux sites actifs en permanence.

Dans la perspective de sa mise en œuvre, le site de secours devra être accompagné d'exercices réguliers d'activation du plan de continuité d'activité – un rythme semestriel semble constituer un standard courant dans le secteur. Ces simulations présentent un coût à prévoir dans le budget de la DGFIP : créneaux temporels, ETP mobilisés, risque de perturbation de l'application etc. Les vulnérabilités exposées par l'incident semblent toutefois justifier la préparation d'une telle solution de secours, qui pourrait par ailleurs être mobilisée en cas de cyberattaque. Le rapporteur considère que, *in fine*, l'impact potentiel d'un tel dysfonctionnement sur l'activité économique – interruption de l'ensemble des flux comptables, corruption des données financières des collectivités et hôpitaux – justifie un investissement supplémentaire à court terme.

Le projet Hélios 2, porté par la DGFIP, prévoirait déjà l'investissement de 60 millions d'euros entre 2025 et 2031 afin de moderniser l'application et de renforcer sa résilience. Ce montant semble à première vue approprié, à la condition qu'il permette effectivement de consolider les opérations de l'application et de répondre aux besoins de ses utilisateurs. L'augmentation des moyens financiers du plan d'investissement devra être envisagée si cela s'avère nécessaire à son complet déploiement. Néanmoins, comme l'indique la DGFIP, l'allocation de moyens n'aura de sens que si la DGFIP a la capacité de les mettre en œuvre d'un point de vue opérationnel.

**Enfin, et plus largement, ce dysfonctionnement de l'application Hélios rappelle le caractère urgent de la réduction des vulnérabilités des systèmes informatiques cruciaux des administrations centrales.** Certes, la DGFIP est déjà engagée dans une trajectoire de résorption de sa dette technique, accélérée dans le cadre de son contrat d'objectifs et de moyens (COM) 2023-2027, à la lumière des recommandations de l'inspection générale des finances (IGF) proposées dans son rapport de septembre 2022 <sup>19</sup>. Cette stratégie repose sur des investissements annuels de 60 à 70 millions d'euros, consacrés exclusivement à la modernisation des systèmes d'informations existants.

Néanmoins, les dysfonctionnements récents d'applications essentielles à la transmission des flux financiers entre acteurs publics et avec les administrés (Hélios, GMBI, OCAPI, FICOBA etc.) permettent de s'interroger sur l'adéquation entre les moyens financiers de l'actuel plan de modernisation et les besoins ainsi révélés. Dès lors, le rapporteur préconise d'accroître les crédits attribués à la DGFIP en vue de la résorption de sa dette technique. Le calcul semble gagnant à terme, en tenant compte du renforcement de l'efficacité de la collecte de l'impôt et de la réduction du risque de cyberattaque, ainsi que du risque de contentieux en cas de perte ou de vol de

---

<sup>19</sup> IGF, 2022, *Bilan du contrat d'objectifs et de moyens de la direction générale des finances publiques pour la période 2020-2022*.

données, ou d'interruption d'un service crucial aux opérations financières des administrations publiques.

Conscient des difficultés de pilotage simultané d'une multiplicité de projets de modernisation, qui se reflèteraient dans une sous-consommation des crédits, le rapporteur propose une trajectoire pluriannuelle pour le prochain contrat d'objectifs et de moyens (COM) 2028-2032 prévoyant une hausse importante des autorisations d'engagement de 250 millions d'euros en 2028, à consommer sur la période, soit 50 millions d'euros par an. Ces crédits pourront financer les priorités numériques de la DGFIP : modernisation des applications, développement de mesures de redondances et de secours, renforcement de la cybersécurité, lancement de *bug bounties*<sup>20</sup>, déploiement de serveurs souverains, recrutements dédiés etc. Ces crédits seraient déployés en fonction d'une analyse actualisée des risques informatiques auxquels est exposée la DGFIP, en particulier concernant la recrudescence des menaces de cyberattaques et l'augmentation de la valeur des données hébergées par le ministère des finances.

Au-delà de la DGFIP, la réduction des vulnérabilités des systèmes d'information des administrations centrales revêt également un caractère urgent. La mutualisation des compétences en matière informatique (conception et déploiement des logiciels, réponse aux incidents) ainsi que des mesures de redondances et de secours (circuits parallèles pour les applications financières, sites miroirs partagés) semblent constituer une piste prometteuse, déjà explorée, qu'il convient d'approfondir en lien avec l'agence nationale pour l'information financière de l'État (AIFE) et la direction interministérielle du numérique (DINUM). Le rôle de pilotage de la DINUM sur ces sujets demeure toutefois à confirmer, alors qu'elle peine à s'affirmer comme la « direction des systèmes informatiques » de l'État.

Enfin, le secteur public local apparaît particulièrement vulnérable à ce type d'incidents techniques et aux cyberattaques. Dans le cadre de la transposition de trois directives européennes à ce sujet, le projet de loi cyber-résilience<sup>21</sup> prévoit, à ce stade de la discussion, la création d'un fonds de soutien d'accompagnement des collectivités locales qualifiées « d'entités importantes ou essentielles » n'ayant pas bénéficié du « parcours de cybersécurité » du plan France relance<sup>22</sup>. Le rapporteur sera vigilant quant aux modalités et au financement de ce dispositif, qu'il convient de préciser par des dispositions législatives, et non réglementaires, afin d'accompagner au mieux les collectivités vulnérables et disposant de faibles moyens.

---

<sup>20</sup> Ces « chasses aux dysfonctionnements » correspondent à un système de récompense monétaire de spécialistes, dont les primes sont calculées en fonction du nombre et de la gravité des failles de logiciel repérées pour le compte de leur commanditaire.

<sup>21</sup> Projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, adopté en première lecture en séance au Sénat et en commission à l'Assemblée nationale.

<sup>22</sup> 5<sup>o</sup> *sexies* de l'article 5 *bis* du texte adopté en commission.

## **2. En vue de renforcer les modalités de gestion de crise, il convient d'anticiper la création d'un plan formalisé de communication et des solutions redondantes**

Globalement, la gestion du dysfonctionnement d'Hélios de février 2026 semble marquée par une bonne volonté de la DGFIP, un engagement exemplaire en faveur du service public des agents des administrations, mais aussi quelques faiblesses en matière de circulation de l'information qui auraient pu être prévenues par la détermination préalable d'un plan de communication formalisé en lien avec les parties prenantes. Un tel plan de communication est indispensable, et devrait être généralisé à d'autres types de dysfonctionnements techniques, en particulier aux cyberattaques, et adapté à d'autres applications de la DGFIP.

Son élaboration dans le cadre du retour d'expérience en cours d'organisation devrait viser à informer régulièrement, tous les deux jours à partir du dépassement d'un délai standard (lequel pourrait être de 48 heures, tout en tenant éventuellement compte des jours non ouvrables), l'ensemble des utilisateurs d'Hélios de l'état d'avancement de la résolution d'un incident. Une attention particulière mériterait d'être portée à l'information directe des petits utilisateurs, en étoffant par exemple les notifications transmises au sein même de l'application défaillante, la foire aux questions et le point de contact entre l'administration centrale et les utilisateurs. Ce plan de communication comporterait notamment :

- une information actualisée sur la possibilité d'avoir recours à certaines fonctionnalités de l'application défaillante – par exemple, pour Hélios, la préparation ou la transmission de certains flux comptables, même en mode dégradé ;
- un guide de communication prêt à l'emploi à l'attention des utilisateurs, afin qu'ils puissent informer leurs partenaires de l'avancement de la situation ;
- un plan de reprise d'activité formalisé, proposant les modalités de priorisation des opérations.

Par ailleurs, soit que la solution du serveur de secours (qui aurait la préférence du rapporteur) ne soit pas retenue, soit en complément de cette solution, **prévoir des redondances ou des solutions techniques de travail en mode dégradé en cas de défaillance** permettrait de pallier à l'avenir une vulnérabilité majeure en cas d'émergence d'un incident similaire. Certes, la DGFIP avait prévu pour Hélios des solutions techniques alternatives pour la transmission des paiements urgents en cas de redémarrage tardif de l'application. Toutefois, ces solutions ne semblent pas avoir été expérimentées à ce jour, et leur mise en œuvre opérationnelle pourrait laisser entrevoir quelques fragilités.

Il conviendrait donc d'expérimenter avec certains utilisateurs volontaires d'Hélios une solution technique garantissant une continuité du service, en mode dégradé, lors d'un dysfonctionnement issu d'une défaillance matérielle ou d'une cyberattaque, avec des cas d'usage. Plusieurs outils susceptibles d'être mobilisés en ce sens ont été mentionnés au cours des auditions de la mission : PIGP, Chorus et Chorus Pro, BDF Directe 2 etc.

Sous réserve des contraintes techniques et normatives en vigueur, la solution technique retenue devrait permettre d'accéder aux données comptables, de transmettre certains flux comptables prioritaires sous un format sécurisé différent du PES V2 ou de préparer les données à transmettre une fois l'incident résolu. Sur ce dernier point, a été évoquée l'idée d'un traitement asynchrone des flux comptables permettant de faciliter l'ensemble du travail préparatoire pendant l'incident technique (accès aux données, envoi des flux au tiers de télétransmission), avant leur réception par la DGFIP au moment de sa résolution.

Le rapporteur invite donc la DGFIP à étudier, en lien avec les parties prenantes, les possibilités techniques les plus pertinentes, leur coût, et l'intérêt même d'une telle redondance au regard de la potentielle création de nouvelles vulnérabilités et d'une surcharge de travail *a posteriori* en raison de la nécessité de contrôler et corriger les flux de données transmis.

## **LISTE DES PERSONNES AUDITIONNÉES PAR LE RAPPORTEUR**

*(par ordre chronologique)*

### **– Fédération hospitalière de France \***

Mme Cécile Chevance, responsable du pôle Offre de soins, finances, FHF Data, recherche et e-santé

Mme Alexandra Liparo, responsable adjointe

### **– Association finances, gestion, évaluation des collectivités territoriales (AFIGESE)**

M. Pascal Bellemin, président

Mme Catherine Coulin, 2<sup>ème</sup> vice-présidente

M. Fabrice Pierre-Abelé, co-pilote du groupe de travail qualité des comptes et certification

### **– Départements de France**

M. Aurélien Barrière, Directeur général délégué ressources internes du département de l'Allier, représentant M. Claude Riboulet, président de la commission Innovation et numérique

Mme Virginie Langlet, conseillère Innovation et Numérique, déléguée à la Protection des données

### **– Association des maires de France et des présidents d'intercommunalités (AMF)**

M. Emmanuel Sallaberry, Maire de Talence (33), co-président de la commission des Finances et de la fiscalité locales

Mme Charlotte De Fontaines, responsable et attachée aux relations avec le parlement

Mme Charlotte Rigault, conseillère budget

M. Antoine Huot, conseiller finances intercommunales

### **Table ronde des organisations syndicales DGFIP**

#### **– Solidaires Finances Publiques**

M. David Boilet, secrétaire national

M. Nicolas Calvel, secrétaire national

Mme Amélie Blanc, conseillère

#### **– CGT Finances publiques**

M. Sylvain Carpentier

M. Frédéric Scalbert

#### **– FO DGFIP**

M. Olivier Brunelle, secrétaire général

M. Jean-Paul Philidet, secrétaire général adjoint

#### **– CFDT DGFIP**

Mme Anthéa Martinez, secrétaire nationale

Mme Florence Bochnakian, secrétaire générale

#### **– CFTC DGFIP**

M. Régis Bourillot, conseiller fédéral

#### **– Direction générale des finances publiques (DGFIP)**

Mme Amélie Verdier, directrice générale

M. Tomasz Blanc, chef du service des systèmes d'information

M. Éric Barbier, chef du service des gestions publiques locales, des activités bancaires et économiques

– **Agence pour l'informatique financière de l'État (AIFE)**

M. Emmanuel Spinat, directeur

M. Nicolas Botton, adjoint au directeur

– **SAP France \***

M. Olivier Nollent, président-directeur général

Mme Pauline Hénaff, vice-présidente en charge notamment des services financiers et du secteur public

Mme Élodie Franco-Ritz, directrice des affaires gouvernementales France et Afrique francophone

– **Ministre de l'action et des comptes publics**

M. David Amiel, ministre délégué à l'action et aux comptes publics

– **Contributions écrites reçues**

Conseils municipaux et intercommunalités de la Haute-Garonne

Centre national des œuvres universitaires et scolaires (CNOUS)

Caisse nationale des allocations familiales (CNAF)

Régions de France

Direction interministérielle du numérique (DINUM)

– **Autres contributions à la mission d'information**

Le rapporteur tient également à remercier Mélissa Martinez, Emmanuel Auger et Céline Carcy pour leur collaboration dans le cadre de cette mission d'information.

\*

\* \*

*\* Ces représentants d'intérêts ont procédé à leur inscription sur le registre de la Haute Autorité pour la transparence de la vie publique*