COMMISSION
EUROPÉENNE

Bruxelles, le 9.10.2024
COM(2024) 451 final

RAPPORT DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

sur le premier examen périodique du fonctionnement de la décision d'adéquation relative au cadre de protection des données UE - États-Unis

1. LE PREMIER EXAMEN PÉRIODIQUE - CONTEXTE, PRÉPARATION ET PROCESSUS

Dans sa décision du 10 juillet 2023 (ci-après la «décision d'adéquation»), la Commission a constaté que le cadre de protection des données UE - États-Unis (ci-après le «CPD») assure un niveau de protection adéquat des données à caractère personnel transférées de l'Union européenne vers des organisations aux États-Unis d'Amérique[1]. La décision d'adéquation impose à la Commission de procéder à des examens périodiques, dont le premier devait avoir lieu dans un délai d'un an à compter de la date de notification de la décision d'adéquation aux États membres. Le présent rapport conclut ce premier examen.

Comme l'exige le considérant 211 de la décision d'adéquation, ce premier examen, effectué après la première année de mise en œuvre du nouveau cadre, visait à vérifier si tous les éléments prévus dans le cadre ont été mis en œuvre et fonctionnent efficacement. Il a couvert tous les aspects du fonctionnement du cadre, y compris à la lumière des évolutions juridiques intervenues depuis l'adoption de la décision d'adéquation.

En vue de préparer l'examen, la Commission a recueilli des informations auprès de parties intéressées concernées, en particulier d'organisations non gouvernementales (ONG) disposant d'une expertise en matière de droits numériques et de protection de la vie privée[2], d'organisations certifiées en vertu du CPD, par l'intermédiaire de leurs associations professionnelles[3], ainsi que des autorités américaines participant à la mise en œuvre du cadre. En outre, la Commission a également recueilli l'avis du grand public au moyen d'un appel à contributions spécifique sur le portail «Donnez votre avis»[4].

Une réunion d'examen a eu lieu à Washington, D.C. les 18 et 19 juillet 2024. Elle a été ouverte par Didier Reynders, commissaire européen à la justice et aux consommateurs, et Gina Raimondo, secrétaire d'État américaine au commerce[5].

---

[1] Décision d'exécution (UE) 2023/1795 de la Commission du 10 juillet 2023 constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le cadre de protection des données UE - États-Unis.

[2] La Commission a envoyé à neuf ONG (Human Rights Watch, American Civil Liberties Union, Consumer Federation of America, Center for Digital Democracy, New America Open Technology Institute, Access Now, Electronic Frontier Foundation, Electronic Privacy Information Center et Center for Democracy and Technology) un questionnaire portant sur les évolutions pertinentes du cadre juridique des États-Unis, les mécanismes de surveillance et d'application et le fonctionnement des mécanismes de recours. Les services de la Commission et les représentants du comité européen de la protection des données ont également rencontré ces ONG en ligne le 9 juillet 2024.

[3] La Commission a envoyé à neuf associations professionnelles (Software & Information Industry Association, U.S. Chamber of Commerce, Information Technology Industry Council, Software Alliance, Centre for Information Policy Leadership, Interactive Advertising Bureau, United States Council for International Business, Computer and Communications Industry Association et Engine) un questionnaire portant sur l'expérience des entreprises certifiées en vertu du CPD, en particulier sur le processus de certification, les mesures prises pour se conformer aux principes du CPD, les mécanismes de traitement des demandes et des réclamations des personnes concernées, etc.

[4] Les avis reçus sont disponibles à l'adresse suivante: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14379-Cadre-de-protection-des-donnees-UE-Etats-Unis-rapport-de-la-Commission-relatif-au-fonctionnement-du-cadre_fr.

[5] La réunion d'examen était organisée par thème, chaque point de l'ordre du jour étant introduit par une brève présentation de l'autorité américaine, du représentant de l'Union européenne ou de l'organisation compétent suivie d'une séance de questions-réponses détaillée. Les «aspects commerciaux» du cadre (c'est-à-dire l'application et le contrôle de l'application des exigences applicables aux entreprises certifiées en vertu du CPD)

Pour l'Union européenne, l'examen a été réalisé par des représentants de la direction générale de la justice et des consommateurs de la Commission européenne, accompagnés de cinq représentants désignés par le comité européen de la protection des données et issus de différentes autorités nationales chargées de la protection des données (APD) et du Contrôleur européen de la protection des données[6]. Du côté américain, des représentants du ministère du commerce, du Département d'État, de la commission fédérale du commerce (Federal Trade Commission, ci-après la «FTC»), du ministère des transports, du bureau du directeur du renseignement national (Office of the Director of National Intelligence, ci-après l'«ODNI»), du ministère de la justice, de l'inspecteur général des services de renseignement, ainsi que des membres du conseil de surveillance de la vie privée et des libertés civiles (Privacy and Civil Liberties Oversight Board, ci-après le «PCLOB») ont participé à cette réunion. En outre, des représentants d'organisations proposant des services indépendants de règlement des litiges et de l'American Arbitration Association (AAA) ont fourni des informations lors des sessions d'examen pertinentes. Par ailleurs, des exposés d'organisations certifiées en vertu du CPD sur la manière dont les sociétés se mettent en conformité avec les exigences du cadre sont venus éclairer l'examen.

Les conclusions de la Commission ont également été étayées par des données accessibles au public, telles que des décisions de justice, des règles et procédures de mise en œuvre édictées par les autorités américaines compétentes, des rapports et études d'organisations non gouvernementales, des rapports concernant la transparence publiés par des sociétés certifiées en vertu du CPD, des rapports annuels émanant d'organes de surveillance indépendants ainsi que des rapports parus dans les médias.

2. CONSTATATIONS

2.1. Aspects commerciaux

2.1.1. Le processus de certification

Afin de pouvoir recevoir des données à caractère personnel transférées depuis l'Union européenne sur la base du CPD, une entreprise américaine doit certifier, puis recertifier chaque année, auprès du ministère du commerce, son adhésion à des exigences spécifiques en matière de protection des données (les «principes du CPD»). Pour pouvoir prétendre à une certification, une entreprise doit être soumise aux pouvoirs d'enquête et aux pouvoirs répressifs de la FTC ou du ministère des transports, déclarer publiquement son engagement à respecter les principes du CPD, publier sa politique en matière de protection de la vie privée et appliquer ces exigences dans leur intégralité[7]. Avant de finaliser une certification, le ministère du commerce vérifie si l'entreprise a satisfait à toutes les exigences de certification[8].

Lors de la réunion d'examen, le ministère du commerce a expliqué qu'au cours de cette première année du CPD, l'accent a été placé sur la mise en place du processus de certification, y compris le développement d'outils informatiques ad hoc, la mise à jour de procédures, le

ont été abordés le premier jour, tandis que les questions relatives à l'accès des pouvoirs publics aux données à caractère personnel ont été examinées le deuxième jour.

[6] Les représentants de la Commission et du comité européen de la protection des données se sont réunis le 12 juin et le 10 juillet 2024 afin de préparer l'examen, d'examiner les contributions reçues et de déterminer les aspects nécessitant la collecte d'informations supplémentaires et des éclaircissements.

[7] Section I.2 de l'annexe I de la décision d'adéquation.

[8] Annexe III de la décision d'adéquation.

dialogue avec les entreprises et la réalisation d'autres activités d'information et de sensibilisation. À la date de la réunion d'examen, plus de 2 800 entreprises étaient certifiées en vertu du CPD. Cela signifie qu'au cours de sa première année de fonctionnement, davantage d'entreprises ont été certifiées en vertu du CPD qu'en vertu du cadre précédent, le bouclier de protection des données[9]. Selon les informations fournies par le ministère du commerce, 70 % des participants sont des PME, et un grand nombre d'entreprises certifiées en vertu du CPD (47 %) sont actives dans le secteur de l'information, des communications et de la technologie. En outre, 60 % des entreprises sont certifiées exclusivement pour les données autres que les données RH, 2,5 % sont certifiées exclusivement pour les données RH et 37,5 % sont certifiées tant pour les données RH que pour les données autres que les données RH.

Le ministère du commerce a adopté les procédures nécessaires pour traiter les demandes des entreprises. Les entreprises doivent soumettre leur demande de certification sur le site web du ministère du commerce consacré au CPD (https://www.dataprivacyframework.gov/). Celui-ci contient des informations sur la manière d'adhérer au CPD[10] et sur les obligations qui incombent à l'entreprise en vertu du cadre[11]. Une équipe spécifique au sein du ministère du commerce, placée sous la responsabilité d'un directeur chargé du cadre de protection des données, est chargée de tous les aspects liés à la gestion et à l'administration du CPD, dont le processus de certification et le contrôle de la conformité. Chaque demande est attribuée à un membre du personnel donné qui reste responsable pour l'entreprise concernée tout au long du processus de certification.

Pour être certifiées en vertu du cadre, les entreprises soumettent une demande, y compris un projet de politique en matière de protection de la vie privée. Le ministère du commerce vérifie si celui-ci est conforme aux exigences applicables du CPD. Lorsque des organisations souhaitent certifier différentes entités au sein d'un groupe d'entreprises (par exemple, différentes filiales), le ministère du commerce demande et examine soit une politique globale en matière de protection de la vie privée qui indique clairement toutes les entités à couvrir, soit des politiques distinctes pour chaque entité. Il vérifie également auprès du mécanisme de recours indépendant (MRI)[12] indiqué dans la demande si l'organisation s'est effectivement inscrite auprès de celui-ci. Pour les entreprises qui sélectionnent le panel d'autorités chargées de la protection des données (par exemple, parce qu'elles traitent des données RH), le ministère du commerce vérifie si l'entreprise a payé les cotisations requises pour recourir au panel. Le cas échéant, il vérifie aussi si le demandeur relève de la compétence de la FTC ou du ministère des transports (et peut donc adhérer au CPD).

Si toutes les conditions sont remplies, le ministère du commerce informe l'organisation qu'elle peut publier sa politique en matière de protection de la vie privée faisant référence au CPD sur son site web. Une fois que cette politique est publique, le ministère confirme la certification et intègre l'entreprise dans la liste du CPD sur son site web. Le CPD peut être invoqué pour

[9] Au cours d'une période équivalente, 2 400 entreprises avaient obtenu la certification dans le cadre du bouclier de protection des données.

[10] https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-(DPF)-Program-(part%E2%80%931).

[11] https://www.dataprivacyframework.gov/key-requirements.

[12] Des mécanismes de règlement des litiges du secteur privé qui permettent d'examiner et de trancher toute réclamation et tout litige rapidement et sans frais pour les personnes concernées.

recevoir des données à caractère personnel en provenance de l'Union européenne à partir de la date à laquelle le ministère du commerce inscrit l'organisation sur cette liste[13].

Comme expliqué lors de la réunion d'examen, les contrôles effectués jusqu'à présent par le ministère du commerce ont abouti au rejet de 33 demandes, parce qu'elles ne satisfaisaient pas aux exigences du CPD. D'une manière générale, le ministère du commerce collabore avec l'entreprise pour remédier à tous les éventuels manquements. Lorsqu'il constate des manquements, il informe l'entreprise qu'elle doit y remédier et que si elle ne répond pas dans un délai imparti ou si elle ne remplit pas sa déclaration d'autocertification conformément aux procédures du ministère, sa demande sera considérée comme abandonnée. Si la certification initiale n'est pas complétée/modifiée dans un délai de 12 mois, le ministère du commerce considère qu'elle a été abandonnée.

La date d'échéance pour la recertification annuelle est précisée dans la liste du CPD pour chaque entreprise. Pour rappeler aux entreprises la nécessité de demander le renouvellement de la certification, le ministère du commerce a créé un système qui rappelle que la certification est sur le point d'expirer. Les organisations reçoivent un rappel un mois avant, puis deux semaines avant et un jour avant la date d'échéance. Celles qui laissent expirer leur certification sont retirées de la liste du CPD. Comme décrit dans l'annexe III de la décision d'adéquation, le ministère du commerce dispose d'une section spécifique sur son site web dans laquelle il énumère les organisations américaines qui ne sont plus des participants actifs et indique les raisons pour lesquelles (par exemple, expiration ou retrait) les entreprises concernées ont été retirées de la liste (la «liste des organisations inactives»). Lorsque des organisations sont retirées de la liste du CPD parce qu'elles ont laissé leur certification expirer, le ministère du commerce prend contact avec elles pour qu'elles confirment si elles souhaitent se retirer ou si elles ont l'intention de renouveler leur certification et, dans ce dernier cas de figure, pour vérifier que, pendant la période d'expiration, elles ont appliqué les principes du CPD aux données à caractère personnel reçues en vertu du CPD et pour préciser les mesures qu'elles prendront pour résoudre les problèmes en suspens qui ont retardé leur recertification. Lorsque les entreprises indiquent au ministère du commerce qu'elles souhaitent se retirer du CPD, le ministère leur demande de confirmer si elles restitueront ou supprimeront les données qu'elles ont reçues alors qu'elles participaient au CPD; si elles les conserveront et continueront d'y appliquer les principes du CPD (ce qui doit être confirmé chaque année); ou si elles les conserveront et mettront en place d'autres protections (telles que des clauses contractuelles types adoptées par la Commission européenne).

Les avis donnés par les associations professionnelles et les entreprises indiquent que les entreprises certifiées en vertu du CPD ont pris un certain nombre de mesures pour garantir le respect des principes du CPD. Par exemple, pour se conformer au principe «*Voies de recours, application et responsabilité*», les organisations ont effectué des contrôles internes soit au moyen d'une autoévaluation, soit au moyen d'un contrôle extérieur de la conformité. Les deux MRI du secteur privé qui ont participé à la réunion d'examen ont expliqué qu'ils prévoyaient également un contrôle extérieur de la conformité en examinant les politiques en matière de protection de la vie privée, et l'un des MRI du secteur privé a expliqué qu'il prévoyait également des audits et des vérifications aléatoires, portant, par exemple, sur les principes «*Accès*», «*Choix*» et «*Transfert ultérieur*». En outre, les entreprises certifiées ont mis au point des mécanismes de surveillance et des programmes de conformité internes, formé des

[13] Section I, point 3, de l'annexe I de la décision d'adéquation.

employés, mis en œuvre des mécanismes permettant aux personnes concernées d'exercer leurs droits, réalisé des analyses des incidences sur la vie privée et examiné les contrats existants.

2.1.2. Contrôle de la conformité, fausses déclarations de participation et contrôle de l'application des règles

Dans le cadre du CPD, le ministère du commerce est chargé de contrôler le respect des principes du CPD au moyen de différents outils, dont des contrôles d'office (de sa propre initiative), des contrôles ponctuels ad hoc et des questionnaires de conformité. Il s'agit notamment de détecter et de traiter les fausses déclarations de participation au cadre, par exemple au moyen de recherches sur l'internet[14].

Pour contrôler le respect des principes par les entreprises certifiées en vertu du CPD, le ministère du commerce s'est principalement appuyé sur des vérifications des médias (sociaux) et des recherches sur le web ad hoc au cours de l'année écoulée. Le ministère du commerce a indiqué qu'il n'a détecté aucun problème de conformité avec les principes du CPD au cours de cette première année et qu'il n'a signalé aucune entreprise à la FTC ou au ministère des transports en vue d'éventuelles mesures coercitives. Il a également mis en place un point de contact spécifique pour faciliter la coopération avec les APD et recevoir les réclamations des personnes concernées et les dossiers soumis par d'autres autorités (par exemple, les APD ou la FTC). Toutefois, aucun dossier ni aucune réclamation n'a été reçu au cours de l'année écoulée. Alors que cette première année de fonctionnement du CPD était axée sur la mise en place du cadre et du processus de certification, lors de la réunion d'examen, le ministère du commerce a expliqué qu'il prévoyait de procéder à des contrôles de conformité à l'aide de procédés automatisés afin de les effectuer de manière plus systématique, et qu'il était en train de mettre au point les outils informatiques nécessaires à cette fin.

La Commission reconnaît que le ministère du commerce devait concentrer ses efforts au cours de cette première année sur la mise en place du cadre et du processus de certification. À l'avenir, il importe que le ministère du commerce redouble d'efforts pour surveiller et contrôler le respect des principes, ce qui est nécessaire pour garantir un niveau constamment élevé de conformité avec le cadre et détecter les cas nécessitant d'autres mesures coercitives, y compris les éventuelles fausses déclarations de participation d'entreprises. À cet égard, la Commission se félicite de ce que le ministère du commerce ait confirmé son intention de mettre au point et d'utiliser des outils (automatisés) pour détecter de manière plus efficace et systématique les problèmes de conformité et les fausses déclarations et estime que cela devrait s'inscrire dans un effort plus large visant à utiliser davantage les différents outils dont il dispose (par exemple, les contrôles ponctuels, les questionnaires de contrôle de la conformité, les demandes d'information, etc.), y compris pour vérifier le respect d'exigences spécifiques du CPD[15].

Les organisations participant au CPD sont soumises à la compétence de la FTC et du ministère des transports. Au cours de la réunion d'examen, le ministère des transports a confirmé qu'il avait mis en place tous les processus nécessaires pour prendre des mesures coercitives appropriées. Il a également expliqué que très peu d'entreprises relevant de sa compétence ont

[14] Voir annexe III de la décision d'adéquation. Il y a fausse déclaration, par exemple, lorsqu'une entreprise affirme participer au CPD et qu'elle n'a jamais entamé le processus de certification, ou qu'elle l'a entamé mais ne l'a pas mené à bien ou a laissé expirer sa certification.

[15] Par exemple, en ce qui concerne les transferts ultérieurs, en recourant à la possibilité offerte par le principe 3 b) du CPD de demander une synthèse ou une copie représentative des dispositions pertinentes relatives à la protection de la vie privée contenues dans les contrats de transfert ultérieur.

adhéré au CPD (à savoir, quelques agents de billetterie, mais aucune compagnie aérienne). La FTC a confirmé qu'elle vérifiait systématiquement l'existence de violations du CPD dans chacune de ses enquêtes sur la protection de la vie privée. À ce jour, la FTC n'a reçu aucun dossier soumis par d'autres autorités. Elle a reçu quelques réclamations mentionnant le CPD, même si deux d'entre elles concernaient des entreprises figurant sur la «liste des organisations inactives», deux concernaient des entreprises qui ne participaient pas au cadre et une ne concernait pas des données à caractère personnel transférées depuis l'Union européenne. Au moment de la rédaction du présent rapport, la FTC n'avait émis aucune décision visant à faire respecter le CPD, bien qu'elle ait confirmé que plusieurs entreprises certifiées en vertu du CPD faisaient l'objet d'une enquête.

La Commission se réjouit de constater que la FTC vérifie systématiquement l'existence de violations du CPD dans toutes ses enquêtes sur la protection de la vie privée. Le maintien de l'efficacité du CPD dépendant de sa mise en œuvre rigoureuse, la FTC devrait continuer d'exercer ses pouvoirs d'enquête en vertu du cadre, y compris en menant de manière proactive des actions «coup de balai» axées sur le respect d'exigences spécifiques du CPD et/ou sur certains secteurs.

2.1.3. Traitement des réclamations

Le CPD offre aux citoyens de l'Union différentes possibilités de recours en cas de non-respect des principes du CPD par des organisations certifiées[16], notamment celle de chercher à obtenir le règlement du litige en prenant directement contact avec une organisation participant au CPD, qui doit fournir une réponse à la personne concernée dans un délai de 45 jours. Les personnes concernées peuvent également introduire une réclamation auprès d'un MRI désigné par une organisation pour examiner et traiter définitivement les réclamations. Selon les circonstances, il peut s'agir soit d'un organisme de règlement extrajudiciaire des litiges, soit d'une APD[17]. Enfin, au cas où aucune des autres voies de recours disponibles n'aurait permis de traiter de manière définitive et satisfaisante la réclamation de la personne concernée, les personnes peuvent déclencher un arbitrage contraignant devant le panel du CPD UE - États-Unis en tant que recours en dernier ressort.

2.1.3.1. Traitement des réclamations par les entreprises

Les réponses des associations professionnelles et des entreprises aux questionnaires envoyés par la Commission indiquent que les entreprises certifiées en vertu du CPD ont reçu très peu de réclamations, voire aucune, de personnes au sujet du non-respect des principes du CPD. Dans le même temps, les entreprises ont mis en place différents mécanismes et outils pour permettre aux personnes concernées d'exercer leurs droits et d'introduire des réclamations, y compris au moyen de formulaires en ligne, de courriers électroniques et d'appels téléphoniques.

2.1.3.2. *Mécanismes de recours indépendants (MRI)*

Les retours d'information reçus au cours de la réunion d'examen et les informations fournies par les associations professionnelles indiquent qu'il y a eu très peu de réclamations auprès de

[16] Voir section 2.4 de la décision d'adéquation.

[17] Les organisations participant au CPD sont tenues de coopérer à l'enquête menée par une APD à la suite d'une réclamation et au traitement définitif de la réclamation par l'APD lorsqu'il s'agit du traitement de données RH collectées dans le cadre d'une relation de travail ou lorsque l'organisation concernée s'est volontairement soumise à la surveillance des APD.

mécanismes de résolution indépendants. Parmi les MRI sélectionnés par les entreprises figurent BBB National Programs, JAMS, TRUSTe et VeraSafe. Le CPD exige que les MRI publient un rapport annuel contenant des statistiques agrégées sur le recours à leurs services de règlement des litiges. Au moment de l'adoption du présent rapport, tous les MRI concernés avaient publié leurs rapports annuels[18].

En outre, lors de la réunion d'examen, BBB et VeraSafe ont présenté en détail leurs activités de l'année dernière. Elles ont fait état d'une augmentation du nombre d'entreprises participantes ayant choisi leurs services par rapport aux cadres précédents et ont indiqué qu'elles avaient reçu un certain nombre de réclamations, même si la grande majorité d'entre elles étaient irrecevables. Par exemple, BBB a reçu 87 réclamations de citoyens de l'Union, dont deux seulement pouvaient faire l'objet d'un règlement des litiges. Bien que BBB ait expliqué que les réclamations sont traitées en moyenne en cinq jours ouvrables, ces deux réclamations ont finalement été closes en raison de l'absence de réponse des personnes concernées. VeraSafe a reçu 26 réclamations, dont six pouvaient faire l'objet d'un règlement des litiges. Deux d'entre elles concernant des demandes d'accès et de suppression ont été tranchées, tandis que deux étaient toujours en cours de traitement, et deux ont été soit retirées, soit closes en raison de l'absence de réponse de la personne concernée. Les deux MRI ont expliqué qu'ils s'efforcent de répondre aux réclamations dans la langue de la personne concernée.

Les entreprises certifiées en vertu du CPD qui traitent des données RH transférées depuis l'Union européenne doivent sélectionner l'APD de l'Union en tant que MRI pour ces données, tandis qu'une entreprise certifiée en vertu du CPD peut, sur une base volontaire, sélectionner l'APD de l'Union en tant que MRI pour d'autres types de données à caractère personnel transférées sur la base du CPD. En fait, plus de la moitié des entreprises certifiées en vertu du CPD au moment de l'examen avaient opté pour cette solution[19], ce dont la Commission se réjouit. Depuis l'adoption de la décision d'adéquation, le comité européen de la protection des données a adopté le règlement intérieur du «panel informel des APD de l'Union européenne».

---

[18] ANA - https://www.ana.net/content/show/id/accountability-dpf-consumers;

BBB National Programs - https://assets.bbbprograms.org/docs/default-source/eu-privacy-shield/dpf_periodicalreport_072024.pdf; ICDR – AAA - https://go.adr.org/rs/294-SFS-516/images/Data%20Privacy%20Framework%20IRM%20Program%20Report%202023-2024%20FINAL.pdf?version=0;

Insights Association - https://www.insightsassociation.org/Portals/INSIGHTS/Insights%20Association%20DPF%20Services%20Program%202024%20Annual%20Report_Final_1.pdf;
JAMS - https://www.jamsadr.com/files/Uploads/Documents/2024-Annual-Report-DPF-Cases.pdf;

PrivacyTrust DPF Services - https://privacytrust.com/fserve/PrivacyTrust_Dispute_Resolution_Report_2023_2024.pdf;

TRUSTe Dispute Resolution - https://trustarc.com/wp-content/uploads/2024/07/2024-Independent-Recourse-Mechanism-Annual-Report.pdf;

et VeraSafe - https://verasafe.com/wp-content/uploads/2020/06/VeraSafe-DPF-Dispute-Resolution-Program-Annual-Report-2024.pdf.

[19] Peu après la date de la réunion d'examen, le site web du CPD indiquait que 1 511 des 2 892 participants disposaient d'une autorité européenne de protection des données comme mécanisme de recours.

Ce panel est compétent pour fournir un avis contraignant aux organisations américaines à la suite de réclamations relatives au CPD en suspens qui ont été introduites par des personnes et portant sur le traitement de données à caractère personnel qui ont été transférées au départ de l'Union européenne au titre du CPD. Conformément à son règlement intérieur, le panel est constitué d'une APD agissant en tant qu'APD principale et d'autres ADP coexaminatrices désignées[20]. Il fournit un avis contraignant dans un délai de 60 jours à compter de la réception d'une réclamation relative au CPD. Le comité européen de la protection des données a également publié un modèle de formulaire de réclamation pour l'introduction de réclamations auprès des APD[21], ainsi que des FAQ pour les citoyens européens[22] et les entreprises européennes[23] sur le CPD. Le panel n'avait reçu aucune réclamation au moment de l'examen.

2.1.3.3. Le mécanisme d'arbitrage contraignant

L'International Centre for Dispute Resolution (ICDR), qui est la division internationale de l'American Arbitration Association, a été choisi par le ministère du commerce pour administrer le mécanisme d'arbitrage contraignant. À la suite de l'adoption de la décision d'adéquation, le ministère du commerce, en collaboration avec la Commission, a sélectionné 11 arbitres ayant une expérience dans le domaine de la protection de la vie privée et issus d'horizons divers, dont l'arbitrage, le pouvoir judiciaire, le monde universitaire et la société civile[24]. De plus, les règles d'arbitrage[25] du panel du CPD et un code de conduite pour les arbitres[26] ont été adoptés et sont tous disponibles sur le site web de l'ICDR. Au moment de l'examen, le mécanisme d'arbitrage n'avait encore été déclenché par aucune personne concernée dans l'Union.

2.1.4. Orientations, coopération et sensibilisation

Depuis l'entrée en vigueur du CPD, le ministère du commerce a mené diverses activités de sensibilisation en organisant des tournées de présentation, des webinaires et des conférences, en s'adressant aux associations professionnelles et en interagissant directement avec plus de 3 000 entreprises afin de fournir des informations sur le CPD. Il a également publié des orientations, y compris sous la forme de FAQ adressées aux personnes concernées, ainsi qu'aux entreprises de l'Union européenne et des États-Unis[27]. Le comité européen de la protection des données a, quant à lui, élaboré des formulaires de réclamation et des FAQ adressés aux personnes concernées et aux entreprises. De même, la Commission a publié des questions et réponses et une fiche d'information sur le CPD lorsqu'elle a adopté sa décision d'adéquation[28].

---

[20] Le 17 avril 2024, le comité européen de la protection des données a adopté le règlement intérieur du «panel informel des APD de l'Union européenne» conformément au cadre de protection des données UE - États-Unis. Il peut être consulté à l'adresse suivante: https://www.edpb.europa.eu/system/files/2024-04/dpf_rules-of-procedure_informal-panel-dpas_en.pdf.

[21] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form_fr.

[22] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-individuals_fr.

[23] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-businesses_fr.

[24] https://go.adr.org/DPF_Arbitrator_Bios.html.

[25] https://go.adr.org/rs/294-SFS-516/images/IC.DR-AAA_EU-US_DPF_AnnexI_Arbitration_Rules.pdf.

[26] https://go.adr.org/rs/294-SFS-516/images/Code_of_Conduct_for_Arbitrators_Appointed_to_EU-US_DPF_AnnexI_Arbitrations.pdf.

[27] Voir, par exemple, https://www.dataprivacyframework.gov/US-Businesses.

[28] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_fr.

Dans le même temps, il est ressorti de la réunion d'examen qu'il convient de redoubler d'efforts pour sensibiliser les personnes concernées et fournir des orientations aux entreprises. Les contributions reçues des entreprises et des MRI, ainsi que le très faible nombre de réclamations, donnent à penser que les personnes concernées n'ont peut-être pas toujours connaissance de leurs droits et/ou du mécanisme pour les exercer. Lors de la réunion d'examen, le ministère du commerce a manifesté son intérêt pour une collaboration avec les APD de l'Union afin de sensibiliser davantage les citoyens de l'Union au cadre. La Commission encourage les initiatives de ce type et prend également des mesures pour mieux informer les personnes, notamment en fournissant des informations supplémentaires sur le CPD sur son site web, par exemple en intégrant des références à des documents d'orientation pertinents adoptés par le comité européen de la protection des données, le ministère du commerce et d'autres autorités américaines et des liens vers ceux-ci.

En ce qui concerne les orientations sur les principes du CPD, les représentants du comité européen de la protection des données ont convenu, lors de la réunion d'examen, de coopérer dans les mois à venir afin de fournir des précisions supplémentaires sur la notion de données RH dans le cadre du CPD et sur les obligations spécifiques qui s'appliquent au traitement de ces données. Différents éléments à inclure dans ces orientations ont été étudiés. Par exemple, ces orientations pourraient aborder certains scénarios pratiques dans lesquels des données sur les salariés seraient traitées dans le cadre du CPD (par exemple, par un fournisseur de services d'informatique en nuage) et expliquer, pour ces scénarios, quelles obligations du CPD seraient pertinentes. En outre, elles pourraient suggérer aux entreprises qui reçoivent des données sur les salariés de citoyens de l'Union (mais qui n'utilisent pas nécessairement ces données dans le cadre d'une relation de travail) de choisir le panel d'APD en tant que MRI. Cela garantirait que ces personnes puissent s'adresser à une autorité géographiquement proche et, le cas échéant, qui connaît mieux les lois nationales applicables aux données RH.

En outre, un aspect spécifique pour lequel il semble que davantage d'orientations seraient utiles (également sur la base des contributions reçues de la part des associations professionnelles) concerne les exigences du CPD applicables aux transferts ultérieurs. De plus, le ministère du commerce a indiqué qu'il serait utile d'examiner si certains secteurs pourraient bénéficier d'orientations supplémentaires sur l'application des principes du CPD à leurs activités, par exemple dans le domaine de la recherche en matière de santé et des services financiers.

La Commission se félicite que les deux parties soient prêtes à élaborer des orientations et espère que les travaux sur les sujets susmentionnés débuteront prochainement.

Plus généralement, plusieurs mécanismes ont été mis en place pour assurer les échanges et la coopération entre les autorités américaines et les APD, notamment grâce à la désignation de points de contact spécifiques au sein de la FTC et du ministère du commerce pour traiter les demandes d'information et les dossiers soumis par les APD.

2.1.5. Évolutions pertinentes du système juridique américain

Depuis l'adoption de la décision d'adéquation, le cadre juridique américain a connu un certain nombre d'évolutions dans le domaine de la protection de la vie privée. Il s'agit notamment d'évolutions de la législation, de la réglementation et de la jurisprudence. Celles-ci témoignent généralement d'une convergence accrue entre les approches de l'Union et des États-Unis en ce qui concerne certains défis en matière de respect de la vie privée, notamment grâce à

l'utilisation de concepts juridiques similaires. Certaines de ces évolutions sont en cours et devront continuer de faire l'objet d'un suivi.

Au niveau fédéral, le président a émis plusieurs décrets présidentiels (Executive Orders, ci-après «EO») qui sont pertinents pour l'utilisation de données à caractère personnel. En particulier, le décret présidentiel 14117 du 28 février 2024[29] interdit ou limite les transactions comportant certaines catégories de données à caractère personnel sensibles (par exemple, les données relatives à la santé, les identifiants biométriques, les données génomiques humaines) avec des entités de certains «pays préoccupants»[30]. Le décret adopté charge le procureur général de proposer des règlements – qui n'avaient pas encore été proposés au moment de l'adoption du présent rapport – visant à préciser davantage sa mise en œuvre. En outre, le décret présidentiel 14110 du 30 octobre 2023 sur l'intelligence artificielle (IA)[31] met l'accent sur le développement d'une intelligence artificielle sûre, sécurisée et digne de confiance. Il impose à plusieurs agences fédérales d'élaborer des lignes directrices et des normes en matière de sécurité en lien avec l'IA, y compris en ce qui concerne les risques spécifiques liés à l'IA pour le respect de la vie privée et les techniques de protection de la vie privée.

Pour ce qui est des travaux législatifs, alors que des projets de lois fédéraux sur la protection de la vie privée ont été introduits au Congrès ces dernières années, en juillet 2024, 20 États américains avaient promulgué des lois complètes sur la protection de la vie privée, dont huit sont entrés en vigueur (Californie, Colorado, Oregon, Virginie, Connecticut, Utah, Texas et Floride). En outre, 17 États américains ont adopté une législation portant sur le traitement automatisé (ou, à tout le moins, certaines formes de traitement automatisé) et autorisant généralement des possibilités de refus pour certains types de décisions fondées sur le «profilage»[32].

Quant à l'évolution de la jurisprudence, plusieurs représentants de la société civile ont attiré l'attention sur le récent arrêt rendu par la Cour suprême dans l'affaire *Loper Bright Enterprises v. Raimondo* (du 28 juin 2024). Cet arrêt renverse de la jurisprudence antérieure relative à la

---

[29] https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related.

[30] Il s'agit notamment, comme proposé par le procureur général dans un avant-projet de réglementation publié le 3 mai 2024, de la Chine, de la Corée du Nord, de Cuba, de Hong Kong et Macao, de l'Iran et du Venezuela. Voir https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and.

[31] https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

[32] Bien qu'il existe des différences entre ce que les différents États entendent par «profilage», le profilage est généralement défini comme étant toute forme de traitement automatisé de données à caractère personnel visant à évaluer, analyser ou prévoir des aspects personnels liés à la situation économique, à la santé, aux préférences personnelles, aux intérêts, à la fiabilité, au comportement, à la localisation ou aux mouvements d'une personne physique identifiée ou identifiable. Ce sont généralement les consommateurs qui peuvent choisir de refuser le traitement aux fins du profilage. Les États suivants ont élaboré une législation sur le profilage: le Colorado (Colo. Rev. Stat. Ann. § 6-1-1306), le Connecticut (Conn. Gen. Stat. Ann. § 42-518), le Delaware (Del. Code Ann. tit. 6, § 12D-104), la Floride (Fla. Stat. Ann. § 501.705), l'Indiana (Ind. Code Ann. § 24-15-3-1), le Kentucky (Ky. Rev. Stat. Ann. § 367.3615), le Maryland [Maryland Online Data Privacy Act (loi du Maryland sur la protection des données en ligne) de 2024, promulgué le 9 mai 2024], le Minnesota (Minn. Stat. Ann. § 325O.07), le Montana (Mont. Code Ann. § 30-14-2808), le Nebraska (Neb. Rev. Stat. Ann. § 87-1107), le New Hampshire (N.H. Rev. Stat. Ann. § 507-H:4), le New Jersey (N.J. Stat. Ann. § 56:8-166.8), l'Oregon (Or. Rev. Stat. Ann. § 646A.574), Rhode Island [Rhode Island Data Transparency and Privacy Protection Act (loi de Rhode Island sur la protection et la transparence des données), promulgué le 29 juin 2024], le Tennessee (Tenn. Code Ann. § 47-18-3304), le Texas (Tex. Bus. & Com. Code Ann. § 541.051) et la Virginie (Va. Code Ann. § 59.1-577).

doctrine *Chevron*, selon laquelle les juridictions appliquent le principe de déférence à l'interprétation raisonnable de la loi par une agence réglementaire en cas d'ambiguïté dans une loi mise en œuvre par cette agence. En particulier, certaines ONG se sont déclarées préoccupées par l'incidence de cet arrêt de la Cour suprême sur l'autorité en matière de réglementation de la FTC dans le domaine de la protection de la vie privée, tout en reconnaissant qu'il pourrait y avoir une incidence nulle ou limitée sur ses pouvoirs coercitifs. Lors de la réunion d'examen, la FTC a indiqué qu'il était encore tôt pour connaître les implications exactes de cet arrêt. Dans le même temps, elle a expliqué qu'elle élaborait les règles en vertu d'un pouvoir qui lui est conféré par le FTC Act qui est différent des pouvoirs conférés à d'autres agences administratives et pour lequel la doctrine *Chevron* était moins pertinente. Le récent arrêt pourrait donc avoir une incidence limitée en la matière.

En outre, la FTC a informé les participants des récentes évolutions de son approche du traitement automatisé et de l'intelligence artificielle. Ainsi, elle a notamment adopté une déclaration commune avec d'autres autorités répressives contre la discrimination et la partialité dans les systèmes automatisés[33], ainsi que plusieurs mesures coercitives, dans lesquelles la FTC se concentre, entre autres, sur la transparence, l'équité du traitement automatisé et la capacité des personnes concernées à contester les résultats. L'affaire la plus notable à cet égard est la décision de la FTC de mars 2024 à l'encontre de *Rite Aid*, par laquelle elle a interdit pendant cinq ans l'utilisation de la technologie de reconnaissance faciale par cette société à des fins de sécurité[34]. La FTC a en particulier considéré que *Rite Aid* n'avait pas pris de mesures raisonnables pour prévenir les résultats erronés et informer les consommateurs de la technologie utilisée. Plus généralement, lors de la réunion d'examen, la FTC a évoqué ses priorités actuelles, et notamment les domaines qui, selon elle, méritent une approche coercitive plus proactive à l'avenir. Il s'agit, entre autres, de la protection des données sensibles (par exemple, les données relatives à la santé, les données biométriques, la géolocalisation)[35], de la protection des enfants[36] et des mineurs en ligne et de la sécurité des données[37].

La Commission continuera de suivre de près ces évolutions ainsi que les autres évolutions aux États-Unis, en particulier toute nouvelle démarche en vue d'une loi fédérale globale sur la protection de la vie privée et l'éventuelle incidence de la récente jurisprudence de la Cour suprême sur le rôle de la FTC dans le domaine de la protection de la vie privée.

La Commission se félicite des informations fournies par la FTC sur ses récentes activités coercitives et sur ses priorités actuelles, qui correspondent dans une large mesure aux tendances

---

[33] https://files.consumerfinance.gov/f/documents/cfpb_joint-statement-enforcement-against-discrimination-bias-automated-systems_2023-04.pdf.

[34] https://www.ftc.gov/legal-library/browse/cases-proceedings/2023190-rite-aid-corporation-ftc-v.

[35] Voir, par exemple, les récentes ordonnances de la FTC contre X-Mode pour la vente et le partage d'informations sensibles sur la localisation (https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf) et contre Monument concernant la divulgation de données sensibles relatives à la santé à des tiers à des fins de marketing (https://www.ftc.gov/system/files/ftc_gov/pdf/MonumentOrderFiled.pdf).

[36] Par exemple, la FTC a récemment annoncé une enquête conduisant à une action en justice contre TikTok et sa société mère, ByteDance, pour violation présumée de la loi relative à la protection de la vie privée des enfants. Ces deux entreprises n'auraient pas respecté l'obligation de notification et d'obtention du consentement parental avant de collecter et d'utiliser des informations à caractère personnel d'enfants de moins de 13 ans (https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law).

[37] Voir vue d'ensemble des récentes activités coercitives sur la page consacrée aux dernières nouvelles concernant la protection de la vie privée et la sécurité des données en vertu du CPD pour 2023: https://ec.europa.eu/commission/presscorner/detail/fr/mex_24_1307.

et aux priorités en matière de contrôle de l'application de la protection des données en Europe. La FTC participe aussi activement au réseau qui rassemble les pays bénéficiant d'une décision d'adéquation de l'Union européenne, que la Commission a lancé en mars 2024[38]. Cette convergence accrue devrait encourager et faciliter une coopération plus étroite entre les autorités chargées de veiller à la protection de la vie privée des deux côtés de l'Atlantique, notamment sur les questions pertinentes pour le fonctionnement du CPD.

2.2. Aspects relatifs à l'accès aux données à caractère personnel transférées au titre du cadre de protection des données UE - États-Unis et à l'utilisation de celles-ci par les autorités publiques américaines

La décision d'adéquation contient une évaluation détaillée des règles qui régissent la collecte et l'utilisation des données à caractère personnel transférées de l'Union européenne vers des entreprises certifiées en vertu du CPD par les autorités publiques américaines, en particulier à des fins répressives et à des fins de sécurité nationale. Depuis l'adoption de la décision d'adéquation, comme les autorités américaines l'ont confirmé lors de la réunion d'examen, il n'y a pas eu d'évolution pertinente en ce qui concerne le cadre juridique applicable à l'accès aux données à des fins répressives ou réglementaires au cours de la première année du CPD. C'est pourquoi les constatations qui suivent ne concernent que les évolutions dans le domaine de la sécurité nationale.

Les conclusions tirées dans la décision d'adéquation sur l'accès des agences de renseignement aux données reposent sur l'analyse des conditions et des limitations qui s'appliquent aux opérations de renseignement d'origine électromagnétique en vertu de plusieurs dispositions juridiques compétentes – en particulier l'article 702 de la loi sur la surveillance des renseignements extérieurs (Foreign Intelligence Surveillance Act, ci-après le «FISA») et le décret présidentiel 12333[39] –, telles que complétées et renforcées par le décret présidentiel 14086 sur le renforcement des garanties pour les activités de renseignement d'origine électromagnétique menées par les États-Unis (ci-après l'«EO 14086») adopté par le président des États-Unis le 7 octobre 2022. Les garanties énoncées dans l'EO 14086 s'appliquent à toutes les activités américaines de renseignement d'origine électromagnétique, quelle que soit la disposition juridique sur laquelle ces activités sont fondées et peu importe où elles ont lieu, et protègent les données des personnes non américaines (y compris des Européens)[40]. L'EO 14086 a également mis en place un nouveau mécanisme de recours par lequel ces garanties contraignantes peuvent être invoquées et appliquées par les personnes concernées dans l'Union européenne.

[38] Voir https://ec.europa.eu/commission/presscorner/detail/fr/mex_24_1307. À la suite de la réunion de mars 2024, il a été décidé d'organiser une série de sessions thématiques. La première a eu lieu en juillet 2024 et a porté sur la mise au point d'outils susceptibles d'aider les petites et moyennes entreprises à se conformer à la législation en matière de protection de la vie privée.

[39] Les autres mesures qui peuvent être prises au titre du FISA en ce qui concerne les données transférées depuis l'Union européenne sont la surveillance électronique des individus (article 105 du FISA), les fouilles corporelles (article 302 du FISA), l'utilisation d'enregistreurs graphiques ou de dispositifs de traçage (article 402 du FISA) et la collecte de documents commerciaux auprès de certaines entreprises (transporteurs publics, établissements d'hébergement public, établissements de location de véhicules ou établissements de stockage, article 501 du FISA). Ces différentes bases juridiques sont analysées en détail dans la décision d'adéquation (considérants 142 à 152).

[40] Pour de plus amples informations, voir section 3.2.1.2 de la décision d'adéquation.

Les sections suivantes décrivent les mesures prises par les autorités américaines depuis l'adoption de la décision d'adéquation pour se conformer à l'EO 14086, ainsi que les évolutions pertinentes concernant le cadre juridique susmentionné.

2.2.1. Évolutions pertinentes concernant le cadre juridique américain

2.2.1.1. Mise en œuvre du décret présidentiel 14086 par les agences de renseignement

Les limitations et garanties introduites par l'EO 14086 complètent celles prévues à l'article 702 du FISA et par l'EO 12333. Elles sont contraignantes pour toutes les agences de renseignement et ont été concrétisées par des politiques et des procédures adoptées par chaque agence.

Dans le cadre du premier examen, les autorités américaines ont confirmé qu'aucune modification n'a été apportée à l'EO 14086 depuis son adoption. En outre, il a été précisé que le président des États-Unis n'a pas fait usage du pouvoir prévu aux articles 2(b)(i)(B) et 2(b)(ii)(C) de l'EO 14086 pour mettre à jour la liste des objectifs légitimes pour lesquels des renseignements d'origine électromagnétique peuvent être collectés ou la liste des finalités pour lesquelles les données collectées en vrac peuvent être utilisées[41]. Afin de définir des priorités plus spécifiques pour lesquelles des renseignements d'origine électromagnétique peuvent effectivement être collectés, l'EO 14086 a mis en place une procédure spécifique. En particulier, le responsable de la protection des libertés civiles de l'ODNI (ci-après l'«ODNI CLPO») doit être consulté pour évaluer, pour chaque priorité, si 1) elle fait progresser un ou plusieurs objectifs légitimes énumérés dans le décret; 2) elle n'a pas été conçue pour la collecte de renseignements d'origine électromagnétique à des fins interdites énumérées dans le décret ni ne devrait donner lieu à une telle collecte et 3) elle a été établie après avoir dûment pris en compte les aspects relatifs à la vie privée et aux libertés civiles de toutes les personnes[42]. Lors de la réunion d'examen, l'ODNI CLPO a confirmé qu'elle avait examiné les priorités proposées par le directeur du renseignement national dans le cadre des priorités nationales en matière de renseignement de 2023, qu'elle avait conclu qu'elles étaient conformes aux exigences susmentionnées et qu'elle avait partagé sa conclusion avec le directeur du renseignement national, lequel a, à son tour, soumis les priorités pour validation au président. L'ODNI CLPO a également dispensé des formations sur les exigences de l'EO 14086 à certaines parties de la communauté du renseignement participant à l'élaboration des priorités en matière de renseignement.

En outre, les autorités américaines ont pris de nouvelles mesures pratiques au cours de l'année écoulée pour mettre en œuvre l'EO 14086 dans leurs opérations quotidiennes. En particulier, les agences de renseignement ont mis en place de nouvelles politiques et lignes directrices internes sur l'application du décret, par exemple des processus internes (au moyen d'exigences d'autorisation interne, de contrôles d'accès documentés, de sorte que seules les personnes qui ont été correctement formées et qui ont les exigences de mission nécessaires ont accès aux informations, etc.) afin de garantir le respect des exigences de nécessité et de proportionnalité

[41] Ces objectifs/finalités légitimes comprennent, par exemple, la protection contre l'espionnage, le sabotage et les assassinats, ainsi que d'autres activités de renseignement menées par un gouvernement, une organisation ou une personne étranger ou pour son compte, ou avec l'aide de celui-ci; et la protection contre le terrorisme, la prise d'otages et la détention de personnes en captivité par un gouvernement, une organisation ou une personne étranger ou pour son compte.

[42] Article 2(b)(iii) de l'EO 14086.

dans le cadre de la collecte tant ciblée qu'en vrac[43]. De plus, des formations concernant l'EO 14086 ont été dispensées au personnel de différentes agences de renseignement (par exemple, la NSA, la CIA, le FBI), y compris des sessions de formation annuelles et ad hoc organisées par l'ODNI CLPO et des formations obligatoires pour tous les nouveaux membres du personnel qui rejoignent l'ODNI.

La Commission se félicite des différentes mesures mises en place pour mettre en œuvre l'EO 14086 et garantir la conformité avec celui-ci. L'expérience acquise concernant l'application pratique des garanties du décret présidentiel ne faisant que croître, la Commission apprécierait de pouvoir discuter d'exemples concrets de la manière dont le décret est appliqué dans la pratique (tout en respectant les considérations de confidentialité applicables) lors des futurs examens.

2.2.1.2. Réactivation de l'article 702 du FISA

L'article 702 du FISA autorise le ciblage de personnes non américaines dont il est raisonnable de penser qu'elles se trouvent hors des États-Unis pour se procurer des informations de renseignement extérieur. L'acquisition a lieu sur la base de certifications annuelles soumises au tribunal de la surveillance du renseignement extérieur (Foreign Intelligence Surveillance Court, FISC) et approuvées par celui-ci. Ces certifications indiquent les catégories spécifiques de renseignements extérieurs à collecter. Le 21 juillet 2023, l'ODNI a annoncé qu'il existait trois certifications approuvées au titre de l'article 702 du FISA, couvrant les catégories suivantes de renseignements extérieurs: 1) gouvernements étrangers et entités apparentées, 2) lutte contre le terrorisme et 3) lutte contre la prolifération[44]. Les certifications doivent également inclure des procédures de ciblage et de minimisation approuvées par le FISC[45]. En particulier, le ciblage est effectué en demandant aux entreprises américaines qui répondent à la définition du «fournisseur de services de communications électroniques» donnée par le FISA de divulguer les données sur les communications électroniques envoyées à des «sélecteurs» ou depuis des «sélecteurs», qui identifient un compte de communication spécifique, par exemple un numéro de téléphone ou une adresse électronique. Le gouvernement américain a publié un certain nombre de documents sur l'article 702 du FISA pour informer le public sur le fonctionnement des programmes de surveillance, les exigences applicables et les mesures de protection de la vie privée, ainsi que sur le rôle du FISC[46].

En raison d'une clause de caducité, l'article 702 du FISA devait expirer fin 2023, à moins que le Congrès ne la réactive. Après une réactivation temporaire sans aucune modification, le Congrès a adopté le 19 avril 2024 la loi sur la réforme du renseignement et la sécurisation de l'Amérique (Reforming Intelligence and Securing America Act, RISAA), qui réactive l'article 702 du FISA pour une période de deux ans et introduit plusieurs modifications. Celles-ci se divisent en deux grandes catégories: 1) les modifications de la portée des activités de

[43] Voir https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguardsin-executive-order-14086, publié le 3 juillet 2023.
[44] https://www.intelligence.gov/ic-on-the-record-database/results/1307-release-of-documents-related-to-the-2023-fisa-section-702-certifications.
[45] Ces procédures limitent la collecte de données à une fin spécifique de renseignement extérieur, limitent l'accès aux bases de données dans lesquelles les informations obtenues en vertu de l'article 702 du FISA sont stockées (y compris au moyen de contrôles d'accès) et imposent des limites à l'utilisation, à la conservation et à la diffusion de ces informations.
[46] https://www.intel.gov/foreign-intelligence-surveillance-act.

surveillance autorisées en vertu de l'article 702 du FISA et 2) les modifications institutionnelles et procédurales.

Modifications de la portée des activités de surveillance autorisées en vertu de l'article 702 du FISA

Le RISAA a apporté trois grandes modifications à la portée des activités de surveillance qui peuvent être menées au titre de l'article 702 du FISA.

Premièrement, la collecte des communications contenant une référence à un sélecteur a été définitivement interdite[47]. Il s'agit de la collecte de communications dans lesquelles le sélecteur au titre de l'article 702 (tel qu'une adresse électronique) n'est pas indiqué dans le champ du destinataire ou de l'expéditeur des communications, mais qui contiennent une référence à ce sélecteur (par exemple, les communications électroniques qui ne sont pas envoyées vers ou depuis l'adresse électronique sélectionnée, mais qui incluent l'adresse électronique sélectionnée dans le texte ou le corps du courrier électronique). Même si la collecte de ces communications avait déjà été exclue à la suite d'une modification du FISA en 2018, le FISA prévoyait toujours la possibilité de recommencer la collecte des communications contenant une référence à un sélecteur à l'avenir, à la suite d'une procédure d'autorisation spécifique associant le FISC et le Congrès. La dernière modification introduite par le RISAA a supprimé cette possibilité.

Deuxièmement, la définition des informations de renseignement extérieur a été élargie pour inclure les informations relatives à la lutte contre la drogue[48]. Au cours de la réunion d'examen, les autorités américaines ont expliqué que cette modification a été introduite compte tenu de l'actuelle crise du fentanyl et de la menace croissante pour la sécurité nationale posée par les trafiquants et fabricants internationaux de stupéfiants. Dans ce contexte, il a été confirmé que cette notion relève de plusieurs des objectifs légitimes énumérés dans l'EO 14086, à savoir comprendre ou évaluer les capacités, les intentions ou les activités d'organisations étrangères qui constituent une menace actuelle ou potentielle pour la sécurité nationale des États-Unis ou de leurs alliés; comprendre ou évaluer les menaces transnationales qui ont une incidence sur la sécurité mondiale, y compris les risques pour la santé publique; et se protéger contre les menaces criminelles transnationales[49].

Troisièmement, le RISAA a élargi la définition du «fournisseur de services de communications électroniques», élargissant ainsi l'éventail d'entreprises pouvant être contraintes de fournir des informations conformément à l'article 702 du FISA[50]. La définition inclut désormais les autres fournisseurs de services qui ont «accès à des équipements qui sont ou peuvent être utilisés pour transmettre ou stocker des communications filaires ou électroniques», tout en excluant expressément les établissements d'hébergement public, les logements, les équipements publics et les établissements de restauration. Dans une lettre adressée au Congrès, le ministère de la justice a mentionné que cette modification était une modification technique visant à couvrir un nombre «extrêmement restreint» d'entreprises technologiques qui, selon de récentes décisions du FISC et de la cour de contrôle de la surveillance du renseignement extérieur (Foreign Intelligence Surveillance Court of Review, FISCR), n'étaient pas couvertes par la définition

[47] Article 22 du RISAA.
[48] Article 23 du RISAA.
[49] Article 2(b)(ii)(A)(2), (3) et (10) de l'EO 14086.
[50] Article 25 du RISAA.

précédente du fournisseur de services de communications électroniques[51]. Dans cette même lettre, le ministère de la justice s'est engagé à restreindre la portée en appliquant cette définition exclusivement pour couvrir le type de fournisseur de services en cause dans les litiges donnant lieu à une décision du FISC. En conséquence, les entreprises concernées sont citées dans une annexe classifiée destinée au Congrès. Plusieurs ONG, y compris celles qui ont donné leur avis dans le cadre de l'examen, se sont déclarées préoccupées par cette extension, soutenant qu'elle pourrait potentiellement couvrir de nombreuses entreprises américaines (puisque nombre d'entre elles fournissent un certain type de service et ont accès à des équipements de communication). À la lumière de ces préoccupations, une nouvelle modification a été proposée, avec le soutien de la communauté du renseignement, dans un projet de loi sur l'autorisation du renseignement pour l'exercice 2025, qui est actuellement soumis au Congrès. Cette modification, si elle est adoptée par le Congrès, garantirait que les entreprises supplémentaires couvertes par la définition du fournisseur de services de communications électroniques se limiteraient uniquement à celles mentionnées dans les décisions précitées du FISC. Le projet de loi prévoit également que chaque directive adressée à une telle entreprise devrait être signalée au FISC, afin de permettre à ce dernier de vérifier si l'entreprise tombe effectivement sous le coup de la définition. Dans sa lettre au Congrès, le ministère de la justice s'est engagé à rendre compte au Congrès tous les six mois de toute application de la définition actualisée afin de permettre au Congrès d'exercer le contrôle approprié en ce qui concerne l'application de la définition au sens strict.

Il importe de relever que les autorités américaines et le PCLOB ont confirmé lors de la réunion d'examen que toutes les garanties de l'EO 14086 continuent de s'appliquer pleinement à l'ensemble des données collectées et utilisées au titre de l'article 702 du FISA, y compris à la suite de ces modifications. Ainsi, même si le RISAA élargit quelque peu l'éventail des entreprises susceptibles d'être destinataires d'une ordonnance, il ne limite pas l'exercice des droits. Néanmoins, il importera de suivre les évolutions (législatives et en matière de rapport) et de recevoir des informations sur l'application de ces nouvelles règles dans la pratique, par exemple sur l'incidence de l'élargissement des définitions du renseignement extérieur et des fournisseurs de services de communications électroniques sur le nombre de cibles au titre de l'article 702 du FISA (tel que communiqué chaque année par l'ODNI, voir ci-dessous concernant la transparence). Le futur rapport de suivi du récent rapport du PCLOB sur l'article 702 du FISA (voir ci-dessous) devrait être particulièrement instructif à cet égard.

Modifications institutionnelles et procédurales

En ce qui concerne les modifications institutionnelles et procédurales, le RISAA a codifié plusieurs procédures déjà suivies dans la pratique et a introduit de nouvelles garanties. Si certaines d'entre elles ne concernent que les ressortissants américains, plusieurs modifications renforcent la protection des personnes tant américaines que non américaines dont les données peuvent être collectées au titre de l'article 702 du FISA[52] et sont donc pertinentes pour le fonctionnement du CPD.

[51] https://www.justice.gov/opa/media/1348621/dl?inline. Voir décision du FISC de 2022 (https://www.intel.gov/assets/documents/702%20Documents/declassified/2022-FISC-ECSP-OPINION.pdf) et décision de la cour de contrôle de la surveillance du renseignement extérieur confirmant cette décision (https://www.intel.gov/assets/documents/702%20Documents/declassified/2023_FISC-R_ECSP_Opinion.pdf).

[52] En outre, le RISAA a introduit quelques modifications en ce qui concerne la surveillance électronique classique des individus conformément à l'article 105 du FISA (sur la base d'un mandat du FISC émis s'il existe une

Premièrement, un certain nombre d'exigences supplémentaires en matière de responsabilité, de surveillance et d'établissement de rapports ont été mises en place. En particulier, le personnel du FBI doit désormais être formé chaque année aux règles applicables à l'interrogation des informations obtenues au titre de l'article 702 du FISA[53]. Le FBI est également tenu de faire rapport au Congrès sur ses activités d'interrogation (par exemple, le nombre d'interrogations utilisant des «technologies de traitement par lots», c'est-à-dire utilisant plusieurs termes d'interrogation dans le cadre d'une seule interrogation) et les mesures en matière de responsabilité mises en place pour garantir le respect des exigences légales en matière d'interrogation (articles 11 et 12 du RISAA). En outre, l'inspecteur général du ministère de la justice est chargé d'établir un rapport sur le respect des exigences en matière d'interrogation par le FBI (article 9 du RISAA). Plus généralement, pour accroître la transparence des procédures devant le FISC, l'ODNI et le procureur général sont désormais tenus de mener à bien l'examen de déclassification des décisions du FISC dans un délai de 180 jours (article 7 du RISAA). En outre, les transcriptions de toutes les audiences devant le FISC et la FISCR (devant laquelle les décisions du FISC peuvent faire l'objet d'un recours) doivent être conservées et transmises au Congrès (article 8 du RISAA).

Deuxièmement, le RISAA a introduit de nouvelles limitations à l'utilisation par le FBI des données collectées au titre de l'article 702 du FISA. L'article 2(d) du RISAA prévoit qu'une interrogation utilisant la «technologie de traitement par lots» ne peut être effectuée qu'après avoir obtenu l'approbation d'un avocat au sein du FBI, sauf en cas de circonstances pressantes. De plus, il est désormais interdit au FBI de vérifier automatiquement les informations non minimisées obtenues au titre de l'article 702 du FISA; il doit faire en sorte que les analystes soient tenus de procéder à une sélection de manière affirmative pour effectuer des recherches dans ces informations. Le RISAA a également interdit au FBI de procéder à des interrogations visant uniquement à trouver et à extraire des preuves d'une activité criminelle (sauf s'il existe un motif sérieux de croire qu'elles pourraient contribuer à atténuer ou à éliminer une menace pour la vie ou des coups et blessures graves, ou si elles sont nécessaires pour se conformer à des obligations de divulgation dans un litige)[54]. De surcroît, il est interdit au FBI d'introduire des données non minimisées dans des référentiels analytiques, à moins que la personne ciblée ne soit pertinente pour une enquête de sécurité nationale existante[55].

Troisièmement, certaines dispositions relatives au statut et au rôle des *amici curiae* devant le FISC ont été modifiées[56]. Les *amici* sont désignés en tant qu'experts pour assister le tribunal (et la FISCR) sur des questions liées à la protection de la vie privée et aux libertés civiles ou pour aider à clarifier des questions technologiques lors du traitement d'une demande spécifique du gouvernement. Alors que la FISA exigeait auparavant que les *amici* disposent d'une expertise en matière de protection de la vie privée et de libertés civiles, de collecte de

présomption sérieuse). Une demande présentée par une agence de renseignement au procureur général en vue d'obtenir une ordonnance pour procéder à une surveillance électronique d'individus nécessite désormais une déclaration sous serment justifiant la conviction que les conditions de l'article 105 du FISA sont remplies [article 6(a) du RISAA]. La durée possible de la surveillance électronique en ce qui concerne les puissances étrangères ou les agents de puissances étrangères a été portée de 120 jours à un an [article 6(g) du RISAA].

[53] Article 2(d) du RISAA.

[54] Article 3(a) du RISAA.

[55] Article 3(b) du RISAA. Lorsque des circonstances pressantes l'exigent, le directeur du FBI peut décider d'une exception à cette disposition, qui doit être notifiée au Congrès.

[56] Par souci de clarté, ces modifications n'ont pas d'incidence sur le statut et le rôle des avocats spéciaux devant la DPRC, comme les États-Unis l'ont confirmé lors de la réunion d'examen.

renseignements, de technologies de la communication ou d'autres domaines pertinents, elle exige désormais, en principe, une expertise en matière de protection de la vie privée/libertés civiles et de collecte de renseignements. Le tribunal avait déjà la possibilité de désigner un *amicus* chaque fois qu'elle le jugeait approprié, et elle était tenue de le faire dans le cadre d'une interprétation nouvelle ou notable de la loi. À la suite de la réactivation, le FISC est désormais également tenu de désigner un *amicus* chaque fois qu'il lui est demandé d'approuver une certification au titre de l'article 702 du FISA et les procédures y afférentes (par exemple, procédures de ciblage), sauf s'il estime que cela ne serait pas approprié ou risquerait d'entraîner un retard injustifié[57]. De plus, au lieu de n'en désigner qu'un, le tribunal peut désormais décider de désigner un ou plusieurs *amici*. Il est également précisé que les informations devant être fournies par les *amici* doivent «se limiter à répondre aux points spécifiques soulevés par le tribunal», bien que les domaines sur lesquels ils peuvent formuler des commentaires soient restés vastes (à savoir, arguments juridiques et informations concernant la protection de la vie privée et des libertés civiles des ressortissants des États-Unis, la collecte de renseignements et les technologies de communication ou tout autre domaine pertinent).

Enfin, l'article 18 du RISAA établit une «commission de réforme du FISA», composée notamment de membres du Congrès, du président du PCLOB, du directeur adjoint principal du renseignement national et du procureur général adjoint, ainsi que d'autres membres devant être nommés par le Congrès[58], afin de recommander des réformes supplémentaires du FISA.

La Commission suivra de près les évolutions en ce qui concerne l'article 702 du FISA, notamment dans le cadre des activités de surveillance du PCLOB (voir ci-dessous), des travaux de la commission de réforme et du prochain réexamen du FISA après deux ans.

2.2.1.3. Activités de surveillance dans la pratique: chiffres et tendances

Le rapport annuel de l'ODNI sur la transparence en matière statistique concernant le recours, par la communauté du renseignement, aux dispositions nationales relatives à la surveillance de la sécurité pour l'année civile 2023 (publié en avril 2024)[59] montre que le nombre de cibles au titre de l'article 702 du FISA est passé de 245 073 au cours de l'année civile 2022 à 268 590 au cours de l'année civile 2023. Il explique que les fluctuations du nombre de cibles peuvent être liées à diverses raisons, notamment des modifications des priorités opérationnelles, des événements mondiaux, des capacités techniques, le comportement des cibles et des changements dans le secteur des télécommunications. Ce rapport indique également qu'aucune personne non américaine (contre une en 2021 et aucune en 2022) n'a été ciblée au titre de l'article 402 du FISA (enregistreurs graphiques et dispositifs de traçage), tandis que six ordonnances (contre 11 en 2021 et en 2022), pour six cibles (contre 13 en 2021 et 11 en 2022), ont été émises au titre de l'article 501 du FISA (accès aux documents commerciaux des transporteurs publics, des établissements de location de véhicules ou des établissements de stockage physique), couvrant 5 412 identifiants uniques (contre 23 157 en 2021 et 55 431 en 2022) utilisés pour communiquer les informations recueillies en vertu de ces ordonnances.

Le rapport annuel du ministère de la justice sur la loi sur la surveillance des renseignements extérieurs présenté au Congrès indique qu'au cours de l'année civile 2023, le FISC a reçu 327 demandes de surveillance électronique et/ou de fouilles corporelles à des fins de

[57] Article 5(b) du RISAA.
[58] L'article 18 exige spécifiquement une représentation extérieure au Congrès.
[59] https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf.

renseignement extérieur en vertu respectivement des articles 105 et 302 du FISA[60]. Le nombre total de personnes ciblées était compris entre 500 et 999. En ce qui concerne les lettres de sécurité nationale, le rapport indique que 10 115 demandes (à l'exclusion des demandes concernant uniquement les informations d'abonnement) ont été émises pour des informations sur des personnes non américaines, sollicitant des informations relatives à 3 033 personnes non américaines différentes[61].

Plusieurs entreprises certifiées en vertu du CPD (par exemple Google, Meta) font usage de la possibilité prévue par le droit américain de publier des rapports de transparence qui indiquent le nombre de demandes au titre du FISA et liées aux lettres de sécurité nationale qu'elles ont reçues au cours d'une période de référence donnée. Au moment de la rédaction du présent rapport, les statistiques sur les demandes au titre du FISA après juillet 2023 n'étaient pas encore disponibles. Google a par exemple déclaré avoir reçu entre 500 et 999 demandes liées aux lettres de sécurité nationale, concernant 2 000 à 2 499 comptes, entre juillet et décembre 2023[62]. Meta a indiqué avoir reçu entre 0 et 499 demandes liées aux lettres de sécurité nationale, concernant 500 à 999 comptes, au cours de la même période de référence[63]. Ces chiffres sont restés relativement stables ces dernières années. Afin d'accroître encore la transparence, certaines entreprises (par exemple, Google) publient de manière proactive les lettres de sécurité nationale qu'elles ont reçues une fois que les restrictions de non-divulgation sont levées[64].

2.2.1.4. Autres évolutions

Dans le cadre de la préparation de l'examen, plusieurs ONG ont soulevé des questions sur de nouvelles formes d'acquisition de données par les agences de renseignement américaines par l'achat de données auprès d'entités commerciales, en particulier de courtiers en données. Elles ont expliqué que, si les données collectées sur cette base doivent toujours être traitées conformément aux autres exigences, y compris, par exemple, au titre de l'EO 12333[65], cette acquisition a lieu en dehors du cadre du FISA et de l'EO 14086.

À cet égard, il convient de rappeler que tout type de partage volontaire de données avec des tiers est soumis à plusieurs conditions détaillées au titre du CPD. Premièrement, une organisation certifiée ne peut partager des données avec un tiers (qui n'agit pas en tant qu'agent/sous-traitant) sans en informer les personnes concernées et leur donner le choix[66]. Deuxièmement, conformément au *principe «Responsabilité en cas de transfert ultérieur»*, tout transfert ultérieur ne peut avoir lieu 1) qu'à des fins limitées et spécifiques, 2) que sur la base d'un contrat entre l'organisation participant au CPD UE - États-Unis et le tiers et 3) que si ce

[60] https://www.justice.gov/nsd/media/1350236/dl?inline.
[61] Ces chiffres sont restés largement stables par rapport à l'année de référence précédente (2022). À titre de comparaison, en 2022, le FISC a reçu 317 demandes finales de surveillance électronique et/ou de fouilles corporelles à des fins de renseignement extérieur. Le nombre total de personnes ciblées par des ordonnances de surveillance électronique était compris entre 0 et 499. Le FBI a présenté 9 103 demandes d'information concernant des personnes non américaines liées aux lettres de sécurité nationale en 2022 (à l'exclusion des demandes concernant uniquement les informations d'abonnement). Source: https://irp.fas.org/agency/doj/fisa/2022rept.pdf.
[62] https://transparencyreport.google.com/user-data/us-national-security.
[63] https://transparency.meta.com/reports/government-data-requests/country/US/.
[64] https://transparencyreport.google.com/user-data/us-national-security.
[65] Voir, par exemple, article 2.4 de l'EO 12333 sur les techniques de collecte.
[66] Voir considérant 40 de la décision d'adéquation.

contrat oblige le tiers à prévoir le même niveau de protection que celui qui est garanti par les principes[67].

Par ailleurs, comme cela a également été indiqué lors de la réunion d'examen, la FTC a pris des mesures coercitives à l'encontre des courtiers en données qui vendent des données sensibles relatives aux consommateurs. Par exemple, dans une affaire contre *X-Mode* et son successeur *Outlogic*, la FTC a adopté, le 9 janvier 2024, une ordonnance interdisant à la société de vendre des données de géolocalisation à des tiers et de supprimer les données qu'elle a utilisées et partagées illégalement. L'enquête de la FTC a notamment révélé que la société n'avait pas pleinement informé les personnes concernées de l'utilisation et de la vente de leurs données de géolocalisation, qu'elle n'avait pas mis en place de mesures permettant aux personnes concernées de renoncer au suivi, qu'elle avait autorisé l'utilisation des données à des fins potentiellement discriminatoires et qu'elle n'avait pas fixé de limites à l'utilisation de ces informations par des tiers[68]. La Commission s'attend à ce que la FTC adopte la même approche si des entreprises certifiées en vertu du CPD devaient partager des données en violation des dispositions susmentionnées.

Enfin, il convient de mentionner qu'en mai 2024, l'ODNI a publié le cadre d'action de la communauté du renseignement pour les informations disponibles commercialement[69]. Ce cadre établit un certain nombre de principes et d'exigences que les agences de renseignement doivent respecter, notamment pour réduire au minimum les risques pour la protection de la vie privée et les libertés civiles lors de l'acquisition et de l'utilisation d'informations dans le cadre d'une transaction commerciale.

2.2.2. Surveillance indépendante

Les activités des agences de renseignement américaines sont soumises à la supervision de différents organes, notamment des délégués à la protection de la vie privée et des libertés civiles, des inspecteurs généraux, du Congrès et du PCLOB. En particulier, l'EO 14086 exige que chaque agence de renseignement dispose de responsables juridiques et de délégués chargés de la surveillance et du respect des règles de haut niveau afin de garantir le respect du droit américain applicable. Cette fonction de surveillance est assurée par des délégués ayant un rôle désigné en matière de respect des règles, ainsi que par des délégués à la protection de la vie privée et des libertés civiles et des inspecteurs généraux[70]. Ceux-ci doivent surveiller régulièrement les activités de renseignement d'origine électromagnétique et veiller à ce que tout cas de non-respect soit corrigé. Les agences de renseignement doivent donner à ces

[67] Voir considérant 38 de la décision d'adéquation.

[68] https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data.

[69] https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf. Les agences de renseignement sont tenues de se conformer au cadre depuis août 2024.

[70] Chaque agence de renseignement dispose d'un inspecteur général dont l'indépendance est inscrite dans la loi et qui est chargé d'effectuer des audits et des enquêtes sur les activités menées par l'agence concernée à des fins de renseignement national. Celui-ci a accès à l'ensemble des documents pertinents (y compris classifiés), si nécessaire au moyen d'une ordonnance, et peut recueillir des témoignages. Les inspecteurs généraux signalent les cas d'infractions pénales présumées à des fins de poursuites et formulent des recommandations sur l'adoption de mesures correctives à l'intention des chefs d'agence. Si leurs recommandations sont non contraignantes, leurs rapports, notamment sur les mesures de suivi (ou leur absence) sont généralement rendus publics et transmis au Congrès. Voir, à cet égard, note de bas de page 136 de la décision d'adéquation sur le rôle de l'inspecteur général.

responsables l'accès à toutes les informations pertinentes pour l'exercice de leurs fonctions et ne peuvent prendre aucune mesure pour entraver ou influencer indûment leurs activités de surveillance.

Le directeur des affaires juridiques du bureau de l'inspecteur général de la communauté du renseignement (ICIG) au sein de l'ODNI – qui est doté de vastes attributions en ce qui concerne l'ensemble des services de renseignement et est habilité à enquêter sur les réclamations ou les informations concernant des allégations de comportement infractionnel ou d'abus d'autorité – a participé à la réunion d'examen. Il a confirmé que l'ICIG vérifie systématiquement le respect de l'EO 14086 dans le cadre de ses activités de surveillance. Il a également fait référence à de récentes activités de surveillance menées par d'autres inspecteurs généraux de la communauté du renseignement, telles que détaillées dans les rapports réguliers. Par exemple, dans son rapport semestriel au Congrès pour la période avril-septembre 2023[71], l'inspecteur général de la NSA a communiqué des informations sur l'évaluation d'un cadre de contrôle interne de la NSA pour cibler les décisions et les demandes. Il a conclu que ce cadre fonctionnait bien pour garantir le respect des lois, des directives et des politiques qui protègent les libertés civiles et la vie privée. Le même rapport mentionne également une enquête qui a révélé l'utilisation abusive d'un outil de renseignement d'origine électromagnétique à des fins non autorisées par un employé de la NSA.

En vertu de l'EO 14086, le PCLOB[72] est chargé de fonctions de surveillance spécifiques[73]. La présidente et les trois membres du PCLOB ont participé à la réunion d'examen et ont indiqué que le PCLOB a fourni des conseils à des agences de renseignement sur leurs projets de politiques et de procédures de mise en œuvre de l'EO 14086 en avril 2023, et a été consulté sur la nomination des juges et avocats spéciaux de la Cour chargée du contrôle de la protection des données (Data Protection Review Court, DPRC). Le PCLOB a également lancé un projet de surveillance visant à 1) examiner la mise en œuvre des politiques et procédures actualisées adoptées par les agences de renseignement afin de s'assurer qu'elles sont conformes au décret présidentiel, et 2) procéder à un examen annuel du fonctionnement du nouveau mécanisme de recours (voir ci-dessous)[74]. Les membres du PCLOB ont confirmé que ce dernier prévoit de procéder à ces deux examens dans un avenir proche. En ce qui concerne les recours, ils ont expliqué qu'en l'absence de réclamations, l'examen du PCLOB se concentrera sur les politiques et procédures adoptées pour mettre le mécanisme en place.

[71] https://oig.nsa.gov/reports/Article/3609957/semiannual-report-to-congress-1-april-2023-to-30-september-2023/.

[72] Le PCLOB est une agence indépendante investie de responsabilités dans le domaine des politiques de lutte contre le terrorisme et de leur mise en œuvre, en vue de protéger la vie privée et les libertés civiles. Il peut avoir accès à l'ensemble des informations pertinentes (y compris classifiées), mener des entretiens et recueillir des témoignages. Il peut adresser des recommandations aux autorités de répression et de renseignement, et fait régulièrement rapport au Congrès et au président. Ses rapports sont rendus publics dans la mesure la plus large possible.

[73] https://documents.pclob.gov/prod/Documents/EventsAndPress/834a1977-f420-4b2a-ae93-8a522b2c7c74/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL)%20-%20Completed%20508%20-%2010202022.pdf.

[74] https://www.pclob.gov/OversightProjects/Details/1115.

Pour ce qui est des autres activités de surveillance, le PCLOB a publié un rapport sur l'article 702 du FISA le 28 septembre 2023[75]. Ce rapport fait suite à un rapport antérieur de 2014 et contient des informations factuelles et juridiques actualisées sur le fonctionnement des programmes de surveillance au titre de l'article 702 du FISA. Il contient également des recommandations sur le respect par les agences de renseignement des exigences applicables et des suggestions au Congrès visant à renforcer encore plusieurs aspects de l'article 702 du FISA dans le cadre de sa réactivation (notamment en codifiant les objectifs légitimes des activités de surveillance énumérées dans l'EO 14086)[76]. Au cours de la réunion d'examen, le PCLOB a indiqué qu'il s'attendait à recevoir prochainement des réponses des agences de renseignement sur la mise en œuvre de ses recommandations, qui alimenteront un futur rapport de suivi. Parmi les autres projets de surveillance en cours figurent un projet sur la lutte contre le terrorisme national et son incidence sur la protection de la vie privée et les libertés civiles, et un projet sur la collecte par le FBI de données de sources ouvertes ou disponibles commercialement[77].

Enfin, les ONG consultées dans le cadre de l'examen se sont déclarées préoccupées par le fait que le mandat de plusieurs membres du PCLOB arrivera à expiration dans un avenir proche, de sorte que le PCLOB pourrait ne plus avoir de quorum. En particulier, le mandat de la présidente a expiré et la période pendant laquelle elle peut exercer ses fonctions après terme prend fin en janvier 2025, tandis qu'un autre siège est vacant, et un troisième sera libéré également en janvier de l'année prochaine. Lors de la réunion d'examen, les membres ont expliqué qu'ils ne s'attendaient pas à ce que le PCLOB finisse par ne plus avoir de quorum, étant donné qu'une nomination a déjà été proposée pour le siège actuellement vacant (et est en attente de confirmation par le Sénat)[78]. Ils ont également souligné que, même si le PCLOB perdait son quorum, cela n'aurait pas d'incidence sur sa capacité à continuer de mener à bien des projets de surveillance. Néanmoins, compte tenu du rôle important du PCLOB dans l'examen de la mise en œuvre de l'EO 14086, la Commission suivra de près la situation concernant les futurs postes vacants et nominations/désignations.

2.2.3. Recours

L'EO 14086, complété par un règlement du procureur général, a mis en place un nouveau mécanisme de recours pour traiter et résoudre les réclamations recevables émanant de personnes concernées au sujet des activités américaines de renseignement d'origine électromagnétique[79]. Toute personne concernée dans l'Union a le droit d'introduire une réclamation auprès du mécanisme de recours concernant une violation présumée du droit américain régissant les activités de renseignement d'origine électromagnétique (par exemple, l'EO 14086, l'article 702 du FISA, l'EO 12333) ayant trait à des données à caractère personnel transférées aux États-Unis qui porte atteinte à ses intérêts en matière de protection de la vie privée et de libertés civiles. Les personnes concernées peuvent introduire une réclamation auprès d'une APD d'un État membre de l'Union, qui transmettra la réclamation, par

[75] https://documents.pclob.gov/prod/Documents/OversightReport/8ca320e5-01d3-4d6a-8106-3384aad6ff31/2023%20PCLOB%20702%20Report%20-%20Nov%2017%202023%20-%201446.pdf.

[76] La Commission fait observer que certaines de ces recommandations ont été intégrées dans le RISAA, notamment la recommandation sur la collecte des communications contenant une référence à un sélecteur ou celle sur le renforcement du rôle des experts du FISC (*amici*).

[77] https://www.pclob.gov/OversightProjects.

[78] https://documents.pclob.gov/prod/Documents/EventsAndPress/deb9cd13-12af-4250-998e-a520a2419a6b/PCLOB%20nominee%20press%20release%206-13-24.pdf.

[79] Considérants 176 à 194 de la décision d'adéquation.

l'intermédiaire du secrétariat du comité européen de la protection des données, au mécanisme de recours. Il s'agit d'un mécanisme à deux niveaux, l'enquête initiale sur les réclamations étant menée par l'ODNI CLPO, avec la possibilité pour les personnes concernées de former un recours contre la décision du CLPO devant une DPRC indépendante. Une fois l'examen de l'ODNI CLPO ou de la DPRC terminé, les personnes concernées sont informées, par l'intermédiaire de l'autorité nationale, du fait que «l'examen n'a pas mis en évidence de violations couvertes ou que l'ODNI CLPO/la DPRC a rendu une décision exigeant des mesures correctives appropriées». Les décisions de l'ODNI CLPO et de la DPRC sont contraignantes pour les agences de renseignement.

Depuis l'adoption de la décision d'adéquation, d'autres mesures ont été prises pour rendre le mécanisme de recours pleinement opérationnel.

En ce qui concerne la création de la DPRC, le 14 novembre 2023, huit juges [soit deux juges de plus que le nombre minimal requis en vertu de l'EO 14086, tel que complété par les règlements du procureur général (28 C.F.R. § 201.3(a))] ont été nommés à la Cour[80]. Ils ont été nommés sur la base des critères énoncés dans l'EO 14086 et conformément à la procédure prévue dans ce dernier, y compris après consultation, entre autres, du PCLOB[81]. Il s'agit notamment d'anciens juges fédéraux d'une cour de district et d'une cour d'appel, d'un ancien procureur général des États-Unis et d'un ancien membre du PCLOB. Comme l'exige le décret présidentiel, au moins la moitié des juges ont une expérience judiciaire antérieure. De plus, en avril 2024, deux avocats spéciaux (des praticiens du droit possédant une expertise en matière à la fois de protection de la vie privée et de sécurité nationale) ont été nommés pour représenter les intérêts des personnes devant la DPRC. Il a été confirmé lors de la réunion d'examen que tous les juges et avocats spéciaux ont reçu l'habilitation de sécurité la plus élevée et peuvent donc avoir accès aux documents classifiés dans l'accomplissement de leurs tâches pour la DPRC. La DPRC avait aussi publié une série de questions fréquemment posées, fournissant davantage d'informations sur son rôle, son indépendance et son fonctionnement[82].

En ce qui concerne le traitement des réclamations, l'ODNI a adopté le 6 décembre 2022 la directive 126 de la communauté du renseignement, qui réglemente en détail (en fixant des délais, en établissant un répertoire électronique sécurisé et des canaux de communication, en exigeant du CLPO et des composantes de la communauté du renseignement qu'ils coopèrent avec le PCLOB dans le cadre de l'examen annuel du mécanisme de recours, etc.) différents aspects du processus d'enquête sur les réclamations et de prise de décision sur celles-ci[83]. Cette directive est applicable dans l'ensemble de la communauté du renseignement des États-Unis et a été complétée par d'autres procédures internes adoptées par les différentes agences de renseignement concernant leur coopération avec l'ODNI CLPO dans le cadre du traitement d'une réclamation (par exemple, mise en place d'un répertoire sécurisé pour le partage des réclamations et des documents demandés, et de communications sécurisées entre les agences concernées). La DPRC publiera également dans les mois à venir des règles plus détaillées sur le traitement des réclamations et d'autres aspects procéduraux.

[80] https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court.
[81] Article 3(d)(A) de l'EO 14086.
[82] https://www.justice.gov/opcl/dprc-resources.
[83] https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf.

Un certain nombre de mesures supplémentaires ont été prises dans l'Union européenne et aux États-Unis pour informer le grand public, ainsi que pour faciliter la soumission et le traitement des réclamations. Il s'agit notamment de l'adoption, par le comité européen de la protection des données, d'une note d'information sur le nouveau mécanisme de recours[84], d'un modèle de formulaire de réclamation (destiné à être traduit et publié par toutes les APD dans leurs langues nationales)[85] et de règles de procédure régissant la coopération entre les autorités nationales de contrôle et le secrétariat du comité[86]. De même, l'ODNI a publié des FAQ et une fiche d'information sur le nouveau mécanisme de recours et a participé à des activités de sensibilisation du public[87].

Par ailleurs, au cours de l'année écoulée, le comité européen de la protection des données et les autorités américaines compétentes ont coopéré étroitement sur plusieurs aspects opérationnels. En particulier, comme cela a été confirmé lors de la réunion d'examen, ils ont mis en place un canal de communication chiffré pour transmettre les réclamations des autorités nationales de l'Union au secrétariat du comité européen de la protection des données, du secrétariat du comité à l'ODNI CLPO et au bureau des libertés civiles et de la vie privée du ministère de la justice (OPCL), ainsi qu'entre l'ODNI CLPO et d'autres autorités du côté américain (par exemple, la DPRC). En outre, l'ODNI CLPO a expliqué que d'autres procédures internes ont été mises en place pour la coopération des différentes agences de renseignement avec l'ODNI CLPO en ce qui concerne le traitement des réclamations.

Enfin, l'OPCL, qui apporte un soutien administratif à la DPRC, a également indiqué que la DPRC opère au titre de sa propre ligne budgétaire spécifique et que les équipements nécessaires à l'accomplissement de ses tâches, dont des ordinateurs et ordinateurs portables sécurisés, des téléphones, etc., sont mis à sa disposition. De plus, comme l'exige l'EO 14086, le ministère du commerce a pris les mesures nécessaires, notamment en mettant en place un canal de communication chiffré avec l'ODNI CLPO, afin de tenir un registre de toutes les réclamations recevables reçues. Le ministère du commerce prendra périodiquement contact avec l'ODNI CLPO pour savoir si des informations relatives à une réclamation donnée ont été déclassifiées. Si tel est le cas, le ministère en informera la personne concernée, afin de lui permettre d'obtenir l'accès à ces informations.

Au moment de la réunion d'examen, aucune réclamation n'avait été reçue par les autorités de contrôle de l'Union européenne et le nouveau mécanisme de recours n'avait donc pas encore été déclenché.

3. CONCLUSION

Sur la base des informations recueillies lors de ce premier examen, la Commission conclut que les autorités américaines ont mis en place les structures et procédures nécessaires pour garantir

[84] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-protection-framework-redress_fr.
[85] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_fr.
[86] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/rules-procedure-data-protection-framework-redress_fr.
[87] https://www.dni.gov/files/CLPT/documents/Fact_Sheets/The_Role_of_the_ODNI_CLPO_FAQs.pdf et https://www.dni.gov/files/CLPT/documents/Fact_Sheets/Data_Privacy_Framework.pdf.

le bon fonctionnement du cadre de protection des données. Dans ce contexte, la Commission apprécie fortement la très bonne coopération avec les autorités américaines aux fins de l'examen.

Bien que ce premier examen ait naturellement porté sur la vérification de la présence de tous les éléments constitutifs du cadre, l'expérience de l'application pratique des garanties applicables tant au traitement des données par les entreprises certifiées qu'à l'accès des autorités publiques aux données est nécessairement limitée après une année seulement de mise en œuvre. La Commission suivra donc de près les évolutions pertinentes au cours des prochains mois et des prochaines années, en accordant une attention particulière 1) aux prochains rapports du PCLOB sur la mise en œuvre de l'EO 14086 et le fonctionnement du mécanisme de recours en matière de renseignement d'origine électromagnétique, en particulier la DPRC; 2) aux éventuelles nouvelles modifications de l'article 702 du FISA; et 3) à la nomination et à la désignation de membres du PCLOB pour pourvoir les postes vacants à venir.

En outre, pour assurer un fonctionnement continu et efficace, la Commission estime qu'il importe que:

- comme annoncé lors de la réunion d'examen, le ministère du commerce utilise davantage les différents outils prévus dans le CPD pour contrôler le respect des principes par les entreprises et détecter les fausses déclarations de participation;
- la FTC continue de développer son approche proactive en matière d'enquête et de contrôle du respect des principes du CPD par les entreprises certifiées; et
- le ministère du commerce, la FTC et les autorités de l'Union chargées de la protection des données élaborent des instruments d'orientation communs sur les exigences clés d'après les principes du CPD, par exemple en ce qui concerne les données RH et les transferts ultérieurs.

À la lumière de ce résultat de l'examen et comme prévu au considérant 211 de la décision d'adéquation, la Commission estime qu'il convient de procéder au prochain examen périodique après trois ans. Cela devrait permettre d'acquérir davantage d'expérience concernant l'application pratique du CPD et de tenir compte des évolutions à venir susmentionnées. La Commission consultera donc, conformément à l'article 3, paragraphe 4, de la décision d'adéquation, le comité européen de la protection des données et le comité institué en vertu de l'article 93, paragraphe 1, du règlement général sur la protection des données sur la périodicité des futurs examens.