EUROPEAN DATA PROTECTION SUPERVISOR

Avis de l'EDPS sur l'utilisation d'un système informatisé par le Parlement européen pour la numérisation de la plénière et des registres centraux d'émargement grâce à la technologie biométrique
(Affaires jointes 2020-0921 et 2021-0355)

1. CONTEXTE

Le présent avis concerne un système actualisé d'attestation de présence des députés au Parlement européen (les «députés»). Le système vise à numériser le registre central d'émargement du Parlement européen pour les députés en remplaçant le système de signature sur support papier existant par une solution fondée sur un lecteur optique d'empreintes digitales. Le système sera utilisé afin d'attester la présence des députés au titre de l'article 12 des mesures d'application du statut des députés[1] et de leur verser les indemnités journalières correspondantes au titre de l'article 24 des mesures d'application du statut des députés.

Le 18 juin 2018, le délégué à la protection des données (DPD) du Parlement européen a d'abord demandé, de manière informelle, au Contrôleur européen de la protection des données (CEPD) de fournir des conseils sur ce projet[2]. À ce stade, le CEPD a noté qu'il n'était pas démontré que l'utilisation d'un système biométrique pour le contrôle des députés était nécessaire et, dès lors, le traitement envisagé de données à caractère personnel serait contraire à l'article 5 du règlement (CE) nº 45/2001[3]. En particulier, le CEPD était d'avis que le même objectif pouvait être atteint par des moyens moins intrusifs, tels que:

- un code PIN;
- des systèmes de pointage par bandes magnétiques;
- une authentification à deux facteurs, par la combinaison de plusieurs des solutions susmentionnées;
- des contrôles aléatoires et périodiques des signatures/présences au moyen d'un contrôle humain.

Le CEPD a également noté que, même si la nécessité du projet avait été établie, le traitement de données biométriques devrait toujours faire l'objet d'un suivi et devrait tenir compte de l'issue d'une analyse d'impact relative à la protection des données (AIPD).

À la suite d'une réunion qui s'est tenue le 26 juin 2018 entre le Parlement européen et le CEPD, le Parlement européen a décidé d'évaluer en interne d'autres systèmes moins intrusifs pour l'enregistrement de la présence des députés.

Le 7 octobre 2020, les députés ont attiré l'attention du CEPD sur le fait que le Parlement européen allait désormais de l'avant, grâce à une mise à jour de son registre central

[1] Mesures d'application du statut des députés au Parlement européen, décision du Bureau des 19 mai et 9 juillet 2008, telles que modifiées par la décision du Bureau du Parlement européen du 17 juin 2019, *PE422.536/BUR*.
[2] Dossier nº 2018-0553 du CEPD.
[3] Le règlement (CE) nº 45/2001 a depuis lors été remplacé par le règlement (UE) 2018/1725.

Adresse postale: rue Wiertz 60 – B-1047 Bruxelles
Bureaux: rue Montoyer 30 – B-1000 Bruxelles
Courriel: edps@edps.europa.eu - Site web:www.edps.europa.eu
Tél.: +32 2-283 19 00 - Télécopie: +32 2-283 19 50

d'émargement en traitant les données biométriques des députés. Afin de vérifier si ses préoccupations antérieures avaient été prises en compte, le CEPD a décidé de demander au Parlement de lui fournir des informations complémentaires à ce sujet.

Le 16 octobre 2020, le CEPD a envoyé une demande d'informations au Parlement européen. Le 11 novembre 2020, le CEPD a reçu la réponse du Parlement européen, qui était constituée d'une lettre portant sur les questions spécifiques du CEPD et de huit annexes[4].

Compte tenu de ce qui précède, le CEPD a décidé de rendre le présent avis, élaboré de sa propre initiative, sur la base de l'article 57, paragraphe 1, point g), du règlement (UE) 2018/1725 (le «règlement»)[5].

2. DESCRIPTION DU TRAITEMENT PROPOSÉ

Le Parlement européen a fourni au CEPD une AIPD concernant la mise à jour du système de contrôle de présence. L'AIPD[6] montre que les députés attesteront leur présence numériquement en scannant leur empreinte sur le lecteur d'empreintes digitales, qui enregistrera leur présence dans le système au moyen d'un horodatage. Ce système remplacera totalement le système actuel de contrôle de présence, qui nécessite l'utilisation d'une signature (il ne numérisera donc pas l'exigence de signature) et ne se fondera sur aucune autre information, telle qu'un mot de passe[7].

Le processus débutera par l'enregistrement des modèles d'empreintes digitales chiffrées du député dans la base de données centrale du système et dans chaque lecteur installé dans les locaux du Parlement européen. Dès qu'un député mettra son doigt sur un lecteur local d'empreintes digitales, ce lecteur scannera l'empreinte digitale pour extraire les éléments nécessaires à la création d'un nouveau modèle biométrique. Ce modèle fera ensuite l'objet d'une comparaison avec les modèles biométriques enregistrés soit dans la base de données centrale soit dans la base de données locale du lecteur. Ces modèles sont enregistrés sur chaque lecteur local d'empreintes digitales, en plus des deux serveurs centraux du Parlement, afin d'éviter qu'une défaillance du réseau empêche les députés d'attester leur présence. Si le

---

[4] Une annexe principale décrivant la structure des différents documents;
Annexe 1.1/1.2: Article 20 du statut des députés au Parlement européen (2005/684/CE, Euratom)/article 12, paragraphe 1, des mesures d'application du statut des députés au Parlement européen (décision du Bureau des 19 mai et 9 juillet 2008);
Annexe 2: Compte rendu de la réunion du Bureau du 11 juin 2018;
Annexe 3 : Compte rendu de la réunion du Bureau du 17 juin 2019;
Annexe 4: Analyse d'impact relative à la protection des données intitulée «Numérisation du registre central d'émargement au moyen de la technologie des modèles biométriques chiffrés» (version 1.6), notamment ses annexes (ci-après les «annexes AIPD»);
Annexe 5. Observations du délégué à la protection des données du Parlement sur la version 1.5 de l'analyse d'impact relative à la protection des données «Numérisation du registre central d'émargement au moyen de la technologie des modèles biométriques chiffrés»;
Annexe 6.1/6.2: Informations sur la solution technique et l'infrastructure du système biométrique proposé;
Annexe 7: Note juridique sur la conformité des solutions biométriques du SCT avec le règlement (UE) 2016/679.

[5] Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

[6] En particulier aux pages 10 et 11.

[7] Le Parlement européen prévoit néanmoins de conserver la signature papier comme procédure de secours, comme indiqué à la page 50 de l'AIPD (annexe 4) «Possibilité de revenir aux signatures manuscrites sur papier (par exemple en cas de problème d'alimentation électrique qui durerait plus de deux heures)».

système trouve un modèle correspondant, le lecteur affiche une lumière verte, enregistre l'horodatage, et le système pourrait être programmé pour envoyer une notification par courriel au député; s'il n'en trouve pas, le lecteur affiche une lumière rouge.

Outre les informations biométriques, l'opération de traitement requiert des **informations générales à caractère personnel liées au travail** pour fonctionner: le nom, la fonction, la date de début et de fin du mandat, l'adresse électronique et le numéro d'identification personnel (persID). Toutes ces informations à caractère personnel sont extraites du registre des députés du Parlement (CODICT). Elles sont ensuite enregistrées dans une base de données spécifique avec les données relatives à la présence des députés (notamment les horodatages obtenus), ainsi que dans la base de données du lecteur local d'empreintes digitales et dans la base de données biométrique centrale.

Le personnel du Parlement peut consulter certaines données relatives à la présence (y compris les noms et les horodatages) en effectuant une recherche directe afin de vérifier la présence. Des utilisateurs spécifiques (le personnel) de la DG FINS[8] et de la DG PERS (pour les données relatives aux sessions plénières du Parlement) travailleront en tant que collecteurs et destinataires de données à caractère personnel. Ces utilisateurs auront accès aux informations importées de la base de données CODICT et des bases de données des modèles biométriques des députés, uniquement en fonction du besoin d'en connaître.

En ce qui concerne l'**intégration au logiciel de paiement**, il est précisé dans l'AIPD que le système générera automatiquement deux fichiers XML une fois par jour, énumérant les persID de tous les députés dont la présence a été enregistrée avec succès. Ces fichiers XML seront mis sur un site réseau scanné par le système intégré de gestion des frais de voyage (iTEMS)[9], auquel le personnel autorisé de la DG FINS aura accès, sur la base du besoin d'en connaître. iTEMS importera automatiquement les fichiers et mettra à jour les présences des députés qui déclencheront le paiement des indemnités journalières, sans qu'aucune intervention humaine ne soit nécessaire.

3. OBSERVATIONS JURIDIQUES ET TECHNIQUES

3.1. Licéité du traitement et base juridique (article 5 du règlement)

Sur la base des avantages énumérés de la solution proposée par rapport au système actuel de registre central d'émargement ou une solution fondée sur des badges, le CEPD croit comprendre que l'**un des principaux moteurs du choix de la finalité biométrique** du système proposé est la **prévention de la fraude financière** (c'est-à-dire pour éviter que le registre d'émargement manuel ou électronique ne soit signé par une autre personne pour le compte du député)[10]. En tant qu'objectif étroitement lié, le CEPD souligne que les députés, en qualité de représentants des citoyens de l'Union[11], devraient montrer l'exemple et être guidés dans l'exercice de leurs fonctions par les principes généraux d'intégrité, d'honnêteté, de responsabilité et de respect de la réputation du Parlement européen[12].

---

8 L'unité Frais de voyage et de séjour des députés, l'unité des technologies de l'information et e-Portal.

9 Le système intégré de gestion des frais de voyage remplacera le logiciel actuel du Parlement en matière de voyages au cours de l'année 2021.

10 Une autre raison est la possibilité pour les députés d'attester leur présence s'ils ont oublié leur badge ou d'autres documents d'identification.

11 Article 14, paragraphe 2, du TUE.

12 Article 1er du code de conduite des députés au Parlement européen en matière d'intérêts financiers et de conflits d'intérêts (https://www.europarl.europa.eu/doceo/document/RULES-9-2019-07-02-ANN-01_EN.html).

Comme pour chaque opération de traitement lancée par une IUE, le système d'enregistrement biométrique proposé doit être fondé sur une base juridique en vertu de l'article 5 du règlement. Selon le Parlement européen, la **base proposée pour la licéité** de l'opération de traitement, à savoir le traitement de données à caractère personnel au moyen d'un système numérique d'attestation de présence des députés, est l'article 5, paragraphe 1, point b), du règlement (ce qui signifie que le traitement serait nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis).

Le CEPD estime que l'article 5, paragraphe 1, point b) ne s'applique que lorsque des institutions de l'UE sont légalement tenues de traiter des données à caractère personnel sans aucune marge de manœuvre quant à sa mise en œuvre. Cela signifie que l'obligation en elle-même doit être suffisamment spécifique quant au traitement requis des données à caractère personnel. Étant donné qu'en l'espèce, il n'existe aucune obligation spécifique imposant au Parlement européen de traiter des informations biométriques, il ne devrait pas fonder l'opération de traitement sur l'article 5, paragraphe 1, point b), du règlement comme base pour la licéité.

Par conséquent, le Parlement européen devrait examiner si **une autre base** peut être invoquée, à savoir **l'article 5, paragraphe 1, point a), du règlement**, à condition que le traitement des données à caractère personnel soit **nécessaire et proportionné** à l'exécution d'une mission effectuée dans l'intérêt public par l'institution de l'UE (sur la nécessité et la proportionnalité, voir la section 3.3).

En ce qui concerne la **base juridique** du traitement qu'il souhaite effectuer, le Parlement européen renvoie à l'article 156 du règlement intérieur du Parlement européen[13], ainsi qu'à l'article 12, paragraphe 1, et à l'article 24 des mesures d'application du statut des députés[14].

L'article 156 du règlement intérieur dispose ce qui suit:

À chaque séance, une feuille de présence est exposée à la signature des députés. 2. Les noms des députés dont la présence est consignée sur cette feuille de présence sont mentionnés comme «présents» dans le procès-verbal de chaque séance. Les noms des députés dont l'absence est excusée par le Président sont mentionnés comme «excusés» dans le procès-verbal de chaque séance.

Dans le même temps, les mesures d'application du statut des députés indiquent ce qui suit:

Article 12
Attestation de présence
1. La présence des députés est attestée par leur signature personnelle de la feuille de présence disponible à l'intérieur de l'hémicycle ou dans la salle de réunion, ou par leur signature personnelle du registre central d'émargement pendant les horaires de son ouverture fixés par

Voir également l'article 3 du code du comportement approprié des députés au Parlement européen dans l'exercice de leurs fonctions (https://www.europarl.europa.eu/doceo/document/RULES-9-2019-07-02-ANN-02_EN.html): «*Les députés ne peuvent, par leurs actions, inciter ou encourager le personnel à violer, contourner ou ignorer la législation en vigueur, les règles internes du Parlement ou le présent code, ni tolérer de tels agissements de la part du personnel placé sous leur autorité*».

[13] Règlement intérieur - 9e législature - juillet 2019 (JO L 302 du 22.11.2019, p. 1).

[14] Mesures d'application du statut des députés au Parlement européen, décision du Bureau des 19 mai et 9 juillet 2008; PE422.536/BUR.

le Bureau. ***Une attestation électronique de la présence d'un député peut être utilisée à la place de sa signature personnelle.***[15]

Article 24
Indemnité de séjour
1. Les députés ont droit à une indemnité de séjour pour chaque jour de présence:
(a) dans un lieu de travail ou de réunion, attestée conformément à l'article 12, lorsqu'ils sont en voyage remboursé par des frais de voyage ordinaires;
[...]

Ces articles, et en réalité l'ensemble des mesures d'application du statut des députés et le règlement intérieur, servent à la mise en œuvre de l'article 223, paragraphe 2, du traité sur le fonctionnement de l'Union européenne [ancien article 190, paragraphe 5, du traité instituant la Communauté européenne], qui prévoit que le Parlement européen fixe le statut et les conditions générales d'exercice des fonctions de ses députés.

Dès ses premières observations en 2018, le CEPD a exprimé des doutes quant à la décision de fonder le traitement d'informations biométriques[16] sur une disposition autorisant le Parlement européen à utiliser une «attestation électronique», mais qui ne contient aucune référence spécifique à la biométrie.

Afin de servir de base juridique à l'opération de traitement envisagée et pour autant qu'il n'existe pas de moyens moins intrusifs pour atteindre l'objectif poursuivi (principalement la prévention de la fraude), le CEPD estime que les règles internes du Parlement européen devraient être adaptées de manière à indiquer clairement et spécifiquement que l'enregistrement biométrique (et pas uniquement l'«attestation électronique») est utilisé (et non pas «peut être utilisé») en règle générale[17] pour attester la présence.

Recommandation nº 1:

Le CEPD estime que l'article 5, paragraphe 1, point a), du règlement devrait être invoqué comme **base pour la licéité** de ce projet, à condition que le traitement soit nécessaire et proportionné à l'exécution d'une mission d'intérêt public et que sa base soit prévue par le droit de l'Union.

En ce qui concerne cette dernière condition, le CEPD estime que la formulation actuelle des règles internes du Parlement européen n'est pas suffisamment claire en tant que **base juridique** pour le traitement d'informations *biométriques* comme *principal moyen* d'attester la présence et recommande au Parlement européen de modifier ces règles en conséquence.

En ce qui concerne les aspects spécifiques liés à la **prise de décision automatisée** en vertu de l'article 24 du règlement, le CEPD renvoie à la section 3.4.

[15] Caractères gras ajoutés.

[16] La définition de «données biométriques» n'inclut pas les signatures manuscrites (article 3, paragraphe 14, du règlement: «les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques»).

[17] Les signatures manuscrites sur papier pourraient constituer une solution de secours en cas de problème d'alimentation électrique qui durerait plus de deux heures (voir p. 50 de l'AIPD).

3.2. Traitement portant sur des catégories particulières de données à caractère personnel (article 10 du règlement)

Comme souligné à la page 12 de l'AIPD, aussi bien les images d'empreintes digitales que les modèles biométriques extraits constituent des catégories particulières de données à caractère personnel au sens de l'article 10 du règlement. Leur traitement est, en règle générale, interdit par le règlement, à l'exception de quelques cas mentionnés à l'article 10, paragraphe 2, dudit règlement.

Le traitement de catégories particulières de données est si strictement limité en raison de son incidence sur les droits fondamentaux des personnes concernées et, en particulier, sur le droit à la protection des données consacré à l'article 8 de la Charte des droits fondamentaux de l'Union européenne (la «Charte»). Les données biométriques ne peuvent pas être modifiées, ou du moins pas facilement. En cas de violation de la confidentialité, les empreintes digitales des députés ne peuvent être réinitialisées ou mises à jour. Si les empreintes d'un député donné ne sont pas reconnues par le système, il n'est pas possible de lui fournir de nouvelles empreintes digitales.

Le traitement des empreintes digitales comporte des risques spécifiques qu'il convient d'atténuer ou d'éviter. Par exemple, des recherches scientifiques ont démontré que les modèles d'empreintes digitales enregistrés permettent la reconstruction partielle de l'empreinte initiale[18]. Cette reconstruction partielle est parfois suffisamment précise pour qu'un autre système biométrique la reconnaisse comme étant l'empreinte initiale.

Il est suggéré dans l'AIPD que le système se fonderait sur l'exception prévue à l'article 10, paragraphe 2, point d), du règlement pour traiter les informations biométriques, mais elle n'étaye pas clairement ce choix. En outre, cette disposition vise à fournir une base juridique, par exemple, aux syndicats et aux organisations religieuses intégrés dans des IUE pour mener à bien leurs activités (qui, par défaut, incluent des informations sensibles). Le CEPD considère donc que cette disposition ne s'applique pas au traitement des informations biométriques des députés pour attester leur présence sur les lieux de travail et aux réunions. Le Parlement européen pourrait examiner l'**article 10, paragraphe 2, point g),** qui autorise le traitement de catégories particulières de données, à condition que ce traitement soit «**nécessaire** pour des motifs d'**intérêt public important**, sur la base du droit de l'Union qui doit être **proportionné** à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des **mesures appropriées et spécifiques** pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée»[19].

Le Parlement européen devrait considérer qu'il est possible que des blessures, des accidents, des problèmes de santé (tels que la paralysie) ou d'autres maladies empêchent temporairement ou définitivement certains députés d'utiliser le système. Si l'AIPD prévoit la «*possibilité de revenir aux signatures manuscrites sur papier (par exemple en cas de problème d'alimentation électrique qui durerait plus de deux heures)*»[20], il ne prévoit pas le risque que le système ne soit pas adapté à certains députés.

---

[18] Cappelli, Raffaele & Maio, Dario & Lumini, Alessandra & Maltoni, Davide. (2007). Fingerprint Image Reconstruction from Standard Templates. IEEE Trans. Pattern Anal. Mach. Intell 29 1489-1503. 10.1109/TPAMI.2007.1087.

[19] Caractères gras ajoutés. Cette disposition applique les exigences de l'article 52 de la Charte pour toute limitation de l'exercice des droits fondamentaux reconnus par la Charte, notamment le droit à la protection des données.

[20] Voir page 50 de l'annexe 4 (AIPD)

Recommandation nº 2 :
Étant donné que l'article 10, paragraphe 2, point d), du règlement n'est pas applicable à l'opération de traitement, le Parlement européen devrait préciser quelle autre exception il invoquerait pour son traitement de **catégories particulières de données à caractère personnel** au titre de l'article 10 du règlement, telle que l'article 10, paragraphe 2, point g), et devrait **fournir une justification plus détaillée** des raisons pour lesquelles cette exception serait applicable.

Recommandation nº 3 :
Si le Parlement européen met finalement en œuvre le système de présence biométrique, le CEPD recommande au Parlement européen de mettre en place une autre procédure d'attestation de présence afin de veiller à ce que les députés dont les empreintes digitales ne sont pas reconnues puissent quand même attester leur présence.

3.3. Nécessité et proportionnalité du traitement au regard de l'objectif poursuivi

La prévention de la fraude financière, notamment la nécessité pour les personnes élues démocratiquement de montrer l'exemple, peut être considérée comme un **motif d'intérêt public important** pouvant justifier le traitement de données biométriques au titre de l'article 10, paragraphe 2, point g), du règlement[21], à condition notamment que l'utilisation de données biométriques soit nécessaire et proportionnée à cet objectif[22].

Comme mentionné dans la section «Contexte», le CEPD a déjà souligné l'importance d'une évaluation approfondie **de la nécessité et de la proportionnalité** pour ce projet.

Le «principe de nécessité» suppose le besoin de procéder à une évaluation factuelle combinée de l'efficacité de la mesure aux fins de l'objectif poursuivi et de déterminer si cette mesure est moins intrusive par rapport aux autres moyens de réaliser le même objectif. Si cela s'avère nécessaire, la mesure doit quand même satisfaire au critère, qui consiste à évaluer quelles garanties devraient accompagner une mesure afin de réduire à un niveau acceptable/proportionné les risques que présente la mesure envisagée pour les droits et libertés fondamentaux des personnes concernées. L'efficacité des mesures existantes par rapport à la proposition de mesure constitue également un autre élément à prendre en considération dans l'évaluation de la proportionnalité. Si des mesures poursuivant un objectif similaire ou identique existent déjà, leur efficacité doit être systématiquement évaluée dans le cadre de l'examen de la proportionnalité[23].

À cet égard, le CEPD se félicite de la section 6 de l'AIPD, qui porte uniquement sur la nécessité et la proportionnalité de l'enregistrement biométrique. Pour étayer davantage ces points, le

---

[21] En ce qui concerne l'utilisation de données biométriques pour prévenir l'usurpation d'identité, voir l'avis de contrôle préalable du CEPD du 15 mai 2014 sur l'utilisation d'un dispositif de vérification biométrique pour les agents de sécurité au Parlement européen.
14-05-15_pc_ep_biometric_data_en.pdf (europa.eu)

[22] À la connaissance du CEPD, un nouveau badge peut être délivré en quelques minutes. Le deuxième avantage de l'utilisation de données biométriques avancé par le Parlement européen ne semble ni valable ni nécessaire/proportionné.

[23] Voir les lignes directrices publiées par le CEPD sur la nécessité et la proportionnalité des mesures législatives, qui peuvent s'appliquer mutatis mutandis à toute mesure visant à restreindre le droit à la protection des données consacré à l'article 8 de la Charte:
- 17-04-11 Boîte à outils sur la nécessité;
- 19-12-19 Lignes directrices sur la proportionnalité

Parlement européen oppose le système à deux systèmes antérieurs qu'il a testés ou utilisés, à savoir:

- un registre physique central d'émargement, à savoir le système actuellement utilisé;
- un système informatisé fondé sur l'utilisation par les députés de leur badge d'accès personnel sur les lecteurs de badges, qui a été testé à la suite des précédentes observations du CEPD.

Lors de la consultation du Parlement européen de 2018, le CEPD a précisé certaines des solutions qui pourraient être envisagées pour éviter le traitement de données biométriques. Seule une d'elles semble avoir été prise en considération: l'utilisation de badges d'accès.

Le CEPD note que, tant pour le système actuel sur support papier que pour le système de badge d'accès, un tableau d'analyse d'impact a été établi pour répertorier, entre autres, les différents risques, leur probabilité et leur incidence, ainsi que les stratégies possibles pour atténuer ou accepter ces risques. Cet exercice a permis de conclure que «la mise en œuvre des deux solutions révèle plusieurs risques élevés et critiques ayant une incidence sur les droits et libertés des personnes concernées, sur la réputation et les finances de l'institution ou sur la sécurité des données traitées».

Si l'on examine l'évaluation plus en détail, plusieurs éléments importants ne sont toujours pas assez précis ou restent inexpliqués. Le CEPD note par exemple qu'il n'existe aucune indication d'une ligne directrice ou d'une politique en matière d'évaluation qui indique la manière dont une différentiation est établie entre «improbable» et «possible». Cela semble essentiel, étant donné que la fréquence «possible» non précisée est associée à tous les risques jugés élevés.

En outre, la plupart des inconvénients imputés aux systèmes de badges ne sont pas clairs ou ne sont pas suffisamment démontrés, tels que:

- «*la protection des données à caractère personnel est hors de contrôle: les numéros de badge traités sont imprimés sur le badge lui-même*». À la connaissance du CEPD, les numéros de badges (ainsi que d'autres données à caractère personnel telles que le nom complet et la photo) sont imprimés sur tous les badges du Parlement. Il n'apparaît pas clairement pourquoi il ressort de l'évaluation qu'il ne s'agit d'un problème grave en matière de protection des données que pour les députés. Il est également difficile de savoir comment la connaissance du numéro de badge d'un député permettrait à un tiers d'attester la présence du député dans l'un des trois systèmes.
- «*l'attestation de présence en temps réel est compromise pendant un certain temps (même un jour) lorsque le badge des députés est à nouveau délivré par la DG SAFE (inefficacité et inefficience)*». À la connaissance du CEPD, il suffit de quelques minutes pour délivrer à nouveau un badge. En outre, l'un des principaux contrôles envisagés dans l'AIPD pour garantir la disponibilité du système proposé est la «possibilité de revenir aux signatures manuscrites sur papier (par exemple en cas de problème d'alimentation électrique qui durerait plus de deux heures)». Nous ne comprenons pas pourquoi cet inconvénient est pertinent alors que la même solution de secours pourrait être utilisée pour y remédier.
- «*il se peut que les députés soient en possession de plusieurs badges (y compris des badges ayant expiré), qu'ils puissent les utiliser et, par conséquent, polluer la base de données (inefficience)*». Si la porte automatique au Parlement peut détecter un badge qui a expiré, nous ne comprenons pas pourquoi le système de présence ne pourrait pas le faire et empêcher l'utilisation de badges ayant expiré.

- «*en raison de la similitude avec le système d'accès de la DG SAFE, les députés utiliseront peut-être les mauvais lecteurs (inefficacité)*». Quelle que soit la solution mise en œuvre, l'ajout d'un marquage extérieur clair ou de couleurs différentes dans l'interface utilisateur permettrait de résoudre facilement ce problème.

À la suite d'une analyse approfondie du système fondé sur les badges, le Parlement européen a estimé que deux risques étaient «élevés»:

- le risque d'usurpation d'identité, par exemple lorsqu'un député peut (aussi) signer à la place d'un député absent; et
- le risque d'accès, par des personnes non autorisées, à des données à caractère personnel (numéro de badge).

Il est difficile de savoir si le Parlement européen dispose de données sur le nombre d'usurpations d'identité qui pourraient avoir eu lieu au cours du test de badge (auquel plus de 270 députés ont participé). En l'absence de telles données, il convient d'expliquer pourquoi le scénario est estimé comme plus qu'«improbable», c'est-à-dire pourquoi le Parlement européen considère qu'il ne s'agit pas d'un événement marginal. Si aucune donnée n'est disponible et qu'aucune estimation ne peut être effectuée, il convient de le mentionner, en particulier parce que la prévention de la fraude ou de l'usurpation d'identité constitue l'objectif clé de la transition vers la biométrie. L'objectif de prévenir la fraude étant le principal moteur du traitement des données biométriques, **il est nécessaire que le Parlement européen justifie et documente davantage l'évaluation du risque de fraude**.

En ce qui concerne le risque d'accès non autorisé à un numéro de badge imprimé sur le badge, le CEPD relève tout d'abord un problème similaire à celui de l'évaluation du risque comme étant «possible» (ce qui conduit à son niveau comme élevé). En outre, le CEPD ne voit pas pourquoi la seule stratégie d'atténuation proposée pour ce risque consiste à «*mettre en œuvre un autre système informatisé qui n'est pas fondé sur l'utilisation de badges*» plutôt que de ne pas imprimer les numéros de manière visible, mais d'utiliser (uniquement) des badges RFID.

Enfin, le CEPD prend note du fait que la **solution fondée sur des badges** était la seule autre solution qui ait été analysée par le Parlement européen. Compte tenu de la réalisation des objectifs susmentionnés, il peut toutefois exister d'**autres solutions** qui permettraient d'assurer un niveau acceptable de sécurité et de prévention de la fraude, tout en ne traitant pas les informations biométriques. Une solution pourrait être, par exemple, la mise en place de mots de passe à usage unique ou d'une fonction de confirmation similaire (par exemple, une authentification NFC ou Bluetooth) générés sur les téléphones des députés lorsqu'ils notent leur présence. En l'espèce, la «facilité» perçue de partager son badge est atténuée par la réticence à partager son téléphone portable avec des assistants ou d'autres députés. Les députés sont peut-être également moins enclins à oublier leur téléphone ou à le perdre, deux autres risques recensés par le Parlement européen.

Recommandation n° 4:

Bien que le CEPD ne s'oppose en principe à aucune technologie particulière ni n'en exige aucune, les responsables du traitement devraient veiller à ce qu'une évaluation de la nécessité et de la proportionnalité fournisse une **évaluation approfondie d'autres solutions moins intrusives qui sont disponibles**. Par conséquent, le CEPD recommande au Parlement européen de **documenter la faisabilité d'autres solutions disponibles** qui ne nécessiteraient pas l'utilisation de données sensibles, de comparer toutes les possibilités et de rendre compte de ses conclusions.

3.4. Décision individuelle automatisée (article 24 du règlement)

Le CEPD croit comprendre que le traitement envisagé ne nécessite aucune intervention humaine[24], ce qui donne lieu à l'application de l'article 24 du règlement sur les **décisions fondées exclusivement sur un traitement automatisé**, produisant des **effets juridiques** à l'égard de la personne concernée ou l'affectant de manière significative de façon similaire.

Les décisions fondées «exclusivement sur un traitement automatisé» ne nécessitent aucune intervention humaine dans le processus décisionnel. Comme souligné dans les lignes directrices sur les décisions individuelles automatisées et le profilage[25]: «*Le responsable du traitement ne peut se soustraire aux dispositions de l'article 22* [~ article 24 du règlement] *en créant l'intervention humaine. Par exemple, si quelqu'un applique systématiquement des profils générés automatiquement à des personnes n'ayant aucune influence réelle sur le résultat, il s'agirait toujours d'une décision fondée exclusivement sur une décision automatisée. Pour qu'il s'agisse d'une intervention humaine, le responsable du traitement doit veiller à ce que tout contrôle de la décision soit significatif, et non simplement un geste symbolique. Il devrait être effectué par une personne ayant l'autorité et les compétences nécessaires pour modifier la décision.*»

À moins que le processus ne comporte une intervention humaine significative à un moment donné, l'article 24 du règlement s'applique au traitement envisagé, produisant des effets juridiques concernant les députés, à savoir le (non-)paiement de leurs indemnités de séjour.

L'article 24, paragraphe 1, établit une **interdiction générale** concernant les prises de décisions fondées exclusivement sur un traitement automatisé. L'article 24, paragraphe 2, du règlement prévoit trois exceptions qui permettent uniquement un processus décisionnel individuel automatisé:

(i) il conditionne la conclusion d'un contrat entre la personne concernée et le responsable du traitement;
(ii) **il est autorisé par le droit de l'Union,** qui prévoit également des **mesures appropriées** pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée;
(iii) il est fondé sur le consentement explicite de la personne concernée.

En outre, la prise de décision automatisée impliquant des catégories particulières de données à caractère personnel n'est autorisée que si l'**article 10, paragraphe 2,** point a) ou g), du règlement s'applique [article 24, paragraphe 4, du règlement].

(i) L'intérêt public important est en jeu

Comme indiqué précédemment[26], la prévention de la fraude ainsi que le respect par les députés, en qualité de représentants des citoyens de l'Union, des principes généraux d'intégrité, d'honnêteté, de responsabilité et de respect de la réputation du Parlement européen, peuvent

[24] Voir la section 2 ci-dessus. Description du traitement.
[25] Voir les pages 20 et 21 des lignes directrices sur les décisions individuelles automatisées et le profilage au titre du règlement 2016/679, (wp251rev1), telles que révisées en dernier lieu et adoptées le 6 février 2018 (approuvées par le comité européen de la protection des données).
[26] Section 3.2. Voir également la page 24 des lignes directrices relatives à la prise de décision individuelle automatisée précisant que la prise de décision automatisée peut être utilisée pour prévenir la fraude.

être considérés comme un **motif d'intérêt public important** relevant du champ d'application de l'article 10, paragraphe 2, point g), du règlement.

(ii) Concept de «droit de l'Union»

La base juridique applicable doit être **un droit de l'Union autorisant la prise de décision automatisée** [article 24, paragraphe 2, point b), du règlement][27]. De l'avis du CEPD, l'expression «droit de l'Union» désigne en principe un acte de nature législative (à savoir un règlement) ou, à tout le moins, un acte exécutif fondé sur un acte législatif. Toutefois, dans ce cas précis, compte tenu du caractère parlementaire de l'institution en cause et étant donné que le droit primaire confère au Parlement européen le pouvoir d'adopter ses propres règles[28], le CEPD reconnaît que les règles internes peuvent prévoir un processus décisionnel automatisé tel que celui envisagé. Néanmoins, comme recommandé ci-dessus (section 3.2), ces règles internes devraient disposer expressément que la présence des députés est attestée au moyen de la technologie biométrique comme moyen principal.

(iii) Mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée

L'article 24, paragraphe 2, point b), exige que **ces règles prévoient** non seulement le traitement automatisé en tant que tel mais **également des mesures appropriées** pour la sauvegarde des droits et libertés et des intérêts légitimes des députés[29]. Comme mentionné au considérant 43 du règlement, ces garanties appropriées devraient comprendre une information spécifique de la personne concernée (voir la section 3.6 ci-après) ainsi que le droit d'obtenir une intervention humaine, d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation et de contester la décision.

Recommandation nº 5: Dans la mesure où le traitement envisagé ne nécessite aucune intervention humaine significative, le CEPD recommande que le Parlement européen **complète ses règles internes** relatives à l'utilisation de la biométrie pour attester la présence des députés, en ajoutant des **mesures appropriées** pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée [article 24, paragraphe 2, point b), du règlement].

3.5. Minimisation des données

En tant que mesure visant à garantir la minimisation des données (biométriques), le Parlement européen souligne que des modèles biométriques seront utilisés pour le traitement au lieu des images brutes des empreintes digitales. Il convient de noter que l'utilisation de modèles, de signatures ou de schémas biométriques est une procédure normale pour l'identificateur biométrique. Ces schémas enregistrent numériquement les caractéristiques physiques, ce qui permet aux algorithmes d'identifier et de différencier les personnes. L'utilisation de modèles biométriques ne devrait donc pas être considérée en soi comme une mesure minimisant les données à caractère personnel.

[27] Le considérant 43 établit que la prise de décision automatisée devrait être permise lorsqu'elle est expressément autorisée par le droit de l'Union.

[28] Article 223, paragraphe 2, du traité sur le fonctionnement de l'Union européenne.

[29] L'article 10, paragraphe 2, point g) et l'article 24, paragraphe 4, prévoient également des mesures appropriées mais l'article 24, paragraphe 2, point b), exige que ces garanties figurent dans les règles autorisant le traitement automatisé de la prise de décision.

À l'inverse, il ressort de l'annexe 6.1. (en particulier les réponses 2.C.6 et 2.C.9) que le contractant utiliserait un algorithme et un modèle propriétaires, qui stockeraient beaucoup plus de données qu'un modèle ISO standard, en plus de stocker, par exemple, des informations sur les pores et la fréquence des crêtes. La justification de ce modèle propriétaire est la suivante: «*Les modèles ISO ne conviennent pas à l'identification de grands groupes (plus de 100 personnes) en raison du nombre et du type limités de données*» et «*ces données supplémentaires permettent une identification fiable des bases de données avec des milliers d'utilisateurs*»[30]. Le CEPD note qu'un rapport du NIST[31] a permis de tester différents modèles par rapport à la norme INCITS 378 - modèle d'empreintes digitales sur des ensembles de données de milliers d'empreintes digitales. Bien qu'il puisse actuellement exister un avantage de précision en ce qui concerne l'utilisation de formats propriétaires spécifiques par rapport aux normes internationales, le Parlement européen devrait apprécier si l'augmentation de la précision vaut la peine de réduire la portabilité des données. Dans ce cas, le nombre d'utilisateurs serait inférieur à un millier, ce qui, en premier lieu, remettrait en cause la nécessité de recueillir ces données supplémentaires. En optant pour une solution propriétaire, le CEPD craint également que le Parlement européen ne soit «bloqué» avec le contractant, étant donné qu'il ne garantit pas pleinement que son modèle pourrait être exporté vers un format ISO. Cela pourrait amener les députés à réenregistrer leurs empreintes digitales si le Parlement européen choisissait ou était contraint de changer de contractants.

Recommandation nº 6:
Le CEPD recommande au Parlement européen d'examiner plus avant la nécessité d'établir le système proposé avec toutes les données biométriques à caractère personnel supplémentaires, compte tenu de la taille de la population qui sera enregistrée.

Si le système pouvait être correctement mis en place avec moins d'informations supplémentaires, le CEPD demande au Parlement européen d'engager son contractant afin de **réduire efficacement la quantité de données à caractère personnel** utilisées.

3.6. Information des personnes concernées

Conformément aux articles 14 à 16 du règlement, le Parlement européen devrait mettre à jour l'avis relatif à la protection des données concernant l'enregistrement de la présence et veiller à ce que les députés soient **spécifiquement informés** du nouveau système et de toutes ses modalités avant de commencer le traitement.

Dans la mesure où le traitement implique une prise de décision automatisée, les informations des députés devraient inclure des informations spécifiques, à savoir des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour ces députés [article 15, paragraphe 2, point f), et article 16, paragraphe 2, point f), du règlement].

[30] Annexe 6.1 Solution technologique et infrastructure

[31] Voir MINEX Performance and Interoperability of the INCITS 378 Fingerprint Template | NIST (MINEX Performance et interopérabilité du modèle d'empreintes digitales INCITS 378 | NIST).

Recommandation nº 7:
Conformément aux articles 14 à 16 du règlement, le CEPD recommande au Parlement européen de mettre à jour l'avis relatif à la protection des données concernant l'enregistrement de la présence et veiller à ce que les députés soient **spécifiquement informés** du nouveau système et de toutes ses modalités avant de commencer le traitement.

Si le traitement implique une prise de décision automatisée, ces informations devraient inclure des informations à savoir des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues du traitement [article 15, paragraphe 2, point f), et article 16, paragraphe 2, point f), du règlement].

4. CONCLUSION

Le CEPD se félicite des efforts considérables déployés par le Parlement européen pour analyser les conséquences du passage à un système biométrique d'attestation de présence des députés en matière de protection des données.

Toutefois, l'analyse ci-dessus a mis en évidence certaines préoccupations majeures devant être prises en considération. Par conséquent, le CEPD a formulé plusieurs recommandations visant à garantir la conformité du traitement avec le règlement.

Le Parlement devrait notamment:

1) se fonder sur l'article 5, paragraphe 1, point a) [et non sur l'article 5, paragraphe 1, point b)] du règlement comme **base pour la licéité**, à condition que le traitement soit nécessaire à l'exécution d'une mission d'intérêt public et que sa base soit prévue par le droit de l'Union et modifier ses règles internes de manière à pouvoir s'en prévaloir comme **base juridique** pour le traitement d'informations *biométriques* comme *principal moyen* d'attester la présence et recommande au Parlement européen de modifier ces règles en conséquence;

2) préciser l'exception qu'il invoquerait pour son traitement de **catégories particulières de données à caractère personnel** au titre de l'article 10 du règlement, telle que l'article 10, paragraphe 2, point g); fournir une justification plus détaillée des raisons pour lesquelles cette exception serait applicable;

3) mettre en place une autre procédure d'attestation de présence afin de veiller à ce que les députés dont les empreintes digitales ne sont pas reconnues puissent quand même attester leur présence;

4) documenter la faisabilité d'**autres solutions disponibles** qui ne nécessiteraient pas l'utilisation de données sensibles, comparer toutes les possibilités et rendre compte de ses conclusions;

5) dans la mesure où le traitement envisagé ne nécessite aucune intervention humaine significative, compléter ses **règles internes** relatives à l'utilisation de la biométrie pour attester la présence des députés, en ajoutant des **mesures appropriées** pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée [article 24, paragraphe 2, point b), du règlement];

6) examiner plus avant la nécessité d'établir le système proposé avec toutes les données biométriques à caractère personnel supplémentaires, compte tenu de la taille de la population qui sera enregistrée; si le système pouvait être correctement mis en place avec moins d'informations supplémentaires, engager son contractant afin de réduire efficacement la quantité de données à caractère personnel utilisées;

7) mettre à jour l'avis relatif à la protection des données concernant l'enregistrement de la présence et veiller à ce que les députés soient **spécifiquement informés** du nouveau système et de toutes ses modalités avant de commencer le traitement. Si le traitement implique une prise de décision automatisée, il devrait inclure des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues du traitement.

Le CEPD attend du Parlement européen qu'il **mette en œuvre les recommandations susmentionnées et fournisse des pièces justificatives** de cette mise en œuvre dans un délai de **trois mois** à compter du présent avis.

Fait à Bruxelles, le 29 mars 2021

[signature électronique]

Wojciech Rafał WIEWIÓROWSKI