EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
CONTRÔLEUR ADJOINT

M. Philippe RENAUDIÈRE
Délégué à la protection des données
Commission européenne
Rue de la Loi, 200
B-1049 Bruxelles

Bruxelles,
WW/EF/ktl D (2017)1691 **C 2017-0509**
Veuillez utiliser l'adresse edps@edps.europa.eu pour toute correspondance

Monsieur,

Nous vous informons que, dans un courrier électronique daté du 22 mai 2017, M. Zioga nous a soumis une consultation au titre de l'article 27, paragraphe 3, du règlement (CE) nº 45/2001[1] (ci-après le «règlement»). Cette consultation portait sur l'analyse de données dactyloscopiques aux fins d'une étude de recherche conduite par le Centre commun de recherche (CCR).

Après examen approfondi, nous estimons que le dossier en question **ne doit pas faire l'objet d'un contrôle préalable** pour les raisons exposées ci-dessous.

1. Faits - Description du traitement

Le traitement, telle que notifié par le responsable du traitement au délégué à la protection des données (DPD), concerne l'analyse de données dactyloscopiques aux fins d'une étude de recherche conduite par le Centre commun de recherche (CCR). Le projet de recherche concerné porte le nom de FLARE (reconnaissance laser des empreintes digitales).

Il a pour but de mener une recherche sur la reconnaissance laser des empreintes digitales en trois dimensions (3D) de nouvelle génération et constituera une avancée par rapport au processus de reconnaissance des empreintes digitales en 2D existant, qui s'accompagne d'un certain taux d'erreur.

[1] JO L 8 du 12.1.2001, p. 1.

Le projet FLARE étudiera la possibilité d'utiliser une nouvelle génération de technologies de détection laser 3D ultra-précise pour acquérir (dans un environnement sans contact) toute la surface d'une empreinte digitale en 3D.

Il sera mené dans les locaux du CCR et s'appuiera sur un prélèvement d'échantillons auprès de 50 membres du personnel qui fourniront volontairement leurs empreintes digitales, à raison de quatre (4) doigts chacun, 5 (cinq) échantillons par doigt et 3 (trois) vitesses de détection.

Au total, 60 (soixante) échantillons seront recueillis, et la session expérimentale durera 15 minutes environ. Ces travaux de recherche n'impliquent aucun risque ni aucune gêne. Selon les documents fournis, l'utilisation d'une diode laser dans le dispositif d'acquisition est conforme aux mesures de sécurité.

Les personnes participant au projet le feront sur la base du volontariat, dans le cadre d'un appel à manifestations d'intérêt. Toutefois, certaines personnes seront contactées sur une base *ad hoc*[2] (ponctuelle).

L'absence de toute mesure défavorable dans le cas où les personnes concernées refuseraient de participer, de même que leur droit à retirer leur consentement à tout moment, sont mentionnés explicitement.

Le traitement a pour finalité exclusive la conduite d'une recherche et a pour cadre juridique le consentement, et donc l'article 5, paragraphe d), du règlement nº 45/2001.

S'agissant de la sécurité des données, les empreintes digitales seront stockées dans un ordinateur dépourvu de tout accès à internet. Elles seront par ailleurs conservées dans une base de données cryptée. Les données seront également pseudonymisées, ce qui signifie que les personnes concernées ne pourront être identifiées qu'au moyen d'informations supplémentaires. Les empreintes digitales ne seront donc pas directement associées à l'identité de la personne concernée: chaque personne concernée se verra attribuer un identifiant numérique et les empreintes digitales seront enregistrées avec cet identifiant. Le lien entre l'identifiant numérique et l'empreinte digitale sera consigné dans un carnet conservé dans un espace protégé du laboratoire.

Les personnes concernées recevront une déclaration de confidentialité et une déclaration de consentement éclairé.

2. Analyse

L'article 27, paragraphe 1, du règlement dispose que les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités sont soumis au contrôle préalable du CEPD. En ce sens, l'article 27, paragraphe 2, point a), du règlement dispose que le traitement des données relatives à la santé relève de cette catégorie.

[2] Selon les informations complémentaires reçues, «il a été demandé à d'autres collègues extérieurs à l'unité mais faisant partie des relations personnelles des principaux chercheurs de l'Ispra s'ils souhaitaient participer au projet de manière purement volontaire également».

En principe, l'analyse des empreintes digitales n'implique pas le traitement de données sanitaires. Cela s'explique par le fait que, bien que cela soit potentiellement envisageable[3], il est quelque peu difficile de déduire des informations sur l'état de santé d'une personne à partir d'un échantillon d'empreinte digitale. Qui plus est, la finalité du traitement n'a ni un lien direct, ni un lien indirect, avec la santé des personnes en ce qu'elle porte sur le test (la recherche) d'une nouvelle technologie.

Néanmoins, selon certaines études, les images d'empreintes digitales peuvent révéler certaines informations ethniques sur la personne concernée[4]. L'article 10 du règlement prévoit que le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique est interdit.[5] Dans la mesure où le traitement considéré ici n'a ni pour objectif, ni pour effet d'évaluer l'origine ethnique des personnes concernées, on ne peut considérer que celui-ci relève de cette catégorie particulière.
Néanmoins, il convient d'examiner si le traitement peut toutefois être soumis à un contrôle préalable étant donné que l'article 27, paragraphe 1, du règlement couvre toutes les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés de la personne concernée.

Premièrement, l'unique finalité du traitement est de permettre la conduite d'une recherche par une direction de la recherche de la Commission. Selon certains avis du CEPD, lorsque le traitement a pour seule finalité la conduite d'une recherche et qu'un certain nombre de garanties sont établies, le traitement ne devrait pas être soumis à un contrôle préalable.[6]

Deuxièmement, la licéité est garantie par le consentement explicite des personnes concernées. Le consentement est une question fondamentale pour ce qui concerne l'utilisation des empreintes digitales à d'autres fins que pour l'application du droit.[7] Un appel ouvert à manifestation d'intérêt permettra de s'assurer que le consentement est donné librement, en parfaite connaissance de cause et de manière éclairée, dans la mesure où il n'existe aucune obligation de participer. Par ailleurs, les personnes concernées pourront retirer leur consentement à tout moment; elles reçoivent un document portant le nom de *consentement éclairé* dans lequel il est notifié que «*tout refus de participer ne donnera lieu à aucune sanction, ni aucune perte d'avantages auxquels vous auriez droit par ailleurs. Vous pouvez retirer votre consentement à tout moment et mettre fin à votre participation sans aucune pénalité* [...]»

Néanmoins, selon les informations complémentaires transmises, d'autres collègues pourraient être invités à participer sur la base du volontariat en dehors de l'appel à manifestation d'intérêt. Le responsable du traitement devrait veiller à ce que ces personnes participent dans les mêmes conditions que celles répondant à l'appel à manifestation d'intérêt, à savoir, sur la base du volontariat et avec la possibilité de retirer leur consentement. Cette égalité des conditions est

[3] Point 29 de l'avis 17/2008 de la Commission de la protection de la vie privée du 9 avril 2008, Avis d'initiative relatif aux traitements de données biométriques dans le cadre de l'authentification de personnes (A/2008/017).

[4] Voir la note de bas de page 15 de l'avis 3/2012 sur l'évolution des technologies biométriques du groupe de travail «Article 29» sur la protection des données, tel qu'adopté le 27 avril 2012.

[5] S'agissant des photos, nous avons indiqué qu'elles ne relèvent pas de l'article 10, à moins que vous les utilisiez aux fins de telles évaluations ; le même raisonnement doit s'appliquer ici (avis 02/2012 du GT art. 29 dans la note de pied de page + CEPD 2013-0717).

[6] Voir, par exemple, la notification de contrôle préalable relative au cyclisme social : une étude de terrain sur l'activité physique et les réseaux sociaux (CEPD, dossier 2017-0080) du 8 mars 2017.

[7] Voir le paragraphe 4.4.2 de l'avis 3/2012 sur l'évolution des technologies biométriques, note de bas de page 4.

nécessaire pour garantir la validité du consentement; en d'autres termes, un consentement libre, en parfaite connaissance de cause et de manière éclairée.

Troisièmement, la période de conservation est équivalente à la durée de la recherche et semble proportionnée, dans la mesure où les données ne seront pas conservées pendant plus de deux ans.

Quatrièmement, les mesures de sécurité adoptées pour garantir la conformité à l'article 22 du règlement sont appropriées, étant donné que les données sont pseudonymisées et que la base de données dans laquelle elles sont conservées est, par ailleurs, cryptée. Le CEPD estime que la conservation des données dans un ordinateur physiquement déconnecté du réseau et inaccessible depuis le monde extérieur relève des meilleures pratiques.

Cependant, la sécurité pourrait être renforcée pour ce qui concerne la pseudonymisation des données. Le lien utilisé pour la pseudonymisation des données pourrait être conservé dans un logiciel/une base de données indépendant(e) au lieu d'être conservé simplement dans un carnet placé dans un espace protégé du laboratoire. Les mesures de sécurité organisationnelles mises en place par le responsable du traitement pour la conservation du carnet peuvent également s'avérer suffisantes. En tout état de cause, le CEPD recommande au **responsable du traitement de mettre en application** les mesures de sécurité techniques et **organisationnelles** appropriées pour limiter les risques (et pouvoir justifier de ces choix).

3. Conclusion

Si l'analyse de données dactyloscopiques aux fins d'une étude de recherche menée par le CCR ne présente pas de risques particuliers au regard des droits et libertés des personnes concernées en vertu de l'article 27 du règlement, le CEPD a identifié deux recommandations à formuler. Le CEPD demande à ce que les recommandations suivantes soient mises en œuvre, mais n'exige aucune preuve documentaire:

1. Le consentement représentant un élément fondamental dans le présent traitement, le responsable du traitement devrait veiller à ce que tous les participants soient traités sur un pied d'égalité et donnent leur consentement libre, valide et sans ambiguïté;

2. Les mesures de sécurité étant primordiales dans le présent traitement, le responsable devrait s'assurer que les mesures techniques/organisationnelles prises concernant la pseudonymisation sont adaptées au risque encouru.

À la lumière du principe de responsabilité, le CEPD attend du CCR qu'il mette en application les recommandations susmentionnées, et décide donc de **clôturer le dossier 2017-0509**.

Wojciech Rafał WIEWIÓROWSKI

Cc : M^me^ Viktoria ZIOGA, Commission européenne