Observations formelles du CEPD sur la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique

1. Introduction et contexte

- Le 3 juin 2021, le CEPD a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725[1] au sujet de la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique[2].
- Selon l'exposé des motifs, le projet de proposition remédierait à certaines lacunes du règlement actuel[3], dont les suivantes:
  - couverture restreinte des schémas d'identification électronique notifiés au titre du règlement actuel,
  - offres limitées d'authentification eIDAS pour les utilisateurs transfrontières de services publics,
  - limitation aux services publics, malgré la demande du marché existante dans le secteur privé,
  - absence de couverture des attributs électroniques, comme les certificats médicaux ou les qualifications professionnelles, rendant difficile la reconnaissance juridique paneuropéenne de tels justificatifs sous forme électronique.
- Cette proposition de révision vise à donner aux citoyens et aux résidents pleinement confiance dans le fait que le cadre européen relatif à une identité numérique donnera à chacun les moyens de contrôler qui a accès à son jumeau numérique et à quelles données exactement.
- Un niveau élevé de sécurité sera assuré en ce qui concerne tous les aspects de la fourniture d'identités numériques, y compris la délivrance d'un portefeuille européen d'identité numérique, et l'infrastructure pour la collecte, le stockage et la divulgation de données d'identité numérique.
- La proposition élargit la liste actuelle des services de confiance eIDAS à trois nouveaux services de confiance qualifiés, à savoir la fourniture de services d'archivage

[1] 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 (règlement 2018/1725).

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281.

[3] Règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, JO du 28.8.2014, p. 73.

électronique, les registres électroniques et la gestion des dispositifs de création de signatures et de cachets électroniques à distance.

- La proposition de règlement eIDAS comporte toujours deux parties principales: le chapitre II (actuellement intitulé «Identification électronique») et le chapitre III («Services de confiance»). Toutefois, le chapitre II est désormais divisé en trois sections, tandis que le chapitre III est doté de trois nouvelles sections, portant à 11 le total de ses sections. Les chapitres IV à VI ne sont pas pertinents du point de vue de la protection des données.
- La mise en œuvre technique envisagée déterminera en définitive si le règlement aurait dû prévoir des garanties supplémentaires en matière de protection des données ou si sa conception sera, en elle-même, conforme au RGPD[4]. Toutefois, comme dans le cas du règlement (UE) n° 910/2014, l'architecture technique ne peut être pleinement évaluée tant que les 28 actes d'exécution que la Commission prévoit d'adopter afin d'établir les spécifications techniques et les normes de référence applicables ne sont pas connus. Ces actes sont eux aussi susceptibles de relever du champ d'application de l'article 42, paragraphe 1, du règlement (UE) 2018/1725 et il est probable que le CEPD sera ultérieurement consulté à leur sujet. Les présentes observations formelles n'empêchent donc pas le CEPD de formuler à l'avenir d'éventuelles observations supplémentaires, en particulier si de nouvelles questions viennent à se poser ou si de nouvelles informations deviennent disponibles, par exemple à la suite de l'adoption d'actes d'exécution ou d'actes délégués connexes.
- Les présentes observations formelles du CEPD sont formulées en réponse à la consultation législative engagée par la Commission européenne le 3 juin 2021, conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725. À cet égard, le CEPD se félicite de la référence faite à cette consultation au considérant 37 de la proposition. Ces observations formelles sont sans préjudice de toute action future que le CEPD pourrait entreprendre dans l'exercice de ses pouvoirs en vertu de l'article 58 du règlement (UE) 2018/1725.

2. Observations

- Le CEPD se félicite du concept général de la proposition, qui exige que le cadre européen relatif à une identité numérique soit pleinement conforme au règlement (UE) 2016/679. La question de savoir si les garanties expressément prévues sont suffisantes dépend principalement de la technologie à utiliser pour mettre en œuvre la proposition. À cet égard, le CEPD se félicite que la proposition réaffirme, dans ses considérants, la pleine applicabilité du RGPD, y compris pour les registres électroniques et les registres électroniques qualifiés[5]. Cette approche est pleinement conforme à l'article 25 du RGPD,

[4] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO du 4.5.2016, p. 1).

[5] Considérant 35.

qui prévoit que le choix de la technologie doit être conforme aux exigences en matière de protection des données, et non l'inverse.

- Il ressort de l'exposé des motifs, en particulier aux pages 10 et 11, que les registres électroniques, en tant que service de confiance, ne constitueront pas un élément nécessaire du portefeuille européen d'identité numérique, mais seront limités à des cas d'utilisation définis. Le CEPD apprécie cette clarification. Il se félicite que l'exposé des motifs confirme que les prestataires de services devront également respecter le RGPD dans les cas d'utilisation des registres électroniques, et que rien dans la proposition n'autorise à déroger aux dispositions du RGPD.

- La technologie des chaînes de blocs est l'une de celles qui mettent en œuvre des registres électroniques. Elle pose plusieurs problèmes de conformité avec le RGPD, notamment en ce qui concerne les transferts de données en dehors de l'UE, l'impossibilité de supprimer ou de corriger des entrées dans une chaîne de blocs, etc. Il se peut donc que cette technologie ne convienne pas à tous les cas d'utilisation possibles et nécessite des garanties supplémentaires. Il convient de noter que le comité européen de la protection des données a prévu dans son programme de travail 2021/2022 d'élaborer des «lignes directrices sur la chaîne de blocs»[6]. Le CEPD recommande que ces lignes directrices, une fois disponibles, soient prises en compte pour l'examen des registres fondés sur la chaîne de blocs dans le cadre de la cette proposition.

- Le CEPD se félicite du fait que le portefeuille européen d'identité numérique offrira à l'utilisateur la possibilité d'exercer un contrôle plus efficace et transparent sur les données qu'il entend partager, avec qui et à quelles fins. La solution technique envisagée permettrait de résoudre les problèmes de traitement de données excessif, car elle permettrait à la personne concernée de ne révéler effectivement que les données nécessaires à une finalité précise. C'est-à-dire que, si l'objectif est de vérifier l'âge, l'utilisateur pourrait choisir de communiquer sa date de naissance sans avoir à divulguer d'autres informations à caractère personnel qui ne sont pas pertinentes à cette fin. Si la finalité est l'identification, par exemple dans le secteur bancaire ou dans celui des télécommunications, comme l'exige la législation, l'utilisateur pourrait ne révéler que les données d'identité à fournir obligatoirement (sans éléments d'identification biométriques, par exemple, si leur traitement n'est pas expressément requis).

- Le CEPD se félicite en outre du fait que le nouvel article 6 *bis*, paragraphe 7, interdise explicitement à l'entité qui délivre le portefeuille européen d'identité numérique de collecter les informations sur l'utilisation du portefeuille qui ne sont pas nécessaires à la fourniture des services qui y sont attachés. Cette interdiction, de même que celle de combiner les données d'identification personnelle du portefeuille avec d'autres données provenant de tout autre service et l'obligation de séparer, de manière physique et logique, les données à caractère personnel relatives à la fourniture des services attachés au portefeuille de toute autre donnée détenue renforceront la confiance dans la sécurité et la confidentialité de cette solution technique.

[6] https://edpb.europa.eu/system/files/2021-03/edpb_workprogramme_2021-2022_en.pdf

- Dans ce contexte, le CEPD se félicite également que l'article 6 *ter*, paragraphe 2, établisse une certification selon les modalités prévues par le règlement (UE) 2016/679 pour certaines exigences applicables aux portefeuilles européens d'identité numérique, visant notamment à empêcher que les prestataires de services de confiance qui délivrent des attestations qualifiées d'attributs puissent recevoir des informations concernant l'utilisation de ces attributs. Le CEPD croit comprendre que cette certification est également obligatoire et n'aura aucun effet disculpatoire.

- L'article 17 définit les tâches de l'organe de contrôle et prévoit une coopération avec d'autres autorités de contrôle, telles que celles prévues par le règlement (UE) 2016/679. Selon cette disposition, les autorités de contrôle de la protection des données seront informées «dans les meilleurs délais, des résultats des audits des prestataires de services de confiance qualifiés, lorsque les règles en matière de protection des données à caractère personnel ont été violées, ainsi que des atteintes à la sécurité qui constituent des violations de données à caractère personnel». Le CEPD note que la formulation, qui semble requérir l'achèvement d'une enquête, tient à l'article 17 du règlement (UE) n° 910/2014 et constitue déjà une amélioration par rapport à cette version actuelle dans la mesure où une violation de données à caractère personnel au sens de l'article 33 du RGPD déclencherait désormais aussi l'obligation d'information. Toutefois, le CEPD attire l'attention du colégislateur sur le fait que la formulation précédente correspondait à un rôle différent des autorités chargées de la protection des données, alors que l'article 33 du RGPD impose aux responsables du traitement de notifier les violations de données remplissant les conditions requises dans les meilleurs délais, au plus tard 72 heures après en avoir pris connaissance, conférant aux autorités de contrôle un rôle actif dans les enquêtes relatives à une violation et dans le choix des mesures à prendre. Pour cette raison, il semble approprié d'aligner la formulation de l'article 17, paragraphe 4, point f), sur celle du point c) du même paragraphe, qui prévoit d'informer les autorités nationales compétentes désignées en application de la directive SRI 2 d'une atteinte (présumée) à la sécurité, que les résultats d'un audit aient ou non constaté une atteinte. Les autorités de contrôle de la protection des données devraient être informées chaque fois que l'organe de contrôle reçoit des informations quant à une éventuelle violation de données à caractère personnel.

- Pour la même raison, la dernière phrase de l'article 20, paragraphe 2, devrait également être alignée sur le RGPD et exiger une notification immédiate, que l'audit soit terminé ou en cours.

- Le projet de proposition prévoit l'utilisation d'un identifiant univoque et constant par les États membres pour faciliter la réconciliation d'identités et garantir l'identification univoque de chaque utilisateur. Cet identifiant servirait ensuite, entre autres, lors de l'ajout d'attestations électroniques d'attributs à un portefeuille.

- Le CEPD apprécie les efforts consentis à l'article 11 *bis* pour renforcer la confiance et l'intégrité en réduisant le risque d'abus ou d'erreurs imputables à une ambiguïté. Il convient toutefois de noter que cet identifiant univoque et constant constitue une autre catégorie supplémentaire de données stockées dans le seul but de faciliter l'utilisation du portefeuille. Cette ingérence dans les droits et libertés de la personne concernée n'est pas nécessairement anodine; dans certains États membres, des identifiants univoques

ont été considérés par le passé comme anticonstitutionnels en raison d'une atteinte à la dignité humaine. Par conséquent, le CEPD recommande d'étudier d'autres moyens de renforcer la sécurité de la mise en correspondance.

- Le CEPD note que l'article 45 *septies* réglemente en outre l'utilisation des données à caractère personnel par les prestataires fournissant des services qualifiés et non qualifiés d'attestation électronique d'attributs. Ils ne peuvent pas combiner les données à caractère personnel relatives à la fourniture de ces services avec des données à caractère personnel provenant de tout autre service qu'ils offrent et ils ont l'obligation de les maintenir séparées, de manière logique, et même de manière physique dans le cas de données à caractère personnel relatives à la fourniture de services qualifiés d'attestation électronique d'attributs, des autres données détenues. Le CEPD est d'avis que ces prescriptions ne peuvent être contournées au moyen de clauses contractuelles ou d'un consentement. Il se félicite de ces prescriptions en ce qu'elles constituent une mesure de nature à prévenir l'utilisation abusive des données et à renforcer la confiance dans le système. En ce qui concerne les prestataires de services qualifiés d'attestation électronique d'attributs, l'article 45 *septies*, paragraphe 4, prévoit même que ces services doivent être fournis dans le cadre d'une entité juridique distincte, ce qui, en combinaison avec les prescriptions susmentionnées, devrait constituer un mécanisme efficace de prévention des conflits d'intérêts et du partage injustifié de données à caractère personnel.

Bruxelles, le 28 juillet 2021

Wojciech Rafał WIEWIÓROWSKI
(signature électronique)