

“Le portefeuille européen d’identité numérique : objet technique ou projet de société ?”

Emile Marzolf

Cette fois, c’est parti : le 8 novembre dernier, le Conseil de l’Union européenne, le Parlement européen et la Commission européenne sont parvenus à un accord sur le futur portefeuille européen d’identité numérique (PEIN), appelé encore *wallet*. Le dispositif, qui devrait entrer en vigueur dès 2027 (d’abord pour les services publics, puis possiblement pour le secteur privé), rassemblera dans nos petits smartphones l’ensemble des données, documents, justificatifs permettant à chacun – personnes physiques ou morales, organismes privés ou publics – de s’identifier dans le monde numérique. Achats en ligne, transactions sécurisées, preuve des diplômes, parcours de santé : le portefeuille européen d’identité numérique est conçu pour être la clef d’accès universelle au monde numérique. En bref : toute action numérique nécessitant une identification fiable de la part de l’utilisateur pourrait passer par le *wallet*.

L’empressement à mettre ce projet sur pied manifeste une confiance, jamais remise en question, dans l’alliance entre technologie numérique et croissance économique.

C’est dire que ce *wallet* sera beaucoup plus qu’un simple portefeuille. À terme, il constituera le passeport d’entrée de tout un chacun dans son existence sociale numérique, passeport qui par conséquent – et c’est essentiel – façonnera cette existence sociale, lui donnera une nouvelle forme. Or ses promoteurs continuent de le présenter comme un simple objet technique, une sorte de superapplication facilitant et sécurisant l’accès au numérique. En réalité, il est une brique essentielle dans le mouvement général de numérisation de la vie sociale. C’est d’ailleurs précisément ce qu’a reconnu, sans peut-être mesurer la portée de ses dires, la députée européenne, rapporteure du règlement (UE) sur l’identité numérique Romana Jerkovic lors de [sa présentation à la presse le 8 novembre](#) : “Le cadre d’identité numérique européen est une législation révolutionnaire qui propulsera la numérisation du secteur public et de la société dans son ensemble.”

C’est dire que l’affaire est sérieuse.

Un problème démocratique

Notre chaire “Valeurs et politiques des informations personnelles” (VP-IP) a déjà eu l’occasion d’alerter sur le problème démocratique majeur que posait, en amont, la procédure qui a mis sur les rails, à marche forcée**, ce projet complexe avant tout débat démocratique, notamment parlementaire. C’était engager une politique du fait accompli sur laquelle nous ne revenons pas ici, si ce n’est pour souligner le problème fondamental suivant : en soustrayant la question du *wallet* à un vrai débat démocratique – jusqu’à aujourd’hui, l’instauration du *wallet* est complètement passée sous les radars citoyens ! –, la Commission européenne court-circuitait du même coup la question fondamentale des finalités – le *wallet*, pour quoi faire ? La seule réponse que l’on puisse inférer à partir des textes et déclarations est : pour fluidifier le marché unique. L’empressement à mettre ce projet sur pied manifeste une confiance, jamais remise en question, dans l’alliance entre technologie numérique et croissance économique. Nous pouvons diagnostiquer là une forme sophistiquée de solutionnisme technologique. Est ainsi restée non débattue la question pourtant fondamentale de savoir si cette société numérisée, économiquement fonctionnelle, était bien l’horizon sous lequel Européennes et Européens voulaient voir grandir leur Europe.

Des problèmes de sécurité

La mise en place du *wallet* est une opération techniquement et juridiquement très complexe, notamment parce que l’UE, n’ayant pas la compétence pour délivrer elle-même un tel portefeuille d’identité, ne peut que viser à harmoniser et coordonner les systèmes d’identité de chacun des 27 États de l’Union. Il en résulte une véritable usine à gaz technologique et juridique, dont la vulnérabilité est proportionnelle à la complexité. Notamment, le nombre d’acteurs intervenant dans le dispositif est tel qu’il ne peut qu’augmenter les failles de sécurité potentielles. Au-delà de cela, signalons 3 points de vigilance principaux :

- En matière de sécurité, le Règlement prévoit une certification en matière de cybersécurité, mais ses modalités d’application font largement débat. Il reste entre autres à adopter des référentiels respectueux des principes européens, chose loin d’être aisée puisque ceux-ci sont adoptés dans des instances internationales, telles que l’ISO, dans lesquelles la Commission européenne elle-même reconnaît l’influence active d’acteurs étrangers.
- En ce qui concerne l’assurance de la protection du nombre incalculable de données personnelles qui transiteront par le *wallet*, une certification au titre du Règlement général sur la protection des données (RGPD) aurait pu être imposée. Hélas, si la Commission européenne a proposé cette certification en juin 2021 (*the wallet shall be certified*), le compromis du 8 novembre 2023 évoque une simple possibilité de certification (*the*

wallet may be certified).

- L'utilisation du *wallet* et la circulation des données personnelles par son intermédiaire ne s'arrêtent pas aux frontières européennes. Les services dits de confiance, tout comme le portefeuille lui-même d'ailleurs, pourront être fournis par des acteurs non européens, notamment américains. Ainsi en sera-t-il notamment des signatures électroniques de niveau de sécurité élevé utilisées par les citoyens, résidents et entreprises établies dans l'UE, de l'archivage électronique ou des attestations électroniques de données. Sur ce point, un mécanisme bien connu, déjà utilisé dans le RGPD, est mobilisé : ces services pourront être fournis par des prestataires établis dans un pays tiers lorsqu'une décision d'exécution aura été adoptée par la Commission européenne ou qu'un accord aura été conclu entre l'Union européenne et le pays tiers.

Les juges n'ont-ils pas souligné l'accès disproportionné et la protection inadéquate des données européennes détenues en masse par les services de sécurité américains ?

Dans ce dernier cas, on peut se demander s'il s'agit d'une véritable garantie. Les 2 décisions adoptées par la Commission européenne reconnaissant que les États-Unis disposaient d'un niveau de protection suffisant pour transférer les données personnelles collectées sur le sol européen n'ont-elles pas été invalidées non pas une fois, mais deux fois par la Cour de justice de l'Union européenne³ ? Les juges n'ont-ils pas souligné l'accès disproportionné et la protection inadéquate des données européennes détenues en masse par les services de sécurité américains, comme l'a révélé pour la première fois Edward Snowden en 2013 ? Le troisième accord UE-États-Unis conclu cet été [ne fait-il pas déjà l'objet d'un nouveau recours ?](#)

Le projet d'une démocratie conforme au marché

Mais indépendamment même de ces problèmes de sécurité technique et juridique, nous aimerions plus globalement questionner la portée sociétale d'un tel dispositif numérique. Car la volonté d'instaurer le PEIN dans l'Union témoigne, mieux que tout autre dispositif, de la tendance européenne au renforcement réciproque des attentes de la Commission européenne, de certains acteurs du marché et de certains États membres. Du côté du marché, les attentes sont celles de la généralisation des services en ligne, sous prétexte de leurs supposées simplification et fluidification, lesquelles iraient de pair avec un accroissement de l'offre des données utilisables à des fins lucratives. Du côté des États, elles sont globalement celles d'une facilitation administrative (par exemple, vérification du permis de conduire), d'une rationalisation budgétaire, d'une interopérabilité de certains systèmes administratifs ([diplômes, santé, transports, etc.](#)) et, d'une manière générale, d'une identification plus sûre des personnes (facilitation des vérifications d'identité, réduction de la fraude, contrôle des déplacements, gestion des frontières).

La confiance que les individus devraient se porter les uns aux autres et à leurs gouvernants se reporte globalement sur le système technique, dont le fonctionnement est conçu sur un imaginaire marchand.

Pour le dire vite : le PEIN participe à la mise en place de ce qu'il faut bien appeler une "démocratie conforme au marché", et il en constituerait l'élément le plus emblématique. Une "démocratie marchande", en quelque sorte, où chacun, doté de droits individuels, gère dans son cockpit ses interactions avec le monde extérieur et les données qu'il est censé souhaiter partager, sur le mode de la transaction marchande. Le PEIN entérine un modèle de coexistence individualiste, où l'intégration des individus est davantage assurée par une technique parfaitement fonctionnelle que par l'adhésion à des valeurs, une histoire ou un projet communs. La confiance que les individus devraient se porter les uns aux autres et à leurs gouvernants se reporte globalement sur le système technique, dont le fonctionnement est conçu sur un imaginaire marchand. La "démocratie conforme au marché" dépolitise la démocratie, en intensifiant le pouvoir technocratique.

D'où une dernière inquiétude, et non la moindre : cette intensification technocratique rend possible, par l'infrastructure technique qu'elle installe, une potentielle gestion chinoise de la vie sociale. Certes, nous en sommes encore préservés par diverses réglementations qui, tel le RGPD, font aujourd'hui la fierté de l'Europe – mais les textes sont plus fragiles que la technique. Un changement de gouvernance, un basculement politique pourraient vite les mettre au rancard. Nous l'avons dit, l'affaire est sérieuse.

[1] Cette tribune est signée Mark Hunyadi, philosophe, professeur de philosophie morale et politique à l'Université catholique de Louvain, en Belgique, en collaboration avec les membres de la [chaire "Valeurs et politiques des informations personnelles"](#) (VP-IP) de l'Institut Mines-Télécom : Claire Levallois-Barth, Ivan Mesequer, Maryline Laurent, et Patrick Waelbroeck.

[2] M. Hunyadi, en collaboration avec C. Levallois-Barth, I. Mesequer, M. Laurent, P. Waelboeck, membres de la chaire VP-IP de l'Institut Mines-Télécom, ["Union européenne : pourquoi un portefeuille numérique à marche forcée ?"](#), 6 mai 2022.

[3] Respectivement le 6 octobre 2015, avec l'arrêt dit Schrems I, et le 16 juillet 2020, avec l'arrêt dit Schrems II.