INTERNATIONAL JOURNAL OF **DIGITAL AND DATA LAW**

REVUE INTERNATIONALE DE DROIT **DES DONNÉES ET DU NUMÉRIQUE**

Vol. 7 - 2021

ISSN 2553-6893

IMODEV
LES ÉDITIONS

International Journal of Digital and Data Law
Revue internationale de droit des données et du numérique

Direction :
Irène Bouhadana & William Gilles

ISSN : 2553-6893

IMODEV
49 rue Brancion 75015 Paris – France
www.imodev.org
ojs.imodev.org

Les propos publiés dans cet article n'engagent que leur auteur.

The statements published in this article are the sole responsibility of the author.

À PROPOS DE NOUS

La **Revue Internationale de droit des données et du numérique (RIDDN)/ the International Journal of Digital and Data Law** est une revue universitaire créée et dirigée par Irène Bouhadana et William Gilles au sein de l'IMODEV, l'Institut du Monde et du Développement pour la Bonne Gouvernance publique.

Irène Bouhadana, docteur en droit, est maître de conférences en droit du numérique et droit des gouvernements ouverts à l'Université Paris 1 Panthéon-Sorbonne où elle dirige le master Droit des données, des administrations numériques et des gouvernements ouverts au sein de l'École de droit de la Sorbonne. Elle est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Elle est aussi fondatrice et Secrétaire générale de l'IMODEV. Enfin, associée de BeRecht Avocats, elle est avocate au barreau de Paris et médiateure professionnelle agréée par le CNMA.

William Gilles, docteur en droit, est maître de conférences (HDR) en droit du numérique et en droit des gouvernements ouverts, habilité à diriger les recherches, à l'Université Paris 1 Panthéon-Sorbonne où il dirige le master Droit des données, des administrations numériques et des gouvernements ouverts. Il est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Il est aussi fondateur et Président de l'IMODEV. Fondateur et associé de BeRecht Avocats, il est avocat au barreau de Paris et médiateur professionnel agréé par le CNMA.

IMODEV est une organisation scientifique internationale, indépendante et à but non lucratif créée en 2009 qui agit pour la promotion de la bonne gouvernance publique dans le cadre de la société de l'information et du numérique. Ce réseau rassemble des experts et des chercheurs du monde entier qui par leurs travaux et leurs actions contribuent à une meilleure connaissance et appréhension de la société numérique au niveau local, national ou international en en analysant d'une part, les actions des pouvoirs publics dans le cadre de la régulation de la société des données et de l'économie numérique et d'autre part, les modalités de mise en œuvre des politiques publiques numériques au sein des administrations publiques et des gouvernements ouverts.

IMODEV organise régulièrement des colloques sur ces thématiques, et notamment chaque année en novembre les *Journées universitaires sur les enjeux des gouvernements ouverts et du numérique / Academic days on open government and digital issues*, dont les sessions sont publiées en ligne [ISSN : 2553-6931].

IMODEV publie deux revues disponibles en open source (ojs.imodev.org) afin de promouvoir une science ouverte sous licence Creative commons_CC-**BY-NC-ND** :

1) la *Revue Internationale des Gouvernements ouverts (RIGO)/ International Journal of Open Governments* [ISSN 2553-6869] ;

2) la *Revue internationale de droit des données et du numérique (RIDDN)/International Journal of Digital and Data Law* [ISSN 2553-6893].

ABOUT US

The **International Journal of Digital and Data Law / Revue Internationale de droit des données et du numérique (RIDDN)** is an academic journal created and edited by Irène Bouhadana and William Gilles at IMODEV, the Institut du monde et du développement pour la bonne gouvernance publique.

Irène Bouhadana, PhD in Law, is an Associate professor in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where she is the director of the master's degree in data law, digital administrations, and open governments at the Sorbonne Law School. She is a member of the Institut de recherche juridique de la Sorbonne (IRJS). She is also the founder and Secretary General of IMODEV. Partner at BeRecht Avocats, she is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

William Gilles, PhD in Law, is an Associate professor (HDR) in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where he is the director of the master's degree in data law, digital administration and open government. He is a member of the Institut de recherche juridique de la Sorbonne (IRJS). He is also founder and President of IMODEV. Founder and partner at BeRecht Avocats, he is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

IMODEV is an international, independent, non-profit scientific organization created in 2009 that promotes good public governance in the context of the information and digital society. This network brings together experts and researchers from around the world who, through their work and actions, contribute to a better knowledge and understanding of the digital society at the local, national or international level by analyzing, on the one hand, the actions of public authorities in the context of the regulation of the data society and the digital economy and, on the other hand, the ways in which digital public policies are implemented within public administrations and open governments.

IMODEV regularly organizes conferences and symposiums on these topics, and in particular every year in November the Academic days on open government and digital issues, whose sessions are published online [ISSN: 2553-6931].

IMODEV publishes two academic journals available in open source at ojs.imodev.org to promote open science under the Creative commons license CC-**BY-NC-ND**:

1) the *International Journal of Open Governments*/ la *Revue Internationale des Gouvernements ouverts (RIGO)* [ISSN 2553-6869] ;

2) the *International Journal of Digital and Data Law* / la *Revue internationale de droit des données et du numérique* (RIDDN) [ISSN 2553-6893].

LES IMPLICATIONS JURIDIQUES RELATIVES À LA GESTION DE L'IDENTITÉ NUMÉRIQUE ET PERSPECTIVES D'INNOVATION EN EUROPE

par **Cristina TIMÓN LÓPEZ,** Chercheuse dans le projet européen OLYMPUS, Doctorante en Droit des Nouvelles Technologies à l'Université de Murcia dans le groupe de recherche iDerTec et Avocate.

La numérisation de la société et des interactions a créé la nécessité d'identifier les individus à travers des réseaux, d'où les différents modèles ou propositions de gestion de l'identité numérique qui ont émergé. Parmi les modèles les plus utilisés, nous pouvons souligner les systèmes délégués ou fédérés. Cependant, de tels modèles ont posé de différents enjeux en matière de cybersécurité et protection de la vie privée.

En ce sens, les Technologies de l'Information et de la Communication (TICs) ont favorisé l'émergence des nouveaux comportements criminels, notamment dans le domaine de la gestion de l'identité numérique, le vol d'identité. D'autre part, les flux continus de données et les possibilités offertes par l'innovation technologique posent des problèmes en termes de contrôle excessif ou de surveillance de l'activité des utilisateurs.

L'objectif de cet article est d'offrir une courte description des systèmes de gestion de l'identité numérique, ses implications en matière de prévention du vol d'identité, ainsi que des pratiques de surveillance. Pour ce faire, nous ferons référence au projet de recherche européen OLYMPUS[1] pour illustrer l'importance de l'innovation technologique dans ce domaine et ses implications juridiques.

Plus spécifiquement, de telles innovations visent à améliorer la prévention des cyberattaques et assurer la conformité au Règlement Européen sur la Protection des Données (ci-après, RGPD) grâce au développement d'une architecture résiliente en utilisant diverses techniques cryptographiques. Cette architecture innovante consiste à virtualiser le fournisseur d'identité qui est proposée dans le projet OLYMPUS, ce qui pourrait être particulièrement avantageux dans le cas de la prévention du vol d'identité et donc la protection des données à caractère personnel. Également, ces innovations ont des implications sur la validité et reconnaissance des identités numériques. Au niveau de l'Union Européenne, le Règlement d'interopérabilité eIDAS fixe les

[1] https://olympus-project.eu/(Grant Agreement 786725).

conditions de reconnaissance mutuelle entre les États Membres. Cependant, l'innovation technologique représente un défi plus complexe afin de respecter de telles conditions, mais elle soulève aussi l'urgence d'une révision du règlement eIDAS.
À propos de cet article, nous soulignerons les principaux défis détectés au cours du développement du projet OLYMPUS et nous conclurons avec une réflexion, compte tenu du processus de révision du règlement eIDAS, sur la possibilité d'étendre ce règlement comme cadre de gouvernance d'un métasystème d'identité numérique au niveau européen, afin de préserver la souveraineté digitale de l'Union Européenne.

§ 1 – LA GESTION DE L'IDENTITÉ NUMÉRIQUE

L'identité numérique fait référence à un ensemble d'attributs (ou de données à caractère personnel), qui permettent d'identifier clairement une personne par le biais d'un processus d'authentification lors de la réalisation d'actions qui ont lieu en ligne[2]. Cette identité est composée d'un ensemble d'attributs qui pourraient être combinés et divisés dans différents environnements.
Nous pouvons faire une première distinction par rapport à l'entité fournissant le service entre[3] :

a) Les identités numériques internes sont celles qui nous permettent d'interagir avec la personne ou l'organisation qui nous en a fourni. Dans ce scénario, il n'y a qu'une personne morale[4].
b) Les identités déléguées ou externalisées pour désigner les identités qui ont été fournies par des organisations ou entités différentes, de façon à ce qu'il y ait deux personnes morales séparées qui auront une relation de base légale (par exemple, le Règlement eIDAS) ou contractuelle. Dans ce dernier cas, l'entité par laquelle le service d'identification est fourni serait considérée comme le fournisseur du service.

Également, nous pouvons faire une deuxième distinction en fonction de la nature juridique du fournisseur du service d'identité numérique entre :

a) Publics, il s'agit des services d'identité numérique fournis pour s'identifier auprès de l'administration ou

[2,3] I. ALAMILLO DOMINGO, "Identidad electrónica, robo de identidad y protección de datos personales", in A. RALLO LOMBARTE, L. ARROYO ZAPATERO (coll.), *Robo de Identidad y Protección de Datos en la red*, Agencia Española de Protección de Datos, Thomson Reuters (Legal) Limited, 2010, pp.17-19.
[4] Par exemple, les banques ont normalement leurs propres systèmes pour l'identification de leurs consommateurs. Leurs systèmes d'identification sont divers (identifiants, authentification à double facteur ou biométriques) en fonction du type d'opération afin d'assurer la conformité aux différentes normatives, à souligner, les exigences KYC (*know-your-costumer*) et AML (*anti-money laundering*).

des services publics (par exemple *Cl@ve*, FranceConnect, *eDNI*…).

b) Privées, comme les plateformes telles que Facebook, Amazon ou Google.

Cependant, la séparation n'est pas absolue sous le droit européen, car le Règlement d'interopérabilité eIDAS a envisagé une possibilité intermédiaire comme c'est le cas des certificats électroniques[5], qui peuvent être fournis aussi pour des entités de nature juridique privée (des services de confiance) qui ont pour but la création d'un processus d'identification auprès des autorités publiques des États Membres de l'Union Européenne[6].

Finalement, nous pouvons faire une dernière distinction concernant la technologie ou modèle de base des systèmes pour la gestion de l'identité numérique entre[7] :

a) Centralisés, il y a un seul fournisseur d'identité qui gère tous les processus d'authentification des utilisateurs.

b) Fédérés, l'utilisateur peut accéder à différents services en utilisant une seule accréditation parmi plusieurs fournisseurs d'identité.

c) Décentralisés, le fournisseur d'identité est intégré par différentes personnes morales qui font partie d'une technologie décentralisée, normalement de la blockchain mais il existe aussi d'autres technologies qui permettent la décentralisation.

Le principal inconvénient du premier modèle est qu'il existe un seul intermédiaire pour toutes les actions de l'utilisateur en ligne. Néanmoins, la « centralisation » est un problème courant pour les deux premiers modèles de gestion d'identité numérique (c'est-à-dire, centralisés ou fédérés), car les données de l'utilisateur apparaissent toujours regroupées dans un seul ou un faible nombre de fournisseurs d'identité, en affectant la sécurité des données et en les rendant exposées à diverses formes de cybercriminalité, tout particulièrement au vol d'identité[8].

---

[5] I. ALAMILLO DOMINGO, « *Identificación electrónica y confianza en las transacciones electrónicas la regulación jurídico-administrativa de las instituciones de acreditación de la actuación electrónica* », *DIGITUM*, Universidad de Murcia, 2018, pp. 41-56 : https://digitum.um.es/digitum/bitstream/10201/61019/6/Ignacio%20Alamillo%20Domingo%20Tesis%20Doctoral.pdf.

[6] L'identification électronique dans le Règlement eIDAS n'est pas envisagée pour être délivrée par des entités de nature juridique privée, mais l'identification est une fonction essentiellement réservé aux États Membres. Toutefois, cette exclusion n'est pas absolue mais il existe la possibilité que les services de confiance (de nature essentiellement commerciale) fournissent des services d'identification électronique au travers de l'émission de certificats électroniques (préférablement des certificats qualifiés) qui au-delà de permettre la signature des documents soient capables d'identifier le signataire.

[7] M. ALLENDE LÓPEZ, "Self-Sovereign Identity: The Future of Identity: Self Sovereignity, Digital Wallets, and Blockchain", *IDB,* 2020, pp.22-24 [https://doi.org/10.18235/0002635]

[8] E. MALER, ET D. REED, "The Venn of identity", *IEEE Security and Privacy*, vol. 6, nº 2, 2008, pp. 16–23 [https://doi.org/10.1109/MSP.2008.50]

Cet excès de centralisation a aussi éveillé l'intérêt pour le développement de nouvelles architectures technologiques qui soient capables d'assurer un niveau plus élevé de confidentialité dès la conception. Toutefois, cette confidentialité ne se limite pas simplement au développement d'architectures plus résilientes contre des attaquants externes, mais aussi contre le fournisseur d'identité.

§ 2 – LES PROBLÈMES LIÉS À LA GESTION DE L'IDENTITÉ NUMÉRIQUE : UNE TENSION DE FORCES

La gestion de l'identité numérique a posé deux problématiques essentielles jusqu'à aujourd'hui qui représentent en même temps une tension de forces. D'une part, les criminels ont profité des possibilités offertes par les systèmes d'identification en ligne pour accéder aux données personnelles des individus et usurper leur identité grâce à différentes pratiques[9].

Les systèmes de gestion d'identité numérique visent à améliorer la prévention de telles attaques et assurer la conformité au RGPD. Pour ce faire, les dernières innovations consistent en différentes techniques de cryptage pour assurer la confidentialité des données en cas de vol[10].

Néanmoins, cette sécurité exige parfois aussi le stockage de plus de données par le fournisseur d'identité, car la technologie précise de cette collecte[11] ou dans les cas plus classiques, le fournisseur du service demande une grande quantité d'informations dans le but de vérifier l'identité de l'individu avant de lui fournir le service. Cela pose, cependant, un autre problème en termes de protection de la vie privée[12].

En effet, comme nous avons fait référence précédemment, le stockage d'un grand nombre des données à caractère personnelle, ainsi que le contrôle de la plupart des processus d'identification effectués par un individu dans un certain domaine permet aux fournisseurs d'identité numérique de développer des pratiques de surveillance. Ces pratiques sont, toutefois, contraires au droit à la vie privée, envisagé par différents textes européens, mais notamment l'article 8 de la Convention Européenne des Droit de

---

[9] M. CHAWKI, M. A. WAHAB, "Identity theft in cyberspace: Issues and solutions", *Lex Electronica,* Vol.11, nº 1, 2006, pp. 4-20: https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/9563/articles_54.pdf?sequence=1.

[10] S. RAHMAN, A.M. FEROZ ET A. KHAN, "Online Identity Theft and Its Prevention Using Threshold Cryptography", *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 10, nº 9, 2010, pp. 18-25: http://paper.ijcsns.org/07_book/201009/20100904.pdf.

[11] Par exemple, dans le projet de recherche OLYMPUS la technique cryptographique qui permet l'authentification distribuée, précise en même temps le stockage des données à caractère personnel dans les différentes parties qui intègrent l'architecture distribuée, en augmentant, par conséquent, le nombre de données stockées.

[12] R. HALPERIN ET J. BACKHOUSE, "A roadmap for research on identity in the information society", *Identity in the Information Society*, Vol. 1, nº 1, 2008, pp.71-87: https://doi.org/10.1007/s12394-008-0004-0.

l'Homme, l'article 6.2 du Traité sur l'Union Européenne, et l'article 16 du Traité sur le Fonctionnement de l'Union Européenne, ainsi qu'au principe de minimisation des données envisagé par le RGPD.

Par rapport au contenu de ce droit, il est important de souligner que la garantie du droit à la vie privée va au-delà du pouvoir de l'individu pour prévenir des menaces externes, mais ce droit fait référence aussi à sa faculté d'utiliser librement ses informations[13]. En conséquence, le droit à la vie privée donne le pouvoir à l'individu pour contrôler et faire l'usage qu'il juge approprié de ses données personnelles (habeas data) et c'est dans ce sens que se sont prononcées les Cours Constitutionnelles[14].

Une telle interprétation est clairement incompatible avec le concept de surveillance lui-même. En premier lieu, car il implique que l'individu perd le contrôle sur ses données et en autre, car il perd le contrôle dans la plupart des cas sur les personnes morales qui connaissent ses données ou même les finalités pour lesquelles elles sont finalement utilisées[15].

À cet égard, le principe de minimisation des données, entre autres, établi par le RGPD, est contraire aussi au concept de surveillance, car la surveillance est fondée sur un « contrôle général » des mouvements des individus, tandis que le RGPD exige que les données soient collectées à des fins spécifiques, et que le consentement qui les concerne se limite exclusivement à l'objet pour lequel il a été donné. Dans le même sens, des décisions européennes en la matière sont contraires à ces pratiques en limitant les cas où il a été conclu qu'il existe une situation de « contrôle disproportionné ». En ce sens, il pourrait être pertinent de citer certaines décisions, telles que la décision de la Cour de Justice de l'Union Européenne dans le cas « Digital Rights vs. Ireland »[16] ou de Cour Européenne des Droits de l'Homme dans le cas « Zakahrov »[17].

Le phénomène de surveillance pose un ensemble de risques qui vont à l'encontre des fondements d'une société libre et démocratique, car la vie privée intellectuelle des personnes surveillées est limitée, et cela crée en même temps un déséquilibre de pouvoirs qui peut déboucher à différentes pratiques

---

[13] R. MARTÍNEZ MARTÍNEZ, "El derecho fundamental a la protección de datos: perspectivas", *Revista de Internet, Derecho y Política (IDP)*, nº 5, 2007, pp.48-58: https://dialnet.unirioja.es/servlet/articulo?codigo=2372613.

[14] Par exemple la décision de la Cour Constitutionnelle allemande en 1983, qui a été suivie par la Cour Constitutionnelle espagnole dans ses décisions 254/1993 du 20 Juillet ou 292/2000 du 30 Novembre.

[15] V. MITSILEGAS, "Surveillance and Digital privacy in the Transatlantic War on Terror: The Case for a Global Privacy Regime", *Columbia Human Rights Law Review*, vol. 47, nº 3, 2016, pp.12-24.

[16] Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others. C: 2014/238 (rendu le 8 avril 2014)

[17] Mr Roman Andreyevich Zakharov vs. Russian Federation C : 47143/06 (rendu le 4 décembre 2015)

malveillantes (par exemple du chantage, de la persuasion, de la discrimination…)[18].

Finalement, il est important aussi de faire une distinction entre la surveillance publique et privée. Dans le cas de la surveillance publique, ses principaux objectifs sont la prévention du terrorisme et la lutte contre la criminalité, ainsi que le concept naissant de *smart surveillance* [19] [20]. Toutefois, bien que ce type de surveillance prétende être au nom de l'intérêt public, comme dans d'autres situations de conflits entre les droits des individus et l'intérêt public, une analyse cas par cas doit être effectuée afin de garantir la proportionnalité des mesures adoptées.

Dans le cas de la surveillance privée, son objectif principal est de maximiser les profits. À cette fin, les entreprises utilisent les données des individus (par exemple les habitudes de navigation sur le web, les centres d'intérêt...), dans la mesure où les données ont une valeur économique extrêmement élevée pour les entreprises, en particulier après l'émergence du phénomène du *Big Data*, qui a démontré la valeur qui provient des modèles dérivés de l'élaboration des liens entre les informations concernant les individus ou un groupe d'individus.

Néanmoins, cette distinction entre la surveillance publique et la surveillance privée n'est pas aussi claire dans la pratique. La surveillance gouvernementale et non gouvernementale se soutiennent mutuellement, car en fin de compte, les deux utilisent les mêmes technologies et techniques, et travaillent habituellement par le biais d'une variété de partenariats, ce qui pose un deuxième problème qui est la monopolisation de la surveillance par un petit nombre d'entreprises[21].

En effet, in fine il existe un même modèle commun, qui favorise ces pratiques, donc il semble clair qu'un premier pas vers leurs restrictions passe par une refonte de la technologie utilisée.

§ 3 – LE PROJET OLYMPUS

A) Architecture

Le projet de recherche européen OLYMPUS (*Oblivious identitY Management for Private and User-friendly Services*) vise à développer une nouvelle architecture pour les systèmes de gestion d'identité déléguée, en limitant son pouvoir de surveillance, ainsi que d'améliorer la sécurité du système.

---

[18] R. NEIL, "The Dangers of Surveillance", *Harvard Law Review*, vol. 126, nº 7, 2013, pp.1937-1965.

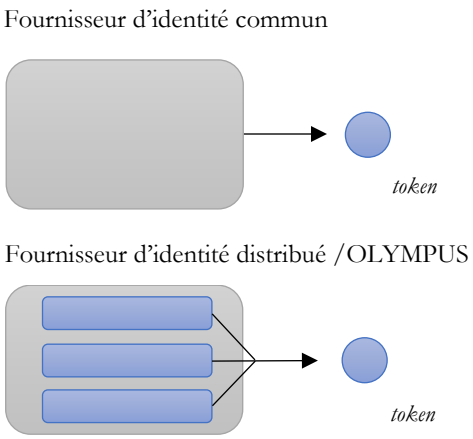
[19] Le concept de « smart surveillance » fait référence au système qui permet l'obtention d'informations pertinentes à partir des données collectées de façon à ce qu'il soit possible de produire une description des évènements qui peuvent éventuellement être utilisées pour prendre des décisions automatisées ou semi-automatisées

[20] M. VERMEULEN ET R. BELLANOVA, "European Smart Surveillance: What's at stake for Data Protection, Privacy and Non-Discrimination", *Security and Human Rights*, vol. 23, nº 4, 2012, p.298.

[21] Ibidem.

Le système pour la gestion de l'identité numérique proposé par OLYMPUS est né dans le contexte de l'utilisation généralisée des modèles délégués et des solutions *Single-Sign-On*. OLYMPUS a pour but d'améliorer les principaux inconvénients de ces solutions, parmi lesquelles nous pouvons souligner la configuration du fournisseur d'identité comme point unique de défaillance et la surveillance de l'activité des utilisateurs[22].
L'architecture d'OLYMPUS a comme point de départ la virtualisation (ou division) du fournisseur d'identité, parmi plusieurs fournisseurs d'identité « partiels » (qui intègrent le fournisseur d'identité « virtualisé ») en gardant une apparence unique du point de vue de l'utilisateur (Figure 1), par le biais de nouvelles approches cryptographiques appliquées aux technologies pour la gestion de l'identité numérique[23].

Figure 1. Architecture d'un fournisseur d'identité standard vs. OLYMPUS



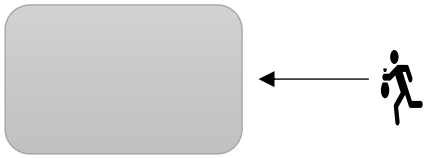
(Source : Auteur,2020)

OLYMPUS représente d'une partie une amélioration du point de vue de la sécurité informatique, car le mot de passe de l'utilisateur est divisé parmi plusieurs fournisseurs d'identité « partiels ». En conséquence, le processus d'authentification sera distribué et requerra la collaboration de tous les fournisseurs d'identité « partiels » pour l'émission du *token* (jeton) correspondant.
En ce qui concerne le vol d'identité, l'attaquant devra avoir le contrôle sur toute la structure, car le mot de passe de l'utilisateur (nécessaire pour l'émission de *tokens*) est divisé parmi les fournisseurs d'identité « partiels ». En outre, OLYMPUS

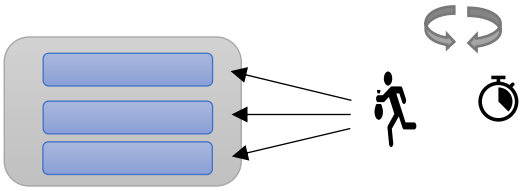
[22] R. TORRES MORENO, J. BERNABE, A. SKARMETA, M. STAUSHOLM, T. FREDERIKSEN, T., N. MARTÍNEZ ET AL., « OLYMPUS: Towards oblivious identity management for private and user-friendly services », *2019 Global IoT Summit (GIoTS)*, 2019, pp.1-6.
[23] J. BERNAL, A. SKARMETA, R. TORRES, E. TORROGLOSA ET AL., "D3.1- Requirements and Design Templates for OLYMPUS", *Horizon 2020 Project OLYMPUS* (Oblivious identitY Management for Private and User-friendly Services), 2019, pp.7-12 : https://olympus-project.eu/wp-content/uploads/2019/07/Olympus_pu_d3_1_v1.0.pdf.

comprend un mécanisme de sécurité proactif qui s'appelle *Key-Resharing* qui permet la redistribution des fragments mots de passe, créant plusieurs étapes à réaliser par l'attaquant, donc dans le cas où il réussit à compromettre l'un des fournisseurs d'identité « partiels », le segment de mot de passe obtenu restera juste valide pendant une courte période de temps[24] (Figure 2).

Figure 2. Comparaison d'un cas de vol d'identité avec un fournisseur d'identité standard vs. OLYMPUS



Compromet toute l'architecture en une seule étape



Doit compromettre tous les fournisseurs d'identité partiels

(Source : Auteur,2020)

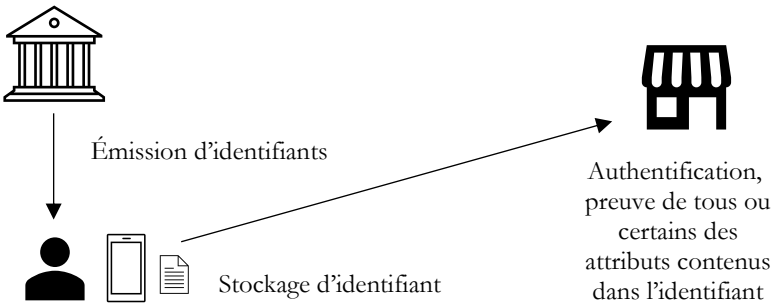
OLYMPUS combine cette architecture innovante avec l'objectif d'un fournisseur d'identité « inconscient » ou « aveugle », de sorte à ce que la vie privée de l'utilisateur soit renforcée en limitant les possibilités du fournisseur d'identité de contrôler ses mouvements en ligne. En effet, un autre objectif d'OLYMPUS est de trouver un moyen d'empêcher les mécanismes existants (*OIDC, SAML...*) de surveiller le comportement de l'utilisateur, en garantissant la confidentialité de manière à ce que le fournisseur d'identité n'ait connaissance que du fait qu'un processus d'authentification est en cours[25].

Cette innovation a déjà été réalisée dans le cas d'une utilisation hors ligne au travers d'une technique cryptographique connue sous le nom de p-ABCs qui permet le stockage de credentials pour son utilisation dans un processus d'authentification ultérieur. D'autre

[24,25] I. ALAMILLO, C. TIMÓN, J. VALERO ET AL., "D3.2- Security and Privacy-aware OLYMPUS Framework Impact Assessment", *Horizon 2020 Project OLYMPUS* (Oblivious identitY Management for Private and User-friendly Services, 2020, pp.50-53 : https://olympus-project.eu/wp-content/uploads/2020/02/Olympus_pu_d3_2_v1_0.pdf.

part, le projet, dans son état actuel, étudie cette possibilité de créer un fournisseur d'identité « inconscient » dans les cas en ligne[26].

Figure 3. Authentification à travers de p-ABCs



(Source : Auteur, 2020)

En conséquence, une technologie comme OLYMPUS pourrait mettre fin aux pratiques de surveillance développées au cours des dernières années par les fournisseurs d'identité couramment utilisés, offrant un niveau adéquat de protection de la vie privée pour les utilisateurs de ceux-ci et garantissant la protection de la vie privée dès la conception.

B) Scénarios

Dans le cadre du projet OLYMPUS deux scénarios sont envisagés. Dans le premier (scénario de dossier de crédit), l'utilisateur vise à obtenir un service financier (par exemple un prêt bancaire) auprès d'une entité financière[27]. À cette fin, il sera normalement tenu de fournir ses données sans savoir si le prêt sera finalement accordé.
Au lieu de cela, les données financières de l'utilisateur sont demandées à des sources externes valides et regroupées dans une plate-forme de fichier de crédit. À un stade ultérieur, nous utilisons OLYMPUS afin de générer un fichier de crédit anonyme à partir des données financières contenues dans la plate-forme de fichier de crédit, qui seront envoyées à l'entité financière qui n'aura pas connaissance du propriétaire des données.
Une fois ces données analysées par l'entité financière, l'utilisateur sera informé sur son adéquation pour obtenir le crédit et dans le cas où l'entité financière le confirme, l'utilisateur enverra désormais

[26] J. HESSE, A. LEHMANN, P. TOWA, "D4.1- Cryptographic design of an oblivious IdM System", *Horizon 2020 Project OLYMPUS* (Oblivious identitY Management for Private and User-friendly Services, 2019, pp. 9-34 : https://olympus-project.eu/wp-content/uploads/2019/12/Olympus_pu_d4_1_v1.0.pdf.
[27] J. BERNAL, A. SKARMETA, R. TORRES, E. TORROGLOSA ET AL., "D6.1- Use cases description*", Horizon 2020 Project OLYMPUS* (Oblivious identitY Management for Private and User-friendly Services, 2019, pp. 8-19: https://olympus-project.eu/wp-content/uploads/2020/10/Olympus_pu_d6_1_v1_1.pdf.

l'*eID token* (jeton d'identité) lié au fichier de crédit anonyme, révélant ainsi son identité réelle afin d'assumer les obligations légales correspondantes.

Malgré la complexité du respect de la réglementation bancaire (par exemple, PSD2 SCA) et l'octroi d'un prêt, en principe, anonymement, ce cas d'utilisation pourrait inciter à repenser les moyens d'éviter les préjugés et la discrimination qui restent malheureusement présents aujourd'hui dans la plupart des activités.

D'autre part, le deuxième scénario se concentre sur la preuve de l'âge à travers d'une identité mobile virtuelle (*mobile identity*), plus précisément, un permis de conduire mobile (*mobile driver's license*)[28]. L'idée est que l'utilisateur sera en mesure de s'authentifier auprès du fournisseur du service correspondant dans un scénario en ligne et hors ligne.

Ce dernier scénario sera plus respectueux de la vie privée, car il n'y aura pas de communication entre l'utilisateur et le fournisseur d'identité pour effectuer l'authentification, mais l'utilisateur utilisera une information d'identification précédemment émise.

En outre, bien que le cas d'utilisation soit envisagé pour l'épreuve de l'âge, l'utilisateur sera en mesure de choisir lequel des attributs contenus dans son permis de conduire mobile (*mobile driver's license*) il souhaite divulguer et une preuve de connaissance zéro (*ZKP*) générée par le portefeuille mobile de l'utilisateur pourrait être suffisant pour attester de l'attribut requis[29].

§ 3 – LA RÉGLEMENTATION D'UN MÉTASYSTÈME D'IDENTITÉ EUROPÉEN : UNE RÉFÉRENCE À EIDAS

Tandis qu'une possibilité pour résoudre les problématiques liées à la gestion de l'identité numérique pourrait être l'adoption de technologies plus respectueuses avec le droit à la vie privée, nous ne pouvons pas ignorer que ces technologies affecteront le modèle de business basé sur l'exploitation de données et donc que son utilisation ne serait pas volontaire de la part des fournisseurs d'identité.

D'autre part, il est nécessaire de prendre en compte que les États sont souverains pour la réglementation des services de gestion de l'identité numérique. En conséquence il est nécessaire de trouver en équilibre et de se concentrer sur la possibilité d'une réglementation des services d'identification dans l'Union Européenne qui respectera la souveraineté des États Membres et

[28] Ibidem, pp.19-34.

[29] Une *ZKP* est une méthode de vérification dans laquelle l'utilisateur est en mesure de prouver au vérificateur qu'il a connaissance d'une information particulière sans révéler l'information elle-même. Plus d'informations disponibles sur le site suivant : https://academy.binance.com/glossary/zero-knowledge-proofs

qui sera aussi cohérente avec la souveraineté numérique de l'Union Européenne[30].

Cette proposition est la réglementation de ces services par le biais d'un cadre de gouvernance d'un métasystème d'identité numérique. En ce sens, l'idée est d'éviter une réglementation directe de ces services, mais d'imposer un ensemble de conditions ou d'exigences qu'un fournisseur devra accomplir pour fournir les services dans le champ d'application de l'Union Européenne.

Le Règlement d'interopérabilité eIDAS constitue déjà un exemple de métasystème d'identité numérique. En effet, le règlement eIDAS ne régule pas directement les services de gestion de l'identité numérique, mais il établit des exigences minimales pour qu'un fournisseur d'identité puisse opérer dans le cadre de l'Union Européenne.

Le Règlement d'interopérabilité eIDAS se présente donc comme un premier exemple de métasystème de gestion de l'identité numérique. En ce sens, il établit un ensemble de règles ou de principes et de normes techniques communes, complété par des spécifications techniques qui permettent aux différents systèmes nationaux d'*eID* (identité numérique) dans l'Union Européenne d'interagir, ou en d'autres termes, un ensemble de critères communs pour l'identification et l'authentification transfrontalières.

Plus spécifiquement, le Règlement eIDAS établit un ensemble de niveaux d'assurance qui se traduisent, en partie, en un ensemble d'exigences techniques minimales, ainsi qu'un ensemble de données minimal d'identification de la personne et certaines règlementations de nature procédurale et portant sur la protection des données. Finalement, ces exigences sont complémentaires avec les conditions de reconnaissance mutuelle visées par l'article 6.1[31].

Toutefois, le Règlement eIDAS est très limité comme métasystème de réglementation de la gestion de l'identité numérique. L'effet juridique de l'identification transfrontalière n'est garanti que dans les relations avec les organismes du secteur public, qui conformément à l'article 3 (7) du Règlement eIDAS, sont définies comme « un État, une autorité régionale ou locale, un organisme de droit public ou une association constituée d'une ou de plusieurs de ces autorités ou d'un ou de plusieurs de ces organismes de droit public, ou une entité privée mandatée par au moins un ou une de

[30] F. ARTEAGA ET R. ELCANO, "La UE : a la búsqueda de la soberanía digital in Comentario Elcano", *Real Instituto elcano*, nº 34/2020, 2020 pp. 1-3: http://www.realinstitutoelcano.org/wps/wcm/connect/03e762ee-6ea1-42db-a7b2-b4997369e17a/Comentario-Arteaga-La-UE-a-la-busqueda-de-la-soberania-digital.pdf?MOD=AJPERES&CACHEID=03e762ee-6ea1-42db-a7b2-b4997369e17a.

[31] Les moyens d'identification doivent être inclus dans la liste publiée par la Commission européenne, puis ils doivent être notifiés par l'État ; ces moyens d'identification doivent avoir un niveau d'assurance égal ou supérieur à celui requis pour accéder à un service public dans l'État membre, et ce niveau d'assurance doit être élevé ou substantiel conformément le Règlement eIDAS.

ces autorités, organismes, ou associations pour fournir des services publics lorsqu'elle agit en vertu de ce mandat »[32].
En conséquence, bien que le Règlement eIDAS encourage également l'utilisation des systèmes d'identification électronique pour les opérations d'authentification transfrontalière dans l'accès à des services privés, c'est-à-dire pour les authentifications auprès des entreprises et d'autres organisations privées[33], son objectif principal est de faciliter l'accès transfrontalier aux services publics.
De même, le règlement eIDAS présente d'autres limitations dont nous discuterons ci-dessous conformément aux conclusions obtenues dans le cadre du projet de recherche OLYMPUS, qui sont, en même temps, conforme au processus d'examen actuel du règlement eIDAS visant à faciliter l'identification dans tous les types de processus au niveau européen.

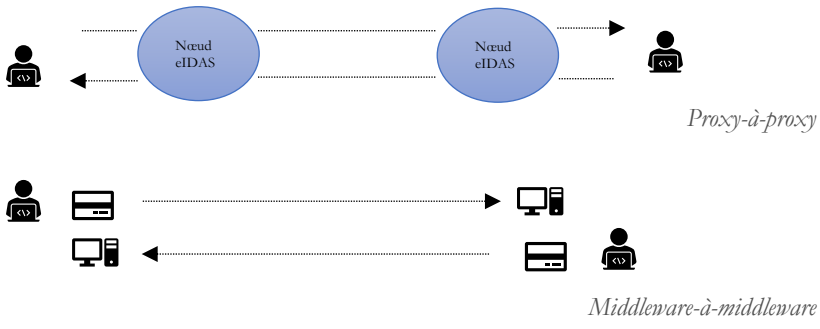
§ 4 – PROPOSITIONS D'EXTENSION DU RÈGLEMENT EIDAS COMME CADRE DE GOUVERNANCE D'UN MÉTASYSTÈME D'IDENTITÉ EUROPÉEN

Dans le cadre du projet de recherche OLYMPUS, nous avons identifié un certain nombre de limitations imposées par la législation d'*eID* (identité numérique), principalement dans le cadre de l'Union Européenne le Règlement eIDAS, qui à son tour a soulevé des possibilités de modification.
En premier lieu, l'article 7 du Règlement eIDAS stipule, entre autres conditions de reconnaissance mutuelle, que le niveau d'assurance de l'identification électronique doit être substantiel ou élevé en ce qui concerne l'accès au service en ligne.
Les règles techniques de qualification du niveau d'assurance sont contenues dans le Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015, selon lequel le moyen d'identification électronique exige au moins deux facteurs de catégories différentes, c'est-à-dire une authentification dynamique, tandis que la conception initiale d'OLYMPUS n'en exigeait qu'un seul, la connaissance du nom d'utilisateur et du mot de passe[34].
Bien que la conception actuelle d'OLYMPUS contient une authentification à double facteur, la conception initiale d'OLYMPUS obtenait un niveau de sécurité élevé même sans inclure celui-ci, cela démontre donc qu'il est possible qu'un moyen d'identification électronique qui ne repose pas sur l'authentification

[32] I. ALAMILLO DOMINGO, "*Identificación electrónica…",* op.cit., pp.41-56
[33] Cette idée est contenue dans le considérant 17 du Règlement eIDAS, car cette harmonisation faciliterait les transactions des parties d'utilisateurs privés, qui sont de plus en plus assujetties à des exigences plus strictes en matière d'identification.
[34] M. STAUSHOLM, T. FREDERIKSEN ET AL, "D3.3 Olympus Blueprint", *Horizon 2020 Project OLYMPUS* (Oblivious identitY Management for Private and User-friendly Services, 2020, pp.25-27:
https://olympus-project.eu/wp-content/uploads/2020/10/Olympus_pu_d3_3_v1_0.pdf.

à double facteur puisse atteindre une sécurité égale, ou supérieure à ceux qui envisagent cette forme d'authentification[35].
Cela serait également contraire au principe de neutralité technologique, car les organisations et les particuliers ne pourraient pas utiliser différents moyens d'identification électronique par rapport aux méthodes d'authentification multi-facteurs pour les opérations transfrontalières[36].
En conséquence, il est nécessaire de revoir cette exigence et de l'adapter aux possibilités technologiques d'aujourd'hui pour permettre des conceptions différentes qui offrent la même protection, voire une protection plus élevée, que l'authentification multi-facteurs.
D'autre part, nous avons soulevé tout au long de cet article les possibilités qu'OLYMPUS représente en termes d'amélioration de la vie privée de ses utilisateurs grâce à un fournisseur d'identité « inconscient », qui perd le contrôle sur les processus d'authentification des utilisateurs. Toutefois, les améliorations réalisées dans la limitation des pratiques de surveillance pourraient être perdues dans le contexte d'une authentification transfrontalière par le biais de nœuds eIDAS.
Plus précisément, le « pont » qui caractérisait l'approche *proxy* place le nœud dans une position privilégiée pour contrôler les communications qui s'y déroulent (Figure 4). C'est toutefois la configuration habituelle dans laquelle le fournisseur du service de l'État membre contacte un *proxy* qui fonctionne comme un « pont » pour entrer en contact avec le fournisseur d'identité situé dans l'État membre envoyant.

Figure 4. Approche *Proxy* vs. *Middleware*



(Source : Auteur, 2020)

Malgré ses avantages en termes d'interopérabilité, l'approche par *proxy* soulève des préoccupations en matière de protection de la vie privée, car ce nœud eIDAS centralisé chargé d'établir ce « pont »,

[35] Dans le cas d'OLYMPUS, la sécurité est obtenue grâce à une cryptographie qui permet l'authentification distribuée, comme expliquée dans la section sur le projet.
[36] Cela est contraire à ce qui est énoncé au considérant 16 du règlement eIDAS, « les exigences établies devraient être neutres sur le plan technologique » et « il devrait être possible d'atteindre les exigences de sécurité nécessaires par le biais de différentes technologies ».

contrôle les opérations d'authentification transfrontalière qui s'y déroulent[37].

En conséquence, il serait intéressant de considérer l'approche par *middleware*. Cette configuration est envisagée par le *nPA* allemand (carte d'identité allemande) Dans ce cas, la communication a lieu entre les appareils, il n'y a donc pas d'intermédiaire dans le processus de communication.

En tant que désavantage, cette approche nécessite l'installation préalable du logiciel capable d'établir cette communication par l'État Membre d'accueil. C'est complexe, car cela pourrait nécessiter une technologie unifiée dans l'Union Européenne. Toutefois, dans un scénario où les deux États membres sont équipés d'un *middleware* (c'est-à-dire une approche *middleware*-à-*middleware*), la vie privée sera garantie.

D'autre part, nous avons trouvé une autre limitation en ce qui concerne l'ensemble minimal de données requis par eIDAS, plus précisément le Règlement d'exécution (UE) 2015/1501 de la Commission du 8 septembre 2015 vise à exclure ces techniques pour limiter la quantité de données divulguées au fournisseur du service. Cela affecte en particulier le cas d'utilisation du permis de conduire mobile (*mobile driver's license*) que nous avons exposé ci-dessus.

Conformément à ce règlement, afin d'être un moyen d'identification notifiable en vertu du Règlement eIDAS dont l'acceptation serait obligatoire pour les autres États Membres, il devra envisager la divulgation complète de l'ensemble minimal de données contenu dans le Règlement d'exécution (UE) 2015/1501, (nom, prénom, date de naissance et identificateur unique), ce qui, d'autre part, nous fera perdre la principale amélioration que ce scénario introduit[38].

Finalement, du point de vue du Règlement eIDAS, nous pouvons voir que l'identification électronique est une collection de services publics électroniques, contrairement aux services de confiance qui sont de nature très commerciale. En l'espèce, nous constatons que la première limitation concerne la prestation de services d'identification électronique par des entités privées, étant donné que l'identification électronique ne constitue pas elle-même un service de confiance, par conséquent, elle ne pourrait pas être fournie en vertu de l'eIDAS par une entité privée.

Cela ne signifie pas que les moyens d'identification électronique ne peuvent pas être émis par le secteur privé, ni qu'ils ne sont pas reconnus, mais que cette activité est menée conformément au droit

[37] C. TIMÓN, N. PONTE ET AL., "D5.3 OLYMPUS support for extended eID models", *Horizon 2020 Project OLYMPUS* (Oblivious identitY Management for Private and User-friendly Services, 2020, pp.16-17: https://olympus-project.eu/wp-content/uploads/2020/10/Olympus_pu_d5_3_v1_0.pdf.

[38] Ibidem, p.21.

national, ou d'une manière auto réglementée fondée sur des accords entre les parties.
Néanmoins, il n'y a pas d'exclusion complète dans la prestation de services d'identification par des entités privées, car certains services de confiance permettent l'identification. C'est le cas des certificats à l'appui des signatures électroniques avancées, compte tenu du fait que cette possibilité doit être autorisée par la loi nationale.
Cela est dû au fait qu'une signature électronique préalable est « capable d'identifier le signataire », selon l'article 26 b) du règlement eIDAS, en particulier lorsqu'elle est basée sur un certificat qualifié, parce qu'un certificat signifie une attestation électronique qui relie les données de validation électronique à une personne naturelle et confirme au moins le nom ou le pseudonyme de cette personne (article 3 (14) du Règlement eIDAS), et cette confirmation est présumée être légalement vraie lorsque le certificat est qualifié. Dans tous les cas, ces certificats électroniques doivent être utilisables pour signer le document ainsi qu'à des fins d'identification. Dans le cas contraire, ce dernier type de certificats serait exclu de l'eIDAS[39].

CONCLUSION

Au début de cet article, nous avons expliqué différents systèmes ou modèles pour la gestion de l'identité numérique. Parmi ces modèles, il semble clair que les modèles fédérés ou décentralisés offrent une plus grande sécurité et une plus grande garantie de confidentialité que les modèles centralisés.
Toutefois, il serait nécessaire de réaliser une étude qui fasse une comparaison entre les modèles fédérés ou décentralisés afin de déterminer lequel d'entre eux offre les meilleures possibilités selon le secteur concerné. De même, des technologies telles que celle exposée par rapport au projet OLYMPUS, qui fait partie de modèles fédérés mais soutient la décentralisation par le biais de technologies distribuées autres que la blockchain, devraient être considérées.
Afin de déterminer si une technologie innovante est appropriée pour la gestion de l'identité numérique, il convient d'examiner si elle établit un juste équilibre entre la sécurité et la vie privée des utilisateurs. À cette fin, il peut être intéressant de procéder à une Analyse d'impact relative à la protection des données (AIPD). Toutefois, cet outil est spécialement conçu pour un cas d'utilisation particulier, il pourrait donc être intéressant d'envisager une adaptation de cet outil pour l'analyse abstraite d'une technologie particulière avant de la mettre en œuvre.
Quoi qu'il en soit, il convient de noter que l'adoption de telles technologies entre en collision avec le modèle d'affaires de capitalisation des données, de sorte à ce que nous ne pouvons pas

[39] I. ALAMILLO DOMINGO, "*Identificación electrónica…",* op.cit., pp.41-56.

nous attendre à ce que le marché s'auto réglemente pour son adoption, en particulier en ce qui concerne les acteurs privés. Par conséquent, de telles limitations ou exigences doivent être imposées sous forme de réglementations.
La réglementation des services d'identification fait partie de la souveraineté de chaque État, et une identité paneuropéenne est loin d'être possible. Par conséquent, la meilleure option pour assurer le Marché Numérique Unique est via l'harmonisation de ces services. L'harmonisation de ces services au niveau de l'Union Européenne est principalement contenue dans le règlement eIDAS, mais elle ne répond pas aux besoins actuels posés par l'identification électronique transfrontalière. Premièrement, sa portée n'est pas suffisante, car elle se limite principalement au secteur public. De même, il limite l'introduction de techniques d'amélioration de la vie privée, présentant ainsi des incohérences avec les réglementations européennes en matière de protection des données. Enfin, cette réglementation représente un degré élevé de centralisation par le biais de nœuds eIDAS et le placement de l'État comme garant des processus d'authentification transfrontaliers.
Finalement, la participation d'entités privées conformément au règlement eIDAS est très limitée. Tant qu'elles ne sont pas qualifiées comme des services de confiance, son activité sera régie par la Directive sur le Commerce Électronique 2000/31/EC, qui, toutefois, ne prévoit pas de réglementation spécifique pour ces services.

BIBLIOGRAPHIE

Articles

ALPÁR H., HOEPMAN J.-H., & SILJEE J., "The Identity Crisis. Security, Privacy and Usability Issues in Identity Management", *arXivLabs*, Cornell University, 2011: http://arxiv.org/abs/1101.0427 (consulté le 25 novembre 2020)

ARTEAGA F., ELCANO R. I., "La UE: a la búsqueda de la soberanía digital", *Comentario Elcano*, nº 34/2020, 2020: http://www.realinstitutoelcano.org/wps/wcm/connect/03e762ee-6ea1-42db-a7b2-b4997369e17a/Comentario-Arteaga-La-UE-a-la-busqueda-de-la-soberania-digital.pdf?MOD=AJPERES&CACHEID=03e762ee-6ea1-42db-a7b2-b4997369e17a (consulté le 27 novembre 2020) [espagnol]

CAVELTY M. D., MAUER V., KRISHNA-HENSEL S. F., "Power and security in the information age: Investigating the role of the state in cyberspace", *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace* (Issue August), 2016 : https://doi.org/10.4324/9781315601793 (consulté le 27 novembre 2020)

CHAWKI M., ABDEL WAHAB M., "Identity theft in cyberspace: Issues and solutions", *Lex Electronica,* Vol. 11, nº 1, 2006 : https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/9563/articles_54.pdf?sequence=1 (consulté le 26 novembre 2020)

FRITSCH L., "Identity Management as a target in cyberwar", *Open Identity Summit 2020*, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn, 2020 : https://dl.gi.de/bitstream/handle/20.500.12116/33182/proceedings-05.pdf?sequence=1&isAllowed=y#:~:text=Identity%20management%20(IdM)%20is%20an,the%20level%20of%20a%20genocide (consulté le 3 decembre 2020)

HALPERIN R., BACKHOUSE J., « A roadmap for research on identity in the information society », *Identity in the Information Society*, Vol. 1, nº 1, Springer, 2008 : https://doi.org/10.1007/s12394-008-0004-0 (consulté le 27 novembre 2020)

LEE H., JEUN I., JUNG H., "Criteria for evaluating the privacy protection level of Identity Management Services", *Proceedings – 2009. 3rd International Conference on Emerging Security Information,* Systems and Technologies, SECURWARE 2009, IdM, 2009 : https://doi.org/10.1109/SECURWARE.2009.31 (consulté le 25 novembre 2020)

MALER E., REED D., "The Venn of identity", *IEEE Security and Privacy*, Vol. 6, nº 2, 2008 : https://doi.org/10.1109/MSP.2008.50 (consulté le 25 novembre 2020)

MALIK A. A., ANWAR H., SHIBLI M. A., "Federated Identity Management (FIM): Challenges and opportunities", *Proceedings - 2015 Conference on Information Assurance and Cyber Security, CIACS 2015*, 1, 2016 : https://doi.org/10.1109/CIACS.2015.7395570 (consulté le 25 novembre 2020)

MARTÍNEZ MARTÍNEZ R., "El derecho fundamental a la protección de datos: perspectivas", *Revista de Internet, Derecho y Política (IDP)*, nº 5, 2007 [espagnol]

MITSILEGAS V., "Surveillance and Digital privacy in the Transatlantic War on Terror: The Case for a Global Privacy Regime", *Columbia Human Rights Law Review,* Vol. 47, nº 3, 2016.

POUNDER C. N. M., "Nine principles for assessing whether privacy is protected in a surveillance society", *Identity in the Information Society*, vol. 1, n° 1, 2008 : https://doi.org/10.1007/s12394-008-0002-2 (consulté le 3 decembre 2020)

RAHMAN S., FEROZ A. M. A., KHAN A., "Online Identity Theft and Its Prevention Using Threshold Cryptography", *International Journal of Computer Science and Network Security (IJCSNS)*, Vol. 10, nº 9, 2010.

http://paper.ijcsns.org/07_book/201009/20100904.pdf (consulté le 26 novembre 2020)

TORRES MORENO R., BERNABE J., SKARMETA A., STAUSHOLM M., FREDERIKSEN T., MARTÍNEZ N., ET AL., "OLYMPUS: Towards oblivious identity management for private and user-friendly services", *2019 Global IoT Summit (GIoTS)*, 2019.

VERMEULEN M., BELLANOVA R., "European Smart Surveillance: What's at stake for Data Protection, Privacy and Non-Discrimination", *Security and Human Rights*, Vol. 23, nº 4, 2012.

Monographies

ALAMILLO DOMINGO I., "Identidad electrónica, robo de identidad y protección de datos personales", in Rallo Lombarte A., Arroyo Zapatero L. (Coll.), *Robo de Identidad y Protección de Datos en la red*, Agencia Española de Protección de Datos, Thomson Reuters (Legal) Limited ,2010 [espagnol]

ALAMILLO DOMINGO I., "Identificación electrónica y confianza en las transacciones electrónicas la regulación jurídico-administrativa de las instituciones de acreditación de la actuación electrónica", *DIGITUM*, Universidad de Murcia, 2018 : https://digitum.um.es/digitum/bitstream/10201/61019/6/Ignacio%20Alamillo%20Domingo%20Tesis%20Doctoral.pdf [espagnol]

ALLENDE LÓPEZ M., "Self-Sovereign Identity: The Future of Identity: Self Sovereignity, Digital Wallets, and Blockchain", *IDB*, 2020 : https://doi.org/10.18235/0002635

PETKOVIC M., JONKER W., "Security, Privacy and Trust in Modern Data Management (Data-Centric Systems and Applications)", *Sringer-Verlag*, Berlin, Heidelberg, 2007.

Documentation de projet

ALAMILLO I., TIMÓN C., VALERO J. ET AL., "D3.2- Security and Privacy-aware OLYMPUS Framework Impact Assessment", *Horizon 2020 Project OLYMPUS* (Oblivious identitY Management for Private and User-friendly Services, 2020, pp. 50-53 : https://olympus-project.eu/wp-content/uploads/2020/02/Olympus_pu_d3_2_v1_0.pdf]

BERNAL J., SKARMETA A., TORRES R., TORROGLOSA E. ET AL., "D3.1-Requirements and Design Templates for OLYMPUS", *Horizon 2020 Project OLYMPUS* (Oblivious identitY Management for Private and User-friendly Services), 2019 : https://olympus-project.eu/wp-content/uploads/2019/07/Olympus_pu_d3_1_v1.0.pdf

BERNAL J., SKARMETA A., TORRES R., TORROGLOSA E. ET AL., "D6.1-Use cases description", *Horizon 2020 Project OLYMPUS* (Oblivious identitY Management for Private and User-friendly Services, 2019: https://olympus-project.eu/wp-content/uploads/2020/10/Olympus_pu_d6_1_v1_1.pdf

HESSE J., LEHMANN A., TOWA P., "D4.1 Cryptographic design of an oblivious IdM System", *Horizon 2020 Project OLYMPUS* (Oblivious identitY Management for Private and User-friendly Services, 2019 : https://olympus-project.eu/wp-content/uploads/2019/12/Olympus_pu_d4_1_v1.0.pdf]

STAUSHOLM M., FREDERIKSEN T. ET AL., "D3.3 Olympus Blueprint", *Horizon* 2020 Project OLYMPUS (Oblivious identitY Management for Private and User-friendly Services, 2020, pp. 25-27: https://olympus-project.eu/wp-content/uploads/2020/10/Olympus_pu_d3_3_v1_0.pdf

TIMÓN C., PONTE N. ET AL., "D5.3 OLYMPUS support for extended eID models", *Horizon* 2020 Project OLYMPUS (Oblivious identitY Management for Private and User-friendly Services, 2020 : https://olympus-project.eu/wp-content/uploads/2020/10/Olympus_pu_d5_3_v1_0.pdf

LÉGISLATION ET JURISPRUDENCE

Réglementation

Convention Européenne des Droits de l'homme, Cour européenne des droits de l'homme Conseil de l'Europe, F-67075 Strasbourg cedex : https://www.echr.coe.int/Documents/Convention_FRA.pdf

Règlement (UE) 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, J.O. L 257/73-257/114 (28 août 2014) : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014R0910&from=FR

Règlement d'exécution (UE) 2015/1501 de la Commission du 8 septembre 2015 sur le cadre d'interopérabilité visé à l'article 12, paragraphe 8, du règlement (UE) no 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur J.O. L 235/1 (9 septembre 2015) : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32015R1501&from=EN

Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures

minimales relatives au niveau de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement (UE) no 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, J.O. *L.* 235/7 (9 septembre 2015) :
https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32015R1502&from=EN

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), J.O. L.119/1 (4 mai 2016) :
https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Traité sur l'Union Européenne, J.O. C 326/13 (16 octobre 2012)
https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0002.02/DOC_1&format=PDF

Traité sur le fonctionnement de L'Union Européenne, J.O. C 326/47 (26 octobre 2012) :
https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:12012E/TXT&from=FR

Jurisprudence

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others. C: 2014/238 (rendu le 8 avril 2014)

Mr Roman Andreyevich Zakharov vs. Russian Federation C: 47143/06 (rendu le 4 decembre 2015)