Calling for the recognition of a right to multiple digital identities[1]

Claire Levallois-Barth (claire.levallois@imt.fr)

Coordinator of the Chair VP-IP, Lecturer/Researcher at the Télécom Paris School

Civil identity, real identity, personal identity, biological identity, professional identity, civic identity.

Such possible identities, whether forced or desired, highlight the need to ascertain that an individual actually is who he or she claims to be or who one believes him or her to be. Identities are compelling us to define a new social structure that relies on legal acts, especially, at the European level, acts on means to identify people at borders, on electronic identification[i] or on the security of EU citizens' identity cards.[ii] At the French level, institutions involved in this debate, i.e., the inter-ministerial mission on secured digital identity solutions,[iii] the French Digital Council[iv] and the National Assembly,[v] confirm the importance of such challenges.

Among the topics addressed, we would like to focus on the issue of users' control over their identities and on the difficulties in defining the notion of digital identity. In philosophy, one way to address such issue is to distinguish between the *idem* and *ipse* identities. '[T]*he* idem *identity corresponds to a view on the individual from the outside, which treats the individual as a sum of stable characteristics. The* ipse *identity [...] corresponds to the individual as he or she relates to him/herself.*'[vi] Law, on the other hand, uses an objective approach by defining the concept of 'identity' as '*what makes an individual him- or herself and not another; by extension, what allows to recognize and distinguish him or her from others; [...] the set of characteristics that allow to identify him or her*'.[vii]

Yet, this does not mean digital identity is civil identity transposed into cyberspace. The exponential increase in the types of attributes made possible by dematerialisation thus highlights the need to refer not to **a** digital identity, but indeed to digital identit**ies** (I). While our identities are constructed and attributed by public and private actors, we should not lose sight of the need to identify the conditions for individuals to act autonomously for them to be able to define by themselves the way they intend to present themselves to others (II). Taking both aspects into account – objective and subjective identity – is of utmost importance from our point of view. This distinction, to us, calls for the recognition of a right to multiple identities.

I. Digital identities: a polysemic notion

from a civil law approach, identity is defined as the way the individual is perceived by the State, especially through the verification of civil status. This external glance considers a person as a sum of

[1] Summary of the article for publication in a book by Larcier following the Study Day organized by the Institute of Private Law, Toulouse Capitole University: *L'identité numérique : quelle définition pour quelle protection ?*, on 12 Dec. 2019.

stable characteristics – surname, first name, direct line of descent, birthplace and date of birth, and gender – that identify him or her unequivocally and continuously.[viii] This aims at strengthening the Nation-State's control over the abstractly considered person.[ix] The potential changes in some traditional components of civil status – gender, surname – may lead to the use of new attributes such as numbers ('*social security number*,' persistent unique identifier)[x] or body features (DNA, iris, hand, voice, vein network). Following this logic, a facial image and two fingerprints, supposed to provide failproof identification, contribute to strengthening the security of identity cards,[xi] biometric passports,[xii] as well as of almost every large-scale information system in the context of border management and public order in the European Union.[xiii]

Thus, more and more types of attributes are being considered when characterising an individual. This increase aims not only to help better identify a person – for security purposes and to create a climate of trust when using online public or private services – but also to single him or her based on highly variable elements. The case law on identity theft[xiv] has penalised, among others, setting up a fake Facebook account using a third party's first name and surname and featuring personal photographs.[xv]

Developed around a hard core of attributes deemed most stable, a person's digital identity can be seen as the combination of lots of personal data,[xvi] spread in the virtual or real world. There is no longer a need to enquire about the person's name. Technologies now allow to '*attribute certain decisions to him or her since the individual's contact point (a computer) no longer necessarily requires the disclosure of his or her* ***identity in the narrow sense***'.[xvii] It is thus important to consider the impact of using a set of information on a person[xviii] that can help to track and single out a person (and thus, to treat them differently).[xix]

The choice and the promotion of those elements can be voluntarily decided by the person as what, in his or her mind, characterises him or her. Beside such **personal digital identity**, individualisation can be initiated by private actors,[xx] not by merely defining several standard profiles, but, in the age of Artificial Intelligence, by modelling human behaviours based on individually a-significant data.[xxi] A new kind of identity is emerging: the **algorithmic digital identity**. Such calculated identity is part of a general movement of reified persons and is bound to provide a partial and distorted view of these persons. Such identity should not be confused with the **civic digital identity**, defined as civil status adapted to the digital era, based on several criteria deemed stable (surname, first name, unique identifier persistent in time, biometric data).

However, such perception of digital identities, which are turning human beings into a static object, raises concern. Should these identities be determined only by private actors and the State? What about our individualities and the opportunity to build ourselves on our own initiative and, finally, to avoid algorithmic confinement?

II. Individual autonomy in defining one's digital identities

Digital identity should also be understood as the possibility for a person to '*project*' him- or herself by choosing the elements he or she wishes to be represented and recognised. This *ipse* refers to identity as voluntarily and actively opening up to others and to society.

The recognition of everyone's right to establish the components of their identity is based on an interpretation of the right to respect for one's private life recognised by Article 8 of the European Convention on Human Rights.[xxii] '*Private life*' is therefore a functional, even extensive, notion. In this

respect, '*Article 8 protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world*'.[xxiii] Establishing details of one's physical and social identity as a human being contributes to this personal development, as an individual's entitlement to such information is of importance because of its formative implications for his or her personality.[xxiv]

Identity being built by the person seeking its components can be explained by the claim to align such components with the experienced identity. It is a requirement for our personalities to develop and our dignities to be respected, '*provided that dignity is extended to the Kantian sense, i.e. as a requirement for considering others as an end, not as a means*'.[xxv] Thus, the **European Court of Human Rights** (ECHR) does not grasp the right to respect for one's private life **only as the protection of a person's privacy** out of the sight of third parties, but also construes this right as an opening to the outside world allowing to '*develop relationships with other human beings*' and, more broadly, as the right to personal autonomy.[xxvi]

It is thus for our democratic society to guarantee that we can be involved in the construction of our future identity, but also that we can make some parts of our past disappear.[xxvii] The issue at stake is the respect for individuals' free choice of information . It is not a textbook case, as testifies the 'real name' policy implemented among others by Facebook, which has led the network to delete accounts belonging to transgender persons, drag queens, homosexuals, Native Americans, and political dissidents.

The difficulty thus lies in maintaining some form of control in a digital environment where individuals have less and less of it. Guaranteeing a person a certain control over his or her identities implies looking at the contexts in which the person expresses his or her complexity. We do not share the same information, nor do we build the same relationships in our family, work, friend or leisure circles. This has been confirmed by the survey carried out by the Chair on Values and Policies of Personal Information with Médiamétrie in April 2019.[xxviii]

Nevertheless, many actors seem to go against such requirement for **contextualized identities**. Digital companies are investing in business sectors that used to be compartmentalized (culture, information, finance, insurance…). The same 'private' identity is indifferently used to make online purchases, take part in political forums, or in professional contexts. Like Facebook Connect, Apple ID or Microsoft's Azure ID, the Google identity, which is almost inevitably required to connect to thousands of third-party services, contributes to locking up a person inside their respective ecosystems. Another notable trend is the unification of the civic and private digital identities. Since 2002, Estonia has been using the electronic ID card both as its national ID card and as a means to identify citizens for online public and private services.[xxix] This strong tendency to merge contexts that are *a priori* not connected is reinforced by the improvement of the security level of 'private' identities, which are so far made available by very few actors.[xxx]

***

Such choices cannot be made outside of a democratic control based on cumulative one-off initiatives. In order not to be affected by the impact of a unique generalised identification by any actor, the effectivity of the right to privacy needs to be strengthened by the recognition of a **new subjective right – the right to multiple digital identities**; exercising that right would guarantee personal development. Such right would cover the right not to disclose one's real identity and not to be forced

to representation. It would help maintain some form of anonymity. To answer the defying political class's objection,[xxxi] one might argue that this anonymity is relative. The competent authority is still entitled to request the internet service provider to disclose the user's identity and to trace back a message.

While using one's civic identity should only be required when necessary to avoid permanent tracking, alternative identities may, if needed, be derived from the stable identity, provided the person is granted the possibility to choose the granularity of the details he or she wishes to disclose. Finally, the right to multi-identity is a relative right. As any right, it should be understood as the balance of the interests at stake, i.e., between any individual's legitimate need to present him- or herself the way he or she pleases and the protection of the interests of third parties and of the general interest by using a civic identity.

In conclusion, two points of view need to be reconciled – the objective digital identity, established by authorities or external actors, and the subjective digital identity, rather determined by one's choices. In this sense, GDPR is only a protective layer to which other layers should be added. There is a potential emergency. If the law does not adapt to the increasingly rapid changes of our time, it will be led to endorse the technological solutions already deployed.[xxxii]

---

[i] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJEU L 257/73 of 28.8.2014 (eIDAS Regulation), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=FR.

[ii] Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement, OJEU L 188/67 of 12.7.2019 (ID Card Regulation), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R1157. In practical terms, France needs to develop its national identity card by August 2021.

[iii] Valérie Peneau's mission letter signed on 5 January 2018 by then French Minister of the Interior Gérard Collomb, Minister of Justice Nicole Belloubet, and Secretary of State for Digital Affairs Mounir Mahjoubi. https://www.interieur.gouv.fr/Archives/Archives-ministres-de-l-Interieur/Archives-Gerard-Collomb-mai-2017-octobre-2018/Communiques-du-ministre/Mise-en-place-de-solutions-d-identite-numerique-securisee-lancement-d-un-programme.

[iv] French Digital Council, *Identités numériques. Clés de voûte de la citoyenneté numérique* [Digital identities – The cornerstone of digital citizenship], June 2020 Report, https://cnnumerique.fr/files/uploads/2020/2020.06_rapport_cnnum_idnum_web.pdf.

[v] Information report submitted pursuant to Article 145 of the Rules of Procedure by the joint fact-finding mission on digital identity and presented by Ms. Marietta Karamanli, President, Ms. Christine Hennion and Mr. Jean-Michel Mis, rapporteurs, MPs, recorded at the Presidency of the National Assembly on 8 July 2020, http://www.assemblee-nationale.fr/dyn/15/rapports/micnum/l15b3190_rapport-information.pdf.

[vi] A. Khatchatourov, 'Digital Regimes of Identity Management: From the Exercise of Privacy to Modulation of the Self', in *Digital Identities in Tension: Between Autonomy and Control*, A. Khatchatourov with P.-A. Chardel, A. Feenberg and G. Peries, London, ISTE Editions, 2019, p. 30.

[vii] G. Cornu (G.) (dir.), *Vocabulaire juridique*, 8th edition, Paris, P.U.F., « Quadrige », 2007, p. 463. Loosely translated from the French.

[viii] '*An interrupted continuity between the first and the last stage in the development of what we consider to be the same individual. […] Thus, we say of an oak tree that it is the same from the acorn to the fully developed tree.*' Paul Ricœur, Soi-même comme un autre, 1990, éd. Le seuil, p. 142.

[ix] In this sense, J. Rochfeld, *Les grandes notions du droit privé* [Key notions of private law], PUF, 2013, 2nd edition, p. 40.

[x] The EU eIDAS Regulation and its Implementing Regulation 2015/1501 require, aside from standard information such as the '*current family name(s)*', '*current first name(s)*' and date of birth, a '*unique identifier […] which is as persistent as possible in time*' to be constructed by each Member State. These four elements make for a minimum set of person identification data that should '*uniquely*' represent the person, therefore enabling his or her identity. What is sought here is indeed the continuity of individualisation. Annex to Commission Implementing Decision (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of the aforementioned eIDAS Regulation, OJEU L 235/1 of 9.9.2015.

[xi] Art. 3(5) of the ID card Regulation, aforementioned.

[xii] Art. 1(2) of Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJEU L 385/1 of 29.12.2004, as amended by Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009, EUOJ L 142 of 6.6.2009.

[xiii] In order to make easier mainly the identification of non-EU citizens who enter or try to enter EU territory, two EU regulations were adopted on 20 May 2019 to establish the conditions for interoperability between information systems in the fields of borders and visas (Regulation 2019/817) as well as of police and judicial cooperation, asylum and migration (Regulation 2019/818). No fewer than eight information systems are involved: the Schengen Information System (SIS), Eurodac, the Visa Information System (VIS), the Interpol database of Stolen and Lost Travel Documents (SLTD database) and Europol data, as well as three new systems: the Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS), and the European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN). All but ETIAS store fingerprints and will eventually include a facial image. The SIS also includes a palm print.

[xiv] In particular, Art. 226-4-1 of the French Criminal Code, introduced by the law of 14 March 2011, provides that: '*the act of impersonating a third party or making use of data of any kind to identify a person in order to disturb their tranquillity or that of others, or damage their honour or consideration, is punishable by one year's imprisonment and a fine of €15,000*'. Framework law No 2011-267 of 14 March 2011 for the performance of interior security ('*Loi d'orientation et de programmation pour la performance de la sécurité intérieure*' or 'LOPPSI 2'), French OJ of 15 March 2011, p. 4582.

[xv] Tribunal de grande instance (Court of First Instance), 17th division, Judgment of 24 March 2015, V. P. and F. Z./A. S. and K. G, https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-17e-chambre-correctionnelle-jugement-du-24-mars-2015/.

[xvi] The General Data Protection Regulation (GDPR) defines this notion as '*any information relating to an identified or identifiable individual*' – 'identifiable' individual meaning '*one who can be identified, directly or indirectly, in particular by reference to an identifier [...] or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*'. Art. 4(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter 'GDPR'), OJEU L 119 of 4.5.2016, p. 1.

[xvii] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP 136, 20 June 2007, p. 15.

[xviii] Information created in particular by networks, smart objects, facial recognition software.

[xix] In this sense, see Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data as updated by CETS amending protocol n°223 adopted on 18 May 2018 (Convention 108+), §18 of the explanatory report, which states that: '*This "individualisation" could be done, for instance, by referring to him or her specifically, or to a device or a combination of devices (computer, mobile phone, camera, gaming devices, etc.) on the basis of […] an IP address, or other identifier*.'

[xx] In behavioural advertising, for instance, users are singled out based on a single digital fingerprint stored remotely, on the operator's server. The fingerprint is computed based among other things on the various fonts installed and used by their browser, network connections or the audio fingerprint of their computer. Using

such information separately may seem innocuous, yet it is very unlikely that two computers have the same font list.

[xxi] As Antoinette Rouvroy puts it, '*therefore, we are often no longer identifiable as authors or senders of data that "matters" and that rules us: "raw data", which is de facto carefully emptied of any tracks of its original context and of any singular meaning… As a result, contradicting the widespread intuition, we might have never been, in our respective singularities, as poorly visible as we are in the digital environment. […] We are no longer 'authoritative' as individuals; we can no longer give an account of ourselves faced with algorithmic profiling. […] What is real […] does not matter.'* A. Rouvroy, '*Des données sans personne : le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des Big Data*' [Personless data: The fetish of personal data vs. the Big Data ideology], Annual study of the French Council of State 'Le numérique et les droits fondamentaux', Paris, 2014, p. 3, https://works.bepress.com/antoinette_rouvroy/55/. Loosely translated from the French.

[xxii] Art. 8(1) of the European Convention on Human Rights provides that '*Everyone has the right to respect for his private and family life, his home and his correspondence*'.

[xxiii] ECHR, *Case of Bensaid v. the United Kingdom*, No. 44599/98, Judgment of 6 February 2001, §47.

[xxiv] ECHR, *Case of Mikulić v. Croatia*, No. 53176/99, Judgment of 7 February 2002. See also ECHR, *Odièvre v. France* [GC], No. 42326/98, §29, 2003-III, which refers to '*the vital interest protected by the Convention in obtaining information necessary to discover the truth concerning important aspects of one's personal identity*'.

[xxv] Y. Poullet, *La vie privée à l'heure de la société du numérique* [Private life in the digital society], 2018, Larcier, CRIDS, p. 76. Loosely translated from the French.

[xxvi] In this sense, ECHR, *Case of Pretty v. the United Kingdom*, No. 2346/02, Judgment of 29 April. 2002, 2002-III, §61, on a request for assisted suicide: '*the Court considers that the notion of personal autonomy is an important principle underlying the interpretation of* [Article 8] *guarantees*'.

[xxvii] In this sense, Article 17 of GDPR, aforementioned, provides a partial solution by establishing the new right to erasure or 'right to be forgotten'.

[xxviii] Chair on Values and Policies of Personal Information, Second survey on personal data – summary of results, April 2019, https://cvpip.wp.imt.fr/2019/09/26/31-octobre-2019-18e-rencontre-deuxieme-enquete-cvpip-mediametrie/.

- On forums, blogs or news websites, 8% of Internet users use an alternative identity and 75% use a pseudonym;
- on online shopping websites, 90% use their 'real' first name and surname;
- when using social networks, fake first and last names or pseudonyms were said to be used by 47% of respondents on non-professional networks and by 29% on professional networks.

[xxix] Tax payment, medical consultations and purchase of prescription medication, voting, access to public transportation, access to children's school results, agricultural subsidy request, and so on.

[xxx] For now, identity providers mostly offer a 'low' eIDAS guarantee level. For instance, as of 4 June 2020, a user of the France Connect identity federation system may choose one of six offers if he or she wishes to have a 'low' guarantee level: impots.gouv.fr, ameli.fr, L'Identité Numérique La Poste, MobileConectetmoi, msa.fr and Alicem). However, in order to get a 'substantial' guarantee level, he or she has no choice but to use La Poste's L'Identité Numérique (digital identity).

[xxxi] 2nd 'great national debate', 18 Jan. 2019, '*Emmanuel Macron avance à découvert sur la levée de l'anonymat sur la toile*' [Emmanuel Macron moves forward with waiving online anonymity], Zdnet, 24 January 2019, https://www.zdnet.fr/actualites/emmanuel-macron-avance-a-decouvert-sur-la-levee-de-l-anonymat-sur-la-toile-39879737.htm.

[xxxii] The strengthening of the security of citizens' identity cards provides a good example. The European Data Protection Supervisor 'EDPS) points out that it is not possible to opt for technologies that store and compare images of fingerprints (1st technology), even though they limit the risk of impersonation in case of a personal data breach. For purposes of making already deployed national systems interoperable, technologies that store and compare a set of fingerprints should be chosen (2nd technology), as it is impossible for a State that has already implemented the 1st technology to obtain fingerprint images from 2nd-technology minutiae. EDPS

Opinion 7/2018 on the Proposal for a Regulation strengthening the security of identity cards of Union citizens and other documents of 10 August 2018, §45-48, https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_en.pdf.