

ACTUALITÉS JURIDIQUES CONCERNANT LE NUMÉRIQUE

n° 3-231122

Le Pôle Numérique FDCA tient à mettre en avant ses membres. Ceux-ci ont désormais la possibilité de se présenter sur le site internet du PN en présentant leurs recherches actuelles, centres d'intérêts et domaines d'expertise. En cas d'intérêt, ils/elles peuvent également publier de brèves contributions portant sur un sujet de leur choix rattaché au numérique, par exemple un résumé d'arrêt ou un commentaire d'une nouvelle législation.

Contact pour les personnes intéressées : alexandre.barbey@unil.ch, assistant diplômé du Pôle Numérique FDCA.

PUBLICATIONS OFFICIELLES

Mise en consultation de l'Ordonnance sur le quota des films européens et investissements dans le cinéma suisse (OQICin) →

Plusieurs dispositions concernant les services à la demande.

Mise en consultation de Loi fédérale sur les allocations pour perte de gain (LAPG) (Numérisation dans les allocations pour perte de gain) →

CENTRE NATIONAL POUR LA CYBERSÉCURITÉ NCSC, *Rapport semestriel 2022/I (janvier-juin). Sécurité de l'information. Situation en Suisse et sur le plan international, s.l. 2022.*

Traite principalement de l'utilisation de la cyber technologie dans les conflits armés. →

Résumé et commentaire : MEYER Pauline, *Rapport semestriel du Centre national pour la cybersécurité : cyberspace et conflits armés*, in : www.swissprivacy.law/183, 9 novembre 2022.

Révision de la Loi fédérale sur le système d'information commun aux domaines des étrangers et de l'asile →

Entrée en vigueur fixée au 22 novembre 2022.

Révision de l'Ordonnance sur le système d'information central sur la migration (Ordonnance SYMIC) →

Entrée en vigueur fixée au 22 novembre 2022.

Révision de l'Ordonnance sur le système de recherches informatisées de police (Ordonnance RIPOL) →

Entrée en vigueur fixée au 22 novembre 2022.

Révision de l'Ordonnance sur le traitement des données signalétiques biométriques →

Entrée en vigueur fixée au 22 novembre 2022.

Révision de l'Ordonnance sur la partie nationale du Système d'information Schengen (N-SIS) et sur le bureau SIRENE (Ordonnance N-SIS) →

Entrée en vigueur fixée au 22 novembre 2022.

Adoption de l'Ordonnance du SEFRI du 28 octobre 2022 sur la formation professionnelle initiale de développeuse de business numérique / développeur de business numérique avec certificat fédéral de capacité (CFC) →

Entrée en vigueur fixée au 1^{er} janvier 2023.

JURISPRUDENCE

Arrêt du TAF A-2630/2020 du 17 février 2022/sic! 2022 p. 519 →

Protection des données, système GEWA

Arrêt du TAF A-661/2022 du 27 octobre 2022. →

Cloud public, communication transfrontière de données

DOCTRINE

AMADDEO Francesca, *Swiss Digital Nomads: from Vis-a-vis to Visa. International attractive strategies for remote work*, in : Jusletter 14 novembre 2022. →


DI TRIA Livio, *Destinataires ou catégories de destinataires ?*, in : www.swissprivacy.law/179, 18 octobre 2022. →


EBELING Mary F. E., *Afterlives of Data. Life and Debt under Capitalist*, Oakland 2022. →

FELLMANN Walter/LEU Simon, <i>Aspekte der Fahrautomatisierung / Autonomes Einparkieren - Haftungsrechtliche Aspekte</i> , in : Jahrbuch zum Strassenverkehrsrecht 2022 (Hardy LANDOLT, Manfred DÄHLER, édit.), Zurich/St. Gall 2022, p. 359-396.	→
GLESS Sabine, <i>Aspekte der Fahrautomatisierung / Strafrechtliche Aspekte der Fahrautomatisierung (Beispiel Parkassistenz) Wird der Mensch zur Knautschzone für das Auto?</i> , in : Jahrbuch zum Strassenverkehrsrecht 2022 (Hardy LANDOLT, Manfred DÄHLER, édit.), Zurich/St. Gall 2022, p. 337-358.	→
HIBBERD Gary, <i>The Art of Cyber Security - A practical guide to winning the war on cyber crime</i> , s.l. 2022.	→
JÖRG Arnold, <i>Aspekte der Fahrautomatisierung / «Autonomes Einparken» - Technische Aspekte Wenn's knirscht noch einen Meter!</i> , in : Jahrbuch zum Strassenverkehrsrecht 2022 (Hardy LANDOLT, Manfred DÄHLER, édit.), Zurich/St. Gall 2022, p. 303-317.	→
LÖTSCHER Basil, <i>Aspekte der Fahrautomatisierung / Strafrechtliche Zurechnung des Nichtverwendens eines Assistenzsystems im Strassenverkehr</i> , in : Jahrbuch zum Strassenverkehrsrecht 2022 (Hardy LANDOLT, Manfred DÄHLER, édit.), Zurich/St. Gall 2022, p. 319-336.	→
MEIER Tim Cédric, <i>Regulierung des medizinischen Metaversums</i> , in : Life Science Recht 2022, p. 223 ss.	→
MEYER Pauline, <i>Encore un géant (Meta) condamné pour traitement illicite de données personnelles d'enfants</i> , in : www.swissprivacy.law/180 , 21 octobre 2022.	→
RICHTER Thomas/KORNSTEINER Tania/ZIEGLER Suzanne, <i>Chancen und Risiken von Hypothekarplattformen</i> , in : SREJ 2022 n° 25, p. 50 ss.	→
WEBER Rolf H., <i>Non-Fungible Tokens - A New (Legal) Phenomenon in the Crypto Universe</i> , in : sic! 2022, n° 11, p. 487 ss.	→
WEBER Rolf. H., <i>Common Heritage of Mankind in Internet Governance</i> , in : Jusletter 14 novembre 2022.	→

ÉVÉNEMENTS

24 novembre 2022	Formation continue en droit de la protection des données	→
14 h 15 à 17 h 30	Datenschutz im Arbeitsverhältnis	
	Université de Fribourg	

25 novembre 2022	Conférence inaugurale des Pôles 	→
9 h 30 à 17 h 00	Numérisation et changement climatique à la FDCA Université de Lausanne, Aula de l'IDHEAP	
25 et 26 mai 2023	Digital vulnerability in European private law. Inaugural conference of the PRIN-Project Call For Papers (flyer en annexe I)	→
	University of Ferrara, Italie	
25 mai 2023	The law applicable to the use of biometrics by armed forces Call For Papers (flyer en annexe II)	→
	Amsterdam, Pays-Bas, Marine Etablissement Amsterdam	

 Conférence organisée par le Pôle Numérique FDCA

ANNEXE I

DIGITAL VULNERABILITY IN EUROPEAN PRIVATE LAW

INAUGURAL CONFERENCE OF THE PRIN-PROJECT Ferrara, 25th and 26th May 2023

Call for Papers

The PRIN-Project “*Digital Vulnerability in European Private Law*” (*DiVE*) is planning its inaugural conference, which will take place on Thursday 25th and Friday 26th May 2023 at the University of Ferrara.

The conference will focus on the current legal status of the concept of digital vulnerability – that is, vulnerability caused by digital technologies – under domestic and EU law, analyzing both how the notion is currently used in European legal terminology and how rules and remedies are currently triggered by unequal situations in the digital environment.

In particular, the aim of the conference is to explore the links between the general notion of vulnerability and that of digital vulnerability, and to analyze how technology might exacerbate preexisting forms of inequality or create new ones.

Against this background, the conference aims to serve as a platform for offering an innovative and critical look on how the multifaceted concept of ‘digital vulnerability’ stands *vis-à-vis* traditional paradigms of protection of weaker parties (such as rules on incapacity, consumer protection, data protection, anti-discrimination, equality before the law) and to what extent it might properly promote a ‘personalized’, human-centered, approach to the digital environment.

If you are interested in participating in the conference as a Speaker, please submit a short abstract to digital.vulnerability@gmail.com by 15th January 2023. Abstracts should be submitted in document text format, and should include: (a) author(s), (b) affiliation, (c) e-mail address, (d) title and (e) body of abstract (apx 300 words). Abstract file should be entitled: Family Name_Last Name. In principle, abstracts should focus on the notion of digital vulnerability under domestic and EU law, but proposals from other disciplines and jurisdictions are also welcome. Authors of accepted abstracts will be notified by 15th February 2023.

Speakers will present for 20 minutes, followed by Q&A and a general discussion. They will be also invited to submit papers to be published in the conference volume.

ANNEXE II



Workshop Call for Papers

The law applicable to the use of biometrics by armed forces

Amsterdam, 25 May 2023

Introduction:

The War Studies Research Centre of the Netherlands Defence Academy is organizing an international workshop on the law applicable to the use of biometrics by armed forces, contractors working with armed forces and ICT companies involved in military acquisition and procurement. The workshop seeks to analyse different aspects of the law concerning such use. The workshop intends to bring together (legal) practitioners working in the area of the use of biometrics by armed forces, contractors working with armed forces and ICT companies as well as academics.

The workshop will take place on 25 May at the Marine Etablissement Amsterdam (Navy Yard Amsterdam) in Amsterdam, the Netherlands. The format is currently planned to be in-person.

Recipients of this call for papers are invited to submit proposals to present a paper at the workshop. Authors of selected proposals may be offered full or partial flight and accommodation expenses.

Submission deadline: 1 December 2022

Background:

Biometric systems are systems used for the purpose of the biometric recognition of individuals based on their behavioural and biological characteristics. Such characteristics include fingerprints, face and finger topography, gait, voice and DNA. These characteristics are unique, which makes them very suitable for recognizing persons.

Biometric systems are used extensively in the civil domain. They are also increasingly used in the context of military activities and operations. Some of these applications concern the use of biometrics internal to the armed forces. Such applications are generally used to limit access to facilities or particular systems. For example, the Royal Canadian Navy is conducting a trial with a biometric system to let staff access certain mission-critical IT systems. Other applications are used in military operations abroad to identify personnel and potential security threats. The United States has been at the forefront of such use, but other States are increasingly following suit. A recent example of the latter is the use of biometric technology to identify dead Russian military personnel in the conflict in Ukraine.

The use of biometrics by armed forces raises a host of legal questions. Some of these have started to be explored in the literature in recent years. However, hitherto this has been limited to a handful of publications. Moreover, the literature has focused on certain specific discrete legal aspects without taking a broader view, and often taking a largely theoretical perspective. The workshop seeks to

delve deeper into the application of law to the use of biometrics by armed forces, bring out the link between different aspects of such use and different fields of law that govern such use, and look at the application of the law in practice.

The workshop organizers invite proposals to present papers dealing with questions concerning the law applicable to the use of biometrics by armed forces, including but not limited to the following questions:

- Applicability of domestic and regional data protection instruments to the use of biometrics in a military context;
- (Comparative) domestic legal regulation of the use of biometrics by armed forces;
- The use of biometrics internal to armed forces and the right to privacy;
- The use of biometrics internal to armed forces and data protection;
- International Humanitarian Law (IHL) applicable to the use of biometrics in military operations and the question whether additional regulation is needed;
- The legal framework for the sharing of biometric information in multinational operations, between operations and outside of operations;
- Rights of persons in mission areas or occupied territories whose biometric data has been captured and stored;
- Potential derogation from human rights and data protection instruments in the context of the use of biometrics in military operations;
- The interaction between IHL and human rights law in the context of the use of biometrics;
- Technical means to ensure compliance with legal requirements;
- Legal aspects of specific use cases of biometrics by armed forces, including the use of biometrics by Ukraine to identify dead Russian soldiers;
- Biometric data as the target of military operations or attacks;
- The use of biometrics by private (military) actors during crisis / armed conflict.
- Development, procurement and deployment of military and dual-use technologies that employ biometric data.

Submissions:

Researchers and practitioners interested in addressing the issues above are invited to respond to this call for papers with a 1-2 page proposal for an article and presentation, along with a brief CV. Proposals should be submitted to prof. dr. Marten Zwanenburg (mc.zwanenburg@mindef.nl), no later than **1 December 2022**.

Publication:

The Military Law and the Law of War Review (an Edward Elgar publication) is interested in publishing selected full length papers based on workshop presentations, subject to its standard review and editing procedures.