Entreprises et Big Data : peut-on forcer les entreprises à partager leurs données non-personnelles (par des licences obligatoires ou des licences « FRAND ») ?

Jacques de Werra*

In the digital age where big data is of key value, companies generate a massive amount of data and make intensive use of data. Given that companies may depend on the access to non-personal data (industrial data) held by other companies to remain competitive, the question arises as to whether companies should be forced to share their non-personal data with each other (B2B data sharing) on the basis of compulsory licensing or FRAND (Fair, Reasonable and Non-Discriminatory) licensing mechanisms. This article (which is based on an expert report drafted by the author for the Swiss Federal Institute of Intellectual Property) examines this issue under Swiss law (in the light of foreign developments specifically those taking place in the European Union which – obviously – play a key role in Switzerland). This article concludes that the compulsory licensing and the FRAND licensing mechanisms do not constitute adequate models for the creation of a non-voluntary sharing mechanism for non-personal-data. The compulsory licensing mechanism under patent law (to which reference is made as a potential model) cannot be replicated one to one for the compulsory licensing of non-personal data. Similarly, the FRAND licensing model that has been developed for so-called standard essential patents (SEPs) cannot be transplanted easily in order to apply it to the licensing of non-personal data.

Table des matières

I. Introduction

A l'ère du numérique et du big data, les entreprises génèrent une quantité massive de données et en font un usage intensif. Les entreprises peuvent dépendre des données détenues par d'autres entreprises pour rester compétitives de sorte que la question se pose de savoir si l'on doit obliger les entreprises à partager leurs données non-personnelles (par licences obligatoires ou licences « FRAND »), ce qui fait l'objet de la présente contribution. Un groupe d'experts « Avenir du traitement et de la sécurité des données » a été créé en 2015 par la conseillère fédérale *Eveline Widmer-Schlumpf* en réponse à une motion du conseiller aux Etats *Paul Rechsteiner* (13.3841) transmise par le Parlement. La tâche des experts consistait à examiner certaines questions qui se posaient à propos du *big data,* du traitement et de la sécurité des données, ainsi que des risques et des opportunités liées à l'évolution des technologies de l'information et de la communication (TIC), compte tenu du contexte social dans lequel s'inscrivent ces questions.

Dans son rapport du 17 août 2018, le groupe d'experts a formulé la recommandation que « [l]a Confédération examine la création d'un système de licences obligatoires sous l'angle de l'accès aux données techniques »[1].

Le 30 octobre 2019, le Conseil fédéral a défini la suite à donner aux recommandations du groupe

* *Jacques de Werra* est professeur à la Faculté de droit de l'Université de Genève (en droit des obligations et en droit de la propriété intellectuelle) et directeur du Centre de Droit du Numérique (CDN) créé à la Faculté <*www.digitallawcenter.ch*>. Le présent article est fondé sur un rapport rédigé dans le cadre d'un mandat d'expertise qui a été confié par l'Institut fédéral de la propriété intellectuelle (IPI) à l'auteur. L'auteur remercie vivement *Hélène Bruderer,* assistante et doctorante au CDN, pour ses recherches et son aide précieuse à la finalisation du rapport d'expertise ayant servi de base au présent article ainsi que M. *Siroos Tanner,* auxiliaire de recherche et d'enseignement au CDN, pour son aide précieuse à la finalisation du présent article.

[1] Rapport du groupe d'experts concernant le traitement et la sécurité des données du 17 août 2018 (« Rapport Experts 2018 », cf. <*https://www.newsd.admin.ch/newsd/message/attachments/55754.pdf*>, chapitre 7.1, 7.1.1 à 7.1.4 ; cf. le communiqué de presse de l'époque, cf. <*https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-72083.html*> ; le groupe d'experts a été institué le 27 août 2015 par le Département fédéral des finances pour une durée de trois ans.

d'experts «Avenir du traitement et de la sécurité des données»[2].

Parmi les suites à donner, le Conseil fédéral a notamment confié à l'Institut fédéral de la propriété intellectuelle (IPI) le soin d'examiner l'une des recommandations du groupe d'experts portant sur la mise en place d'un système de licences obligatoires pour faciliter l'accès aux données non-personnelles (appelées également «données techniques»), données qui se définissent par opposition aux données personnelles[3]. L'IPI a ainsi été chargé d'examiner la situation actuelle en Suisse relative à l'accès aux données non-personnelles des entreprises et des organisations privées et de formuler des propositions pour faciliter l'accès à ces données techniques, en examinant le système de licences obligatoires, mais aussi d'éventuelles solutions alternatives[4].

La question de l'accès aux données est également mentionnée dans le cadre de la stratégie Suisse numérique. Ainsi, la stratégie dispose que «4.7.1. La Suisse dispose d'une base légale moderne et cohérente concernant les droits relatifs aux données, à l'accès à celles-ci et à leur utilisation» en indiquant que «[l]a Suisse crée une base légale moderne et cohérente pour exploiter le potentiel de l'économie des données. De nombreux acteurs nationaux et internationaux différents sont impliqués dans la production, l'accès et l'utilisation de ces données, et de ce fait une coordination réglementaire au niveau national, voire international, est souhaitable»[5].

La thématique de l'accès aux données se pose aussi sous l'angle du développement de l'intelligence artificielle (IA) dès lors que l'IA repose sur le traitement de données massives. Ainsi, dans un rapport du groupe de travail interdépartemental «Intelligence artificielle» au Conseil fédéral du 13 décembre 2019, l'importance de l'accès aux données a été confirmée[6].

L'objet du présent article est de présenter une analyse de la faisabilité, de la désirabilité et de la compatibilité aux normes internationales de la création d'un système de licences obligatoires ou de la mise en œuvre de licences FRAND[7] visant à concéder un droit d'accès non-volontaire aux données non-personnelles détenues par des sociétés privées. On relèvera d'emblée que la clarté du cadre légal et la sécurité juridique sont des conditions essentielles à l'exploitation des données non-personnelles par les entreprises[8] et que ces conditions devraient s'appliquer également en matière de licences obligatoires ou de licences FRAND sur des données non-personnelles.

Afin de pouvoir traiter ces questions, il est nécessaire de délimiter le champ du présent article (cf. ci-dessous I.1) et d'examiner certaines sources de

2 CF – Mise en œuvre de recommandations sur le traitement et la sécurité des données, *<https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-76854.html>* (cit. Communication CF 2019) ; voir le Rapport sur les recommandations du groupe d'experts sur l'avenir du traitement et de la sécurité des données – Prise de connaissance et suite de la procédure du Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC du 15 octobre 2019, *<https://www.newsd.admin.ch/newsd/message/attachments/58797.pdf>*.

3 Voir ci-dessous note 12.

4 Communication CF 2019 (note 2) : «Les chercheurs, les entreprises et la société civile ont intérêt à un accès aussi libre que possible aux données techniques des entreprises et organisations privées. L'Institut fédéral de la propriété intellectuelle (IPI), en collaboration avec d'autres offices, analysera donc la situation actuelle en Suisse et à l'étranger, et formulera des propositions pour éliminer les obstacles. Outre le système de licences obligatoires mentionné par le groupe d'experts, il examinera également d'autres solutions pour l'accès aux données techniques. Le rapport de l'IPI devrait être disponible d'ici mars 2021.»

5 Stratégie «Suisse numérique» adoptée par le Conseil fédéral le 5 septembre 2018, *<https://strategy.digitaldialog.swiss/fr/donn%C3%A9es-contenus-num%C3%A9riques-et-intelligence-artificielle#objectif-1>;* cf. document pdf complet à : *<https://strategy.digitaldialog.swiss/fr/strategie-digitale-schweiz-pdf>;* plan d'action comporte une «Initiative sur les données» *(<https://strategy.digitaldialog.swiss/fr/plan-d-action>)*.

6 *<https://www.sbfi.admin.ch/sbfi/fr/home/politique-fri/fri-2021-2024/themes-transversaux/numerisation-fri/intelligence-artificielle.html>* (4.5 Accès aux données et protection des données).

7 FRAND (Fair, Reasonable and Non-Discriminatory).

8 Voir en particulier le livre blanc du 13 janvier 2020, WEF (en coopération avec le Boston Consulting Group), Share to Gain : Unlocking Data Value in Manufacturing, janvier 2020 (cit. «Livre blanc WEF 2020»), *<https://www.weforum.org/whitepapers/share-to-gain-unlocking-data-value-in-manufacturing>* (accessible directement à : *<http://www3.weforum.org/docs/WEF_Share_to_Gain_Report.pdf>*), p. 17 ; le présent article se concentre sur une analyse juridique, étant relevé qu'un partage de données pose aussi de nombreux défis d'ordre technique, notamment sous l'angle du format et de l'interopérabilité des données qui doit être assurée afin de permettre un tel partage.

protection juridique des données non-personnelles (cf. ci-dessous II.1).

1. Délimitations

Le présent article porte sur la thématique des licences obligatoires et des licences FRAND pour l'accès aux données non-personnelles détenues par des sociétés privées.

Il convient dès lors de délimiter le champ de cet article dès lors que la thématique de l'accès aux données est extrêmement vaste. Cet article porte ainsi sur :

– l'accès *non-volontaire* aux données non-personnelles, soit un accès qui n'est pas consenti sur une base consensuelle (soit un fondement contractuel)[9], l'accès volontaire étant une thématique distincte[10]; il est précisé que cet article se concentre sur l'accès non-volontaire lorsque cet accès est justifié sur le plan légal, par contraste à un accès *illégal* aux données non-personnelles, soit un accès qui résulte d'une opération illégale, en particulier d'un acte illégal intentionnel commis par un tiers qui obtient un accès illicite aux données non-personnelles[11].
– l'accès non-volontaire aux *données non-personnelles,* ces dernières étant définies par opposition aux données personnelles[12]. Cette catégori-

9 On notera qu'une prétention à accéder à certaines données peut se fonder sur des moyens contractuels, comme l'obligation de rendre des comptes en droit du mandat (cf. art. 400 du Code des obligations), cf. Rapport Experts 2018 (note 1), p. 105 ; la doctrine évoque ainsi l'application de cette disposition en matière de droit à la portabilité des données, *Adrien Alberini/Yaniv Benhamou,* Data portability and interoperability : an issue that needs to be anticipated in today's IT-driven world, Expert Focus 2017/8, p. 518, *<https://archive-ouverte.unige.ch/unige:96170>;* pour les données échangées sur une base volontaire, le Rapport Experts 2018 (note 1), p. 111, évoque la notion de « données volontaires », soit les données « que des personnes se transmettent volontairement entre elles ».

10 Le partage de données peut s'opérer sous la forme d'accords de partage de données (Data sharing agreements) ; voir le Document de travail des services de la Commission du 25 avril 2018 – Orientations concernant le partage des données du secteur privé dans l'économie européenne des données accompagnant le document : Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions « Vers un espace européen commun des données », COM(2018) 232 final (« Document de travail CE 2018 »), *<https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52018SC0125&from=EN>;* de très nombreux travaux et projets sont en cours au sein de l'Union européenne concernant le partage de données, cf. notamment l'intéressant rapport du 24 janvier 2020 du Support Center for Data Sharing (SCDS), B2–Analytical report on EU law applicable to sharing of non-personal data, *<https://eudatasharing.eu/sites/default/files/2020-02/EN_AR%20on%20EU%20law%20applicable%20to%20sharing%20of%20non-personal%20data.pdf>* et plus généralement le site du SCDS : *<https://eudatasharing.eu>;* on notera toutefois que les licences FRAND (qui sont examinées dans le présent article) pourraient être considérées comme des licences volontaires dès lors qu'elles reposent sur une déclaration d'accord du titulaire du brevet concerné, voir ci-dessous texte à notes 125–126.

11 Un tel accès illégal est susceptible d'être sanctionné pénalement, voir ci-dessous note 96. La thématique de l'accès illégal aux données est critique dans l'environnement numérique de même que celle de la cybersécurité des données devant être protégées contre les cyberattaques, ce qui soulève des questions de responsabilité, cf. notamment *Jacques de Werra/Evelyne Studer,* Regulating cybersecurity : what civil liability in case of cyber-attacks ?, Expert Focus 2017/8, pp. 511–517, p. 513, *<https://archive-ouverte.unige.ch/unige:96220>*.

12 Il convient d'être conscient qu'en pratique, il est fréquent qu'un ensemble de données (dataset) soit composé à la fois de données à caractère personnel et de données à caractère non personnel (ensemble de données mixtes), ce qui pose la question de la délimitation de l'application des régimes respectifs, cf. art. 2 al. 2 Règlement DNP (dont la référence complète est donnée ci-après dans le corps du texte) et les Lignes Directrices relatives au règlement concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne du 27 mai 2019 (cit. Lignes Directrices), *<https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52019DC0250&from=EN>;* il peut ainsi y avoir un ensemble de données mixtes, concernant « des données relatives à l'internet des objets, lorsque certaines des données permettent d'émettre des hypothèses sur des individus identifiables (par exemple, présence à une adresse et modalités d'utilisation particulières) » (Lignes Directrices précitées, para. 2.2) ; « si les données à caractère non personnel et les données à caractère personnel sont ‹inextricablement liées›, les droits et obligations en matière de protection des données découlant du RGPD s'appliquent pleinement à l'intégralité de l'ensemble de données mixtes, même lorsque les données à caractère personnel ne représentent qu'une petite partie de l'ensemble de données » *(ibid.);* les données sont « inextricablement liées » dans la « situation où un ensemble de données contient des données à caractère personnel ainsi que des données à caractère non personnel et où une séparation entre les deux serait soit impossible, soit considérée comme économiquement inefficace ou techniquement impossible par le responsable du traitement » *(ibid.);* dans ces circonstances, en cas d'ensembles de données mixtes, la réglementation

sation et cette terminologie sont celles utilisées en droit européen, en particulier dans le Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne des données non-personnelles («Règlement DNP»). Les données non-personnelles y sont définies par opposition aux données personnelles, l'art. 2 al. 1 du Règlement DNP prévoyant ainsi que «[l]e présent règlement s'applique au traitement de données électroniques autres que les données à caractère personnel […]». Les données personnelles font en effet l'objet de réglementations spécifiques et de normes particulières instituant notamment un droit d'accès[13]. Sur le plan terminologique, référence sera ainsi faite aux données non-personnelles plutôt qu'aux «données techniques»[14]. Parmi les données non-personnelles figurent en particulier les «données industrielles» (industrial data)[15] qui peuvent notamment être générées dans le cadre de l'utilisation d'objets connectés (Internet des objets/Internet of things)[16].

On se réfère ainsi parfois à l'Internet industriel des objets (*Industrial Internet of Things,* IIoT)[17]. Les objets connectés posent en effet des questions et risques juridiques spécifiques, notamment sous l'angle de la cybersécurité (ceci vient d'être évoqué par le Conseil fédéral)[18].

– L'accès aux données non-personnelles détenues *par des sociétés privées,* par opposition aux données détenues par le secteur public; le présent article ne traite donc pas de la question de l'accès aux données détenues par le secteur public (Public Sector Information, PSI) qui fait l'objet de règles spécifiques[19] et de développements prop-

en matière de protection des données personnelles s'appliquera de sorte que les ensembles mixtes sortent du cadre du présent article; il faut en outre relever que la catégorisation de données déterminées comme données personnelles ou comme données non-personnelles est susceptibles d'évoluer dès lors que des données personnelles peuvent être anonymisées (sous réserve de risque et du potentiel de désanonymisation ultérieure, cf. Lignes Directrices précitées, para. 2.1).

13 La Loi fédérale sur la protection des données du 19 juin 1992 (LPD, RS 235.1) sera remplacée par la Loi fédérale sur la protection des données du 25 septembre 2020 (nLPD) qui devrait entrer en vigueur en 2022; au sein de l'Union européenne, le Règlement (UE) 2016/679 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 (RGPD) est entré en vigueur le 25 mai 2018; le RGPD s'applique aux entreprises suisses dont les activités de traitement sont liées à l'offre de biens ou de services à des personnes concernées dans l'UE et au suivi du comportement de ces personnes (art. 3 al. 2 RGPD); l'art. 8 LPD, l'art. 25 nLPD et l'art. 15 RGPD prévoient un droit d'accès aux données personnelles; l'art. 20 RGPD prévoit par ailleurs un droit à la portabilité des données qui sera consacré dans la nLPD (art. 28 al. 2).

14 Les termes de «données techniques» ont été utilisés dans le Rapport Experts 2018 (note 1) et dans les documents officiels.

15 Pour une définition de Industrial data, voir Industrial Data and Regional Economic Development, Georgia Tech, Energy Policy and Innovation Center – Center for Urban Innovation (Draft v. 1.1, February 2018), Phase 1 Study and Findings – Industrial data in power generation, <*http://www.energy.gatech.edu/sites/default/files/documents/industrial_data_whitepaper.pdf*>, « Industrial data (ID) are data obtained by measuring and assessing the production and operations of industrial equipment, processes, and systems. These include: 1. Production data: Production data are data from industrial equipment, processes, and systems during production. […] 2. Operations data: Operations data are data from industrial equipment, processes, and systems during operation. »

16 Voir le livre blanc (white paper) du Fraunhofer Institut, Industrial Data Space – Digital Sovereignty over Data (2016), <*https://www.fraunhofer.de/content/dam/zv/en/fields-of-research/industrial-data-space/whitepaper-industrial-data-space-eng.pdf*>; ceci est aussi lié au fait que les données industrielles sont au cœur de la stratégie européenne pour les données publiées le 19 février 2020, cf. Communication de la Commission européenne du 19 février 2020, COM(2020) 66 final (cit. Communication CE 2020), <*https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_fr.pdf*> et le site: <*https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_fr*>.

17 Voir Conseil fédéral – Normes de sécurité pour les appareils connectés à Internet (Internet des objets) Rapport du Conseil fédéral du 29 avril 2020 en réponse aux postulats *Glättli* 17.4295 du 15 décembre 2017 et *Reynard* 19.3199 du 21 mars 2019 (cit. Rapport CF IdO), <*https://www.efd.admin.ch/dam/efd/fr/dokumente/home/dokumentation/berichte/internet-things.pdf.download.pdf/29042020%20Bericht-IoT-f.pdf*>.

18 Rapport CF IdO (note 17), p. 5.

19 Cf. la loi fédérale du 17 décembre 2004 sur le principe de la transparence dans l'administration (LTrans, RS 152.3) et les lois cantonales correspondantes; pour l'Union européenne, voir en particulier la Directive (UE) 2019/1024

res notamment en lien avec la politique d'Open Government Data[20]; la thématique de l'accès aux données non-personnelles en matière de recherche scientifique (open science)[21] ou de publications scientifiques (open access)[22] émanant du secteur public ne sera pas traitée non plus[23].

– L'accès aux données non-personnelles de sociétés privées *par d'autres sociétés privées* (soit dans les relations horizontales entre opérateurs du secteur privé dans le contexte de «business-to-business (B2B) data sharing»)[24]; cet article ne traite ainsi pas de l'accès aux données non-personnelles de sociétés privées par l'Etat et par le secteur public (soit reverse Public Sector Information ou business-to-government (B2G) data sharing[25], soit dans les relations verticales entre le secteur privé et l'administration publique). Cet article se concentre ainsi sur l'accès aux données entre entreprises privées (rapport *horizontal* de marché) et pas sur l'accès aux données par l'Etat (rapport *vertical* entre administrés et administration publique). Le Rapport Experts 2018 fait quant à lui la distinction entre deux types d'intérêts justifiant l'accès, soit «l'accès à des données pour des raisons d'intérêt public et l'accès à des données d'un concurrent»[26]. Cette distinction fondée sur les intérêts n'est pas optimale, car les intérêts ne sont pas toujours faciles à distinguer et peuvent ainsi se recouper[27]; ainsi l'accès aux

du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte); selon son art. 19, cette directive abrogera avec effet au 17 juillet 2021 la Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public telle que modifiée par la Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public; pour une analyse très récente, voir *Heiko Richter,* Exposing the Public Interest Dimension of the Digital Single Market: Public Undertakings as a Model for Regulating Data Sharing (21 mars 2020), Max Planck Institute for Innovation & Competition Research Paper No. 20-03, <*https://ssrn.com/abstract=3565762*>.

20 Voir le portail <*https://opendata.swiss/*>; cf. <*https://www.bfs.admin.ch/bfs/fr/home/services/ogd.html*> et la Stratégie Open Government Data 2019–2023, <*https://www.bfs.admin.ch/bfs/fr/home/services/ogd/strategie.html*>.

21 Pour une définition, cf. <*https://www.swissuniversities.ch/fr/themes/digitalisation/open-science*>.

22 Cf. <*https://www.swissuniversities.ch/fr/themes/digitalisation/open-access*>.

23 Ainsi, les exigences en matière d'open access figurant dans la stratégie 2020–2024 s'appliquent en matière de «publication académique financée par de l'argent public» qui «se rapporte aux contributions réalisées dans le cadre des activités d'une institution qui est financée à 50% au moins par des fonds publics», cf. plan d'action de la Stratégie nationale suisse sur l'Open Access du 29 novembre 2017, <*https://www.swissuniversities.ch/fileadmin/swissuniversities/Dokumente/Hochschulpolitik/Open_Access/Plan_d_action-f.pdf*>.

24 Sont visées ici les relations entre entreprises privées industrielles ou commerciales, soit les relations B2B, et pas les relations entre les plates-formes Internet fournisseuses des services numériques (en particulier les fournisseurs de services – selon la terminologie du droit de l'Union européenne – «d'intermédiation en ligne» et leurs clients commerciaux (Platform to Business, P2B, cf. <*https://ec.europa.eu/digital-single-market/en/business-business-trading-practices*>); ces dernières relations peuvent être réglementées spécifiquement, comme c'est le cas au sein de l'Union européenne en vertu du Règlement (UE) 2019/1150 du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne, et faire l'objet de règlementations particulières concernant le droit d'accès aux données et les conditions de partage de celles-ci (cf. art. 9 al. 1).

25 Voir <*https://ec.europa.eu/digital-single-market/en/news/experts-say-privately-held-data-available-european-union-should-be-used-better-and-more*> et le rapport Towards a European strategy on business-to-government data sharing for the public interest – Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing, 2020, <*https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64954*>.

26 Rapport Experts 2018 (note 1), p. 105; la version en allemand du Rapport Experts 2018 distingue ainsi entre «der Zugang zu Daten aus Gründen des öffentlichen Interesses und der Zugang zu Daten eines Wettbewerbers» («Zwei Konstellationen stehen im Kontext der Datenzugangsrechte im Vordergrund: der Zugang zu Daten aus Gründen des öffentlichen Interesses und der Zugang zu Daten eines Wettbewerbers»).

27 *Florent Thouvenin/Rolf H. Weber/Alfred Früh,* Elemente einer Datenpolitik, Center for Information Technology, Society and Law 7, Zurich 2019, p. 98 note 326; il est noté que les auteurs précités ont publié (parfois avec d'autres auteurs) différentes contributions évoquant ou portant directement sur la thématique faisant l'objet du présent article, voir notamment *Rolf H. Weber,* Zugang zu maschinengenerierten Daten, Jusletter 2. Dezember 2019, <*https://jusletter.weblaw.ch/fr/dam/publicationsystem/articles/jusletter/2019/1003/zugang-zu-maschineng_64a893cb04/Jusletter_zugang-zu-maschineng_64a893cb04_de.pdf*> (cit. *Weber,* Jusletter 2019); *Alfred Früh,* Datenzugangsrechte, Rechtsrahmen für einen neuen Interessen-

données non-personnelles peut parfois être justifié pour des «raisons d'intérêt public» *et* pour des raisons de concurrence sur le marché privé ; il est dès lors plus adéquat de distinguer, comme fait ici, en fonction de la nature privée ou publique de l'entité en faveur de laquelle un accès aux données peut être institué. Il faut toutefois relever ici que le partage de données non-personnelles avec une autorité publique peut aussi bénéficier (par ricochet) au secteur privé et à la concurrence dans certaines circonstances.

– L'accès aux données non-personnelles de sociétés privées par *d'autres* sociétés privées ; le présent article ne traite dès lors pas de la question de l'accès par une société privée à *ses propres* données non-personnelles qui sont détenues par un tiers (fournisseur de services, p.ex. de services d'informatique en nuage (cloud computing) ni la question de la portabilité de telles données non-personnelles d'un fournisseur de service vers un autre fournisseur de services à la demande du client concerné)[28].

– L'accès aux données non-personnelles qui ne sont *pas accessibles* (et donc gardées confidentielles par les sociétés privées concernées) ; ainsi, la question de la protection contre un usage abusif de données (non-personnelles et/ou personnelles) accessibles qui résulterait de l'emploi de techniques automatisées de reprise à large échelle des données (web/data scraping) ne sera pas examinée[29].

L'analyse sera faite sur la base du droit suisse en prêtant toutefois une attention particulière au droit de l'Union européenne et au droit international dans la mesure utile[30].

Vu la très grande variété de données non-personnelles ainsi que la multiplicité des modalités de leur usage et des spécificités sectorielles, une analyse juridique spécifique devrait être conduite en fonction des circonstances particulières et du secteur économique concerné. Pour cette raison, le présent article se limite à la présentation d'une analyse juridique générale et transversale qui ne sera pas nécessairement pertinente en fonction des données en cause et du secteur concerné. On relèvera ainsi que certaines réglementations sectorielles sont susceptibles de pré-

ausgleich in der Datenwirtschaft, sic ! 2018, p. 521 ; *Alfred Früh,* Datenzuordnung und Datenzugang. Eine Übersicht über Stand und Entwicklungspotenziale zweier komplementärer Aspekte der Datenpolitik, digma 2019, p. 172 ; *Florent Thouvenin,* Wem gehören meine Daten ? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs, RSJ 2017, p. 21 ; *Rolf H. Weber/Florent Thouvenin,* Dateneigentum und Datenzugangsrechte-Bausteine der Informationsgesellschaft, RDS 2018, p. 37 ; *Florent Thouvenin/Alfred Früh/Alexandre Lombard,* Eigentum an Sachdaten : Eine Standortbestimmung, RSDA 2017, p. 25 ; *Alfred Früh,* Zum Bedarf nach Datenzugangsrechten, Jusletter IT Flash vom 11. Dezember 2017 ; il sera fait référence essentiellement à la publication collective mentionnée en début de la présente note de bas de page qui est la plus récente et la plus extensive.

28 Cf. art. 6 du Règlement DNP (texte ad note 12) ; la portabilité des données est également discutée dans le Rapport Experts 2018 (note 1), chap. 7.1.5 p. 107 ss pour lequel une recommandation avait aussi été formulée par le groupe d'experts comme suit : «La Confédération étudie la possibilité de réglementer la portabilité des données techniques, en tenant compte des évolutions observées sur le plan international» ; le Conseil fédéral n'a toutefois pas donné une suite positive à cette recommandation ; voir *Thouvenin/Weber/Früh* (note 27), p. 97 (soulignant que l'objectif est ici de protéger les clients contre le risque de dépendance envers les fournisseurs de services «vendor lock in»).

29 Le webscraping est discuté dans le Rapport Experts 2018 (note 1), p. 116, comme «cette technique consistant à obtenir des informations en prélevant des données souhaitées à partir d'autres sites web (par ex. au moyen d'un crawler ou robot d'indexation) pose un problème qui n'a pas encore été suffisamment abordé» ; sur cette question, voir *Damian Stauber,* Webscraping, Jusletter IT Flash du 11 décembre 2017 ; voir aussi ATF 131 III 384 ; voir le récent arrêt américain hiQ Labs, Inc. v. LinkedIn Corp, 938 F.3d 985 (9th Cir. 2019).

30 La thématique de la protection des données non-personnelles et de l'accès à celles-ci fait l'objet de très nombreuses réflexions et travaux qui ne peuvent pas tous être mentionnés ni être utilisés dans le cadre du présent article ; on signalera en particulier les documents suivants : OCDE, Enhancing Access to and Sharing of Data : Reconciling Risks and Benefits for Data Re-use across Societies, Paris 2019 (cit. Rapport OCDE 2019), *<https://doi.org/10.1787/276aaca8-en> ;* voir aussi World Economic Forum (WEF), Unlocking Value in Manufacturing through Data Sharing, voir le site : *<https://www.weforum.org/projects/data-sharing-for-manufacturing>,* et le Livre blanc WEF 2020 (note 8); voir aussi l'article de *Yaniv Benhamou,* Big Data and the Law: a holistic analysis based on a three-step approach – Mapping property-like rights, their exceptions and licensing practices, publié dans ce numéro de la RSDA, p. 393 ss.

voir un partage non-volontaire de données non-personnelles entre entreprises privées (B2B data sharing). Celles-ci ne sont toutefois pas analysées dans le présent article qui se concentre sur une analyse horizontale (non-sectorielle) de la thématique.

2. Structure de l'article

Le présent article est structuré de la manière suivante : il analysera tout d'abord le statut des données non-personnelles (ci-dessous II.1) en examinant certaines sources de protection juridique de ces données (ci-dessous II.1.2). Il traitera ensuite de la question de l'accès non-volontaire aux données non-personnelles (ci-dessous II.2) avant de formuler des conclusions résultant de l'analyse conduite (ci-dessous III).

II. Analyse juridique

1. Statut juridique des données non-personnelles

1.1 Introduction

Les données non-personnelles ne sont pas définies en droit suisse et ne sont pas soumises à un statut juridique particulier, au-delà de leur notion qui est définie par opposition aux données personnelles protégées par la LPD[31]. Les données non-personnelles couvrent en particulier les données dites industrielles (« industrial data »)[32].

L'existence actuelle et le besoin de création d'un droit de propriété sur les données non-personnelles, qui serait conçu comme un droit exclusif de nature absolue qui serait opposable à tous, donne lieu à de nombreux débats dogmatiques[33]. A l'heure actuelle, il n'existe pas de droit de propriété sur les données non-personnelles en droit suisse[34] et l'intérêt à créer un tel droit n'est pas établi[35]. Il convient d'examiner si des données non-personnelles peuvent faire l'objet d'une protection résultant de réglementations existantes du droit de la propriété intellectuelle ou du droit de la concurrence déloyale qui protégeraient contre un accès et/ou un usage non-autorisés par un tiers dans certaines circonstances. Une analyse de ces sources potentielles de protection permet de déterminer non seulement si les données non-personnelles sont protégeables sur le fondement de ces sources, mais aussi, à supposer que les données non-personnelles soient considérées comme protégeables, si ces différentes réglementations permettent de créer un droit d'accès non-volontaire à ces données (p.ex. sur la base d'exceptions au droit d'auteur) et comporteraient ainsi une autorisation d'accès non-volontaire aux données.

31 Loi fédérale sur la protection des données du 19 juin 1992 (LPD, RS 235.1), cf. définition des données personnelles à l'art. 3 let. a LPD comme « toutes les informations qui se rapportent à une personne identifiée ou identifiable ».

32 Voir ci-dessus note 15.

33 Voir en particulier *Thouvenin/Weber/Früh* (note 27), p. 91 ; voir aussi Position Statement du Max Planck Institut, *Josef Drexl/Reto M. Hilty/Luc Desaunettes/Franziska Greiner/Daria Kim/Heiko Richter/Gintarė Surblytė,* Data Ownership and Access to Data, 16 août 2016 (cit. Position Statement MPI 2016), *<http://www.ip.mpg.de/en/link/positionpaper-data-2016-08-16.html>, <https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/positionspaper-data-eng-2016_08_16-def.pdf>,* para. 4 ; une partie de la doctrine est favorable à la création d'un droit de propriété sur les données, voir *Marc Amstutz,* Dateneigentum – Funktion und Form, AcP 218(2), 2018, p. 438 ; voir aussi *Herbert Zech,* Information as Property, 6 JIPITEC 2015, p. 192.

34 Voir en particulier *Thouvenin/Weber/Früh* (note 27), p. 19–91 concluant (p. 91) à l'absence de motif convaincant justifiant l'introduction d'un droit de propriété sur les données (« Dateneigentum ») ; on trouve des opinions comparables à l'étranger, voir p.ex. *Lothar Determann,* No One Owns Data, Hasting Law Journal 2019, vol. 70, Issue 1, p. 1, *<http://www.hastingslawjournal.org/no-one-owns-data-2/> ;* la question reste débattue, certains considérant positivement la propriété sur les données, voir p.ex. *Herbert Zech,* Daten als Wirtschaftsgut – Überlegungen zu einem « Recht des Datenerzeugers », Computer und Recht 2015, vol. 21, p. 137.

35 *Rolf H. Weber/Florent Thouvenin,* Dateneigentum und Datenzugangsrechte – Bausteine der Informationsgesellschaft ?, RDS 2018, p. 63 ; voir aussi OFCOM, Jalons d'une politique des données en Suisse, 23 août 2018, *<https://www.bakom.admin.ch/bakom/fr/page-daccueil/l-ofcom/informations-de-l-ofcom/ofcom-infomailing/bakom-infomailing-48/eckwerte-fuer-eine-datenpolitik-der-schweiz.html>*. « S'agissant des données, la question de la propriété revient sans cesse. Le Conseil fédéral a fait examiner ce point par l'Office fédéral de la justice (OFJ), qui estime que l'introduction d'une propriété générale des données dans le droit suisse ne serait pas judicieuse » ; dans le même sens, dans une perspective européenne, voir *Alain Strowel,* Big data and data appropriation in the EU, in : Research Handbook on Intellectual Property and Digital technologies (Tania Aplin éd.), Edward Elgar, 2020, p. 107, p. 126, qui considère que la création d'un droit de propriété n'est pas adéquate pour protéger un objet fluide, difficile à identifier et évolutif comme le sont les données de « big data ».

Les sources envisageables qu'il convient ainsi d'analyser sont[36]:

– Le droit d'auteur (voir ci-dessous (1.2.1) ;
– Le droit de la concurrence déloyale (voir ci-dessous (1.2.2) ;
– La protection des secrets d'affaires (voir ci-dessous (1.2.3) ;
– D'autres sources de protection juridique des données (voir ci-dessous (1.2.4).

1.2 Sources de protection juridique contre l'accès à et/ou l'utilisation non-autorisées de données non-personnelles

1.2.1 Droit d'auteur

Le droit d'auteur suisse porte sur la protection de l'œuvre, qui est définie comme suit : « Par œuvre, quelles qu'en soient la valeur ou la destination, on entend toute création de l'esprit, littéraire ou artistique, qui a un caractère individuel »[37]. L'exigence de « caractère individuel » signifie que l'œuvre doit revêtir une individualité suffisante, ce qui doit se manifester dans l'œuvre elle-même[38].

Sur cette base, une donnée individuelle non-personnelle (en particulier des données industrielles générées de manière automatique) ne peut pas constituer une œuvre protégeable par le droit d'auteur[39]. Un ensemble de données non-personnelles (en particulier une base de données) pourrait être protégé à certaines conditions.

L'art. 4 al. 1 LDA consacre en effet une règle spécifique pour les œuvres constituant des « recueils » en prévoyant ainsi que « [l]es recueils sont protégés pour eux-mêmes, s'ils constituent des créations de l'esprit qui ont un caractère individuel en raison du choix ou de la disposition de leur contenu ». La protection d'un recueil par le droit d'auteur est indépendante de la protection potentielle des éléments qui composent le recueil (soit le contenu du recueil), ces éléments pouvant ou non être protégés par le droit d'auteur. Si tel est le cas, l'intégration de ces éléments dans le recueil supposera l'autorisation des titulaires des droits d'auteur sur ces éléments[40]. Un recueil au sens de l'art. 4 LDA peut être une base de données qui pourra ainsi être protégeable par le droit d'auteur en cas d'individualité dans le choix ou la disposition du contenu de la base de données. Une utilisation sans autorisation de tout ou partie de la base de données par un tiers pourra constituer une violation du droit d'auteur sur la base de données pour autant que la partie de la base de données qui a été reprise reprenne les éléments protégés de la base de données (soit le choix ou la disposition du contenu de la base de données). La reprise des données comme telles qui figurent dans la base de données ne constitue pas une violation du droit d'auteur sur le recueil/la base de données.

Les données industrielles qui sont générées de manière automatique ou sans qu'on puisse considérer qu'il s'agirait d'un processus créatif (p.ex. « data obtained by measuring and assessing the production and operations of industrial equipment, processes, and systems »[41]) ne peuvent pas constituer une œuvre protégeable par le droit d'auteur faute de processus créatif humain dans leur création. Une base de données rassemblant de telles données industrielles pourrait cas échéant être protégeable pour autant que le choix ou la disposition des données puisse être considéré comme individuel et ainsi créatif au sens du droit d'auteur. Si toutes les données industrielles récoltées sont reprises dans la base de données, on ne pourrait pas considérer qu'elle est protégeable par le

36 Il est renoncé à présenter le droit des brevets d'invention ; pour une brève discussion, voir *Josef Drexl,* Designing Competitive Markets for Industrial Data – Between Propertisation and Access, JIPITEC 2017, 257 para 1, *<https://www.jipitec.eu/issues/jipitec-8-4-2017/4636/JIPITEC_8_4_2017_257_Drexl>*, para. 57–61.

37 Art. 2 al. 1 de la Loi fédérale sur le droit d'auteur et les droits voisins (Loi sur le droit d'auteur, LDA) du 9 octobre 1992 (RS 231.1).

38 ATF 142 III 387 consid. 3.1 ; la jurisprudence a ainsi notamment jugé que le Répertoire des produits dangereux (ou Guide orange des sapeurs-pompiers genevois) est une oeuvre (ATF 136 III 225) mais qu'un compendium contenant des informations sur des médicaments manque de l'individualité requise (ATF 134 III 166).

39 Communication de la Commission européenne du 10 janvier 2017 « Créer une économie européenne fondée sur les données, SWD(2017) 2 final, *<https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52017DC0009&from=EN>* (cit. Communication CE 2017), para. 3.3. » Les données brutes produites par des machines ne sont pas protégées par les droits de propriété intellectuelle existants puisqu'elles ne sont pas considérées comme étant le fruit d'une création intellectuelle et/ou comme présentant une quelconque originalité » ; voir aussi (sous l'angle de la protection des bases de données en droit européen, *Drexl* (note 36), para. 45.

40 Art. 4 al. 2 LDA « La protection des œuvres réunies dans les recueils est réservée ».

41 Cf. ci-dessus note 15.

droit d'auteur, faute de créativité dans le choix ou la disposition des données.

A supposer que la base de données puisse être protégée par le droit d'auteur, seule la reprise non autorisée par un tiers des éléments protégés (soit le choix ou la structure de la base de données) pourrait constituer une violation du droit d'auteur sur la base de données[42].

Sur cette base, la protection des données non-personnelles par le droit d'auteur n'interviendra que dans des circonstances exceptionnelles. Même à supposer que les données non-personnelles puissent être protégeables par le droit d'auteur, il faut relever que le droit d'auteur suisse ne comporte pas d'exception générale qui permettrait de créer un droit d'accès et d'usage non-volontaire en faveur d'entreprises sur ces données non-personnelles détenues par d'autres entreprises[43].

1.2.2 Droit de la concurrence déloyale

Une protection des données non-personnelles est envisageable sur la base de l'art. 5 let. c LCD qui prévoit qu'agit de façon déloyale celui qui « reprend grâce à des procédés techniques de reproduction et sans sacrifice correspondant le résultat de travail d'un tiers prêt à être mis sur le marché et l'exploite comme tel ».

Cette disposition n'offre toutefois qu'une protection restreinte, en raison notamment de son application restrictive par la jurisprudence qui porte en particulier sur l'existence d'un « sacrifice correspondant » consenti par la partie qui reprend le résultat du travail d'autrui[44]. De plus, l'art. 5 let. c LCD exige (parmi ses conditions d'application) que cette partie « exploite comme tel » « le résultat de travail d'un tiers prêt à être mis sur le marché ». L'application de l'art. 5 let. c LCD en matière de reprise de base de données est ainsi très restrictive[45].

Cette disposition n'offre en tout état pas de protection contre l'usage de données non-personnelles d'un tiers qui serait fait à des fins internes par une autre entreprise[46]. En effet, l'art. 5 let. c LCD « ne vise pas à instituer la protection d'une nouvelle catégorie de biens juridiques. Il ne s'oppose à la reprise des prestations ou à leur copie qu'en présence de circonstances qui conduisent à admettre une concurrence déloyale. Il n'interdit pas l'exploitation de la prestation intellectuelle matérialisée dans l'objet, mais l'utilisation du support matériel *afin de réaliser un produit concurrent* » (italique ajouté)[47].

Dans ces circonstances, vu l'application restrictive de cette disposition par la jurisprudence et vu son absence d'application en cas d'usage interne de données non-personnelles par une entreprise qui ne serait pas offert sur le marché (étant rappelé que l'art. 5 let. c LCD exige que le tiers exploite « comme tel » le résultat du travail repris[48]), l'art. 5 let. c LCD ne confère qu'une protection très limitée contre la reprise

42 *Philippe Gilliéron,* CR–PI, Bâle 2013, N 10 ad art. 4 LDA.

43 La LDA prévoit des exceptions au droit d'auteur (dont certaines sont entrées en vigueur le 1er avril 2020) qui permettent d'utiliser une œuvre protégée sans l'autorisation de l'auteur et sans rémunération due à ce dernier ; l'art. 24d LDA prévoit en particulier une exception en faveur de l'utilisation d'oeuvres à des fins de recherche scientifique, étant relevé que celle-ci ne devrait pas s'appliquer largement dans le contexte d'utilisation d'œuvres faites dans un contexte entreprise à entreprise (B2B) sauf s'il s'agit d'un usage fait à des fins de recherche scientifique ; de plus, cette exception (comme les autres) ne s'applique qu'aux œuvres divulguées de sorte qu'elle ne permet pas de créer un accès à une œuvre non divulguée.

44 Voir en particulier ATF 139 IV 17 (« Cardsharing ») et ATF 131 III 384 ; voir l'excellente analyse critique et les propositions de nouvelle approche dans l'application de l'art. 5 let. c LCD faite par *Florent Thouvenin,* Art. 5 lit. c UWG – reloaded, sic ! 2018, p. 595, p. 612 ; il propose ainsi une réinterprétation des conditions d'application de l'art. 5 let. c LCD sous l'angle de la notion de sacrifice correspondant, pouvant conduire à la création d'une sorte de licence obligatoire résultant du droit de la concurrence déloyale (« bb) Zwangslizenz » Folgt man dem hier vorgeschlagenen Verständnis des angemessenen eigenen Aufwands, wird der Tatbestand von Art. 5 lit. c UWG zu einer Art wettbewerbsrechtlichen Zwangslizenz »).

45 ATF 134 III 166 (compendium) (pour juger du caractère approprié du sacrifice, il faut aussi examiner si le premier concurrent a déjà amorti ses dépenses au moment de la reprise. Le « critère de l'amortissement » joue un rôle aussi bien pour la limitation temporelle de la protection découlant de l'art. 5 let. c LCD que pour l'appréciation du sacrifice) ; ATF 131 III 384 (« Suchspider »).

46 Voir *Thouvenin* (note 44), p. 610 (« Klarzustellen ist schliesslich, dass Art. 5 lit. c UWG nur greift, wenn das unmittelbar übernommene Arbeitsergebnis am Markt auch unmittelbar verwertet wird. So muss es bspw. zulässig sein, Datenbestände Dritter unmittelbar zu übernehmen, um diese unternehmensintern zu analysieren und die gewonnenen Schlüsse auf dem Markt zu verwerten » [et les références citées en note 160]).

47 ATF 139 IV 17 consid. 1.3.

48 ATF 131 III 384 consid. 4.3 se référant à l'existence d'une concurrence parasitaire et ainsi à la reprise comme telle du résultat du travail d'autrui.

par une entreprise de données non-personnelles créées par une autre entreprise[49].

1.2.3 Droit des secrets d'affaires

Des données non-personnelles et particulièrement des données industrielles peuvent constituer des secrets d'affaires pour autant que les conditions de protection soient remplies. La protection des secrets d'affaires[50] repose sur différentes bases légales en droit suisse qui ne définit pas dans la loi les conditions de protection des secrets d'affaires. Sur le plan du droit international, la protection est consacrée à l'art. 39 ADPIC[51].

Selon la jurisprudence (en matière de droit pénal et de droit de la concurrence déloyale)[52], la notion de secrets d'affaires est définie comme suit : « Constitue un secret, au sens du ces dispositions, toute connaissance particulière qui n'est pas de notoriété publique, qui n'est pas facilement accessible, dont un fabricant ou un commerçant a un intérêt légitime à conserver l'exclusivité et qu'en fait il n'entend pas divulguer (cf. ATF 80 IV 27). Il faut entendre par secrets de fabrication et secrets commerciaux des informations qui peuvent jouer un rôle sur le résultat commercial »[53].

La protection des secrets d'affaires repose ainsi sur trois conditions cumulatives : (1) une exclusivité de fait, (2) la volonté de conserver le secret et (3) un intérêt légitime au secret[54].

L'exclusivité de fait, qui est la première condition, signifie que la connaissance particulière « n'est pas de notoriété publique » et « n'est pas facilement accessible »[55]. L'absence de notoriété publique de l'information concernée ne signifie pas que d'autres acteurs du marché notamment des concurrents ne doivent pas en avoir connaissance (notion de secret *relatif*)[56].

La volonté de l'ayant droit (détenteur du secret d'affaires) de préserver le secret, qui est la deuxième condition, concrétise l'exigence posée à l'art. 39 ch. 2 lit. c ADPIC en vertu de laquelle les informations concernées (soit les « renseignements non divulgués » selon la terminologie de l'art. 39 ADPIC) doivent avoir « fait l'objet de la part de la personne qui en a licitement le contrôle de dispositions raisonnables, compte tenu des circonstances, destinées à les garder secrets »[57].

49 Voir *Thouvenin* (note 44), p. 610 (extrait cité en note 46) ; la protection conférée en droit européen par le droit *sui generis* institué par la Directive 96/9/CE du Parlement européen et du Conseil, du 11 mars 1996, concernant la protection juridique des bases de données n'est pas non plus adaptée à la protection des données industrielles, voir *Drexl* (note 36), para. 46–50.

50 Référence est faite ici par souci de clarté à la notion de « secrets d'affaires » qui vise à couvrir les différentes catégories de secrets protégés par les normes spécifiques du droit suisse, spécifiquement l'art. 162 du Code pénal qui sanctionne la violation du secret de fabrication ou du secret commercial ; les art. 4 let. c et 6 LCD se réfèrent pour leur part au secret de fabrication et au secret d'affaires ; sur la question de la terminologie, voir *Ralph Schlosser,* Les secrets économiques dans les relations de travail, les collaborations et les procès civils, in : La protection des secrets d'affaires/The protection of trade secrets, vol. 6 de la série propriété intellectuelle – intellectual property (Jacques de Werra éd.), Genève/Zurich 2013, p. 65 (en accès libre : <*https://archive-ouverte.unige.ch/unige:34257*>).

51 Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (ADPIC) ; annexe 1C de l'Accord instituant l'Organisation mondiale du commerce du 15 avril 1994 (RS 0.632.20).

52 La définition des secrets d'affaires n'est pas uniforme entre celle donnée en droit pénal et en droit de la concurrence déloyale et celle en droit du travail (art. 321*a* al. 4 CO), voir *Schlosser* (note 50), p. 66.

53 ATF 103 IV 283 consid. 2 ; cette jurisprudence qui est assez ancienne est toujours considérée comme pertinente et applicable pour la définition des secrets d'affaires, cf. *Schlosser* (note 50), p. 66 ; la jurisprudence plus récente adopte parfois une définition plus synthétique des secrets d'affaires (sans qu'elle dénote une volonté de s'écarter des conditions établies par la jurisprudence antérieure), cf. p.ex. Tribunal fédéral, arrêt 6B_496/2007 du 9 avril 2008 consid. 5.1 ; la notion de secrets d'affaires peut faire l'objet d'autres définitions dans d'autres réglementations, cf. p.ex. (sous l'angle de la Loi fédérale sur la transparence du 17 décembre 2004, LTrans, RS 152.3), TF, 1C_562/2017 du 2 juillet 2018 consid. 3.2.

54 Voir *Schlosser* (note 50), p. 67 ss.

55 ATF 103 IV 283 consid. 2.

56 En droit du travail, la notion est plus étroite et porte sur la notion de secret absolu, soit de secret qui n'est pas connu en dehors de l'entreprise concernée (ATF 138 III 67 consid. 2.3.2 ; voir *Schlosser* (note 50), p. 69–70 (qui critique cette distinction et propose une conception uniforme du secret entre droit pénal/droit de la concurrence déloyale et droit du travail qui devrait se fonder sur la notion de secret relatif telle que conçue par la jurisprudence sous l'angle du droit pénal et du droit de la concurrence déloyale).

57 Comme l'exprime *Schlosser* (note 50), p. 71, il s'agit d'une condition de protection des secrets d'affaires et pas d'un élément de la définition du secret (comme l'exprime l'art. 39 al. 2 ADPIC).

L'intérêt légitime au secret[58], qui constitue la troisième condition, doit être admis lorsque l'information concernée peut «jouer un rôle sur le résultat commercial»[59] ou lorsque sa divulgation serait de nature à accélérer l'apparition de produits concurrents ou à diminuer les frais de production de produits concurrentes produits par d'autres sociétés[60]. On doit concevoir largement l'intérêt légitime d'une entreprise à garder une information secrète concernant la marche de ses affaires[61].

Sur la base des conditions à la protection des secrets d'affaires, on peut considérer que des données non-personnelles, particulièrement des données industrielles, sont susceptibles de constituer des secrets d'affaires. Ces données ne sont en effet pas de «notoriété publique» et ne sont pas facilement accessibles[62]. L'entreprise qui les génère aura la volonté de préserver le secret et aura ainsi pris les «dispositions raisonnables, compte tenu des circonstances, destinées à les garder [secrètes]»[63]. Ces données ont enfin une valeur commerciale dans la mesure où elles peuvent donner un avantage concurrentiel à l'entreprise qui les détient de manière secrète[64]. On doit certes relever que des données brutes, soit des données qui ne sont «ni traitées ni modifiées depuis leur enregistrement»[65] ne sont pas nécessairement directement lisibles et compréhensibles par des tiers. Cela ne doit pas empêcher qu'elles puissent avoir une valeur commerciale pour l'entreprise concernée.

En matière de données industrielles, on peut considérer que les données de performance (d'une machine, d'un véhicule, etc.[66]) sont particulièrement

58 L'art. 39 al. 2 let. b ADPIC prévoit que les renseignements non divulgués doivent avoir «une valeur commerciale parce qu'ils sont secrets».

59 ATF 103 IV 283 consid. 2.

60 ATF 80 IV 22 consid. 2a; voir *Schlosser* (note 50), p. 71.

61 Voir aussi (sous l'angle de la LTrans) TF, 1C_562/2017 du 2 juillet 2018 consid. 3.2.

62 *Drexl* (note 36), para. 54, distingue en fonction du type de données (en l'espèce des données collectées sur des senseurs relatifs à des objets connectés) («while the secrecy could be confirmed for data that is produced by the machines inside a factory, data collected by smart cars on freely accessible roads could be collected by the cars of many manufacturers and, hence, will not fulfil this requirement»); on peut toutefois relever que, même pour des données prélevées sur des véhicules intelligents, la condition du secret peut être remplie, car même si ces données sont prélevées sur des routes librement accessibles, les données comme telles ne le sont pas nécessairement (notamment concernant les performances du véhicule dans certaines conditions de circulation, p.ex. pluie, neige); cela dépend naturellement du type de données collectées: s'il s'agit de données concernant des nids de poule sur les routes identifiés grâce à des senseurs embarqués, il ne s'agira naturellement pas de données secrètes car les nids de poule sont visibles de tous, cf. Position Statement MPI 2016 (note 33), para. 23: «if, for instance, potholes are automatically detected by passing cars, the same opportunity – to know where the potholes are – is available for everyone; the data generated are not absolutely ‹secret› to begin with».

63 *Drexl* (note 36), para. 54, met en doute la protection des données industrielles comme secrets d'affaires aussi en raison de l'incertitude sur les démarches attendues pour garder l'information secrète («it is very unclear which steps will be required of the person in control to keep the information secret»); il est certes difficile de garder le secret dans un environnement numérique d'objets connectés (voir *Andreas Wiebe,* Protection of industrial data – A new property right for the digital economy?, GRUR Int. 2016, p. 877, p. 880); cela n'exclut toutefois pas la protection des secrets d'affaires comme telle, la question étant celle de déterminer, conformément à la condition exprimée à l'art. 39 al. 2 let. c ADPIC, quelles «dispositions raisonnables, compte tenu des circonstances, destinées à les [les informations confidentielles] garder secrets» doivent être prises par le détenteur de ces informations dans l'environnement numérique connecté.

64 *Drexl* (note 36), para. 54, est plus réservé en constatant qu'une valeur commerciale résulte de la corrélation d'une information individuelle avec d'autres données («while data may nowadays have great commercial value, it is quite questionable whether it will always be possible to establish a causal link between the secrecy of the information and its commercial value. In the context of big data analyses, an individual piece of information may appear quite trivial, but particular value may arise from correlations with other data»); on peut toutefois constater que certaines données industrielles ont une valeur commerciale p.ex. les données concernant la production/productivité d'une machine.

65 Communication CE 2017 (note 39), para. 3.

66 Ceci a aussi été illustré dans le cadre de certains litiges ayant éclaté dans le cadre de sports à haute composante technologique (compétition de voile de l'America's Cup), «Performance information takes months to accumulate, filter, process and evaluate. […], the performance data is extremely expensive, and time consuming to accumulate» (décision du America's Cup Arbitration Panel du 21 octobre 2001, «final decision on performance information in case ACAP 01/4», para. [10] citant et approuvant le mémoire d'une partie au litige (Golden Gate/Oracle), publiée dans l'ouvrage Arbitration in the America's Cup: the XXXI America's Cup arbitration panel and its decisions, La Haye, 2003, p. 129 ss, p. 132, *<https://archive-ouverte.unige.ch/unige:24811>;* sur cette thématique, voir *Jacques de Werra,* How to Protect Trade Secrets in High-Tech Sports?

importantes et susceptibles de constituer des secrets d'affaires[67].

La protection légale des secrets d'affaires ne crée pas de droit de propriété exclusif en faveur de celui qui les contrôle licitement[68] (que l'on peut ainsi considérer comme «le maître du secret»[69]). La protection vise au contraire à sanctionner certains comportements qui sont considérés comme déloyaux[70]. Dès lors que la protection des secrets d'affaires ne crée pas de droit exclusif sur les données non-personnelles, elle est jugée plus adéquate pour l'économie des données[71].

En matière de données non-personnelles et spécifiquement de données industrielles, il convient d'identifier qui peut être le maître du secret, ce qui dépendra naturellement des circonstances du cas d'espèce[72]. On peut estimer que si des données non-personnelles sont collectées sur des machines ou autres objets connectés individuels et consolidées auprès du fabricant des machines ou des objets, ce dernier pourrait être considéré comme le maître du secret sur les données non-personnelles ainsi agrégées[73].

On a estimé par contraste que les données individuelles collectées sur chacune des machines ou objets ne constituent pas nécessairement un secret d'affaires au motif que ces données n'ont pas de valeur commerciale propre[74]. En effet, la valeur des données industrielles résulte essentiellement de leur cumul et de leur agrégation[75]. Il n'est toutefois pas exclu que les données collectées sur les machines connectées qui sont utilisées par des clients puissent constituer des secrets d'affaires, qui sont communiqués aux fabricants (p.ex. des données sur le volume de production)[76] dont les propriétaires ou utilisateurs des

An Intellectual Property Analysis Based on the Experiences at the America's Cup and in the Formula One Championship, European Intellectual Property Review, vol. 32, Issue 4, 2010, p. 155, *<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2149767>*.

67 Cf. définition de «Operations data: Operations data are data from industrial equipment, processes, and systems during operation […]» (ci-dessus note 15).

68 Cette formulation correspond à celle figurant à l'art. 39 al. 2 ADPIC (italique ajouté): «Les personnes physiques et morales auront la possibilité d'empêcher que des renseignements *licitement sous leur contrôle* ne soient divulgués à des tiers ou acquis ou utilisés par eux sans leur consentement et d'une manière contraire aux usages commerciaux honnêtes […]».

69 Voir la formulation dans l'arrêt du TF, 1C_562/2017 du 2 juillet 2018 consid. 4.5.1.1: «Il s'agit de tout fait qui n'est ni notoire ni généralement accessible au public et qu'un industriel en sa qualité de maître du secret souhaite légitimement garder secret, plus concrètement, dont la divulgation à des concurrents pourrait porter atteinte au succès commercial de l'entreprise ou entraîner une distorsion de concurrence […]».

70 *Drexl* (note 36), para. 56 («[…] trade secrets protection is much narrower in scope than an exclusive data use right. It does not protect against any use of the data, but requires 'unlawful' conduct which, to summarise the different provisions of the Directive, can be regarded as contrary to honest commercial practices»); l'art. 39 al. 1 ADPIC expose qu'«[e]n assurant une protection effective contre la concurrence déloyale conformément à l'article 10*bis* de la Convention de Paris (1967), les Membres protégeront les renseignements non divulgués conformément au paragraphe 2 et les données communiquées aux pouvoirs publics ou à leurs organismes conformément au paragraphe 3».

71 *Drexl* (note 36), para. 182.

72 *Drexl* (note 36), para. 54, indique que le fait que les données sont générées dans un écosystème de réseau de valeur («value network») peut rendre délicate l'identification de la personne contrôlant le secret; *Wiebe* (note 63), p. 880.

73 Communication CE 2017 (note 39), para. 3.4 «Dans certains cas, les fabricants ou les prestataires de services peuvent devenir les propriétaires 'de fait' des données que leurs machines ou leurs processus génèrent, même si ces machines sont la propriété de l'utilisateur».

74 Voir *Tania Aplin,* Trading Data in the Digital Economy: Trade Secrets Perspective, 2017, in: Trading data in the digital economy: Legal Concepts and Tools Münster Colloquia on EU Law and the Digital Economy III (Sebastian Lohsse/Reiner Schulze/Dirk Staudenmayer éds.), Baden-Baden 2017, p. 59, p. 64, considérant qu'une donnée individuelle ne constitue pas un secret d'affaires au sens de la Directive 2016/943 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites (p. 66).

75 *Drexl* (note 36), para. 5.4.

76 Voir *Petteri Günther,* Industrial Internet Solutions and Data Ownership Versus Control Over Data, in: Regulating Industrial Internet Through IPR, Data Protection and Competition Law (Rosa Maria Ballardini/Petri Kuoppamäki/Olli Pitkäne éds.), La Haye 2019, texte à notes de bas de page 49 et 50 («This would mean that a customer provides to the vendor its internal data, which may include its confidential information, and that data will then be used for generating analytics data (inferred data) resulting from the service performance. Information on how the system performs in certain circumstances may include customer's proprietary data, such as information on production volumes […]»).

machines concernées seraient détenteurs (et seraient ainsi les maîtres de ces secrets).

Il convient toutefois de s'assurer que les données aient fait l'objet de dispositions destinées à les garder secrètes[77], ce qui suppose que les propriétaires ou utilisateurs de ces machines connectées aient pris les dispositions techniques correspondantes ou que ces dispositions de protection soient assurées (avec leur accord) par des tiers (en particulier par les fabricants des objets connectés concernés)[78].

On doit relever dans ce contexte la discussion qui est en cours (notamment au sein de l'Union européenne) visant à reconnaître un droit de contrôle sur les données non-personnelles en faveur du « producteur de données » défini comme « le propriétaire ou l'utilisateur à long terme du dispositif (le locataire) ». Ce droit de contrôle vise ainsi à lui conférer « un droit d'utiliser et d'autoriser l'utilisation de données à caractère non personnel » produites par le dispositif (la machine dont il est propriétaire/ou l'utilisateur à long terme[79]. Ce droit est destiné à se manifester particulièrement sur le plan contractuel dans les relations entre l'utilisateur et le fabricant des machines concernées afin d'assurer une répartition des droits équitables entre eux, ce qui peut faire l'objet de solutions sectorielles[80].

Il est ainsi attendu que les contrats entre utilisateurs et fabricants reconnaissent que « plusieurs parties ont contribué à la création des données lorsque celles-ci sont générées en tant que sous-produit de l'utilisation d'un produit ou d'un service »[81], ce qui vise le cas des données générées par des machines. Cette attente repose sur la reconnaissance de la « création commune de valeur » faisant partie des principes à respecter en matière de partage des données.

77 Communication CE 2017 (note 39), p. 12 : « Pour que des données puissent être considérées comme des ‹secrets d'affaires›, elles doivent avoir fait l'objet de dispositions destinées à les garder secrètes car elles représentent le capital intellectuel de l'entreprise ».

78 Même s'il appartient en principe au maître du secret de prendre les mesures requises pour assurer la confidentialité des données concernées, il n'est pas exclu qu'il confie cette tâche à un tiers (comme cela est fait dans le contexte de traitement de données d'une entreprise par des tiers dans le cadre de solutions informatiques dans les nuages/ cloud computing) ; ce tiers fournirait ainsi une solution de sécurisation des données générées par les machines, ce qui est de toute manière attendu p.ex. dans le cadre des objets connectés, cf. Rapport CF IdO (note 17), p. 16 « Quant aux entreprises qui exploitent des systèmes connectés, il est essentiel qu'elles considèrent que l'IdO fait partie intégrante de leur infrastructure informatique, et qu'elles mettent aussi en oeuvre des procédés dûment éprouvés pour garantir leur sécurité » ; la fourniture de solutions de sécurisation peut faire partie des prestations fournies par le fabricant d'objets connectés qui est susceptible d'être rémunérée par le client, ce d'autant que le client et le fabricant en ont besoin afin de pouvoir prétendre à la protection des secrets d'affaires.

79 Communication CE 2017 (note 39), p. 12 : « Droit du producteur de données : il serait possible d'accorder au ‹producteur de données›, c'est-à-dire le propriétaire ou l'utilisateur à long terme du dispositif (le locataire), un droit d'utiliser et d'autoriser l'utilisation de données à caractère non personnel. Une telle approche aurait pour but de clarifier la situation et d'offrir un choix plus étendu au producteur de données, en donnant aux utilisateurs la possibilité d'utiliser leurs données, ce qui contribuerait à libérer les données produites par des machines. Il faudrait cependant préciser expressément les exceptions pertinentes, notamment en ce qui concerne la fourniture d'accès non exclusif aux données par le fabricant ou par les pouvoirs publics, par exemple pour des motifs liés à l'environnement ou à la gestion de la circulation » ; pour une discussion voir, *Ivan Stepanov,* Introducing a property right over data in the EU : the data producer's right – an evaluation, International Review of Law, Computers & Technology (2020), 34 :1, p. 65 (qui ne considère pas que ceci soit opportun).

80 On peut ainsi se référer à l'intéressant code de conduite de l'Union européenne adopté en matière de partage de données agricoles (EU Code of conduct on agricultural data sharing by contractual agreement, 2019, (cit. Code de Conduite UE données agricoles), *<https://www.copa-cogeca.eu/img/user/files/EU%20CODE/EU_Code_web_2019_rEN.pdf>;* ce code expose des principes (non-contraignants) en soulignant le rôle central de l'agriculteur en matière de données agricoles, p. 3 : « The farmer remains at the heart of the collection, processing and management of agricultural data ».

81 Voir le site général : *<https://ec.europa.eu/digital-single-market/en/guidance-private-sector-data-sharing>* et en particulier la Communication de la Commission européenne « Vers un espace européen commun des données du 25 avril 2018, SWD(2018) 125 final, *<https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52018DC0232&from=EN>,* para. 4)a) concernant le partage de données entre entreprises (B2) (cit. Communication CE 2018).

Ces principes[82] et leur mise en œuvre[83] donnent une place particulière au besoin de protection des « secrets commerciaux » des parties. Les parties négociant un contrat de partage de données sont ainsi invitées à définir « des règles de non-divulgation concernant les parties en aval » et à s'assurer que « des mesures adéquates sont prises afin de protéger [leurs] données »[84].

On retrouve ces principes dans d'autres documents tels que le Code de conduite UE sur le partage des données agricoles qui expose que les parties sont tenues de protéger les données sensibles des parties[85] et particulièrement celle du « data originator »[86], soit l'agriculteur[87].

Ces réflexions (visant à établir des bonnes pratiques contractuelles en matière de partage volontaire de données) sont très intéressantes sous l'angle du droit des secrets d'affaires et confirment l'analyse juridique que l'on peut faire sous cet angle. On peut en effet considérer que le client est détenteur de certains secrets d'affaires relatifs aux données générées par la machine qu'il utilise (p.ex. données concernant le volume de production), données qu'il partage avec le fabricant, ce dernier agrégeant toutes les données reçues des machines de ses clients. A défaut d'accord du client quant au partage de ses secrets d'affaires avec le fabricant, le fabricant accéderait potentiellement indûment aux secrets d'affaires du client[88].

Chaque client est ainsi susceptible de concéder une licence contractuelle de secrets d'affaires au fabricant dont les modalités doivent être définies, notamment quant à la rémunération[89] et aux modalités d'usage des secrets d'affaires par le fabricant et à la possibilité pour le fabricant de concéder des sous-licences (ce qui devrait être autorisé par le « data originator »[90]). Cette licence (sous réserve d'autres solutions résultant du droit applicable au contrat de licence) devrait pouvoir être résiliée notamment dans le cas où le « data originator » souhaiterait reprendre le contrôle et la gestion de ses données non-personnelles ou les transmettre à un tiers[91].

Ceci touche la question du droit au portage/à la portabilité des données non-personnelles dans le cas où « un utilisateur professionnel souhaite changer de fournisseur de services ou transférer ses données pour les rapatrier vers ses propres systèmes informatiques »[92]. Selon le droit de l'Union européenne, un client pourra bénéficier de certains droits visant à faciliter le portage des données dans certaines circonstances[93].

82 Cf. note précédente sous lettre c) « Respect des intérêts commerciaux de chacune des parties : les accords contractuels doivent répondre à la nécessité de protéger les intérêts et secrets commerciaux tant des détenteurs de données que des utilisateurs de données ».

83 Cf. le document très instructif : Orientations concernant le partage des données du secteur privé dans l'économie européenne des données accompagnant le document : Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions « Vers un espace européen commun des données », COM(2018) 232 final du 25 avril 2018, *<https://ec.europa.eu/digital-single-market/en/news/staff-working-document-guidance-sharing-private-sector-data-european-data-economy>,* accès direct à : *<https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52018SC0125&from=EN>*.

84 *Ibid.*

85 Code de conduite UE données agricoles (note 80), p. 8.

86 Code de conduite UE données agricoles (note 80), p. 6.

87 Code de conduite UE données agricoles (note 80), p. 8.

88 Rapport CF IdO (note 17), p. 13 (« Certaines informations sans référence à des individus que transmettent les appareils connectés permettent également d'identifier d'éventuels secrets d'affaires ou de fabrication. En l'occurrence, il est essentiel que les parties concernées s'informent mutuellement et s'accordent sur la finalité de la collecte des informations (maintenance par ex.) et sur la date à laquelle ces dernières seront effacées. Faute d'un tel accord, une dénonciation pour espionnage économique ou pour infraction au droit de la concurrence est à craindre ») ; l'accès à ces données par le fabricant pourrait en effet être considéré comme déloyal et contraire « aux usages commerciaux honnêtes » (art. 39 al. 2 ADPIC).

89 La rémunération peut être faite en espèces ou sous d'autres formes, cf. Code de conduite UE données agricoles (note 80), p. 8.

90 Code de conduite UE données agricoles (note 80), p. 8.

91 Ce scénario est envisagé dans le Code de conduite UE données agricoles (note 80), p. 9–10.

92 Cf. Règlement DNP (texte ad note 12), art. 6 al. 1 let. b.

93 Voir Art. 6 al. 1 du Règlement DNP (texte ad note 12) ; selon l'art. 6 al. 3, « [l]a Commission encourage les fournisseurs de services à terminer le développement des codes de conduite au plus tard le 29 novembre 2019 et à les mettre effectivement en œuvre au plus tard le 29 mai 2020 » ; des projets de codes de conduite sont ainsi en cours d'élaboration et de validation, cf. *<https://scope-europe.eu/en/projects/swipo-code-of-conduct/>* ; *<https://scope-europe.eu/en/detail/news/swipo-working-group-officially-presents-codes-of-conduct-to-enable-competition-and-data-portability/>* ; les documents sont accessibles à : *<https://swipo.eu/media/SWIPO_documents.zip>* ; voir aussi *<https://ec.europa.eu/digital-single-market/en/dsm-*

Le fabricant peut par ailleurs également être détenteur d'autres secrets d'affaires sur les données agrégées et consolidées résultant des machines utilisées par ses clients[94]. Le fabricant peut en particulier être détenteur de secrets d'affaires portant sur l'analyse prédictive résultant d'un traitement (fondé sur des méthodes d'intelligence artificielle) des données collectées auprès de ses clients.

Il peut ainsi en résulter différents ensembles de données (datasets) qui sont protégeables comme secrets d'affaires dont les détenteurs peuvent être différents, soit en particulier les données initiales collectées sur la machine du client (dont ce dernier peut être détenteur) et les données dérivées et agrégées par le fabricant de la machine concernée (dont ce dernier peut être détenteur)[95].

Le droit des secrets d'affaires peut ainsi s'appliquer aux données non-personnelles étant noté que le régime juridique en matière de secrets d'affaires ne comporte pas de règle spécifique créant un droit d'accès non-volontaire sur ces données ou un droit d'usage non-volontaire de celles-ci.

1.2.4 Autres sources de protection juridique des données

Dans certaines circonstances, les données non-personnelles peuvent être protégées par d'autres moyens juridiques et régies par d'autres sources de réglementation. Le droit pénal pourra interdire en particulier la soustraction de données et l'accès indu à un système informatique[96], et d'autres réglementations sectorielles peuvent conférer une certaine « exclusivité de données »[97]. Dans certaines circonstances, la communication de secrets d'affaires à des entités (publiques ou privées) étrangères pourra être sanctionnée en tant qu'acte d'espionnage/service de renseignements économiques[98].

En outre comme évoqué plus haut[99], des données non-personnelles qui seraient combinées avec des données personnelles dans le cadre d'un ensemble de données mixte pourraient se trouver soumises au régime juridique applicable aux données personnelles (par un phénomène d'« absorption » juridique) faisant en sorte que le régime juridique (jugé prévalent) applicable aux données personnelles s'appliquerait à l'ensemble de données mixte.

1.2.5 Conclusion

Il résulte de l'analyse qui précède que les données non-personnelles ne font pas l'objet d'un droit exclusif de propriété intellectuelle en droit suisse, et ne sont en particulier pas protégeables comme telles par le droit d'auteur. Une base de données comportant des données non-personnelles pourrait être protégeable par le droit d'auteur en cas d'individualité du choix ou de la disposition de son contenu, une telle protection ne portant toutefois pas sur le contenu de la base de données et donc pas sur les données comme telles. Cela signifie ainsi qu'un droit d'accès aux données non-personnelles ou un droit d'utilisation de telles données sur une base non-volontaire ne peut pas découler des règles applicables en matière du

cloud-stakeholder-working-groups-cloud-switching-and-cloud-security-certification>.

94 On peut rappeler dans ce contexte que l'art. 39 al. 2 let. a ADPIC expose que le caractère secret d'informations peut être admis lorsque les informations concernées sont secrètes « dans la configuration et l›assemblage exacts de leurs éléments », ce qui montre que le caractère secret et donc protégeable (pour autant que toutes les autres conditions soient remplies) peut aussi résulter de la configuration ou de l'assemblages exacts d'informations (même si celles-ci ne sont individuellement pas secrètes) ; voir aussi *Günther* (note 76), texte à note de bas de page 50.

95 Code de conduite UE données agricoles (note 80), p. 8, distinguant les données individuelles fournies par un agriculteur (comme « data originator ») et les données collectives générées et agrégées par un traitement de données émanant de plusieurs « originators » (p.ex. par le fabricant des machines concernées).

96 Art. 143 al. 1 du Code pénal suisse du 21 décembre 1937 (CP, RS 311.0) ; art. 143*bis* al. 1 CP.

97 Cf. art. 11*a* de la Loi fédérale du 15 décembre 2000 sur les médicaments et les dispositifs médicaux (LPTh, RS 812.21) conférant une « exclusivité des données » sur les données soumises avec une demande d'autorisation de mise sur le marché des médicaments ; un accès à ces données sera susceptible d'être concédé dans certaines circonstances.

98 Art. 273 CP ; le Rapport CF IdO (note 17), p. 13, mentionne le risque d'espionnage économique comme suit (italique ajouté) : « Certaines informations sans référence à des individus que transmettent les appareils connectés permettent également d'identifier d'éventuels secrets d'affaires ou de fabrication. En l'occurrence, il est essentiel que les parties concernées s'informent mutuellement et s'accordent sur la finalité de la collecte des informations (maintenance par ex.) et sur la date à laquelle ces dernières seront effacées. Faute d'un tel accord, une dénonciation *pour espionnage économique* ou pour infraction au droit de la concurrence est à craindre. »

99 Voir ci-dessus note 12.

droit d'auteur (et spécifiquement des exceptions au droit d'auteur).

Pour ce qui concerne la protection des données non-personnelles en dehors du droit d'auteur telle que résultant du droit de la concurrence déloyale, on doit relever que la protection contre la reprise de données non-personnelles fondée sur l'art. 5 let. c LCD est limitée. Cette protection ne vise en particulier pas l'usage de données non-personnelles provenant d'une entreprise qui serait fait par une autre entreprise à des fins internes. Des données non-personnelles (notamment de données industrielles) sont néanmoins susceptibles de constituer des secrets d'affaires dont l'accès peut être protégé par le droit des secrets d'affaires dans certaines circonstances.

Sur la base de ce qui précède, on peut constater que les sources de protection examinées (droit d'auteur et droit de la concurrence déloyale spécifiquement en matière de protection des secrets d'affaires) n'offrent qu'une protection limitée contre un accès non-volontaire aux données non-personnelles et contre une utilisation non-volontaire de ces dernières. En outre, les différentes sources juridiques examinées ne comportent pas de règle spécifique créant un droit d'accès non-volontaire ou un droit d'usage non-volontaire sur ces données non-personnelles. Il convient ainsi d'examiner la question de la création d'un accès non-volontaire aux données non-personnelles sur les modèles des licences obligatoires ou des licences FRAND.

2. Accès non-volontaire aux données non-personnelles

La question de la création d'un accès légal non-volontaire aux données non-personnelles d'une société ne se pose pas seulement dans le cas où cette société bénéficie d'un droit de propriété exclusif sur ces données. Pour que la question de la création d'un droit d'accès obligatoire se pose, il suffit en effet que l'entreprise exerce un contrôle factuel (et donc pas nécessairement juridique sur ces données non-personnelles[100]. Tel peut particulièrement être le cas de secrets d'affaires qui doivent au demeurant faire l'objet de mesures de contrôle et de protection factuelles par leur détenteur afin d'être protégeables.

Cette situation n'est pas spécifique à la thématique des données non-personnelles dès lors que d'autres situations de contrôle factuel (et pas juridique) peuvent permettre une exploitation des biens intangibles concernés en l'absence d'un droit exclusif et peuvent aussi donner lieu à des restrictions visant à limiter l'exclusivité de l'exploitation commerciale découlant du contrôle factuel exclusif[101].

Pour procéder à l'analyse de la faisabilité, de la désirabilité et de la compatibilité aux normes internationales de la création d'un système de licences obligatoires ou la mise en œuvre de licences FRAND visant à concéder un droit d'accès non-volontaire aux données non-personnelles détenues par des sociétés privées, il convient tout d'abord d'exposer quelques réflexions concernant le système de licences obligatoires en présentant la réglementation existante en matière de brevets d'invention et en le comparant à la situation des données non-personnelles (cf. ci-dessous 2.1). Il convient de présenter également quelques réflexions concernant le système de licences FRAND tel qu'il est appliqué en matière de brevets essentiels à une norme (Standard Essential Patents) en le comparant à la situation des données non-personnelles (cf. ci-dessous 2.2).

Comme la possibilité de créer un droit d'accès non-volontaire aux données non-personnelles de tiers a été évoquée au sein de l'Union européenne et que ceci a servi de source d'inspiration dans le cadre des travaux en Suisse, il convient de présenter cer-

[100] *Alfred Früh,* Datenzugangsrechte, Rechtsrahmen für einen neuen Interessenausgleich in der Datenwirtschaft, sic! 2018, p. 521, p. 522 se référant à *Francesco Mezzanotte,* Access to Data: The Role of Consent and the Licensing Scheme, in: Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps (Reiner Schulze/Dirk Staudenmayer/Sebastian Lohsse éds.), Baden-Baden 2017, p. 167.

[101] *Drexl* (note 36), para. 69 («[…] markets can also develop with relatively little legal exclusivity where access can effectively be controlled by technical means») qui se réfère spécifiquement au cas des droits de transmission des évènements sportifs (para. 71); le «Hausrecht» en matière de droits de transmission concernant un évènement sportif confère en effet des droits de contrôle à celui qui «a les clés» du lieu où l'évènement sportif se déroule (p.ex. un stade), cf. p.ex. *Ian S. Blackshaw,* International Sports Law: An Introductory Guide, La Haye 2017, p. 69 («the broadcasting rights are controlled by the party holding ‹the keys of the door›») sans que la création d'un droit exclusif soit indispensable; les droits dérivés de ce contrôle factuel exclusif (comme les droits de transmission des évènements sportifs) peuvent être limités, notamment par le droit de la concurrence.

tains travaux conduits au sein de l'Union européenne à ce propos (cf. ci-dessous 2.3).

Il convient aussi d'examiner la création d'un tel droit d'accès non-volontaire sous l'angle du droit international de la propriété intellectuelle (cf. ci-dessous 2.4).

Enfin, une analyse (synthétique) de la thématique sous l'angle du droit de la concurrence sera effectuée (cf. ci-dessous 2.5).

2.1 Réflexions sur les licences obligatoires en matière de brevets d'invention en comparaison d'un système potentiel de licence obligatoire en matière de données non-personnelles

La création d'un droit d'accès non-volontaire, ou par miroir, d'une obligation de donner accès aux données non-personnelles d'entreprises a fait l'objet de réflexions et de solutions sous différents angles juridiques sur lesquels il conviendra de se pencher.

Avant d'y procéder, il convient de s'intéresser sur le plan du principe à la nature particulière de l'objet d'un tel droit d'accès, l'accès obligatoire visant à mettre à disposition des données non-personnelles qui ne sont pas accessibles et donc sont confidentielles (et qui peuvent être protégées comme secrets d'affaires lorsque les conditions de protection sont remplies). Si ces données étaient accessibles, la question de la création d'un droit d'accès ne se poserait naturellement pas.

Or, un partage non-volontaire de données n'est pas neutre pour leur protection juridique ou pour leur contrôle de fait. En effet, tout partage de données confidentielles (même s'il est fait sur une base volontaire) comporte des risques pour la partie qui les partage[102]. En effet, si les données constituent des secrets d'affaires, le risque juridique d'un partage est que ce dernier puisse conduire à la perte de la protection si les secrets venaient à être divulgués (faute de remplir la condition du secret). Même en l'absence de protection juridique comme secret d'affaires, un partage de données signifie une perte du contrôle factuel sur celles-ci dès lors que les données ne sont alors plus sous le contrôle exclusif de leur détenteur. Lorsque le partage de données intervient sur une base contractuelle, la partie qui partage les données est en mesure de prendre des mesures afin de viser à préserver au mieux ses intérêts. L'institution d'une licence obligatoire en matière de données non-personnelles comporte ainsi des risques qui ne sont pas mineurs.

En matière de propriété intellectuelle, l'octroi de licences obligatoires est prévu en matière de brevets d'invention[103] et en matière de droit d'auteur[104]. Pour ce qui concerne l'octroi de licences obligatoires en droit des brevets, un tel octroi est soumis à des conditions strictes et bien définies et doit reposer sur une décision judiciaire. La licence obligatoire en matière de brevets d'invention porte sur un objet déterminé (soit une ou plusieurs invention[s] brevetée[s]) qui est ainsi bien identifié et statique (l'objet de la licence obligatoire n'évolue pas au fil du temps). La licence obligatoire peut en outre être retirée par le juge qui doit en particulier veiller à la « protection adéquate des intérêts légitimes » de l'ayant droit[105].

Une licence obligatoire permettant l'accès et l'utilisation de données non-personnelles porterait par contraste sur un objet qui est en général moins bien défini et qui est dynamique. Les données qui

102 Voir la célèbre formule de Lord *Donaldson,* dans le jugement anglais Attorney General v Newspaper Publishing plc, [1989] 2 FSR 27 (Ch) 48 (« Give it [soit un cube de glace, qui est comparé à une information confidentielle confiée à autrui] to the party who undertakes to keep it in his refrigerator and you still have an ice cube… Give it to the party who has no refrigerator and will not agree to keep it in one, and… you just have a pool of water which neither party wants. It is the inherently perishable nature of confidential information which gives rise to unique problems »).

103 Art. 36–40*e* de la Loi fédérale sur les brevets d'invention (Loi sur les brevets, LBI) du 25 juin 1954 (232.14) ; cf. *Thouvenin/Weber/Früh* (note 27), p. 116, évoquant l'art. 31 ADPIC comme source d'inspiration potentielle.

104 Cf. art. 23 LDA ; il est noté que la notion de licence obligatoire n'est pas uniforme en droit de la propriété intellectuelle ; référence sera faite ici à la licence obligatoire prévue en droit des brevets d'invention qui paraît la plus pertinente concernant la thématique faisant l'objet du présent article ; il sera fait abstraction de la réglementation particulière applicable en matière de licences obligatoires pour l'exportation de produits pharmaceutiques (art. 40*d* LBI et art. 31bis ADPIC).

105 Art. 40*e* al. 6 LBI « Le juge décide de l'octroi et du retrait de la licence, de son étendue et de sa durée, et de la rémunération à verser. En particulier, il retire la licence à l'ayant droit si les circonstances qui ont justifié son octroi cessent d'exister et qu'il est vraisemblable qu'elles ne se reproduiront pas. La protection adéquate des intérêts légitimes de l'ayant droit est réservée » ; on notera plus généralement que les conditions des licences obligatoires figurant dans la LBI reprennent celles de l'art. 31 ADPIC.

pourraient faire l'objet de la licence obligatoire vont fréquemment évoluer et leur volume certainement augmenter au fil du temps. Ainsi, des données non-personnelles relatives aux statistiques d'utilisation de machines industrielles ou d'objets industriels connectés auront progressivement plus de volume et ainsi plus de valeur plus la période de prélèvement de ces données sera longue et portera sur un nombre croissant de machines/objets connectés. L'objet d'une licence obligatoire sur des données non-personnelles d'une entreprise (p.ex. des données agrégées par un fabricant d'objets connectés, p.ex. des tracteurs) est complexe car les données peuvent comporter non seulement des données qui ont été générées par l'entreprise concernée (ici le fabricant) mais aussi des données provenant de tiers (p.ex. des données provenant des clients utilisateurs des objets connectés, p.ex. les utilisateurs des tracteurs). Dans un tel scénario, un mécanisme de licence obligatoire sur de telles données devrait prendre en compte cette situation et assurer que tous les titulaires de droits sur les données concernés (ici le fabricant et le client qui sont susceptibles d'être détenteurs de secrets d'affaires relatifs à ces données[106]) soient dûment rémunérés et protégés[107]. Une telle situation est manifestement plus complexe que celle d'une licence obligatoire en matière de brevets d'invention qui porte sur un droit exclusif identifié (une invention brevetée) dont le titulaire est identifié (soit le propriétaire du brevet d'invention concerné).

L'octroi d'une licence obligatoire sur des données non-personnelles soulève également la question de la responsabilité éventuelle du donneur de licence notamment en cas d'inexactitude des données[108] ou d'autres défauts affectant le droit d'utilisation sur les données qui viendraient entraver leur usage par le preneur de licence obligatoire[109] (p.ex. dans le cas de prétentions de tiers sur les données concédées sous licence obligatoire ou d'autres causes de manque de fiabilité des données faisant l'objet de la licence, p.ex. en raison du fait qu'elles auraient fait l'objet de manipulations, potentiellement par des tiers dans le cadre d'une cyberattaque, à l'insu du donneur de licence). Ceci sera fréquemment réglé expressément dans le cadre d'un partage volontaire de données[110]. Si cette question se pose certes également en matière de licences obligatoires de brevet d'invention[111], elle est sensiblement plus délicate pour un système de licences obligatoires sur des données non-personnelles.

Il est en outre vraisemblable que l'usage des données qui sera fait par un preneur de licence obligatoire (notamment l'agrégation des données concédées en licence avec d'autres données dans le contexte de l'exploitation de données massives et d'outils d'intelligence artificielle) soit un usage tel qu'il ne sera pratiquement pas possible de le faire cesser ultérieurement car les données seront agrégées et combinées avec d'autres de sorte qu'elles seront « inextricablement liées »[112] entre elles. Il ne sera dès lors pratiquement pas possible de mettre un terme à un tel usage et donc de mettre un terme à la licence obligatoire[113].

106 Voir texte à notes 79–80 ci-dessus.

107 La question se posera notamment des modalités de répartition de la rémunération qui sera due à ces titulaires.

108 Ceci peut être lié à la responsabilité en matière de décisions automatisées/basées sur de solutions d'intelligence artificielle, voir *Clara-Ann Gordon/Tanja Lutz,* Haftung für automatisierte Entscheidungen – Herausforderungen in der Praxis, RSDA 2020, p. 53 ; une responsabilité peut aussi découler du risque de désanonymisation de données qui étaient initialement des données personnelles avant d'avoir été anonymisées et qui, recoupées avec d'autres données, pourraient conduire à la réidentification des personnes concernées et donc à des risques de violation de la réglementation en matière de données personnelles.

109 Par comparaison, on notera que la jurisprudence confirme la responsabilité d'un donneur de licence dans un contrat de licence de savoir-faire qui est garant « de la possibilité d'exécution et d'utilisation des instructions techniques », ATF 115 II 255 (regeste « Le donneur de licence est garant, en particulier si le rapport contractuel est onéreux, de la possibilité d'exécution et d'utilisation des instructions techniques »).

110 La question de la responsabilité d'un donneur de licence volontaire est naturellement très importante et fait l'objet de réflexions, p.ex. dans le code de conduite UE pour le partage des données agricoles (note 80), p. 12.

111 Le risque peut aussi exister en matière de licence obligatoire sur une invention brevetée, mais il est sensiblement réduit compte tenu de l'objet déterminé de l'objet de la licence (soit une invention déterminée) ; une question ouverte reste néanmoins de déterminer le sort des redevances payés en cas de déclaration ultérieure de nullité du brevet ; on peut supposer que la question sera réglée par analogie à l'approche jurisprudentielle applicable en matière de licence contractuelle (ATF 116 II 191).

112 Pour reprendre ici la formule utilisée dans les Lignes Directrices (note 12), para. 2.2.

113 Etant relevé qu'en matière de licence obligatoire en droit des brevets, « L'étendue et la durée de la licence sont limitées aux fins auxquelles elle a été octroyée » (art. 40*e* al. 2 LBI).

Dans cette mesure, on peut estimer que, dans nombre de cas, la licence obligatoire qui serait concédée sera factuellement une licence définitive et sans limite de temps[114], ce qui pourrait se refléter dans la rémunération due en contre-partie de l'octroi de la licence obligatoire ou dans d'autres obligations que pourrait avoir le preneur de licence envers le donneur (obligation de partager à son tour les données) dans un mécanisme de licences croisées.

En matière de licence obligatoire sur des brevets d'invention, la licence porte sur l'utilisation d'un brevet suisse (ou de la partie suisse d'un brevet européen) et est ainsi géographiquement limitée à l'usage de l'invention dans l'Etat concerné (en vertu du principe de la territorialité), la licence étant de surcroît « octroyée principalement pour l'approvisionnement du marché intérieur »[115]. En matière de licence obligatoire sur des données, il sera par contraste sensiblement plus délicat de déterminer et de restreindre la portée territoriale de la licence et ainsi l'aire géographique de l'usage des données sur un territoire déterminé (par hypothèse la Suisse) compte tenu de la mobilité des données et de la globalité de l'usage de celles-ci. Ceci peut soulever des questions complexes de droit applicable (droit impératif) et de « souveraineté sur les données » (data sovereignty).

Compte tenu de ces éléments, l'octroi d'une licence obligatoire sur des données non-personnelles est beaucoup plus complexe qu'une licence obligatoire sur une invention brevetée[116]. Il est ainsi d'autant plus difficile de déterminer la « rémunération adéquate »[117] qui devrait être due en contrepartie de l'octroi de la licence obligatoire permettant l'usage des données. La détermination du prix de données est en effet très délicate et variable en fonction des circonstances (la taille et aussi – surtout – la qualité – du jeu de données (ce qui pose la question de la manière de déterminer comment celle-ci devra être appréciée), l'activité/le secteur d'activités de l'entreprise concernée, la position sur le marché de celle-ci, etc.), et présente le risque d'asymétrie d'information[118]. Ce risque d'asymétrie de l'information rend d'ailleurs beaucoup plus complexe tout le processus de négociation entre les parties qui doit en principe précéder l'initiation d'une procédure judiciaire d'octroi de licence obligatoire (une licence obligatoire n'étant octroyable que « lorsque les efforts entrepris par le requérant afin d'obtenir une licence contractuelle à des conditions commerciales raisonnables n'ont pas abouti dans un délai raisonnable », art. 40*e* al. 1 LBI), dès lors qu'un preneur de licence potentielle ne connaît pas le contenu des données non-personnelles auxquelles il souhaiterait potentiellement demander l'accès (à la différence d'une licence obligatoire en matière de brevets d'invention où l'objet de la négociation est clairement identifié – soit l'invention brevetée –).

2.2 Réflexions sur les licences FRAND en matière de brevets essentiels à une norme (Standard Essential Patents, SEP) en comparaison d'un système potentiel de licence FRAND en matière de données non-personnelles

Le concept de licence FRAND (Fair, Reasonable and Non-Discriminatory) s'est développé en matière de brevets dits « essentiels à une norme » (Standard Essential Patents)[119]. Un brevet est considéré comme

114 Voir dans ce context, les réflexions intéressantes du tribunal anglais dans l'affaire Regina Glass Fibre Ltd v Werner Schuller [1972] FSR 141 (« [W]hen confidential information or know-how is given so as to enable a business to be established, it is given for all time. When the agreement comes to an end, there is no right to acquire further information, but the recipient can go on using that which he has already received. He is not bound to close down the business which he has built up by using it. »).

115 Art. 40*e* al. 4 LBI (sous réserve de la situation particulière régie par l'art. 40*d* LBI).

116 On notera que le Rapport Experts 2018 (note 1), p. 106–107, ne discute pas ces questions et semble estimer que l'octroi des licences obligatoire en matière de données ne soulève pas de difficultés additionnelles majeures ; ce rapport identifie néanmoins quelques points devant être réglementés par le législateur.

117 Art. 40*e* al. 5 LBI (« Le titulaire du brevet a droit à une rémunération adéquate. Celle-ci est déterminée compte tenu du cas d'espèce et de la valeur économique de la licence »).

118 Voir Rapport OCDE 2019 (note 30), chap. IV, titre « Misaligned incentives, and limitations of current business models and markets », *<https://www.oecd-ilibrary.org//sites/276aaca8en/1/2/4/index.html?itemId=/content/publication/276aaca8-en&_csp_=a1e9fa54d39998ecc1d83f19b8b0fc34&itemIGO=oecd&itemContentType=book#section-d1e10164>*.

119 Voir *Jorge L. Contreras,* A Brief History of FRAND : Analyzing Current Debates in Standard Setting and Antitrust Through a Historical Lens, 80 Antitrust Law Journal 39 (2015), American University, WCL Research Paper No. 2014-18, *<https://ssrn.com/abstract=2374983>* ; dans une perspective suisse, voir *Florian Brunner,* « FRAND »-Obliegenheiten bei standardessentiellen Patenten aus

essentiel à une norme (établie par un organisme de normalisation, par exemple l'European Telecommunication Standards Institute, ETSI[120]) lorsque l'exploitation d'un tel brevet est « indispensable à tout concurrent envisageant de fabriquer des produits conformes à la norme à laquelle il [le brevet] est lié »[121]. Tel est en particulier le cas de nombreux brevets d'invention portant sur des technologies de l'information et de la communication (notamment afin d'assurer l'interopérabilité des systèmes de communication, p.ex. en matière de wifi). Afin de prévenir le risque d'abus qui pourrait être commis par les titulaires de tels brevets essentiels à une norme (qui exigeraient une rémunération excessive en contrepartie d'une licence d'utilisation de leurs brevets de la part d'entreprises qui souhaiteraient fabriquer et commercialiser des produits – exploitant les brevets concernés – compatibles à la norme concernée), les titulaires de tels brevets sont tenus de déclarer leurs brevets à l'organisme de normalisation et de prendre l'engagement formel (écrit) d'être disposés à accorder des licences à des conditions équitables, raisonnables et non discriminatoires (« FRAND » – « fair, reasonable, and non-discriminatory ») sur leurs brevets essentiels à la norme[122]. Ce système fait que les titulaires de brevets essentiels à une norme sont tenus de tolérer l'utilisation de leurs brevets par des entreprises tierces sur la base de licences FRAND.

Sous l'angle du droit de la concurrence, le refus d'un titulaire de brevets essentiels à une norme d'octroyer une licence FRAND sur ses brevets est en effet susceptible de constituer un abus de position dominante[123]. De plus, le titulaire de brevets essentiels à une norme peut être contractuellement tenu de concéder une licence FRAND selon l'interprétation faite de la nature contractuelle (ou précontractuelle) de l'engagement pris par le titulaire des brevets en application du droit applicable à cet engagement (étant noté que le fondement contractuel d'une telle obligation reste débattu)[124].

Sur cette base, tant le droit de la concurrence que le droit des contrats font que les titulaires de brevets essentiels à une norme sont soumis à une obligation de concéder des licences FRAND sur leurs brevets aux entreprises qui souhaitent les utiliser pour la fabrication et la commercialisation de produits compatibles à la norme concernée. Toutefois, ce que constitue matériellement le contenu de licences FRAND (en particulier comment calcule-t-on des redevances de licence FRAND ?) n'est pas défini et fait encore l'objet de nombreuses interrogations et de pratiques jurisprudentielles divergentes.

La question est ainsi de déterminer si le modèle des licences FRAND développé en matière de brevets essentiels à une norme peut être utilisé comme modèle afin de créer un système de licence FRAND en matière de données non-personnelles. Si l'on compare le contexte des licences FRAND en matière de brevets essentiels à une norme à celui existant en matière de données non-personnelles, force est de constater que ceux-ci sont juridiquement très différents.

En matière de brevets essentiels à une norme, la licence porte tout d'abord sur des brevets d'invention. Ces brevets sont ensuite jugés essentiels à une norme (et permettent ainsi aux entreprises qui souhaitent

vertrags- und kartellrechtlicher Perspektive, sic! 2019, p. 1 (cit. *Brunner,* « FRAND »-Obliegenheiten) ; *Florian Brunner,* Standardessentielle Patente und « FRAND » im Zivilprozess, sic! 2019, p. 131 (cit. *Brunner,* « FRAND » im Zivilprozess) ; sous l'angle de l'harmonisation internationale, voir *Jacques de Werra,* Les licences FRAND : Chance ou risque pour l'harmonisation globale du droit des contrats de licence de brevets ?, sic! 2019, p. 77, <*https://archive-ouverte.unige.ch/unige:114455*>) ; *Mark Anderson,* How to Draft a License Agreement that is Fair, Reasonable, and Non-Discriminatory : A Ten-Point Plan, 13 Journal of Intellectual Property Law & Practice 377 (2018) ; *Jeff Dodd/Jacques de Werra,* The Need for a Global Framework for Knowledge Transactions : Cross Border Licensing and Enforcement, in : Trade in Knowledge (Antony Taubmann éd.), à paraître en 2020.

120 <*https://www.etsi.org/*>.

121 Para. 49 du jugement de la CJUE du 16 juillet 2015 dans l'affaire C-170/13 Huawei c. ZTE.

122 Cf. p.ex. art. 6.1 de la ETSI Intellectual Property Rights Policy, <*https://www.etsi.org/images/files/IPR/etsi-ipr-policy.pdf*> (et la déclaration correspondante figurant dans l'annexe A – Appendix A) : « When an ESSENTIAL IPR relating to a particular STANDARD or TECHNICAL SPECIFICATION is brought to the attention of ETSI, the Director-General of ETSI shall immediately request the owner to give within three months an irrevocable undertaking in writing that it is prepared to grant irrevocable licences on fair, reasonable and non-discriminatory (»FRAND«) terms and conditions […] ».

123 Para. 53–54 du jugement de la CJUE du 16 juillet 2015 dans l'affaire C-170/13 Huawei c. ZTE (en application du droit européen de la concurrence, soit l'art. 102 TFUE) ; pour une discussion du droit de la concurrence, voir ci-dessous (5).

124 Pour une discussion sous l'angle du droit des contrats suisse, voir *Brunner,* « FRAND »-Obliegenheiten (note 119), p. 1 ss.

les utiliser de commercialiser des produits qui sont compatibles à la norme concernée) et enfin leur titulaire est soumis à des obligations contractuelles et de droit de la concurrence le contraignant à concéder des licences aux conditions FRAND à des tiers.

En matière de données non-personnelles, la licence FRAND ne porterait par contraste pas sur un ou plusieurs brevet(s) d'invention identifié(s) (objet statique et défini) mais sur un jeu de données (objet généralement dynamique et indéfini). Ensuite, la licence FRAND qui pourrait être octroyée sur des données non-personnelles ne viserait pas à permettre aux entreprises de commercialiser des produits qui seraient compatibles avec une norme technique élaborée par un organisme de normalisation (comme p.ex. l'ETSI qui définit et adopte les normes techniques et gère le processus de déclaration des brevets essentiels aux normes qu'elle édicte)[125]. Enfin, faute d'organisme de normalisation en matière de données non-personnelles, aucun engagement des détenteurs de telles données par lequel ils s'engageraient à concéder des licences FRAND sur leurs données ne peut aisément être obtenu, au contraire de la déclaration faite par les titulaires de brevets essentiels à une norme qui est faite en faveur des organismes de normalisation (une telle déclaration jouant un rôle fondamental sous l'angle du droit des contrats et du droit de la concurrence afin de créer un droit d'accès et d'utilisation non-volontaire des brevets essentiels à une norme). A supposer qu'un tel engagement contractuel puisse être obtenu de détenteurs de données non-personnelles (comme le sont les engagements pris par les titulaires de brevets essentiels à une norme en faveur des organismes de normalisation), on relèvera qu'il s'agirait alors d'un accès concédé *volontairement* aux données non-personnelles car opéré sur la base d'un engagement contractuel des détenteurs de telles données (ce qui sortirait alors de l'objet du présent article qui est consacré à l'analyse de l'accès non-volontaire aux données non-personnelles).

On constate en tout état qu'il existe des différences structurelles majeures entre le cas des brevets essentiels à une norme pour lequel le concept des licences FRAND s'applique et celui d'un hypothétique système de licences FRAND en matière de données non-personnelles[126]. Il apparaît sur cette base que le concept de licences FRAND n'est pas adapté au partage non-volontaire de données non-personnelles entre des entreprises, ce qui n'exclut pas l'application des principes du droit de la concurrence à ce scénario[127].

De plus, les observations qui ont été faites ci-dessus (cf. (1)) concernant les défis de la création d'une licence obligatoire sur les données non-personnelles par rapport au système de licence obligatoire existant en matière de brevet d'invention valent également dans une large mesure concernant la mise en œuvre potentielle d'un mécanisme de licences FRAND en matière de données non-personnelles.

Enfin, même à supposer que le principe des licences FRAND puisse être jugé pertinent afin de créer un accès aux données non-personnelles entre entreprises (B2B data sharing), force est de souligner que la détermination des conditions des licences FRAND reste très complexe même en matière de brevets essentiels à une norme, et ce non seulement pour ce qui concerne la rémunération due mais également pour les autres termes contractuels qui doivent également être FRAND. De nombreuses questions sont ainsi encore ouvertes s'agissant des licences FRAND en matière de brevets essentiels à une norme[128]. Les difficultés ne seront qu'accrues pour ce qui concerne l'application des principes FRAND en matière de licence sur des ensembles (datasets) de données non-personnelles. Il sera en particulier extrêmement délicat d'appliquer l'exigence de non-discrimination (Non

[125] *Thouvenin/Weber/Früh* (note 27), p. 136–137, considèrent que si les données ne sont pas reproductibles par un concurrent (p.ex. s'il s'agit de données historiques, ces auteurs relevant toutefois que les données n'ont en général de la valeur que si elles sont à jour de sorte que les données historiques n'en ont pas), il pourrait s'agir d'un cas de standardisation de fait (de facto) pour lequel le modèle de licence FRAND pourrait être pertinent.

[126] *Heiko Richter/Peter R. Slowinski,* The Data Sharing Economy: On the Emergence of New Intermediaries, IIC – International Review of Intellectual Property and Competition Law 2019, vol. 50, p. 4 (2019), *<https://doi.org/10.1007/s40319-018-00777-7>,* p. 20–21.

[127] *Richter/Slowinski* (note 126), p. 22.

[128] Sur la question, voir *Jacques de Werra,* Les licences FRAND: Chance ou risque pour l'harmonisation globale du droit des contrats de licence de brevets ?, sic! 2019, p. 77, *<https://archive-ouverte.unige.ch/unige:114455>*); *Brunner,* «FRAND»-Obliegenheiten (note 119), p. 1; *Brunner,* «FRAND» im Zivilprozess (note 119), p. 131; *Mark Anderson,* How to Draft a License Agreement that is Fair, Reasonable, and Non-Discriminatory: A Ten-Point Plan, 13 Journal of Intellectual Property Law & Practice 377 (2018)*; Dodd/de Werra* (note 119).

Discriminatory) entre les licences. En effet, il sera en général très difficile de comparer des ensembles de données et la rémunération due pour l'usage de ceux-ci, afin de faire en sorte que l'exigence de non-discrimination soit bien respectée, vu le caractère souvent unique et ainsi difficilement comparable de jeux de données non-personnelles. Ainsi, même en admettant que le système des licences FRAND constitue un modèle potentiel sur le plan du principe pour un mécanisme de licence en matière de données non-personnelles, ceci ne sera pas véritablement utile dès lors qu'il subsistera des incertitudes majeures sur ce que signifie matériellement (soit sous l'angle du contenu des obligations pécuniaires et non-pécuniaires) une licence FRAND pour le preneur d'une telle licence.

Dans ces conditions, prévoir un système de licences FRAND pour permettre l'accès aux données non-personnelles ne constitue pas une solution aisée, aussi en raison de l'absence de clarté juridique du contenu des licences FRAND (étant rappelé que les échanges de données non-personnelles supposent la création d'un cadre juridique clair et la sécurité juridique).

2.3 Travaux au sein de l'Union européenne et leur influence en Suisse

Dans le Rapport Experts 2018, le groupe d'experts s'est référé aux travaux de la Commission européenne concernant la possibilité d'introduire un système de licence obligatoire[129]. Les travaux concernés de la Commission européenne sont la Communication de la Commission du 10 janvier 2017 « Créer une économie européenne fondée sur les données »[130]. Dans cette communication, la Commission a ainsi exposé : « Dans le cadre de ses dialogues avec les parties prenantes, la Commission entend examiner les possibilités suivantes, caractérisées par différents niveaux d'intervention, pour régler le problème de l'accès aux données produites par des machines : […] – Accès moyennant rémunération : il serait possible d'établir, pour les détenteurs de données tels que les fabricants, les prestataires de services ou des tiers, un cadre potentiellement fondé sur certains principes clés, telles que des conditions équitables, raisonnables et non discriminatoires (cadre ‹FRAND›), afin qu›ils puissent donner accès, moyennant rémunération, aux données qu'ils détiennent après anonymisation de ces dernières. Il convient de tenir compte des intérêts légitimes en cause ainsi que la nécessité de protéger les secrets d'affaires. Pour tenir compte des particularités de chaque secteur, il serait aussi possible d'envisager des régimes d'accès différents en fonction des secteurs et/ou modèles économiques. Par exemple, dans certains cas, la solution de l'accès ouvert (total ou partiel) aux données pourrait être privilégiée, à la fois pour les entreprises et pour la société »[131].

On soulignera que les travaux de la Commission se concentrent ainsi sur les « données produites par des machines », soit celles qui sont « générées sans intervention humaine directe, par des processus informatiques, des applications ou des services, ou par des capteurs qui traitent des informations reçues d'équipements, de logiciels ou de dispositifs virtuels ou réels »[132], ce qui constituent ainsi des données industrielles[133].

La thématique de l'accès aux données non-personnelles a fait l'objet de nouveaux développements au sein de l'Union européenne. Elle a notamment fait l'objet de réflexions importantes dans la Communication de la Commission « une stratégie européenne pour les données » du 19 février 2020[134]. La Commission européenne a ainsi indiqué qu'elle « examinera la nécessité d'une action législative sur des questions ayant une incidence sur les relations entre les acteurs dans une économie habile à tirer parti des données, afin de prévoir des incitations au partage transsectoriel des données horizontales (en complément du partage des données intrasectoriel tel que décrit dans l'appendice [qui sera évoqué plus bas]). Une ou plusieurs des questions suivantes pourraient faire l'objet d'une loi sur les données (2021) : […]

– l'accès aux données ne devrait être rendu obligatoire que lorsque des circonstances spécifiques l'exigent[39] [le texte de la note de bas de page 39 expose : ‹ Un droit d'accès aux données devrait toujours être sectoriel et n'être accordé qu'en cas de défaillance du marché avéré ou prévue et à laquelle le droit de la concurrence ne peut remédier. La portée d'un droit d'accès aux données devrait tenir compte des intérêts légitimes du

129 Rapport Experts 2018 (note 1), p. 106.
130 Communication CE 2017 (note 39).
131 Communication CE 2017 (note 39), para. 3.5.
132 Communication CE 2017 (note 39), para. 3.1.
133 Note 14.
134 Communication CE 2020 (note 16).

titulaire des données et doit respecter le cadre juridique applicable›], et lorsque tel est le cas, dans des conditions équitables, transparentes, raisonnables, proportionnées et/ou non discriminatoires[40] [le texte de la note de bas de page 40 expose : ‹Des variantes de ce principe s'appliquent en particulier en ce qui concerne certaines informations relatives à la réparation et l'entretien des véhicules à moteur devant être rendues accessibles en application du règlement (CE) nº 715/2007, ainsi que pour les informations résultant d'essais sur des animaux vertébrés en application du règlement (CE) nº 1907/2006 (REACH)›] »[135].

L'appendice à la Communication de la Commission 2020 donne des informations complémentaires concernant la création d' « espaces de données spécifiques à certains secteurs et domaines »[136] sous le titre d' « Espaces européens communs des données dans des secteurs stratégiques et des domaines d'intérêt public »[137] et vise ainsi à fournir « des informations complémentaires sur les politiques et la législation sectorielles qui sous-tendent la création de ces espaces dans les différents secteurs et domaines »[138]. L'appendice traite en particulier de l' « Espace européen commun des données relatives à l'industrie (manufacturière) »[139] à propos duquel la Commission indique qu'elle « traitera les questions liées aux droits d'exploitation des données industrielles co-produites (données de l'internet des objets créées en milieu industriel), dans le cadre d'une loi plus générale sur les données (T4 2021) »[140] et qu'elle « rassemblera les principaux acteurs du secteur manufacturier pour s'accorder, d'une manière conforme aux règles de concurrence et aux principes des contrats équitables, sur les conditions dans lesquelles ils seraient prêts à partager leurs données et sur les moyens de renforcer la production de données, à l'aide notamment de produits connectés intelligents (à partir du T2 2020). Lorsque des données produites par des personnes sont concernées, il convient de prendre leurs intérêts pleinement en compte dans le cadre d'un tel processus et de garantir le respect des règles en matière de protection des données »[141].

L'appendice mentionne ainsi spécifiquement les « questions liées aux droits d'exploitation des données industrielles co-produites », conçues comme des « données de l'internet des objets créées en milieu industriel ». On doit ainsi comprendre que la notion de données « co-produites » vise les données collectées et ainsi « co-produites » sur des objets connectés (internet des objets), ces données étant ensuite envoyées au fabricant et consolidées (et donc « co-produites ») par ce dernier.

2.4 Droit d'accès non-volontaire aux données non-personnelles en droit international de la propriété intellectuelle

Dès lors que les données non-personnelles peuvent être protégées comme secrets d'affaires, se pose la question de la mesure dans laquelle un accès à ces données peut être concédé sans l'accord du détenteur de ces secrets, particulièrement dans le cadre de licences obligatoires, soit de licences qui sont concédées à certaines conditions sans l'accord du titulaire du droit.

En droit international de la propriété intellectuelle, le mécanisme de licence obligatoire prévu en matière de brevets d'invention (art. 31 et 31bis ADPIC) permet de conférer un droit d'utilisation d'une invention brevetée sans l'accord du titulaire du brevet d'invention.

L'ADPIC ne comporte pas de disposition traitant des licences obligatoires en matière de secrets d'affaires (soit de « renseignements non divulgués » selon la terminologie de l'art. 39 ADPIC). Dans le cadre des négociations de l'ADPIC, la Suisse avait proposé une disposition interdisant l'octroi de licences obligatoires sur les « informations propriétaires » (proprietary information)[142]. Cette disposition n'a toutefois

135 Communication CE 2020 (note 16), p. 16.
136 Communication CE 2020 (note 16), p. 31.
137 *Ibid.*
138 *Ibid.*
139 *Ibid.*
140 *Ibid.*
141 *Ibid.*
142 Doc. Standards and Principles Concerning the Availability, Scope and Use of Trade-Related Intellectual Property Rights – Addendum on Proprietary Information – Communication from Switzerland, MTN.GNG/NG11/W/38/Add.1 du 11 décembre 1989, qui disposait : « Standards on Proprietary Information – The following standards are essential in order to achieve effective protection of proprietary information : […] (iv) There shall be no compulsory licensing of proprietary information » ; le texte de la proposition de la Suisse figure à la p. 214 de l'ouvrage de

pas été retenue dans le texte final de l'art. 39 ADPIC qui ne comporte ainsi aucune référence en matière de licence obligatoire sur les secrets d'affaires (l'ADPIC ne comportant aucune disposition à ce propos).

Une telle absence d'interdiction d'octroi de licences obligatoires en matière de secrets d'affaires, par contraste à ce qui est expressément prévu en matière de droit des marques (art. 21 ADPIC[143]) a été conçue par un auteur comme une autorisation de concéder des licences obligatoires[144].

Une restriction à la protection des secrets d'affaires qui serait imposée contre la volonté du détenteur des secrets d'affaires devrait en tout état pouvoir se justifier sous l'angle des principes généraux de l'ADPIC[145]. Une licence obligatoire sur les données non-personnelles pourrait aussi se fonder sur le droit de la concurrence (art. 40 ADPIC), qu'il convient ainsi d'examiner.

Il en résulte ainsi que le droit international de la propriété intellectuelle n'exclut pas le principe de l'octroi de licences obligatoires sur des données non-personnelles (lorsque celles-ci sont protégées comme secrets d'affaires).

2.5 Droit de la concurrence

Le droit de la concurrence peut offrir la possibilité de donner un accès non-volontaire à des données non-personnelles dans certaines circonstances[146]. Tel est en particulier le cas lorsque le refus d'accès à ces données par leur détenteur constitue un abus de position dominante[147]. Un tel refus ne pourra toutefois pratiquement être sanctionné qu'à l'encontre d'un nombre très restreint d'acteurs économiques à qui un tel abus de position dominante pourrait être reproché. En droit suisse, l'art. 7 LCart[148] dispose que «les pratiques d'entreprises ayant une position dominante sont réputées illicites lorsque celles-ci abusent de leur position et entravent ainsi l'accès d'autres entreprises à la concurrence ou son exercice, ou désavantagent les partenaires commerciaux» (al. 1) et qu'est en particulier réputé illicite «le refus d'entretenir des relations commerciales (p.ex. refus de livrer ou d'acheter des marchandises)» (al. 2 let. a).

L'art. 3 al. 2 1re phrase LCart dispose pour sa part que la LCart «n'est pas applicable aux effets sur la concurrence qui découlent exclusivement de la législation sur la propriété intellectuelle». Conformément à la jurisprudence, on doit considérer que l'art. 3 al. 2 LCart qui prévoit ainsi un traitement préférentiel des titulaires de droits de propriété intellectuelle est d'application restrictive et que le droit de la concurrence doit ainsi largement s'appliquer. Ainsi, la question de l'application potentielle du droit de la propriété intellectuelle doit faire l'objet d'une analyse dans le cadre de l'application matérielle du droit de la concurrence (sans que l'on puisse dès lors considérer

Nuno Pires de Carvalho, The TRIPS Regime of Antitrust and Undisclosed Information, La Haye 2008.

143 L'art. 21 ADPIC.

144 *Pires de Carvalho* (note 142), para. 39.3.197 p. 309.

145 Art. 7 et 8 ADPIC.

146 Le présent article ne peut pas traiter de manière détaillée toutes les questions complexes et en cours d'évolution relatives à l'application du droit de la concurrence dans l'économie des données; voir le très récent ouvrage de *Beata Mäihäniemi,* Competition Law and Big Data: Imposing Access to Information in Digital Markets, Cheltenham (Edward Elgar) 2020; *Sebastian Louven,* Shaping Competition Policy in the Era of Digitization – Access to Data, 2018, *<https://ec.europa.eu/competition/information/digitisation_2018/contributions/sebastian_louven_oldenburg_centre_for_law_of_the_information_society.pdf>; idem,* Datenmacht und Zugang zu Daten, Neue Zeitschrift für Kartellrecht 2018, p. 217; *Sebastian Telle,* Kartellrechtlicher Zugangsanspruch zu Daten nach der essential facility doctrine, in: Immaterialgüter und Digitalisierung (Moritz Hennemann/Andreas Sattler éds.), Baden-Baden 2017, p. 73; voir aussi l'intéressant rapport conjoint de l'Autorité de la concurrence française et du Bundeskartellamt allemand, Droit de la concurrence et données, 10 mai 2016, *<https://www.autoritedelaconcurrence.fr/sites/default/files/2019-05/rapport-concurrence-donnees-vf-mai2016.pdf>* (version anglaise: *<https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.html>*); on rappellera que le droit de la concurrence joue un rôle important dans le cadre de l'octroi de licences FRAND sur les brevets essentiels à une norme, cf. ci-dessus 2.2.

147 D'autres approches sont explorées afin de justifier un droit d'accès aux données au-delà de l'abus de position dominante, cf. p.ex. (sous l'angle de la dépendance économique), *Thomas Tombal,* Economic Dependence and Data Access, IIC – International Review of Intellectual Property and Competition Law 2020, vol. 51, p. 70, *<https://doi.org/10.1007/s40319-019-00891-0>;* à l'inverse, un partage de données peut aussi être constitutif de violations du droit de la concurrence dans certaines circonstances (accords illicites), voir *Heike Schweitzer,* Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung, GRUR 2019, p. 569, p. 572.

148 Loi fédérale sur les cartels et autres restrictions à la concurrence (Loi sur les cartels, LCart, RS 251) du 6 octobre 1995.

que les titulaires de droits de propriété intellectuelle seraient entièrement soustraits à l'application du droit de la concurrence)[149].

La détermination de l'existence d'un abus de position dominante en matière d'accès à des données non-personnelles est complexe et délicate[150] et le droit est encore en évolution[151]. Cette question s'inscrit dans le cadre de la thématique plus large de l'application du droit de la concurrence à l'économie numérique[152] et aux données massives (big data), étant relevé que l'adaptation potentielle du droit européen de la concurrence pour faire face aux défis posés par les grandes plates-formes Internet fait l'objet d'une consultation par la Commission européenne[153]. Parmi les options de réforme évoquées figure en particulier l'adoption de mesures *ex ante* qui pourraient permettre de créer un accès non-volontaire aux données non-personnelles[154].

L'application du droit de la concurrence suppose en particulier de déterminer le marché pertinent et le caractère substituable (ou non) des données, ce qui est très complexe s'agissant de données[155]. La démonstration du caractère abusif du refus de concéder un accès aux données est également délicate, et ce même si ces données ne sont pas protégées par le droit de la propriété intellectuelle. De manière synthétique, un refus d'octroyer l'accès aux données est considéré comme abusif s'il porte sur des données qui sont indispensables pour être actif sur un marché (en aval), si le refus d'octroyer l'accès conduit à une exclusion du marché concerné et empêche l'introduction d'un nouveau produit (pour lequel il existe une demande potentielle) sur ce marché et si ce refus n'est pas objectivement justifiable[156].

L'application du droit de la concurrence, et particulièrement des règles en matière d'abus de position dominante, n'est pas jugée optimale pour résoudre de manière systématique et générale la question de l'accès aux données non-personnelles des entreprises, particulièrement en raison des modalités de la mise en œuvre du droit de la concurrence résultant de son approche ex post, et de la lourdeur ainsi que de la durée des procédures de droit de la concurrence)[157].

149 Voir l'arrêt du Tribunal administratif fédéral B-831/2011 du 18 décembre 2018 dans l'affaire Six Group AG/SIX Payment Services AG c. COMCO, para. 85–88 ; il faut relever que la procédure est pendante devant le Tribunal fédéral ; voir aussi para. 47 du jugement de la CJUE du 16 juillet 2015 dans l'affaire C-170/13 Huawei c. ZTE.

150 Pour un aperçu en droit européen de la concurrence, voir *Drexl* (note 36), para. 123 ss.

151 La jurisprudence est assez rare, voir le litige ayant opposé PeopleBrowsr et Twitter aux Etats-Unis d'Amérique, et l'analyse de cette affaire faite par *Zachary Abrahamson,* Essential Data*,* 124 Yale L.J. (2014), *<https://digitalcommons.law.yale.edu/ylj/vol124/iss3/7>*.

152 *Nicolas Petit,* Big Tech and the Digital Economy, Oxford 2020; *Viktoria H.S.E. Robertson,* Antitrust Law and Digital Markets : A Guide to the European Competition Law Experience in the Digital Economy (February 28, 2020), *<https://ssrn.com/abstract=3631002>;* voir aussi *Adrien Alberini,* Pouvoir de marché dans le secteur numérique : l'accès à de larges quantités de données est-il suffisant ?, RSDA 2019, p. 31 et *Maurice E. Stucke/Allen P. Grunes,* Big Data and Competition Policy*,* Oxford 2016.

153 Voir Paquet législatif sur les services numériques – instrument de régulation ex ante des très grandes plateformes en ligne jouant le rôle de contrôleurs d'accès (« gatekeepers »), 2 juin 2020, <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12418-Digital-Services-Act-package-ex-ante-regulatory-instrument-of-very-large-online-platforms-acting-as-gatekeepers>.

154 Voir Analyse d'impact initiale, Ares (2020)2877647, 4 juin 2020 (anglais) accessible depuis *<https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12418-Digital-Services-Act-package-ex-ante-regulatory-instrument-of-very-large-online-platforms-acting-as-gatekeepers>,* sec. B.3b.

155 Voir *Thouvenin/Weber/Früh* (note 27), p. 127 ss, p. 129 ; *Weber,* Jusletter 2019 (note 27), para. 24–27 ; Position Statement MPI 2016 (note 33), para. 33 : « it is by no means clear how the relevant market for data should be defined when access concerns not individual data, but large data sets for datamining purposes, and under what conditions different data sets can be considered as substitutable ».

156 *Weber,* Jusletter 2019 (note 27), para. 28 ; *Thouvenin/Weber/Früh* (note 27), p. 131–132, en référence à la jurisprudence dans l'affaire Morningstar c. Commission européenne, jugement T-76/14 du 15 septembre 2016 ; voir aussi *Rolf H. Weber,* Improvement of Data Economy through Compulsory Licences ?, in : Trading Data in the Digital Economy : Legal Concepts and Tools, Münster Colloquia on EU Law and the Digital Economy III (Sebastian Lohsse/Reiner Schulze/Dirk Staudenmayer éds.), Münster 2017, p. 135 ; pour des réflexions en droit allemand, voir Bundeskartellamt, Big Data und Wettbewerb, Schriftenreihe Wettbewerb und Verbraucherschutz in der digitalen Wirtschaft» , No. 1, Bonn 2017, p. *<https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Schriftenreihe_Digitales/Schriftenreihe_Digitales_1.pdf?__blob=publicationFile&v=3>*.

157 *Weber,* Jusletter 2019 (note 27), para. 29 ; *Drexl* (note 36), para. 185 ; Position Statement MPI 2016 (note 33),

La question de l'abus de position dominante peut particulièrement se poser en matière d'accès aux interfaces de programmation d'application (Application Programming Interfaces API) qui peuvent être essentielles pour les entreprises souhaitant être actives sur le marché[158], ce qui soulève la question de leur protection potentielle par le droit d'auteur, même si l'existence ou non d'une telle protection n'a pas nécessairement d'impact sur l'analyse à conduire en droit de la concurrence[159].

III. Conclusion

A la lumière des éléments analysés dans le présent article, il apparaît que l'introduction d'un système général et horizontal (soit non-spécifique à un secteur) de licence obligatoire et de licences FRAND visant à créer un accès non-volontaire aux données non-personnelles des sociétés soulève de nombreuses questions.

Certains instruments juridiques existants peuvent offrir des solutions ponctuelles. Le droit de la concurrence peut ainsi créer un tel accès selon les modalités et contingences qui lui sont propres (comme c'est le cas pour les licences FRAND développées en matière de brevets essentiels à une norme). Le droit de la concurrence n'est toutefois pas adapté pour offrir une solution générale et systématique, en raison de l'approche *ex post* qui vise essentiellement à sanctionner des abus de position dominante se produisant dans des circonstances exceptionnelles (soit celles dans lesquelles l'abus de position dominante peut être établi). Le droit de la concurrence ne permet donc pas de fonder un mécanisme général de partage et d'échange généralisé de données non-personnelles entre entreprises (étant rappelé que la Commission européenne explore actuellement une réforme du droit de la concurrence pouvant conduire à l'adoption d'une approche *ex ante* qui ne serait toutefois applicable qu'aux très grandes plateformes en ligne jouant le rôle de contrôleurs d'accès (« gatekeepers »)[160].

Sur le plan général, dans la mesure où la création d'un accès non-volontaire à des données non-personnelles d'une entreprise peut créer un risque particulier pour cette dernière (soit celui de la perte de contrôle sur ces données), il convient de prendre en compte ce risque et ainsi de ne considérer l'introduction d'un partage obligatoire de données que si cela est indispensable afin d'atteindre certains objectifs d'intérêt public poursuivis qui seraient jugés prépondérants. Sur cette base, l'on doit considérer avec retenue l'introduction de mécanismes juridiques non-volontaires de partage de données non-personnelles[161] et ne considérer cette solution qu'en l'absence d'efficacité des mécanismes de partage volontaire de données non-personnelles[162].

Au-delà de cette considération générale, on peut répondre aux questions relatives à la faisabilité, la désirabilité et la compatibilité aux normes internationales de la création d'un système de licence obligatoire ou de licence FRAND (qu'il convient de traiter de manière séparée) visant à concéder un d'accès

para. 32 et 38 ; voir aussi *Christian Rusche/Marc Scheufen,* On (intellectual) property and other legal frameworks in the digital economy : An economic analysis of the law, IW-Report, No.48/2018, Institut der deutschen Wirtschaft (IW), Cologne, p. 25, *<https://www.econstor.eu/bitstream/10419/190945/1/104386220X.pdf>*.

158 Voir le litige SIX (note 149).

159 Arrêt du Tribunal administratif fédéral B-831/2011 (note 149), para. 939–949 (ce en raison de l'art. 21 LDA qui prévoit une exception en faveur des décompilations) ; sur le plan général, conférer un accès non-volontaire à des données qui ne sont pas protégées par le droit de la propriété intellectuelle devrait être soumis à des conditions moins strictes par comparaison à l'octroi d'un accès non-volontaire à des données qui sont protégées par le droit de la propriété intellectuelle, cf. *Thouvenin/Weber/Früh* (note 27), p. 131–132.

160 *<https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12418-Digital-Services-Act-package-ex-ante-regulatory-instrument-of-very-large-online-platforms-acting-as-gatekeepers>*.

161 Voir Rapport OCDE 2019 (note 30), 4. Risks and challenges of data access and sharing/Misaligned incentives, and limitations of current business models and markets, *<https://www.oecd-ilibrary.org//sites/276aaca8-en/1/2/4/index.html?itemId=/content/publication/276aaca8-en&_csp_=a1e9fa54d39998ecc1d83f19b8b0fc34&itemIGO=oecd&itemContentType=book#section-d1e10164>*.

162 Voir le très intéressant rapport du gouvernement hollandais (Ministry of Economic Affairs and Climate Policy), Dutch Digitalisation Strategy – Dutch vision on data sharing between businesses, février 2019 (cit. Dutch Vision 2019), *<https://www.government.nl/documents/reports/2019/02/01/dutch-vision-on-data-sharing-between-businesses>*, p. 21 ; cf. aussi le tableau contenu dans ce rapport qui représente un intéressant arbre de décision (« decision tree »), p. 25.

non-volontaire aux données non-personnelles détenues par des sociétés privées comme suit :

S'agissant de l'introduction d'un *mécanisme général de licences obligatoires* permettant de donner un accès non-volontaire aux données non-personnelles entre entreprises, on peut considérer qu'un tel système est théoriquement faisable, sachant qu'il est pratiqué dans certains cas et secteurs spécifiques[163]. Le droit de la concurrence (certes dans des conditions spécifiques, soit en cas d'abus de position dominante) le permet d'ores et déjà (même si ceci n'est envisageable que dans certains cas particuliers, vu notamment la difficulté d'établir un abus de position dominante).

– Quant à sa *désirabilité,* un tel système généralisé ne paraît pas souhaitable en raison des difficultés liées à sa mise en œuvre (résultant en particulier des différences existant entre une licence obligatoire de brevet d'invention et une licence obligatoire en matière de données non-personnelles) et des risques qu'il créerait pour les intérêts du détenteur des données non-personnelles. Un tel système pourrait être adéquat ponctuellement dans certains secteurs particuliers dans lesquels l'existence d'un intérêt public prépondérant pourra être établi et dont les conditions d'application seraient spécifiées[164]. La mise en œuvre de multiples solutions sectorielles reste toutefois un processus lourd et risque de créer des approches cloisonnées susceptibles de soulever des questions de cohérence et de traitements différenciés entre domaines. De plus, la pondération des intérêts à effectuer entre l'intérêt à la protection de la confidentialité des données et celui de l'intérêt public prépondérant au partage de celles-ci sera souvent délicate.
– Quant à la compatibilité aux normes internationales et particulièrement avec le droit international de la propriété intellectuelle, un système de licence obligatoire y est en principe compatible pour autant qu'il respecte les règles générales de l'accord ADPIC (étant rappelé que les restrictions au droit de propriété intellectuelle peuvent particulièrement résulter du droit de la concurrence, cf. art. 40 ADPIC).

Dans ces conditions, la mise en œuvre d'un système de licence obligatoire pour l'accès à des données non-personnelles ne devrait être conçue qu'à titre subsidiaire et n'être ainsi envisagée que lorsque toutes les mesures visant à promouvoir le partage et l'échange volontaires de données non-personnelles ont échoué (c'est ce que prévoit la loi comme principe général pour l'octroi de licences obligatoires en matière de brevets d'invention en vertu de l'art. 40*e* al. 1 LBI).

Pour ce qui concerne l'analyse de la faisabilité, de la désirabilité et de la compatibilité aux normes internationales de la création d'un *mécanisme général de licence FRAND,* on peut douter qu'une telle approche soit faisable sur le plan du principe au vu des différences systémiques existant entre la situation des brevets essentiels à une norme pour laquelle les licences FRAND se sont développées et celle de l'accès aux données non-personnelles. Il est ainsi très délicat de percevoir comment le système des licences FRAND tel qu'il est appliqué en matière de brevets essentiels à une norme pourrait être transposé afin de créer un accès général aux données non-personnelles entre entreprises (B2B data sharing). Sur cette base, une telle approche ne paraît pas désirable vu les obstacles auxquels elle se heurte. En outre, le fait d'exiger que le contenu de licences en matière de données non-personnelles soit FRAND n'est pas d'une grande utilité dès lors que le contenu matériel des licences FRAND reste incertain même en matière de brevets essentiels à une norme. De plus, l'application de l'exigence de non-discrimination entre licences FRAND en matière de données non-personnelles sera très délicate en pratique vu la grande difficulté à comparer des jeux de données non-personnelles. La compatibilité d'un

163 Cf. p.ex. l'obligation des constructeurs automobiles de partager les informations sur la réparation et l'entretien des véhicules en faveur des opérateurs indépendants en vertu du Règlement européen 715/2007 du 20 juin 2007 (tel que modifié par différents réglements postérieurs) relatif à la réception des véhicules à moteur au regard des émissions des véhicules particuliers et utilitaires légers (Euro 5 et Euro 6) et aux informations sur la réparation et l'entretien des véhicules (art. 6–9) ; cf. aussi l'obligation similaire de partage d'informations instituée par le Règlement européen 2018/858 du 30 mai 2018 relatif à la réception et à la surveillance du marché des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, modifiant les règlements (CE) no 715/2007 et (CE) no 595/2009 et abrogeant la directive 2007/46/CE, applicable dès le 1er septembre 2020 (art. 61 à 66).

164 Cf. art. 8 al. 1 ADPIC ; s'agissant d'une restriction potentielle à la protection des secrets d'affaires ; cf. aussi Dutch Vision 2019 (note 162), p. 21.

système de licence FRAND avec le droit international ne devrait toutefois pas être problématique dans la mesure où un tel système reposerait sur l'application du droit de la concurrence et/ou sur un engagement contractuel pris par le détenteur des données non-personnelles (qui aurait pris l'engagement de concéder des licences à des conditions FRAND, comme le font les titulaires de brevets essentiels à une norme).

Il résulte de cette analyse concernant les licences obligatoires et les licences FRAND que ces mécanismes ne constituent pas une source adaptée pour la création d'un mécanisme d'accès non-volontaires aux données non-personnelles (cette approche ne garantissant en effet pas la clarté et la sécurité juridique[165]) et que l'approche à privilégier est ainsi celle visant à favoriser un partage volontaire des données non-personnelles[166].

En tout dernier lieu, il convient d'être conscient, sur un plan stratégique et concurrentiel sur le marché global des données non-personnelles, qu'aussi désirable que puisse paraître la création d'un droit d'accès (en faveur d'entreprises suisses) aux données non-personnelles détenues par des entreprises étrangères, et particulièrement aux masses de données détenues par les géants (étrangers) des données (visant à ainsi à tenter de faire face à un phénomène de colonialisme des données – « data colonialism »[167] –)[168], force est de constater que l'octroi d'un tel droit d'accès obligatoire pourrait également et à l'inverse être susceptible de donner à toute entreprise (et donc aussi à de puissantes entreprises étrangères) un accès non-volontaire aux données d'entreprises suisses. La réflexion concernant l'introduction d'un tel droit d'accès doit ainsi être conduite également à la lumière de ces développements de géopolitique des données[169].

165 Cf. note 8.

166 Voir Dutch Vision 2019 (note 162), p. 17, exposant trois principes dont le premier est de privilégier le partage volontaire : « The guiding principles for data sharing between businesses are : Voluntary data sharing is preferable ; Data sharing will be made compulsory, where necessary ; People and businesses will retain control of their data »).

167 Voir *Yuval Noah Harari,* Who Will Win the Race for AI ?, *<https ://foreignpolicy.com/gt-essay/who-will-win-the-race-for-ai-united-states-china-data/>* (« […] the world could soon witness a new kind of colonialism – data colonialism – in which raw information is mined in numerous countries, processed mainly in the imperial hub, and then used to exercise control throughout the world. For example, data giants in San Francisco or Shanghai could compile the entire medical and personal history of politicians and officials in distant countries and use it to influence them or manipulate public opinion about them. Beyond that, those who control the data could eventually reshape not only the world's economic and political future but also the future of life itself ») ; voir aussi *Nick Couldry/Ulises A. Mejias,* The Costs of Connection : How Data Is Colonizing Human Life and Appropriating It for Capitalism, Stanford 2019.

168 *Thouvenin/Weber/Früh* (note 27), p. 198 (concluant l'ouvrage en indiquant : « Ein möglicher Ansatz ist hingegen die Einführung von griffigen Zugangsrechten zu Daten marktmächtiger Unternehmen ») ; ceci pose au demeurant la question du champ d'application territorial du droit d'accès aux données non-personnelles (cf. ci-dessus texte à note 115) : à supposer qu'un droit d'accès non-volontaire puisse être créé sur des données non-personnelles d'une société ayant son siège à l'étranger, on peut douter que cette société puisse être contrainte de concéder un droit d'accès pour toutes ses données sur le plan global ; la tension entre opérations globales des entreprises et ordres judiciaires locaux est naturellement connue et fréquente en matière de litiges relatifs à l'économie du numérique et relatifs aux plateformes Internet.

169 Voir p.ex. *Amaël Cattaruzza,* Géopolitique des données – Pouvoir et conflits à l'heure du Big Data, Paris 2019.