Five Things You Need to Know About IP & Technology Law in 2022

Since 2020, the Covid-19 pandemic has disrupted business continuity and work habits, and most organisations have had to adapt their organisational and business processes to deal with the situation. The vast majority have thus had to adopt digital tools and technologies to allow for more flexible working arrangements, thereby accelerating the digital transformation some had already started.

In the field of IP & technology law, we have identified the following five trends, triggered by this movement, which will shape your agenda in the coming year. Increasingly digitalised ways of doing business and working have led to a rise in the automatic processing of personal data. Homeworking, the steady growth of e-commerce, and the digital transformation of companies powered by cloud solutions all raise GDPR compliance issues, resulting in effective enforcement measures (Trend #1).

The increasing use of digital tools calls for a solid cybersecurity framework (Trend #2), while the implementation of such tools raises legal questions to which the courts and regulators must find answers (Trend #3). Digitalised ways of doing business, which bring with them increasing cybersecurity risks, also make organisations more vulnerable to the loss of their trade secrets (Trend #4). Finally, the interconnection and making available of data, coupled with the rise of digital data, the new oil as some say, and the emergence of data economies, can offer many opportunities (Trend #5).

Trend #1 - GDPR enforcement

> More CNPD sanctions and investigations

In the past year, GDPR fines increased tremendously by 521%, reaching a total of over a EUR 1 billion.[1] In addition, the Luxembourg data protection authority (the CNPD) issued its first fining decisions, including one imposing a record fine of EUR 746 million on Amazon. More sanctions and investigations are expected in 2022 in several areas. Focus areas include adtech (e.g. the use of cookies), Covid-19-related data processing, and international data transfers.

The recently updated CNPD guidelines on cookies and other tracking devices[2] contain *inter alia* recommendations and examples of good practices when using cookies. For instance, the CNPD indicates the recommended format of the pop-up window to be displayed in order to obtain free, prior and informed consent to the use of non-essential cookies. Websites using such cookies must not have a misleadingly designed consent button (e.g. size, colour or contrast) that could influence the user's choice.

The CNPD's Q&A on data protection in the context of CovidCheck was last updated on 12 January 2022 and is likely to be updated throughout the coming year. Finally, the CJEU's *Schrems II* judgment[3] has drawn attention to international data transfers. In this regard, it is important not to forget to implement the new SCCs. Contracts concluded before 27 September 2021, based on the old SCCs, can be used for data transfers until 27 December 2022, provided the processing operations remain unchanged. By 27 December 2022, however, the old SCCs should be replaced with the new ones.

Trend #2 - Cybersecurity

> An increase in cybercrime

Cybercrime is nothing new, but the rapidly accelerating digital transformation (sometimes organised in an improvised fashion, as in the case of working from home) and the recent Log4j security vulnerability have led to an increase in criminal acts committed online through electronic communications networks and information systems. Although all types of organisations were affected, financial institutions were among those hardest hit in 2021. Attracted by the rising volume of financial data generated by the mobile banking boom, cybercriminals targeted fintech applications and online payment systems, as well as more traditional banking platforms, with phishing or malware attacks.

A multidisciplinary approach is required to tackle these types of offences, the legal aspects of which should not be neglected, from both from a proactive (IT governance policies, the contractual organisation of resilience throughout the value and supply chains, cyber insurance, etc.) and reactive (liability litigation, sector and data protection notification requirements, and regulatory investigations) perspective.

In any case, laws and regulations in the area of cybersecurity are clearly increasing. A second Network and Information Security (NIS) Directive is in the works, and the existing myriad rules and regulations in the financial sector (e.g. CSSF Circular 20/750[4] and the corresponding EBA guidelines[5]) will culminate in the DORA Regulation[6] (aka the EU's Digital Operational Resilience Act for the financial sector) in order to tackle IT security holistically and further foster the digital resilience of financial players. DORA is intended to create a common set of standards at the EU level to mitigate cyberattacks and other IT risks faced by financial entities. Amongst other things, it establishes an incident reporting mechanism and introduces new powers for financial supervisors as well as a thorough IT testing system. The DORA Regulation is expected to apply to a broader range of actors, from credit institutions and investment firms to crypto-asset and crowdfunding service providers.

Trend #3 - Digital transformation

> Acceleration of digital transformation due to Covid-19

The Covid-19 crisis has further accelerated the need for digital client onboarding and a digital client journey, AI-based processes (e.g., chatbots and data analytics), and electronic signature and archiving solutions. The legal challenges raised by these phenomena and the responses of lawmakers, regulators and the courts are constantly changing. In 2021, certain initiatives saw the light, such as the proposal for an EU regulation on AI, which will introduce different requirements for AI systems depending on their level of risk. AI systems falling into an unacceptable risk category would no longer be permitted in the EU, and high-risk systems would be subject to stringent requirements.

The European Commission also published a proposal to amend the eIDAS Regulation, which governs a number of trusted services, in particular the use of electronic signatures across the EU. The proposal is intended to better and more uniformly regulate other types of trusted electronic services, such as electronic archiving, electronic ledgers, digital wallets and unique identification services. Many of these digital processes are based on outsourced services and/or are made possible via cloud solutions. These in turn trigger sector regulatory issues and, in the wake of the CJEU's *Schrems II* judgment, raise data protection questions (see also Trend #1).

The financial (including investment funds) and insurance sectors should be particularly attentive to the applicable sector regulatory framework. Many financial institutions had to be compliant with the EBA guidelines on outsourcing arrangements[7] by 31 December 2021, and the CSSF will publish its revamped circular on outsourcing in the coming weeks. Unlike the EBA guidelines, the new CSSF circular on outsourcing will apply to all supervised entities. While the current guidelines on ICT and cloud outsourcing are set out in multiple CSSF circulars (such as CSSF Circular 12/552, as amended, CSSF Circular 17/656, as amended, and CSSF Circular 17/654, as amended), the new CSSF circular on outsourcing is expected to consolidate these rules. In addition to the EBA guidelines in this field and the ESMA cloud outsourcing guidelines, specific rules are likely to apply in Luxembourg to intragroup outsourcing as well as to the outsourcing of internal audit or control functions and financial and accounting functions.

The DORA proposal deals with ICT organisation in the financial sector, but some of its provisions can be expected to have a significant impact on outsourcing rules as well. Traditional banking and payment service providers are already accustomed to a strict regulatory framework for IT outsourcing but will still have to close a gap. We expect that the funds sector, in particular, will really have to gear up when it comes to outsourcing compliance. In the meantime, many insurance companies must comply with the EIOPA guidelines on outsourcing to cloud service providers,[8] declared applicable by CAA Circular 21/15.[9]

In addition to the requirements of the EIOPA guidelines, Luxembourg insurance companies must comply with specific requirements relating to professional secrecy and supplementary contractual requirements, for example with regard to data and system resiliency in the EU. They must also document their self-assessment on compliance with the aforementioned CAA circular.

Trend #4 – Protection of trade secrets

> Heightened attention to the value of information and the need for protection

Cybersecurity and data protection rules and regulations have raised awareness within organisations of the value of information and the need to protect it. Only if valuable internal information is adequately protected, it can benefit from the EU's harmonised and enhanced protection and enforcement regime for trade secrets, introduced by Directive (EU) 2016/943[10] (and the 2019 Luxembourg implementing legislation).[11] Indeed, this regime only applies to information "*not generally known*", that has "*commercial value*" and which has been "*kept secret by the person lawfully in control of [it] by making reasonable provisions*". Businesses are now clearly more aware of this regime, integrating it into their overall IP protection and cybersecurity strategy and, finally, enforcing it. They should nevertheless pay attention to the lawful exceptions and the fact that the regime does not grant an exclusive right to information, meaning relying exclusively on trade secret protection may be insufficient in some cases.

Trend #5 - Open data

> New rules to support data economy by fostering data sharing

Various legislative initiatives have been taken to support data economy by fostering the exchange of data, even when it appears difficult to reconcile with data protection. In the payment services sector and other financial sectors, open banking, reinforced by the Second Payment Services Directive,[12] is on the rise. It goes without saying, however, that the open data movement is not limited to banking.

More horizontal initiatives, such as the Data Governance Act,(13) will further bolster data sharing and the reuse of public-sector data, even when protected by IP or personal data regulations. This act provides a framework for «data intermediation» services and encourages «data altruism», permitting individuals and companies to make data voluntarily available for the common good such as scientific research. In 2022, a major new legislative initiative, the Data Act, is expected, which will complement the Data Governance Act and aims to facilitate business-to-business data sharing, amongst other things.

Conclusion

While the past two years highlighted the need for digital tools to maintain normal business operations, 2022 will be the year in which companies can review the choices they made during uncertain times, consolidate the methods and processes that worked, and assess the new risks that have arisen. In the end, the new tools, practices and applications will significantly benefit from a clearer and more harmonised regulatory framework, which is mainly what we need to keep an eye on in the coming year.

Vincent WELLENS (picture), Partner,
Carmen SCHELLEKENS, Counsel
Lindsay KORYTKO, Senior Associate
Sigrid HEIRBRANT, Senior Associate
Yoann LE BIHAN, Senior Associate
Antoine PETRONIN, Associate

NautaDutilh Avocats Luxembourg

1) *Atlas VPN article of 5 January 2022, "GDPR fines hit over €1 billion in 2021"*
2) *CNPD Guidelines of 20 October 2021 on cookies and other tracking devices*
3) *CJUE judgment of 16 July 2020, no. C-311/18*
4) *CSSF Circular of 25 August 2020, no. 20/750*
5) *EBA Guidelines of 24 November 2019, no. EBA/GL/2019/04*
6) *EC Proposal of 24 September 2020, no. COM(2020) 595 final*
7) *EBA Guidelines of 25 February 2019, no. EBA/GL/2019/02*
8) *EIOPA Guidelines of 6 February 2020, no. EIOPA-BoS-20-002*
9) *CAA Circular of 5 August 2021, no. 21/15*
10) *EU Directive of 8 June 2016, no. 2016/943*
11) *Act of 26 June 2019 on the protection of know-how and undisclosed commercial information (trade secrets) against unlawful obtaining, use and disclosure*
12) *EU Directive of 25 November 2015, no. 2015/2366*
13) *EC Proposal of 25 November 2020, no. COM/2020/767 final*