April 2020 - REPORT INDICAM

ONLINE REGULATION

Edited by:
Claudio Bergonzi
Mariachiara Anselmino

INDICAM
Istituto di Centromarca
per la lotta alla contraffazione

Indice

Preface

With this first Report INDICAM further widens its activities for the support of Intellectual property. The goal of this work of analysis and guideline is to sustain the dissemination of IP knowledge that, for more than 30 years, has been representing the main mission of the Association.

The task our Members entrust us with is more and more challenging because of the growing threats to their Intellectual Property rights.
The document you are about to read consists in an analysis of several acts that were brought to our attention in these past few months. The main topic is the online world that is currently not disciplined in a way that is adequate to the real digital market. Some of the principles or topics that we are going to debate in the next pages can appear, to someone, already expressed.

Actually, this report deals with new starting points, although it is also necessary to consider who this document addresses to. To our Members, of course, that can have our positions clear in mind, but also to interlocutors that over the years have not made this long journey together with us: other actors belonging to the IP world like policy makers, institutions and any other subject that is willing to delve into the topic of the online that nowadays is part of everyone's life.
Have a good read and thank you.

Claudio Bergonzi

Introduction

E-commerce represents more and more one of the structures through which the market expresses and no longer an isolated channel. The growth rates are often, but not always, double-digit, almost everywhere in the world. Some operators and many consumers by now focus more on the online experience rather than the offline one. Finally, it is entered in a real omni-channel relationship with the consumer. The potentialities are huge for any business and opportunities are remarkable if we think of the world still left to connect to a digital network and, above all, how much can be achieved through a mobile device and a virtual shopping cart.

The online market has changed the rules of the game. Payment and logistic services have dealt with new paradigms, in which the "old" parameters were no longer able to be effective in the context of this "revolution". The cross-contamination among different sectors of the digital world has made "that" world no longer distinguishable from "this" one, the physical world.
Things, after all, find in the digital universe a powerful channel of exchange, knowledge, trade.
In two decades, first with the arrival and then with the success of the digital channel, trade has shaken up its own rules and has made subjects that did not exist until then or figures committed to other forms of business huge vehicles of "things". This often leads to a frustrating and sometimes disarming disintermediation that risks pushing brands away from their consumers, bringing products to the attention of consumers without the brand even knowing it.
The power in the hands of few subjects that represent the big nodal points of the digital network as we know it, led to the birth of hybrid figures, not just editors, not just social media, not just marketplaces, not just search engines.

This evolution occurred in only twenty years, the same time that has elapsed in Europe since the drafting of the E-Commerce Directive (2000/31/CE). Twenty years during which the law never matched with the reality: this synchronization would have been indispensable for a healthy growth of trade, considering the progress of technology and businesses linked to it.
This has led to the current situation where the massive spread of digital services is halted by a poor discipline with regard to duties and responsibilities on the Internet, while thanks to the present limbo some continue to operate undisturbed.

The rate at which online violations are perpetrated is higher than the growth of e-commerce itself, to the detriment of two fundamental categories of the digital and physical market: consumers and companies.
It is time that the EU takes action: in the past five years the European Commission chaired by J.C. Juncker never faced the topic concretely, and just promulgated non-binding recommendations, leaving many commitments on hold. However, it seems that Mrs. von der Leyen's approach is different, as we have analyzed in the present report; this is also the wish of more than 500 million of European consumers and the IPR-intensive industries that contribute for the 44% of the UE GDP.

In the current situation online operators enjoy an almost total limitation of responsibility that is unlikely to be scratched. The three macro-categories defined by the E-Commerce Directive (mere conduit, caching provider and hosting provider) are responsible in exceptional cases for the illicit contents that through their channels are spread among consumers, mainly whenever: i) they do not intervene although they have knowledge about illicit conducts; ii) they are active parts of these illicitconducts; iii) if they change the conveyed information, making their behavior active. Once, the limitations regarding liability were imagined for an acceptable purpose, that was highlighting online operators' role as engines of the digital innovation without any of them fearing of halting their rise because of excessive controls that a greater responsibility would have implicated. But in twenty years this liability structure was never adjusted to the evolution of the market: today the online operators find themselves in a position of strength in the relationship – also economical – with companies and consumers using their services.
The result, that both the Court of Justice of the EU and the national courts were partially and not easily able to mitigate for a trustworthy digital environment – and not even in a homogeneous manner if we look at the jurisprudence in several MS – is that companies have to deal with a very arduous and demanding work to monitor the online offer involving their IP rights. Rightholders are also in charge of reporting to operators the illegal bids in order to have them removed and then… they have to do it all over again, while online intermediaries keep waiting for them to repeat every time the same notices, instead of proactively using the information received to block further illicit contents of the same nature or offered by the same seller.
Moreover, between the brand owner's action and the online operators' reaction, there is often a temporal hiatus – whose duration is unpredictable at first glance – during which a sort of debate – whose result is unpredictable as well – takes place, regarding the concealing of the illicit nature of the suspect product (for example the suspect product (for example through partial or blurred views of the goods). Of

course this represents a huge obstacle to the important investments made by rightholders on online brand protection: not only it generates serious difficulties in the tackling of counterfeiting on the Internet, but also a sort of "war of attrition" with the online operators that in various cases did implement proactive measures to fight fakes (yes, far from being fully effective, but still relevant to improve the situation). The consequence is a digital environment that in the meantime solidified around the principle of "safe harbor" by which consumers are not properly protected against counterfeit products disguised as original goods. This of course damages also the investments made by some online operators to strengthen the detection of violations perpetrated through their services. In absence of better-defined legislative obligations, the proactive commitment of platforms to control in advance what is being offered to the public through their channels relies on the interpretation of judicial decisions made by the single online operator itself.

Therefore, the effectiveness of this commitment varies depending on the subject that implements these measures, with regard to the types of illicit contents or products. The transparency of these activities, when put in place, is poor and data exchange with rightholders is often incomplete and almost always too generic. The voluntary temporary measures, often bland and surely not adopted by all the online operators, introduced in Europe with the MoU "on the sale of counterfeit goods via the Internet", were proved to be inadequate. The document counts among its signatories very few online operators, less than ten, and few brand owners, less than thirty, that are now heavily criticizing its efficacy and true meaning. This tool is no longer the shield behind which the European Commission on one hand and online intermediaries on the other can hide, by declaring out loud the benefits of a voluntary collaboration. It is frustrating, as INDICAM witnesses first-hand during the recurring meetings it holds with the big players of the digital world, to listen to confrontations on different levels between rightholders and platforms or search engines, in which the latter exploit the lack of regulations to illustrate proactive measures sometimes various but always many steps behind online counterfeiters.

With the present analysis INDICAM starts from these elements and from the necessity to change the situation by making use of binding laws and not only voluntary agreements. What follows is an examination of the same topic in the U.S., where the regulation of the digital players seems to move far more faster, thanks to the awareness of the highest levels of the Administration and the legislative initiatives that are being supported by bi-partisan groups in the Congress. We will then delve into the EU Digital Service Act that was just presented to the newborn Commission and we will conclude with a series of considerations aiming at remarking INDICAM position on these matters. That is necessary to have

a new legal framework in the EU to discipline the liability of online operators in a homogeneous way, including proactive measures to ensure the most effective action against counterfeiting and therefore the best protection for consumers and IPRs that contribute to the European economy.

61%

WORLD POPULATION USING THE INTERNET

85%

EUROPEAN POPULATION USING THE INTERNET

Approximately 4 million consumers have access to e-commerce, mainly through mobile devices. Europe counts the highest spending per-capita compared to US and Asia, that however boast higher numbers in penetration. Italy still holds a gap in comparison to other MS, albeit the double-digit growth. What halts a full development is the digital discrepancy in the peninsula.

2.875 billion $

E–COMMERCE VALUE IN 2018 (22% IN EU)

3.4%

EU GDP RESULTING OF E–COMMERCE

48%

ITALIAN E–SHOPPERS (41.5MIL €)

41.3%

SERVICES AND FREE TIME

28%

TOURISM

14.5%

MARKETPLACE

E–COMMERCE TURNOVER SECTION BY CATEGORIES IN ITALY

COMBATING TRAFFICKING IN COUNTERFEIT AND PIRATED GOODS

A REPORT BY THE DEPARTMENT OF HOMELAND SECURITY OF THE UNITED STATES OF AMERICA

> ...This report was prepared pursuant to President Donald J. Trump's April 3, 2019, Memorandum on Combating Trafficking in Counterfeit and Pirated Goods. The President's historic memorandum provides a much warranted and long overdue call to action in the U.S. Government's fight against a massive form of illicit trade that is inflicting significant harm on American consumers and businesses. This illicit trade must be stopped in its tracks...

GOALS

More safety in the e-commerce, more responsibility for online players, more control of the supply chain, a shift of the perception around IP violations.

WHAT IS

The Department of Homeland Security report to the President of U.S.A., following the MoU issued in 2019 for a sharp action against online illicits.

PERSPECTIVES

Reforming online platforms' role as guarantors for trade and consumers. Creating solid foundations for an expanding digital market.

TACKLING ONLINE ILLICITS

On the 24th of January 2020 the Department of Homeland Security of the United States (DHS) published the report Combating Trafficking in Counterfeit and Pirated Goods, following the Memorandum on Combating Trafficking in Counterfeit and Pirated Goods issued in April 2019 by President Trump that sent out a "call to action" to study the phenomenon and the tools needed to stem it.

Furthermore, the report follows the executive order issued by the Trump Administration on the 31st of January 2020 to various state agencies for the adoption of effective measures to ensure a safe and legitimate digital market for consumers, businesses, supply chains and Intellectual Property rights.

The DHS report fully goes towards this direction without being reduced to a simple overview document on the current counterfeiting situation, but instead it is a precise vademecum of concrete actions and best practices. We are witnessing a first-ever, of a country – which is, by the way, the cradle of many important e-commerce realities – that on paper dictates immediate actions that governmental authorities have to carry out to tackle counterfeiting and piracy, crimes that seem to take a position of absolute priority that is not frequently to be found in political agendas of the majority of countries.

But the most disruptive aspect surely consists in the series of best practices addressed to e-commerce platforms hosting marketplaces where third-party subjects promote and sell products and other similar online intermediaries. The report states that the adoption of these practices will be recommended, encouraged and monitored by the National Intellectual Property Rights Coordination Center (IPR Centre), run by the United States Immigration and Customs Enforcement (ICE).

Again, nothing similar was ever developed by any national government and this uniqueness makes the DHS report an incredible step ahead in recognizing digital intermediaries liable for the illicit contents uploaded by users on their channels. A major step ahead that the rest of the world, the European Union in primis, have to look up to and make their own, starting with drawing up a clearlegal framework that takes into account the evolution that have been affecting Internet giants for over twenty years.

Surely the nature of recommendations excludes the recognition of a real legal responsibility for the platforms, however, it confirms a turnaround compared to the principle of "safe harbor" in which the big online players have been basking since forever, thanks to obsolete laws imposing a duty of reaction on the platform only in case of "knowledge" of the violation and "control" over contents.

What emerges from the DHS report is a wide spectrum of actions that digital intermediaries should put into effect proactively, starting from complete and thorough "Terms of service", that make explicit the prohibition of promoting and selling products infringing Intellectual Property rights, providing the platform with a legal tool to quickly act against transgressors. Likewise, it is recommended the insertion of a list of the consequences the user will have to face in case of violation: first, suspension, then elimination and finally interdiction of the account without a judicial decision. Moreover, the presence of a proportional enforcement system for the most serious infringements and frequent infractions is largely endorsed: from the permanent elimination of the seller's account and the profiles associated to the seller, to the confiscation and destruction of the infringing goods in the warehouses and logistical centers run by the platform.

Finally, "Terms of service" should allow platforms to impose appropriate limitations on listings, to require data on the country of origin of the goods, besides banking and compensation information, in order to improve the identification of sellers before they are actually able to sell the products.

The identification of sellers is a crucial point on which the DHS report insists when listing all the best practices platforms are invited to put in place.
Know your customer. Make sure that whoever promotes and sells on your platform is a reliable subject selling legal wares. And if not, remove them. This concept is declared in the recommendation "Significantly Enhanced Vetting of Third-Party Sellers", by which platforms should collect sufficient information for identifying sellers, their listings, accounts and business locations, before they are even able to use the platform. Other relevant information should concern the seller's history: were they ever banned or removed from other platforms? Were they ever implicated in the sale of counterfeit or pirated goods? Besides confirmation that the seller is really entitled to sell those goods.

The lack of this data, that platforms should be able to collect also through technological tools, with the analysis of public and historical information, the risk assessment of repeat transgressors and the audit programs for high-risk offenders, would exclude the chance for the seller to subscribe to the platform or their breaching of the "Terms of service".

Moreover, being aware of the identity of the seller answers to a further purpose: allowing consumers to take informed actions when they are about to choose a product or finalize a transaction. This level of transparency can be achieved only if the platform makes the consumer aware of the identity of sellers and the subjects responsible for the transaction.
Today, for any user, it is possible to create more accounts on the same platform, without any evident link among them and this can clearly hinder the identification of the infringing profiles. Therefore the DHS recommends platforms to require sellers to provide precise information regarding all the sales related to the same subject: this also in order to ease the monitoring, that as we all know is an onerous and complex activity that burdens rightholders.

Therefore, it is evident that the direction taken by the United States – even if through recommendations and not proper laws – shows no tolerance for the opacity that characterizes the digital market, where today uncertainty often rules: about who is selling the goods, the product itself and about the reliability of a boundless space where anyone can artfully build their own profile.

Furthermore, among the best practices, a section is dedicated to the renowned mechanism of "Notice and take down", whereby the platform removes the infringing content after receiving a notification from the rightholder. It is a time-consuming method that requires lots of resources from brand owners that are already burdened with the identification of the transgressors before issuing the notice to the platform.
To fix this evident asymmetry among the obligations overloading rightholders and platforms, it is recommended to the latter to create and uphold a precise, clear and quick enforcement system characterized by: a) minimal registration for rightholders to participate in the process; b) reasonable rules that consider as businesses/professional operators profiles promoting a wide number of products on C2C platforms; c) transparency to rightholders as to how their complaints are handled and all other activites in which the seller is implicated.

Dataflow does not end here: platforms are invited to share with the damaged rightholders all the details related to infringing goods and remaining stock of counterfeit and pirated goods in their warehouses. Likewise platforms, within their capabilities, should put in place all the measures needed for the removal of goods or their expulsion from the legal market, also through an immediate engagement with law enforcement, that should be provided with intelligence and relevant information.

These are just a few actions platforms would already be able to carry out to tackle

fakes. Brand owners know it, e-commerce giants know it and also politics is aware of the radical transformations that affected digital platforms in the past few years, making them the real holders of the economic power in our era.
Starting from data mining, that through artificial intelligence, statistical science and machine-learning, allows digital platforms the extraction of useful data to know users and consumers and, as a consequence, to have control over the contents they post online.

If on one hand the DHS identifies important best practices that platforms should adopt, on the other it displays a series of immediate actions that the Department itself, through the US Customs and Border Protection (CBP), will implement with enforcement activities and recommendations to the U.S. Government.
Among the former, there is the recognition of a responsibility of "due diligence" for all the entities involved in import operations (like platforms and other intermediaries running warehouses and logistical centers), besides the collection of data related to platforms' different business models in order to evaluate potential legal gaps and analyze distribution and stocking mechanisms, as well as identifying sellers and the nature of the imported wares.

A further relevant aspect is the intention to hold accountable not only online intermediaries, but also offline ones, like couriers, postal services, etc., who will have to share with law enforcement data on importers who have been suspended or excluded from a sort of "white-list" created for importers working in the U.S..
Moreover, civil fines and penalties are imposed on intermediaries that are proved to have directed, financially assisted, aided and encouraged the import of fakes. The DHS recommends a regulatory change allowing the government to promulgate injuctions against marketplaces and platforms where counterfeits are sold.

The intention to prioritize crimes linked to IP regardless of their reach and to investigate and pursue these violations at every level of the supply chain is praiseworthy. It is not a trivial assertion, considering how these kinds of crimes are often widely underestimated and, as a consequence, weakly tackled, both from a political and an enforcement perspective.

A further aspect on which the report insists on is the necessity to have a better collaboration among the various actors involved in the distribution chain, starting from entities designated for the postal service management, that are required to share essential information to identify and track airmail parcels.
There is also the institution of an "E-Commerce Working Group", within the IPR Centre, for the promotion of a bigger dataflow between platforms and

intermediaries such as couriers, shippers, payment service providers etc., and of an "anti-counterfeiting consortium" for the exchange of data related to intermediaries involved in trafficking of counterfeit and pirated products and the automation techniques for the creation of proactive targeting systems allowing the automatic monitoring of platforms.

A more radical approach to fight IP infringements passes also through a modification of the legal framework. Therefore, DHS addresses the modernization of laws concerning Intellectual Property, wishing that counterfeits will be assimilated to narcotics, also to underline the importance of tackling counterfeiting for the Government.

Finally, the DHS recommends the Government to evaluate platforms' liability for IP infringements also on the basis of judicial decisions. Overseas, as in Europe, in more than one occasion courts have recognized the responsibility of online operators, even in constancy with the current laws limiting liability. In our continent it already happened in 2009 with L'Oréal v. eBay (C-324/09) case before the CJEU, where judges confirmed the active role of the well-known e-commerce platform and its exclusion from the safe harbor regime.
The point is that courts realized long before legislators that the online world had deeply changed since 2000, when the E-Commerce Directive came to life. They have acknowledged that Internet giants are operators of a different size covering a wide range of roles on the market and often taking an active one over the uploaded contents.

The DHS report represents a fundamental proof of political awareness with regard to the role of online operators in the digital ecosystem: a similar shift is also wished for the EU, where a new regulation that disciplines Internet Service Providers – and their liability for the infringing contents with duties of proactive action - is very much needed.

Big online players, as previously mentioned, once necessary information is made available by rightholders to determine the illicit nature of the content, have all the technical, economical and organizational tools to effectively fight the phenomenon. But it is clearly necessary to have a regulatory substratum that forces their enforcement actions, even for future transgressions that may occur on the platform. In the U.S. things are, once again, moving a lot faster: the Shop Safe Act is the most recent demonstration (see the following section). We are in a crucial time and we must take resolute and brave decisions, for a more transparent market, for safer and more informed consumers and for legal companies suffering both from an economical and reputational perspective.

STOPPING HARMFUL OFFERS ON PLATFORMS BY SCREENING AGAINST FAKES IN E-COMMERCE ACT OF 2020

AMENDMENT PROPOSAL OF THE U.S. TRADEMARK ACT SUBMITTED TO THE HOUSE OF REPRESENTATIVES

"...A BILL To amend the Trademark Act of 1946 to provide for contributory liability for certain electronic commerce platforms for use of a counterfeit mark by a third party on such platforms, and for other purposes..."

GOALS

A law disciplining e-commerce in the U.S. with better guarantees for consumers as to dangerous products.

WHAT IS

A bipartisan bill submitted to the House of Representatives.

PRERSPECTIVES

The process needs to be closely followed as well as the support it might receive. It is useful to observe the conversation that will occur with U.S. big online players.

The Shop Safe Act

By Act 6058 of the House of Representatives, on 2 March 2020 six U.S. congressmen submitted an amendment bill of the Trademark Act of 1946, in order to give a better cohesion to the legislative structure during this era of e-commerce expansion. Before analyzing the document, we believe it is appropriate to give a brief reminder of how the legislative procedure works in the U.S., as disciplined by the Constitution. As reported by the official site of the House of Representatives, here it is the summary of the legislative procedure.

First of all, one or more congressmen submit and support a bill that is then assigned to a committee to be analyzed. If the committee gives a positive opinion, the bill is scheduled to be voted, discussed or amended. If the bill passes by a simple majority (NDA: the House of Representatives is one of the two branches of the U.S. Parliament, that includes 435 voting members representing the 50 States in proportion to population. Following elections in 2018, the majority is currently Democrat with 235 representatives against 200. Since January 2019 Nancy Pelosi has been serving as Speaker) or with 218 votes (note: the House of Representatives currently counts 435 voting representatives and six with no voting right) the bill passes to the Senate (note: the Senate of U.S.A. counts two representatives for each of the 50 States and it is chaired by the Vice President, that is currently Michael "Mike" R. Pence).

In the Senate, the bill is assigned to another commission and, if released, it is discussed and voted. Even in this case if the bill passes by a simple majority (51 voters in favor out of 100), it is definitive. Then a conference committee composed with congressmen and senators solves the possible differences between the versions released in the House of Representatives and in the Senate. At this point the bill gets back to the two branches of the Parliament for the final ratification. The press office of the Government prints the bill. The U.S. President has then ten days to sign or veto the bill.

That being said, we can get back to the analysis of bill 6058 that offers several interesting points to better balance the actions that online platforms could carry out for a more effective control and screening of the offers posted by third-party sellers using their channels.

The name of the bill already sums up what it proposes, and it deserves attention just for its proponents. The U.S. mechanism envisages a proponent and some supporters. In this specific case what is praiseworthy is that the proposal is totally bipartisan. In fact, the six involved congressmen (the proponent – Rep. Nadler – and 5 supporters – Rep. Collins, Rep. Johnson, Rep. Roby, Rep. Deutch, Rep. Cline) are equally split between Republicans and Democrats. This situation, that is not frequent in the European parliaments, is meaningful also because the discussion about online infringements is active in the U.S. especially since President Trump in 2019 hurled against illicits perpetrated through digital channels. Therefore it would have been logic that more Republicans supported the proposal; instead, this bipartisan aggregation shows how the argument focuses not on the role or power of online operators, but exactly on the opposite, that is represented by those who benefit from the online world: citizens.

The bill is technically a proposal of amendment of the Trademark Act of 1946, therefore to be circumscribed in the matter of infringements against trademarks. The Act is composed of two sections: first ,the short title of the bill itself, that is the acronym of Stopping Harmful Offers on Platforms by Screening Against Fakes in E-commerce Act of 2020, that is "Shop safe" act. Quick, sharp, self-explanatory.
Section two represents the key to the proposal and is titled "Contributory liability for electronic commerce platforms".

It starts with the purpose of the bill, that is amending the Trademark Act of 1946 (15 U.S.C. 1114) and it ends with a series of provisions regarding e-commerce. The goal is to identify which responsibilities online operators can be accounted for, together with the third-party users that sell, advertise, promote and distribute products bearing counterfeit trademarks affecting health and safety (note: in the end we will get back to these two requirements).

The bill aims at identifying a series of actions and duties that platforms should carry out in order to hinder third-party sellers' conducts that could put at risk consumers' health and safety through the offer of fakes.
The actions platforms are asked to put in place in order to prove they are not jointly responsible with the transgressor are those typical of an accurate "due diligence". INDICAM has been asking for years that online intermediaries comply with these kinds of duties.

In short words, if the bill does become law, the first step that an online operator should carry out is a correct and complete identification of the seller, that nowadays represents a really lacking aspect.

As an example, Chinese platforms, that act under another legal framework, classify a series of personal data and identifiers that are at authorities' disposal. They share this data with authorities so that enforcement actions are carried out against transgressors, until their arrest (note: Alibaba, in its IPR Report 2019, mentions that in 2018 more than 4500 individuals were arrested thanks to collaborations between the platform and Chinese authorities) either they are involved in the production or distribution of infringing products.

This instruction in the U.S. bill is very important even if generating a couple of issues that need to be solved: first, how to manage sellers' identification in compliance with privacy law – like the European GDPR, for example – and second the future use of this data when similar conditions may occur. What is missing in the Chinese case is, in fact, a return of the information to rightholders, that would be extremely useful especially to cross that data with what they already own, to carry out further investigations, actions or analysis. Another cause that would exclude contributory liability could be the submission, from the third-party seller, of guarantees related to a previous verification of authenticity of the goods linked to the used trademark. There should be an intermediate system between rightholders and sellers that could validate the authenticity of the products through an active verification. According to the Chinese e-commerce regulation, the platform is not "arbiter" between the seller and the company and with the mechanism of N&TD leaves every burden on rightholders. In the U.S. bill, instead, the responsibility weighs automatically on the platform, whenever the operator does not prove to have required the third-party seller these verifications.

The spirit of the bill continues by ruling that platforms have to impose third-party sellers not to use counterfeit trademarks in connection to the sale, offer, distribution or advertisement of goods on the platform and to accept, under the contract agreement with the platform, to be subject to U.S. jurisdiction in relation to any legal actions that may be filed.The most important element of the bill can be found in the following section, that deals with the topic of automatic proactive – the term INDICAM has been underlining for years in every lobbying activity regarding the digital matter - mechanisms to avoid the sale, offer, advertisement or distribution of fakes.

This aspect, besides being innovative, is the heart of the "duty of care" concept.
Another significant passage concerns images, that third-party sellers must be entitled to use. The topic of images has been discussed many times, because it represents a complex matter and not very clear even in the same claims of brand owners. The issue is worth mentioning but in its inevitable vagueness on this point the bill does not determine how and to what extent it is opportune to intervene.

However, the principle remains interesting, that third-party sellers must be entitled to use the image and they are liable to prove their legitimacy. We do not deny that this could be ground for debates, as images, sometimes, are owned by their authors (such as photographers) and not the companies holding trademark rights over the products accompanied by those images.

Then, two provisions concern the possibility that an infringer keeps posting illicit offers. In this case the bill requires once again a prior due diligence through tools that could serve this purpose: a threshold for the expulsion of third-party sellers that keeps reiterating their violations is considered. Three strikes should be enough, according to the proponents, to remove for good the infringing seller. In substance, what the proposal would establish is that the third-party seller committing more than three IP violations can be expelled and prevented from using the platform ever again, also through technological measures that verify that the excluded sellers do not re-enter the platform with the same or different accounts. This approach is already exploited by some operators (like Alibaba) and would impose a homogeneous conduct from e-commerce actors.

Interesting is that under the bill platforms would be required to share, with law enforcement agencies and rightholders, information and identifiers of the infringing seller removed from the platform according to the three strikes policy. As a matter of fact, this point, if revolutionary, it also needs to be read more like something to wish for, more than a real sign of victory for companies and law enforcement agencies. As a matter of fact, in this case it seems we are witnessing what happened on 25th May 2018 in ICANN as far as the information regarding registrants of websites. In fact, lots of service providers in accordance with the European GDPR, blocked all data concerning registrants that could be useful both for public and private IPRs enforcement. Regardless of ICANN definition of exactly what kind of information could be disclosed without violating GDPR or privacy law, rightholders and law enforcement are still struggling to get this data.

Likewise, we could imagine a boycotting action in front of a provision that would allow data disclosure to identify transgressors. It seems that platforms could cling to privacy regulations to avoid exposing both their business and operators that through their channel violate IPRs. We will see what kind of discussion will be raised in the commission debating the bill.

The law would address the specified e-commerce actors and what strikes is that hybrid subjects that should be included are vaguely mentioned. For example, could Facebook marketplace be inserted in the following subsection “The term ‘electronic commerce platform’ means any electronically accessed platform that includes

publicly interactive features that allow for arranging the sale, purchase, payment, or shipping of goods, or that enables a person other than an operator of such platform to sell or offer to sell physical goods to consumers located in the United States"? It seems it could, if Facebook is identified as a platform allowing the above-mentioned operations. Besides, as third-party seller, the bill identifies anyone using platforms' services to sell, distribute or promote offers of counterfeit goods. This could help solving many doubts regarding hybrid platforms.

At the beginning of the bill, you remember, fake products that can harm health and safety are expressly mentioned. It could be a relevant clarification considering on whom the burden to prove these dangers lies. The bill points out that dangerous goods are "...goods the use of which can lead to illness, disease, injury, serious adverse event, allergic reaction, or death..." which appears as a pretty conventional definition if we do not consider the following formulation "...if produced without compliance with all applicable Federal, State, and local health and safety regulations and industry-designated testing, safety, quality, certification, manufacturing, packaging, and labeling standards". This principle is similar to what in 2018 was debated in Europe in relation to the "Goods package", a process to review Regulaments and Directives concerning production standards, certifications and rules of very specific and vertical sectors. What was seized as an opportunity within AIM (note: the Association International des Marques, an organization representing more than 2500 companies and trade associations based in Brussels and tireless engine for lobbying activities to support brands) and then explained to various European interlocutors from Unifab, Markenverband and INDICAM was the chance to introduce in this "harmonization package" about compliance the principle that a counterfeit product is indeed a non-compliant product.

Especially INDICAM covered a major role in that positive journey of lobbying, because the speaker of the package was Congressman Nicola Danti, an Italian Euro MP. Many encounters took place with him (some readers might remember Mr Danti as lecturer at INDICAM Forum 2018) in Strasburg and Brussels, to share details on the topic and to identify, together with French and German colleagues, the point in which this principle should have been inserted. The final text recognized the requests coming from the above-mentioned proponents and established that a counterfeit good is a product not compliant with safety rules, because never tested, certified nor authorized.

We highlight that the definition of "safety and health" present in the bill, then better specified as lack of compliance with certification criteria and testing, would open a scenario that could lead to an extended definition of safety and health,

getting to the topic of the "non-compliance by default" of any fake product.

Therefore, the bill 6508 has been welcomed as a meaningful step ahead in the discussion about subjects dominating e-commerce and their liability for contributing to spread illicit contents on the Internet. In fact, it is about protecting, with American pragmatism, that relevant share of U.S. citizens buying online, worth circa 4 billion dollars in 2020, 15% of total trade.

The principles enshrined in the bill, related to duties of surveillance, identification, a definitive removal from the platform for repeat offenders and a wide concept of fakes as dangerous goods, are great starting points. There are still some gaps and vague descriptions that could raise discussions over these gray areas. The fact that platforms are the only actors mentioned may appear a little unsatisfying. The description of online operators is so precise that search engines are automatically excluded. But where do search engines stand? It is fundamental to recognize that they are not direct e-commerce operators, but they cover a very crucial role on the Internet. A subject like Google, that hybrid indexing figure and advertising provider, by itself filters 85% of the Internet traffic. What role to give, then, to BigG and its competitors allowing consumers to enjoy illicit contents whereas legal provisions lack clarity in the definition of liability and duty of care? No answer comes from the bill, that is silent on this topic.

Besides, it is plausible that this act, although bipartisan, goes towards a direction of making accountable only platforms and not also other crucial actors in the digital environment. It is not a mystery that the current Administration holds no affection – nor receives back one – for Jeff Bezos or Mark Zuckerberg's empires. No signs of intolerance were shown instead to Larry Page or Sergey Brin, that were mentioned and thanked even during the Covid-19 pandemic (in some cases without Google even knowing anything about the initiative the President had ascribed to them).
However, this bill represents a cornerstone which the European discussion for a reform of the e-commerce environment needs to start from. But as you will see in the following section, it is still a long way to go.

SHAPING EUROPE'S DIGITAL FUTURE

THE EUROPEAN PROGRAM 2019/2024 FOR THE DIGITAL WORLD

> ...In this context, it is essential that the rules applicable to digital services across the EU are strengthened and modernised, clarifying the roles and responsibilities of online platforms. The sale of illicit, dangerous or counterfeit goods, and dissemination of illegal content must be tackled as effectively online as it is offline...

GOALS

Programming a series of interventions to push the EU to become the heart of a work of digitalization.

WHAT IS

The first step for a Digital Act that represents a re-balance as to the roles of digital actors, by creating a safer environment for consumers and businesses.

PRESPECTIVES

In 2020 already to kick off a process of reviewing the current legislation (Directive 31/2000) to establish more responsibilities for online gate-keepers and level out offline and online worlds.

The digital political guidances of the EU

"…For the generation of my parents, Europe was an aspiration of peace in a continent too long divided. For my generation, Europe was an aspiration of peace, prosperity and unity that we brought to life through our single currency, free movement and enlargement. For the generation of my children, Europe is a unique aspiration…".

This is how Ursula von der Leyen's manifesto paper would begin. This thought, of a Europe that must become a true aspiration, is a purpose showing through the programs of the new European Commission that is now chaired by Mrs von der Leyen herself.

The three generations addressed in the document are clearly the active backbone in our continent, a still young Union although it already bears the signs of the time, between more and less extremist souverainisms and exiting countries (that never really integrated to be honest…). The current Commission has a very hard task, that is making the EU an aspiration rather than an abstract topic often nebulous and fluctuating on key arguments.

Beyond any other subject that is not up to INDICAM to discuss, our analysis would like to focus on one of the hottest and most neglected aspects of the European scenario: the digital world.

The EC chaired by Mr Jean-Claude Juncker did not stand out in this sense, it was empty as far as the contents were concerned despite many words being said out loud. Words, unfortunately, not followed by facts: ambitious commitments like the Digital Single Market were discussed and left a tangible trace only on the geo-blocking rules. Of all the rhetoric expended by the EC exiting in 2019, rightholders were not able to see anything concretely useful for the support of Intellectual Property.

What is missing – it is evident also in the light of the legislative developments related to big socio-economical scenarios like the U.S. (see previous section) and even in China although among many contradictions – is a legal framework adequate for the current evolution phase of e-commerce and radically different –

especially for the economic power of the actors involved – from how it was at the beginning, as reflected in the liability limitations enshrined in the Directive 2000/31/CE. The legal framework needs to be adjusted to the current digital era, in order to ensure the continuity of its development. With the present legislative tools, trust in the Internet and in everything spreading through it (news, goods, opinions, data) is dealing with a crisis.

The pillars by which the newborn EC identifies the need to intervene as far as the digital environment is concerned are oriented to this goal. AI, web security and data protection, contents and responsibilities. A wide-reach framework that should fill the gap Europe has in comparison to U.S. and China.

Since the first few lines of "Shaping Europe's digital future" what emerges is exactly this: that we are late.

The first point the document deals with is data, also underlined by other sources of the EC.
It is not a mystery, for example, that there is the ambitious purpose to make the EU a climate-neutral space by 2050. Of course, in order to achieve this goal, various, important and structural reforms need to be put in place in the MS, but something will also go through data. And IP.

It is a little clearer, in fact, what the EC meant in a meeting in Alicante last September, when it brought out the role of IP as a driver for this change. It was not clear, back then, which connection could occur. Not that now the situation is radically changed, but at least we know that IP is meant like innovation, also through a massive use of data (and AI) that may lead to a necessary digitalization, especially for SMEs, that are the fundament of the European economy.

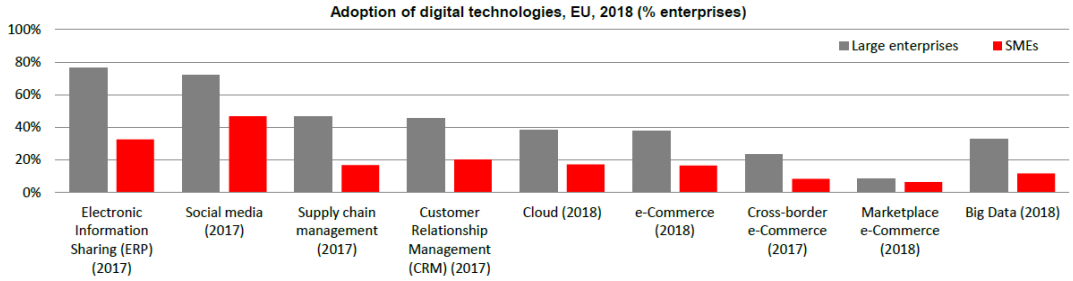
Acknowledging the European delay represents a starting point. It is interesting to notice how the EC's documents often refer to a "European way", as to data, protection of contents, security, circular economy. These are cases that show how Europe is eager to become more independent from other extra-EU suppliers, by affirming a sort of "Europeans do it better" that would sound like a sort of claim of ethical and sustainable values superior to U.S and China's. It is mentioned, for example, that GDPR has been taken as a model from other systems. But how positive was its application in correlation to IP online protection? We already talked about its negative impact on the disclosure of registrants and social accounts' data and identifiers. Still today, this question has never been settled and online operators have been taking advantage of the opportunities left by these gaps.

Therefore, that the "European way" to the digital enhancement may be the best is a declaration in front of which we remain neutral, without embracing or rejecting it. Of course, as said, what happened before is not encouraging.

As to data, the EC highlights the importance of having a wider and stronger security infrastructure, considering the massive investments in the digital area that could be put on the table (like 5G technologies and even 6G ones!). A total of 65 billion euros that should increase the European GDP for over 14 points by 2030 thanks to a different kind of digitalization that includes a safe use of the collected and analyzed data, and also gives better economic opportunities to businesses and citizens.

It is an ambitious project for sure, even if delayed as noticed by the EC itself. However, it is one thing if we are talking about a territory run by a central government (like in the U.S. and in China, the latter being even more radical in the centralization), another one if the project needs to be adjusted to 27 different realities, where the single GDP varies from Norway 70K Euro/per capita to a little more than Bulgaria 21K. Besides, there are countries (Italy and Spain to mention some of them, but partly Germany too) having significant discrepancies within their own national borders. This directly affects the digital literacy, MS's internal resources (since the EU cannot be the only payer of the digital revolution) and businesses' structure itself. Therefore, in order not to fall again into the rhetoric expressed by the previous EC, these topics need to be inserted in a general reform process of the EU.

The general lines of progress as to these areas pass through a white paper on AI, on massive investments for cutting-edge solutions in tech field, data analysis, infrastructures serving these activities and components industry. Other mentioned investments regard cybersecurity, that is more and more at risk in an interconnected world, and a pervasive digital education at European level, targeting both citizens and companies. Further papers address especially SMEs because they suffer a significant gap in comparison to the same realities in different parts of the world. Data use, eased by technology, should first deal with a better awareness of companies, that need to be able to tell how they produce this information, how they protect it and exploit it. Below you can find a chart showing digital imbalance among companies extracted by the document "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS An SME Strategy for a sustainable and digital Europe", issued on 10th March 2020.



Fonte: Euroistat

Two further points dealt by the EC, not analyzed in this report since they are not pertinent to INDICAM scope, are work sustainability for platforms' employees (do you remember the matter concerning workers in Amazon's warehouses in Italy? Or riders?) and a common platform for public data.

The document continues with an evaluation of the intervention steps for what is defined as a fair and competitive economy. Rules should aim at creating a "level playing field" for the competitive uniformity by 2023.
This of course can be achieved through an overall assessment at European level to evaluate the "fitness" of the various rules. By 2023 this must lead, in the EC's intentions, to a better competitiveness, considering that in the meantime a legislative harmonization should have occurred (the topic of heterogeneous taxation in every MS strongly affects the cross-border digital trade for example). Hence, these points require a wide reform plan and not to excessively commit, it has been declared that a strategic package for industries will be one of the EC's tasks, though no date within which publishing it and kicking off the confrontation process is defined.

The most interesting part for IP owners, however, is the one titled "An open, democratic and sustainable society". Trust is the introduction topic, that consists in all those rules and values that must structure the digital offer so that citizens may be able to benefit from it in a guaranteed manner. This is the cornerstone of the fight against online illicits: a product bearing a counterfeit trademark is by definition a threat for the user, considering the trust relationship brand builds and incorporates in the jeopardized trademark.

The second important concept is the equivalence between online and offline, that keeps coming back in various parts of the document. This is an interesting point: what has been said is that consumers have the right to find in the digital world what they find in the physical one. Translated in simpler terms, it means that for example a third-party seller should be identified in an unequivocal way through the available data and this information should be kept by the ISPs, in compliance with the GDPR, for further necessities. The EC declares that, since it is not possible

to predict digital development, European values, ethics, environment and sustainability rules should be all applied also to the digital world. We could read this passage as a big question mark, asking ourselves if future legislations will be generic enough to cover new types of digital players: this could not be an advantage because the risk is not being able to frame lots of very specific categories.

At this point, the document opens to a series of important activities for many rightholders, INDICAM members included. We reference in full what appears to be a crucial passage: "In this context, it is essential that the rules applicable to digital services across the EU are strengthened and modernized, clarifying the roles and responsibilities of online platforms. The sale of illicit, dangerous or counterfeit goods, and dissemination of illegal content must be tackled as effectively on-line as it is offline". Here it is where the EC should start from to deal with the reform.
And where stakeholders should start from as well. In fact, the debate within the network of European trade associations INDICAM usually confronts with is open. This time the approach needs to be one. Often in the past lobbyists acted each on their own, while our opponents in the conversation regarding e-commerce reform proceed like monoliths in controlling any space of communication with the EU institutions.

The theme around equivalence between offline and online is recurring in the market trend analysis, where the digital trade is increasing and positively contributing to the economy. It is not a case that even in critical times (like spring 2020 during Covid-19 pandemic), digital channels have allowed a prosecution of essential activities but also supported the few business activities still ongoing.

Equalizing offline and online worlds would mean, beyond identification data collection, to put in place a more effective system of liability. For example, a third-party seller effectively identified, whose details like supply chain, financial stability, certifications and authorizations to use others' IPRs are tracked by the platform, could be classified with a great precision. Reversing the perspective, after some data collection and verifications, the platform would be able to allow the activity of a third-party seller through its channels and would be liable for those checks. In other terms: a platform permitting the use of its services to a shady subject would bear the burden for that choice and consequently would be accountable for the actions carried out by that user.

This is the key point the debate over E-Commerce Directive review revolves around. But there is more: regarding data exchange, level of transparency, public

information, platforms' actual knowledge. Topics over which stakeholders like INDICAM become a priority in the dialogue with UE institutions.

Platforms' knowledge is an important chapter as to the application of the "safe harbor" principle under the current legislative scheme. As a matter of fact, only when online operators are aware of the illicit content they must intervene. But when does this moment occur? Here jurisprudence comes in aid: for 20 years judges have been helping to overcome limits and gray areas of the E-Commerce Directive. For example, in Italy for the case RTI Mediaset vs Facebook (sentence Trib. Roma 3512/19). Between the moment of the notification from RTI Mediaset regarding their IPRs'violation and the actual take down of the infringing Facebook page 2 years passed by. This long lapse was ruled as a violation and led to a damage compensation to the plaintiff, because of the principles enshrined in the Directive and therefore in the national transposition law 70/2003.

Communication to consumers should be disciplined as well. In fact, following the principles the EC would like to pursue as far as consumers' protection, consumers should be able to enjoy a better transparency when it comes to online contents. If the aim is to have more guarantees from platforms, users should be informed about the removal of illicit contents. This principle, that was about to be inserted in the Juncker's Commission "New deal for consumers" in 2019, was never accepted at the end. However, supporting activities and position papers from stakeholders – among which INDICAM – are converging towards this point.

A significant aspect of this attempt of reviewing the Directive is underlining and specifying the meaning of "active role" of online intermediaries.

Since the memorable L'Oréal vs eBay in 2009, as well as Mediaset RTI vs Vimeo in 2019 in Italia or Tommy Hilfiger vs. Facebook in 2018 in Holland, ISPs' active role has been recognized in some of their offered services: the consequence, in all of these decisions, was holding the online operator accountable for the illicit contents uploaded by third-party sellers. This jurisprudence is therefore fundamental in the path towards the E-Commerce Directive review, since these cases have taken into account the specific business models of various digital intermediaries.

From a wider perspective, the point is considering how access to online information actually happens. The EC, in its document, mentions intermediaries as gate-keepers, and maybe this definition proves the awareness achieved regarding their presence in the digital lives of millions of consumers.

In more passages the EC states that new rules will have to be defined in order to regulate the digital environment and identify whether gate-keepers are liable for the posted contents.

Platforms, as already analyzed in the previous section, are more easily classifiable in a series of due diligence provisions as well as proactive or indexing activities. The word "gate-keeper" pushes us to think about the liability of those actors that do not fit into the "platforms" category, like search engines. Search engines are the true gate-keepers of the digital environment, since they make available for users all the things we can find on the Internet. The indexing of contents is the most active of activities, together with profiling and data storage. Search engines are in charge of the "promotion" of contents (websites, news, information and more), based on proprietary algorithms operating by a multitude of factors. These web junctions can be fully considered gate-keepers and, as a consequence, the EC is expected to include them in the range of subjects that should be held accountable for a much more effective surveillance and proactive control on online contents.

An important topic that the EC for now is not dealing with (maybe because the programmatic documents that have been drafted until now are too generic) concerns repeat infringers. Not even an improvement related to enforcement is mentioned.

In any case, Mrs von der Leyen's Commission directly tackles relevant topics, making a huge step ahead if compared with the generic and disregarded recommendations on the online protection of IPRs drafted by the previous EC. In this case we know that the subject will be tackled and that it will lead (or to be realistic, it should lead) to a more solid digitalization for building a European system of reference. This, without all the doubts related to infrastructures and the difficulties of even out 27 different realities, would mean balancing back rights and duties of online operators.

Final Observations

In 2020 e-commerce is no longer the "other commerce", the little brother of offline trade. Especially in the first months of the year, dramatic because of the Covid-19 pandemic, when the forced isolation has made us all aware of how much of our lives can be entrusted with the online, we have noticed that this interdependence with the Internet needs a better definition of the gate keepers' role, as the new EC has been calling them, showing a trend inversion in comparison with the previous Commission. Whatever we call them, gate keepers, online intermediaries, platforms or OTP, their role in the circulation of contents (information, products, services) is the life itself of the web. By this report INDICAM aimed at analyzing two big systems with almost a billion consumers, most of which are advanced Internet users.

What are USA and Europe saying they will do and actually doing as to Internet governance in order to level the playfield? The warning from the Department of Homeland Security (note: a department created right after 09/11 that rules the internal security of the U.S.) is a clear sign that the situation went very far without interventions.
The U.S. and the intelligence authorities know well how much information circulate through the web where there is no filter regarding illicit contents, except few regulated areas. In fact, this is the real starting point: legislation. It is more and more evident that evolution processes, especially in the digital field, in comparison with the regulatory ones follow a different speed flow; likewise legislators should intervene with a clear, compulsory and updated legal framework, without leaving to the private free initiative the regulation that after all these years is proved to be inadequate to effectively tackle counterfeiting. As far as news, contents and public information, gate keepers' role is simply everything and these subjects cannot longer operate in a virtual territory that because of many indulgent laws in their favor has become a sort of no man's land, where the rule in force when it comes to infringements is the one that big online players auto-impose. The bill, proposed by a bipartisan group of U.S. Representatives, is the sign that something, even in the heart of the country that more than others has seen big online operators thrive under the "safe harbor" protection, can and must change.
Europe has been losing ground in relation to digitalization, if we look at infrastructures, literacy, contents. The heterogeneity of the 27 MS has not helped. Opposed to this fragmentation, there are few and well-organized successful players that hold a significant media presence as those gate-keepers that put

pressure on the previous EC so that it stayed off a review of the liability regime, also by underlining their role in the market. But it is time that stakeholders' efforts join together, leaving behind that fragmentation that has done nothing but weaken their voice.

IPR-intensive industries represent 44% of the EU GDP, a percentage that online intermediaries do not even come close to. However, each of those companies, by acting on its own, has very little chances to leave a mark. INDICAM, by this report, intends to carry out its task of blending the various stakeholders' interests into a common effort. The goal is to condense a series of analysis and considerations for building a journey that leads the EU to review e-commerce regulations and to acknowledge what IP actually means and how it needs support and protection, even online. In the next few months in Brussels an important match will be played and INDICAM will be a part of it, together with its sister associations in Europe. By communicating with our associates and with the suggestions we receive from them, many progresses will be made to achieve our goal, for a digital environment freed by IP violations and the recognition of intermediaries' responsibilities for illicit contents. The present document marks only the beginning of our game and it is the first of a series of reports on the topic.