

# COMBATTING THE ONLINE ILLCIT TRADE OF REGULATED PRODUCTS



# COMBATTING ONLINE ILLICIT TRADE

Products whose distribution and sale are publicly regulated

UNIFAB – ALCCI

## INTRODUCTION

While cybersecurity regularly features in public debate, online illicit trade receives much less attention. Yet, this issue is strategic for the sustainability of industry in France and for making French digital space secure.

One of the aims of this UNIFAB-ALCCI White Paper is to show the extent of online illicit trade, as well as the reality of the risk and harm for consumers, manufacturers<sup>1</sup> and the State.

From a more operational perspective, this White Paper is a reflection of the desire to create an Observatory with online law enforcement capabilities. The objective is for this Observatory to become a Public Interest Grouping (“GIP”) by the end of 2018 under the auspices of the State. It will also involve private-sector stakeholders who are part of the value chain.

This White Paper ties in with the government’s efforts to promote a “cyber intelligence<sup>2</sup>”-based approach and to combat the “uberisation” of crime.<sup>3</sup>

Firstly, we will provide a situational overview of the online illicit trade of products whose distribution and sale are publicly regulated. This analysis will then be extended to other business sectors. The impact of this illicit trade will also be measured.

Secondly, solutions will be proposed:

- setting up an Observatory that is dedicated to monitoring, prevention and law enforcement,
- a series of recommendations illustrated by interviews with the economic and institutional stakeholders concerned.

**Unifab :** the **Union des Fabricants** is the French association for combatting counterfeiting, which brings together 200 companies and trade associations from all business sectors, in order to promote and defend intellectual property law.

**Alcci :** the **Association de lutte contre le commerce illicite** is a recently-formed organisation, which seeks to federate companies, which, in addition to being victims of counterfeiting, are also victims of unfair competition from illicit trade due to resale, smuggling, non-compliance and breaches of commercial rules.

<sup>1</sup> This White Paper will focus on the pharmaceutical, wines and spirits and tobacco industries.

<sup>2</sup> [http://www.lemonde.fr/pixels/article/2018/02/08/cybersecurite-le-gouvernement-veut-mettre-les-telecoms-a-contribution-pour-detecter-les-attaques\\_5253808\\_4408996.html](http://www.lemonde.fr/pixels/article/2018/02/08/cybersecurite-le-gouvernement-veut-mettre-les-telecoms-a-contribution-pour-detecter-les-attaques_5253808_4408996.html)

<sup>3</sup> Cf. the “Perceval” and “Thésée” platforms, which aim to combat fraud involving means of payment and online scams.



---

# SECTION 1.

## SITUATIONAL ANALYSIS

### 1. CHARACTERISTICS OF ONLINE ILLICIT TRADE

#### Definition of illicit products

Various categories can be identified:

- **Resale:** products that are stolen or obtained fraudulently to the detriment of manufacturers and distributors.
- **Parallel market<sup>4</sup>:** trade by retailers who profit from differences in product prices between countries, by importing a product unofficially in order to sell it at a price that is lower than that applied by the manufacturer (medicines, wines and spirits, tobacco).
- **Smuggling<sup>5</sup>:** original brand products that were illegally imported into a country and sold, without paying customs duties and taxes (tobacco, wines and spirits, in particular).
- **Counterfeit goods:** fraudulent imitation in whole or in part of authentic products, illicit manufacturing, distribution and sale, which can take various forms, including the recycling of empty authentic packaging that is then filled with other contents (medicines, wines and spirits and tobacco).
- **Non-compliance:** products that do not meet administrative health and safety standards or that do not have the requisite regulatory authorisation (medicines).

#### Main drivers of illicit trade<sup>6</sup>

Consumer preferences	Business conditions	Regulatory framework
<ul style="list-style-type: none"><li>- Access to premium brands</li><li>- Lower priced products</li><li>- Social acceptance of illicit trade</li><li>- Limited knowledge about illicit products and how to identify them</li></ul>	<ul style="list-style-type: none"><li>- Price gap between licit products and illicit products</li><li>- High levels of excise taxes</li><li>- Availability of ingredients and packaging materials</li></ul>	<ul style="list-style-type: none"><li>- Ineffective enforcement</li><li>- Weak rule of law</li><li>- Corruption</li><li>- Inadequate sanctions</li></ul>

4 <http://www.mercator.fr/lexique-marketing-definition-importation-parallele-marche-gris>

5 Philip Buchanan, Lourdes Chavarria, How to Understand the Impact of Illicit Trade on Business Around the World, Euromonitor, 2015.

6 Philip Buchanan, Lourdes Chavarria, How to Understand the Impact of Illicit Trade on Business Around the World, Euromonitor, 2015

## Internet

On the page dated March 16th 2017 of the “Vie publique” portal there is the following statement: “With a continual rise in the penetration rate of internet use by individuals and businesses, all new digital products or services are a potential target for cyber-attacks and all vulnerabilities in digital systems and platforms will be systematically exploited. The “exposed surface area” is continually increasing with the permanent influx of new technologies and new practices”. In 2017, there were 37 million<sup>7</sup> online buyers in France, i.e. 700,000 more than in 2016.

French online purchasers spent €81.7 billion<sup>8</sup> in 2017, which is almost twice as much as in 2012. These figures have been rising continually for several years.

**Internet<sup>9</sup> has become the main distribution channel for illicit trade and, in particular, for counterfeit goods,** due to its anonymous nature, its ability to operate across several jurisdictions and the ease with which it can be used to display sophisticated replicas of official online stores and, above all, its capacity to reach a large number of potential customers easily.

**The rise in the number of e-commerce platforms (such as eBay, PriceMinister and Alibaba) and social networks (such as Facebook, Twitter and Instagram) has made it possible for traffickers to extend their illicit activities considerably<sup>10</sup>.**

Online Illicit trade<sup>11</sup> has two main characteristics:

- Sale to the public in breach of the law (on property, tax, compliance and contracts), which offers a competitive advantage (no taxes, purchasing or manufacturing costs, copyright or standards, for example).
- It is an innovative entrepreneurial activity that exploits the opportunities granted by the vulnerabilities of the internet.
- According to a 2016 OECD and EUIPO report, 63% of counterfeit seizures were in postal or courier parcels, many of which can attributed to online, e-commerce sales.

**Products whose online distribution and sale are regulated:**

## Medicines

It is important to stress that since 2013<sup>12</sup>, the online dispensing of medicines in France is authorised and highly regulated: in practice, only French websites that sell medicines for which a prescription is not obligatory, which are part of a brick and mortar dispensary and that have first obtained authorisation from the Agence régionale de santé (Regional Healthcare Agency or “ARS”), are authorised.

The legality of these websites can be verified through the display of a common European logo and by consulting the list of the authorised websites that is kept by the French Ordre national des pharmaciens (French Chamber of Pharmacists). Brick and mortar dispensaries remain a bastion against counterfeit medicines, due to the quality of pharmaceutical distribution, as well as the pharmacist’s role of advisor and his/her proximity to patients.



[Click to verify the legality of the website]

In contrast, the online sale of medicines for which a prescription is obligatory is still prohibited, as the French Supreme Administrative Court reiterated in its decision of July 17<sup>th</sup> 2013.

7 [https://www.journaldunet.com/ebusiness/commerce/1172030-chiffre-d-affaires-e-commerce-france/?een=533fb5bf0640b57b376c9cfce2712de2&utm\\_source=greenarrow&utm\\_medium=mail&utm\\_campaign=ml50\\_bilane-commerce](https://www.journaldunet.com/ebusiness/commerce/1172030-chiffre-d-affaires-e-commerce-france/?een=533fb5bf0640b57b376c9cfce2712de2&utm_source=greenarrow&utm_medium=mail&utm_campaign=ml50_bilane-commerce)

8 [https://www.journaldunet.com/ebusiness/commerce/1172030-chiffre-d-affaires-e-commerce-france/?een=533fb5bf0640b57b376c9cfce2712de2&utm\\_source=greenarrow&utm\\_medium=mail&utm\\_campaign=ml50\\_bilane-commerce](https://www.journaldunet.com/ebusiness/commerce/1172030-chiffre-d-affaires-e-commerce-france/?een=533fb5bf0640b57b376c9cfce2712de2&utm_source=greenarrow&utm_medium=mail&utm_campaign=ml50_bilane-commerce)

9 Unifab, Contrefaçon et terrorisme, 2016, p. 3

10 Unifab, Contrefaçon et terrorisme, 2016, p. 24.

11 Dominique Lapprand, ALCCI, Hyperconnection, International Cybersecurity Forum, 23-24 January 2018.

12 Source: Order of June 20th 2013 on best practices in the dispensing of medicine by electronic means. <https://www.legifrance.gouv.fr/eli/arrete/2013/6/20/AFSP1313848A/jo>

## Wines and spirits

According to Article L 3331-4 of the French Public Health Code (CSP), the remote sale of alcohol is regarded as a take-out sale of alcohol. The sale of alcohol via a website therefore requires compliance with the typical formalities for take-out sales of alcohol<sup>13</sup>.

## Tobacco products

The French General Tax Code (CGI)<sup>14</sup> prohibits the sale of cigarettes other than through the network of tobacconists: remote sales of cigarettes on French territory are therefore prohibited. Article 568 ter of the CGI specifically prohibits all remote sales and purchases, whether online or via correspondence, of manufactured tobacco products.

Nevertheless, the Member States of the European Union have differing approaches to the prohibition of online sales. Indeed, when the retail site is not located on French territory, enforcement is more complicated in practice due to the free movement of goods.

## 2. THE EXTENT OF ONLINE ILLICIT TRADE: A SECTORAL ISSUE

**Within the European Union, one-third of all counterfeit goods that are seized have a connection with online distribution networks<sup>15</sup>.**

**In France, the customs authorities seized a total of 8.4 million counterfeit items in 2017<sup>16</sup>. The French customs seized 2.3 million counterfeit items from the express freight and postal networks in 2017, which represent more than 27% of the total quantities of counterfeit items intercepted<sup>17</sup>.**

### a. Medicines

According to the WHO<sup>18</sup>, **a patient has a 90% risk of being “misled” when purchasing medicines on the internet** and around 50% of patients run the risk of purchasing a fake medicinal product. At global level, it is estimated that there are up to **50,000 active online pharmacies**, around 95% of which do not comply with the laws and industry standards that were introduced to protect patients<sup>19</sup>. Around 30,000 illicit websites are believed to target the European market<sup>20</sup>.

The templates, which are models of fake dispensaries, give the impression of a global network; however, in reality, there are not many actual networks behind the trafficking.

According to the data gathered in the OECD-EUIPO database on global customs seizures, between 2011 and 2013<sup>21</sup>, India was by far the main provenance economy of counterfeit pharmaceuticals, being the origin of 55% of the total seized value of counterfeit pharmaceutical products worldwide (Figure 2.5). It was followed by China (33%), the United Arab Emirates (4%) and Hong Kong (China) (3%).

### France

> 129,257 counterfeit medicines were seized by the customs authorities in 2017<sup>22</sup>. **In the same year, 91% of counterfeit medicines were seized in the express freight and postal networks<sup>23</sup>.** More than 75% of counterfeit medicines are intercepted in packages following online orders.

> **In June 2015 more than 960,000 illicit healthcare products and around 1.4 tonnes of miscellaneous pharmaceutical products from online sales were seized<sup>24</sup>.**

13 One of the two following licences are required for take-out sales of alcohol (CSP, Art. L 3331-3): either, the licence for small-scale take-out sales (beverages in group 3), or the standard licence for take-out sales (all beverages for which the sale is authorised).

14 Decree no. 2010-720 of June 28th 2010 that was enacted pursuant to Article 568 of the French General Tax Code defines the rules associated with the capacity of tobacconist.

15 Luxury Daily, Online anti-counterfeiting strategies preserve brand equity: NetNames, 2015: <https://www.luxurydaily.com/online-anti-counterfeiting-strategies-preserve-brand-equity-netnames/>

16 Directorate General of Customs and Excise, 2017 Results, p. 12.

17 Directorate General of Customs and Excise.

18 <http://www.iracm.com/observatoire-thematique/falsification-sur-internet/>

19 Peter Behner et al., PWC, Fighting counterfeit pharmaceuticals, new defenses for an underestimated - and growing - menace, p. 9.

20 Source: Alliance for Safe Online Pharmacies/Pharmaceutical Security Institute.

21 Source: OECD/EUIPO (2017), Mapping the Real Routes of Trade in Fake Goods, OECD Publishing, Paris, <https://doi.org/10.1787/9789264278349-en>

22 Directorate General of Customs and Excise, 2017 Results, p. 31.

23 Directorate General of Customs and Excise.

24 Directorate General of Customs and Excise, 2016 Results, p. 8.

The internet is the only means of penetrating the legal market. There are not really any cases of websites that are hosted on French territory; however, there are cases involving websites located outside of France that are accessible to French consumers. Having said that, as prescription sales are in principle prohibited in France, the regulations make it easier to identify illegal sites. In contrast, it is more difficult for consumers to know which websites are illegal, as they are not always aware of the French legal environment.

> The international operation<sup>25</sup> conducted by Interpol between 12 and 19 September 2017 led to the **seizure in France of more than 433,000 illicit healthcare products and 1.4 tonnes of healthcare products in bulk form. More than 70% of the products seized came from Asia (mainly India and Singapore).**

In total, **185 illegal websites selling counterfeit medicines** were identified in France during the operation:

- 174 illegal websites were identified by the customs authorities and 27 investigations, primarily concerning medicines (in particular erectile dysfunction medicines), bulk products (in powder or tablet form) and performance enhancing drugs, were opened.
- Legal action was taken against 11 illegal websites selling counterfeit medicines that were identified by the OCLAESP<sup>26</sup> (French Central Bureau for Combatting Harm to the Environment and Public Health) and the SCRC/C3N<sup>27</sup> (Central Agency for Criminal Intelligence/Centre for Combatting Criminal Digital Activity). These same websites were also reported to the foreign authorities.

## Causes

With distribution expanding geographically and the number of points of sale multiplying, monitoring the logistics chain has become increasingly complex in terms of capacity. Those shortcomings are more pronounced at the patient's end of the chain. For products that are distributed online, effectively monitoring the logistics chain is nearly impossible<sup>28</sup>. The growing culture of self-diagnosis<sup>29</sup>, self-prescription and self-treatment has made it relatively easy for mediocre products to infiltrate their way into the supply chain.

## The online offer of illicit medicines in France

In France<sup>30</sup>, online sales of fake medicines are made via temporary websites that specialise in counterfeiting or falsification ("parasite websites"), which are directly created by the producers of illicit medicines in order to attract retailers (Business to Business or B2B transactions) and/or final consumers (Business to Consumer or B2C transactions), or, via platforms that allow for private sales (B2C and Consumer to Consumer or C2C transactions).

B2B websites sell raw materials.

Criminals have been able to hijack some B2C websites – French "virtual pharmacies" that are part of brick and mortar pharmacies – and redirect their traffic to other, apparently Canadian, websites, for example.

The selling point of the C2C websites is the price, which is not at all obvious, as the prices are often similar to those of licit medicines but such websites are still attractive when they are used to avoid obtaining a prescription.

A distinction should also be made between "mirror" websites and "placeholder" websites, which are awaiting activation. **Some traffickers can set up several thousand "mirror" websites on the basis of a single "root" website in order to mislead the investigations.** This shows the difficulty in being able to retrace the channels directly on the internet, and the extent to which the traffickers must be regarded as skilled entrepreneurs.

25 <http://ansm.sante.fr/S-informer/Communiqués-Communiqués-Points-presse/Résultats-français-de-l'opération-PANGÉA-X-contre-les-réseaux-de-vente-illicite-de-medicaments-et-de-produits-de-santé-Communiqué>

26 OCLAESP: French Central Bureau for Combatting Harm to the Environment and Public Health

27 SCRC/C3N: Central Agency for Criminal Intelligence/Centre for Combatting Criminal Digital Activity.

28 WHO Global Surveillance and Monitoring System for substandard and falsified medical products, 2017, p. 38.

29 WHO, Global Surveillance and Monitoring System for substandard and falsified medical products, 2017, p. 48.

30 FAKECARE, Developing expertise against the online trade of fake medicines by producing and disseminating knowledge, counterstrategies and tools across the EU, Andrea Di Nicola et al., December 2015.

## **It can be very difficult to distinguish between legitimate virtual pharmacies and fake pharmacies.**

Some websites based in Asia (India) are sometimes partially written in French. A large percentage of online purchasers choose “home delivery” of their products. Online purchases are therefore primarily delivered by express freight or post.

Concerning online sales of fake medicines, case studies show that all therapeutic classes are concerned by counterfeiting; however, seizures most frequently concern performance enhancing drugs, such as anabolic steroids, and lifestyle or comfort drugs, such as erectile dysfunction products or weight loss products. Every year, hundreds of thousands of people throughout the world fall victim to counterfeit, fake medicines.

## **Crime**

Most criminals who are involved in the illicit trade in France can be perceived as opportunists, as they are already active in the healthcare sector on a global scale. Customs reports and police seizures show that the illicit medicines that transit via France are for the most part destined for Latin America or Africa. Most fake medicines that are sold online are imported from China, India, Pakistan, Thailand and other Asian countries; some European countries are also used as transit points for the medicine traffickers.

According to the French customs authorities, the criminal organisations involved are set up in two ways, either, for direct sales to final customers, or, via more complex logistics circuits with intermediary/transitional structures in France or Europe, which store the products abroad then sell them – with easy, high profits – in the target country.

To take the example of one case, in 2017 several dozen French websites were hacked <sup>31</sup> so that advertisements for low-cost erectile dysfunction products would be displayed on their pages. These illegal pharmacies targeted various websites: the Rhône Tourist Office, the Records Department of the City of Rennes, Beauvais Hospital or the Salvation Army.

Well-known websites are ideal targets for traffickers. Among other things, cybercriminals use “black hat SEO <sup>32</sup>” techniques, which involve benefiting from the high ranking of these lawful websites in search engines in order to promote their illicit activities.

## **Strategic interest of the parallel market**

Illicit trade also concerns the parallel market, which is a growing problem for many online industries that produce regulated products.

The “Cracking Counterfeit Europe” study <sup>33</sup>, which was commissioned by Pfizer in 14 European countries, estimated that the parallel market for medicines in Europe represents more than €10.5 billion per year. In France, this market is thought to represent around €1 billion. One-fifth of the persons surveyed – i.e., the equivalent of 77 million people – admitted having purchased medicines that are usually prescription-only outside of the authorised circuits. In France, 14% of respondents disclosed this information, which is equivalent to 6.9 million people.

### **b. Wines and spirits**

The OECD estimates that the **consumption of alcohol of illicit origin accounts for 25% of worldwide adult consumption**<sup>34</sup>. On the internet, most sector observers acknowledge the difficulty in compiling statistics on wines and spirits but have observed a significant increase in the problem for French brands and a rise in the risk.

**French brands operating on the international market have stated that they are encountering problems with counterfeiting or online parallel markets.**

<sup>31</sup> <http://www.iracm.com/2017/01/france-plusieurs-dizaines-de-sites-web-francais-pirates-dans-le-de-vendre-des-produits-erectiles-illegaux>

<sup>32</sup> Search engine optimisation.

<sup>33</sup> Quoted in the LEEM press pack, Contrefaçon de médicaments, une atteinte à la santé publique, June 2014, p 5.

<sup>34</sup> OECD (2016), Illicit Trade: Converging Criminal Networks, OECD Reviews of Risk Management Policies, OECD Publishing, Paris, <https://doi.org/10.1787/9789264251847-en>.

## Counterfeiting

**For French brands operating on the international market, counterfeiting does not only concern luxury wines and spirits**, such as cognac, vodka, champagne and certain fine wines - in terms of distribution to the consumer, these products are above all found on C2C platforms - but also more accessible products.

**The specificity of online sales to consumers is that these illicit wines and spirits are sold on e-commerce websites or legal online market places.** The traffickers sometimes replace very high-end content with content of lower quality, but that is still high-end. Consumers who are unaware when using these websites are therefore clearly exploited, all the more so as the sale prices are between 80% and 100% of the original prices. The traffickers' margins are therefore particularly high.

However, **it is the B2B websites, which sell the materials and equipment needed for counterfeiting, that are the major challenge**, as the largest amounts of trafficked counterfeit goods transit via these websites. Chinese glassmakers thus offer their products online on certain well-known platforms, such as Alibaba. A Chinese intermediary can, for example, offer to supply 10,000 empty vodka bottles per month on an Asian marketplace, and supply up to 1 million empty bottles of major French brands. In Asia and Eastern Europe, production lines or bottling machines can be purchased online. This data gives an idea of the production capacity, the resources provided and the fast response times of the counterfeiters.

**An entire industry devoted to counterfeiting wines and spirits has therefore spread across the internet, in particular for French luxury brands.** It is not only empty bottles that are sold online, but also labels and even the anti-counterfeit technologies that are dedicated to these products. Rudimentary content is then added (e.g. ethanol) before these bottles are sold on B2C websites, which often target Asia or Eastern Europe.

It should nevertheless be noted that the traffickers rarely focus on more than one product, given the specificity of the sector and the major investments required.

On the internet, the main risk areas for French wines and spirits are:

1. China / Asia.
2. Russia / Eastern Europe.
3. Latin America / the Caribbean.
4. Africa / the Middle East.

## The parallel market

Wines and spirits also suffer due to the existence of the parallel market. The difficulty for brands lies in the fact that distribution contracts do not obligatorily prohibit such a practice. **Some distributors can also use the parallel market as a technique to obtain high financial profits, in particular by exploiting the difference in tax levels between various countries.** Distributors in Eastern countries and the Middle East are particularly concerned, as is China, for example, where sales are also made on online platforms. In general, **the parallel market for wines and spirits is closely tied to the internet as there always comes a point when it is necessary to sell the stock and to make it visible on the legal market.** Fragmented distribution through lawful online stores facilitates such trafficking and makes it all the more complex to monitor.

**The percentage of online “counterfeit” and “parallel market” sales are respectively estimated at around 30% and 70% in the wines and spirits sector.**

**On French territory** the problem is less prevalent; however, cases involving counterfeit vintages have been identified for wines and champagnes sold at auctions or on C2C market place-type websites. The traffickers tend to target rare vintages, which are difficult to date and therefore hard to identify with certainty in wine producers' records. In France, a potential risk also concerns the parallel market, with the development of marketplaces and social networks.



## c. Tobacco products

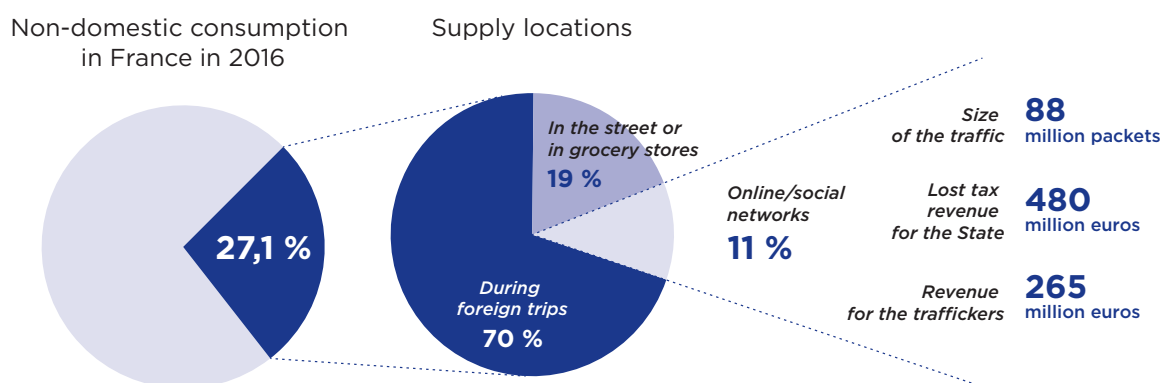
In 2016, the smuggling and counterfeiting of cigarettes were estimated to account for more than 9% of the total consumption in Europe. This represents a lost tax of €10.2 billion<sup>35</sup>. According to the latest results of the French customs authorities, **238.2 tonnes of counterfeit and smuggled tobacco products were seized on French territory**<sup>36</sup>.

**In France, cigarettes not purchased from the network of tobacconists represent 27.1% of the total consumption**, i.e., around 16.5 billion individual cigarettes (around 800 million cigarette packs). While around half of this non-domestic consumption is legal (imported tobacco products within the authorised limits), **the volume of smuggled and counterfeit cigarettes represented nine billion individual cigarettes in 2016 (around 450 million cigarette packs)**.

Consumers who wish to obtain products at cheaper prices than those applied in the official network of tobacconists often opt for illegal cigarettes. Indeed, France is a country where taxes on cigarettes are very high, which makes it the country in continental Europe with the highest sales prices.

The methods of transport most frequently used for smuggled and counterfeit products are road haulage, across borders with EU countries, and air or sea freight, from countries outside the EU such as African and Asian countries.

### Online Illicit cigarette sales<sup>37</sup>



Online sales of tobacco products are an emerging trend. They represented around 10% of total tobacco products seizures<sup>38</sup>. Smuggled and counterfeit products<sup>39</sup> are offered either via websites, and then sent by post, or on social networks such as Facebook, where products are delivered by hand.

In France, it is already estimated that 11% of non-domestic consumption<sup>40</sup>, i.e. around 88 million cigarette packs, come from the internet and social networks sales. The increase of one euro on March 1st 2018 could therefore have a direct impact on smuggled and counterfeit cigarettes, in particular on social networks (500 additional traffickers on Facebook are expected by the next quarter, according to Webdrone).

<sup>35</sup> KPMG, SUN report, 2016.

<sup>36</sup> Directorate General of Customs and Excise, 2017 Results, p. 4.

<sup>37</sup> Daniel Bruquel, PMF, Hyperconnection, International Cybersecurity Forum, 23-24 January 2018.

<sup>38</sup> Savona, TRANSCRIME THE FACTBOOK ON THE ILLICIT TRADE IN TOBACCO PRODUCTS, number 8, 2016, p. 59, source 2012.

<sup>39</sup> The customs authorities do not make a distinction between smuggled and counterfeit goods in seizures.

<sup>40</sup> 2016 Nielsen Study for PMF.

## Two types of illicit distribution dominate on the internet:

- **E-commerce websites based outside France** (but not linked to a platform in France). A wide range of websites with French-language content or that offer delivery to France, are clearly targeting French consumers. These websites are set up in the same way as classic e-commerce sites: they have a range of products on offer, a shopping cart, promotions, online payment facilities and offer shipping to a postal address. They are listed by the most well-known search engines, or even recommended (or not), on numerous forums.

They offer a very wide choice of smuggled or counterfeit tobacco products, with a major price difference: a pack of cigarettes costs between €1 and €5 on the internet (compared to €8 for the highest selling brand in France in 2018).

From a commercial standpoint, in addition to the attractive prices applied, they make every effort to attract and reassure the consumer.

For some sites, including those based in the European Union, the economic model is simple and effective: it involves purchasing cigarettes on the local legal network in countries with the cheapest prices and then reselling them online.

**Around thirty websites, with content correctly drafted in French and well-designed as legal e-commerce websites, are targeting French consumers and can register more than 100,000 hits per month.** One of the most visited websites registered 170,000 hits, 95% of which were from French consumers, in December 2017 alone.

- **Sale of tobacco products on social networks.**

**It is estimated that two-thirds of the illicit trade in tobacco products transit via social networks. There has been an exponential increase in supply on these networks, and particularly on Facebook.**

Small- and large-scale traffickers post advertisements on personal accounts (using pseudonyms) asking to be contacted via private message. These advertisements can then be passed on via Facebook groups (e.g. “good deals for smokers”). Once these groups reach a critical size, they become private and are invisible to law enforcement.

An analysis of cigarette sellers performed in 2017 generated the following results<sup>41</sup>:

- **350 Facebook groups make up an estimated network of 5 million people and therefore 5 million potential consumers.** These group have 14,000 members on average and the largest has 374,000. 35% of them are closed groups and 3% are secret groups.

The profile of traffickers, who are single or repeat offenders, reflects a genuine commercial and marketing strategy. These criminals use other networks, such as Instagram, Snapchat and Pinterest to advertise their Facebook page, where they display their illicit commercial offering.

Most of the time, they are local criminals who use these distribution methods and deliver illicit cigarette cartons directly to consumers. We are witnessing a reproduction of the physical networks in the virtual world, which makes it possible to offer a complete range of illicit products.

## Two examples of cases:

- **The illicit website ruedutabac.com (shut down in 2015)**



This website enjoyed considerable success due to its search engine ranking and its graphic charter, which was to a large extent inspired by a major e-commerce website.

As is the case for many illicit sales networks (that offer counterfeit products, pharmaceutical products and cigarettes), this website did not exist in isolation. On the contrary, it was at the centre of a “system” of websites used for listing purposes, in particular via the domain name (rueutabac.net.) and links

<sup>41</sup> Didier Douilly, Webdrone, Hyperconnection, International Cybersecurity Forum, 23-24 January 2018.

placed on websites that sell cigarettes.

The content of the website was regularly updated, as were the graphic themes.

However, this façade did not stand up to in-depth analysis. Even if we only examine the information that was visible on the website, it became clear that the telephone number displayed (+4477xxxxxxx) was a British number. A basic search engine query led to a company that is based in a tax haven in the Seychelles.

The website's IP address, which is a kind of digital licence plate, showed that it was hosted in Russia.

A search revealed that this hosting space had several websites with suspect online stores for the sale of steroids, pharmaceutical products and counterfeit goods. For the payment, users were redirected to an external page linked to another website hosted in Russia.

The economic model for these websites is aiming at building loyalty among purchasers by sending actual products. The commercial support is present and responsive. In parallel, the traffickers organise a listing campaign combined with the publication of numerous, fake, positive comments on opinion websites.

During a second phase, once trust has been obtained, payment for orders is collected by the website, but the products are no longer delivered and the seller no longer responds to contacts. Purchasers who use this illicit set-up have no means of action against the seller. Once the scam becomes known (on forums and through negative opinions), the websites close down, then re-open under a new identity.

#### - A recent case in Lyon

On March 6th 2018, the National Customs Judicial Department (Lyon unit)<sup>42</sup> and the Lyon district company of gendarmes dismantled a network of smuggled tobacco goods that was supplying the parallel market of clients for the entire region of Lyon. The investigation, which lasted around two years, made it possible to identify a structured organisation, which, in particular, used online social networks to sell large quantities of cigarette cartons. The goods were offered for sale online with a system of quantity-based price discounts (between €35 and €40 for a carton, i.e., around half the price in force on the national legal market). The deals took place in clearly identified zones, in the same way as drug trafficking. In total, 2.4 tonnes of cigarettes, i.e., 122,220 cigarette packets, and €75,000 in low-denomination banknotes were intercepted. Seven persons were also arrested.

## 3. ONLINE ILLICIT TRADE: A KEY MARKET FOR CRIMINALS AND TERRORISTS

### Crime

Criminal networks have been able to adapt and profit from the globalisation of markets and the economy, as well as the development of new technologies and the internet. The new face of organised crime is more and more like that of a typical commercial company, but with completely flexible structures, which make it dangerously responsive to changes in its environment.

**The most significant criminal cases involving the internet**, in the sectors of activity covered by this White Paper, allow us to identify the **following characteristics**:

- **The sophistication of the methodologies** used by the online traffickers when setting up illicit websites. These criminals can have **powerful research and development departments** (above all in China or in Russia) for their online organisation.
- **The excellence of the online promotion** of the illicit websites: numerous mirror websites, cutting-edge SEO techniques, fake promotional advertisements on forums, etc.

<sup>42</sup> Le Progrès, Démantèlement d'un réseau de contrebande de cigarettes en région lyonnaise, March 8th 2018.

- **The de-territorialisation of the set-up**, for example for hosting or payments.
- **The significant growth of social networks** in the distribution of illicit products on the French market.
- **The relationship of trust that these websites manage to create with the consumer**. They are well-designed and can blend lawful and illicit marketing.

## Terrorism

In the 2000s, numerous paramilitary and terrorist groups sought to diversify their financing methods by turning to counterfeiting, and the illicit trade of raw materials, which gave these activities a new dimension. The Institut de Recherche Anti-Contrefaçon de Médicaments (Institute for Research into Combatting the Counterfeiting of Medicines - IRACM) published a study in 2013 entitled “Contrefaçon de médicaments et organisations criminelles” (“Counterfeiting of medicines and criminal organisations”), which stated that the trafficking of fake medicines is a source of financing for global terrorism. A UNIFAB<sup>43</sup> report entitled “Contrefaçon et Terrorisme” (“Counterfeiting and Terrorism”) in 2016 identified a series of terrorist groups (Hezbollah, ISIS and Al-Qaeda) that are involved in such trafficking. The Silk Road online black market that the FBI shut down at the end of 2013 also revealed the risks caused by the darknet, where groups of terrorists, and criminals, could trade in counterfeit goods anonymously.

For some years now, social networks have taken on genuine importance in these “terrorism-counterfeiting” relations. The European Commission thus recently stated that it wished to “urge social networks to develop and expand the use of automatic tools for recognising and taking down illegal content”<sup>44</sup>, in particular of a terrorist nature. Measures to tackle counterfeiting, and, more generally, products that are harmful to consumers, are included in its recommendation of March 1<sup>st</sup> 2018.

---

# SECTION 2.

## IMPACTS OF ILLICIT TRADE

### 1. IMPACTS ON THE CONSUMER/PATIENT

#### Medicines

**According to the WHO, around 50% of medicines that are sold online are counterfeits<sup>45</sup>.**

#### High levels of demand in Europe<sup>46</sup>

This risk is even greater at present, as the populations of all the countries, including the most developed countries, appear to underestimate the danger. More than two million patients consult a website selling medicines every day in Europe for advice or in order to make a purchase (European Association of Mail Service Pharmacies).

Despite a high level of awareness<sup>47</sup>, numerous purchasers state that time pressures, financial concerns and preferring to remain anonymous are all reasons for people to purchase medicines via unconventional methods, despite the known risks. Moreover, **the tendency for people to self-medicate is increasing in France and is a major contextual factor with regard to the online demand for medicines**. According to the IFDP (the training centre for pharmaceutical experts), the rising number of online purchases of

<sup>43</sup> UNIFAB, Contrefaçon et Terrorisme, 2016.

<sup>44</sup> Derek Perrotte, Terrorisme, contrefaçon : Bruxelles tacle les géants du Web, les Echos, 2-3 March 2018.

<sup>45</sup> Peter Behner et al., PWC, Fighting counterfeit pharmaceuticals, new defenses for an underestimated - and growing - menace, p. 9.

<sup>46</sup> <http://www.iracm.com/observatoire-thematique/falsification-sur-internet/>

<sup>47</sup> FAKECARE, Developing expertise against the online trade of fake medicines by producing and disseminating knowledge, counterstrategies and tools across the EU, Andrea Di Nicola et al., December 2015.



medicines by the French can also be understood due to the problems undermining the social security system.

In France, there is a potential demand for illicit medicines, in particular for non-prescription medicines for which a prescription is now required.

Moreover, the internet is a source of information that is widely used by young people who utilise medicine for “sensation-seeking”, and it is becoming more common for this sector of the population to be targeted by illegal pharmacies that use social networks in order to advertise their products. In the United Kingdom, Xanax is thus purchased on social networks such as Instagram and Facebook by young adolescents.<sup>48</sup>

However, research and observation of forums have shown that illicit cyber-pharmacies also appear to target:

- Disabled persons, and persons who do not have health or medical insurance,
- Individuals who wish to remain discrete with regard to their health and the product purchased, and persons who live far from a pharmacy, such as residents in rural areas.

## Tobacco products

### Risks for the consumer

Consuming products that potentially do not comply with French legislation in terms of the levels of tar and nicotine, the health warnings and the composition of cigarette in the case of counterfeits, can be risky for consumers.

Internet also facilitates uncontrolled access to tobacco for minors.

There is above all **poor knowledge of the law**<sup>49</sup> by French consumers: **40% of adult smokers surveyed did not know that it is prohibited to purchase tobacco products over the internet.**

## Wines and spirits

Counterfeit products that are intended for human consumption, such as wines and spirits, must be treated more seriously than any other type of infringement of intellectual property. Contrary to leather goods, in particular, counterfeit food products are generally sold at the same price and in the same places as legitimate food products. Now, no consumer wants to drink fake alcohol for the price of genuine alcohol. For most of the products, counterfeit simply means “poor quality”. For food products, counterfeit can mean “seriously harmful”.

## 2. IMPACTS ON BUSINESSES AND ON THE ECONOMY

### Medicines

Within the European Union<sup>50</sup>, the total effect of counterfeiting is estimated at 4.4% of the turnover of the medicines sector, which is equivalent to €10.2 billion and 37,700 lost jobs.

If we take into account the direct and indirect effects<sup>51</sup>, counterfeiting in this sector causes lost sales of around €17 billion for the EU’s economy and around 91,000 lost jobs<sup>52</sup>.

**In France, the lost turnover, including the indirect effects, totals €1,851 million, with a loss of 9,212 jobs.**

The impact is also significant in terms of image and trust (of healthcare professionals and patients).

48 <http://www.bbc.com/news/uk-england-43048406>

49 Daniel Bruquel, PMF, Hyperconnection, International Cybersecurity Forum, 23-24 January 2018. Source: Etude CSA, 2017

50 EUIPO, THE ECONOMIC COST OF IPR INFRINGEMENT IN THE PHARMACEUTICAL INDUSTRY, September 2016. The estimate of the model was made on the basis of the data of 19 Member States, which represent 94% of the total consumption in the 28 EU States.

51 These indirect effects result from the fact that the various sectors of the economy purchase products and services from each other in order to use them in the production processes.

52 EUIPO, THE ECONOMIC COST OF IPR INFRINGEMENT IN THE PHARMACEUTICAL INDUSTRY, September 2016, p. 5.

## Wines and spirits

It is estimated that counterfeiting in the wines and spirits industries, if the repercussions for the other industries and public revenues are taken into account, causes lost sales of around €3 billion for the European Union economy and the loss of 23,400 jobs.

**In France, the direct and indirect effects of counterfeiting wines and spirits result in a loss of €492 million of turnover and more than 2,500 lost jobs.**

## Tobacco products

**In France, in addition to the lost tax revenue, job losses in the tobacco sector are, in particular, linked to the closure of more than 1,500 tobacconists over the past three years<sup>53</sup>.**

## 3. IMPACTS ON THE STATE

### Medicines

Within the European Union, the lost public revenue due to the direct and indirect effects of counterfeiting is estimated at around €1.7 billion<sup>54</sup> per year.

### Wines and spirits

Within the European Union, the lost public revenue is estimated at around €1.2 billion per year, which includes the direct and indirect effects<sup>55</sup>. **Lost revenue in the wines and spirits sector in France is estimated at €100 million<sup>56</sup>.** The reference period for the financial losses on medicines, wines and spirits is 2008-2013.

### Tobacco products

**The tax revenue losses caused by the online illicit trade of cigarettes are estimated at €480 million for the French State<sup>57</sup>. Improved knowledge on the part of suppliers and customers is necessary in order to make a system of “due intelligence” more adapted to the illicit trade that targets them.**

---

## SECTION 3. TOWARDS NEW METHODS OF WORKING TOGETHER

### 1. The importance of a shared commitment to action

<sup>53</sup> Source: Tobacconists' federation.

<sup>54</sup> EUIPO, THE ECONOMIC COST OF IPR INFRINGEMENT IN THE PHARMACEUTICAL INDUSTRY, September 2016, p. 5.

<sup>55</sup> EUIPO, THE ECONOMIC COST OF IPR INFRINGEMENT IN SPIRITS AND WINE, July 2016.

<sup>56</sup> EUIPO, THE ECONOMIC COST OF IPR INFRINGEMENT IN SPIRITS AND WINE, July 2016, p. 18.

<sup>57</sup> 2016 Nielsen Study for PMF.

## 1.a. A multi-sectoral problem that involves a variety of stakeholders

The issue of working together not only concerns industries for which the distribution is regulated by the State, such as online gaming, but also industries for which the online sale of products is prohibited, such as tobacco.

The online distribution of medicines, wines or spirits is subject to conditions, as described above (cf. section I.1).

A variety of intermediaries such as payment service providers, mail delivery companies and logisticians are also concerned by the problem.

In a second phase, an Observatory could be created, involving other industries, such as cosmetics, toys or spare parts industries, each of which has specific issues concerning online sales.

## 1.b. Restricted law enforcement approaches

Current enforcement is difficult to set-up, due to the **delocalised, fragmented structure of illicit websites**.

Counterfeiters reserve hundreds of domain names: In fact, websites with “.fr” top-level domains that sell illicit products are frequently hosted outside France.

Means of payment are also delocalised and the small quantities ordered by consumers make customs inspections extremely difficult. Moreover, the “takedown”<sup>58</sup> strategies, which involve using service providers to eliminate the illicit advertisements, are long and costly processes.

To sum up, numerous factors contribute to making law enforcement missions increasingly complex.

In the public sector, government law enforcement services cannot investigate all the online offences as this would involve far greater resources and instantaneous response time. When researching information to support drafting this “White Paper”, most of the stakeholders surveyed acknowledged that **a paradigm shift is required in the approach to prevention and law enforcement**.

## 2. How can the stakeholders work together?

### 2.a. The need for an Observatory that is dedicated to combatting the illicit trade of products whose distribution and sale are subject to public regulations

Given the current limits of law enforcement, most professionals, manufacturers and service providers that are victims of illicit trade agree that several factors justify the implementation of an **Observatory that is dedicated to combatting the illicit trade of products whose distribution and sale are regulated**:

- The importance of **improved real-time monitoring** of the risks associated with illicit trade, with **information sharing between stakeholders**.
- A **more cross-cutting approach** to problem solving.
- **Pooling of efforts** by chain stakeholders.
- **Faster, more effective prosecution** of cases.
- **Sharing of field experiences** and **operating methods**.
- The project should allow for **intra-stakeholder** mobilisation (of the networks within each of the private-sector or public-sector stakeholders) and **inter-stakeholder** mobilisation.

**The public authority** could be set up on an ad hoc basis in the form of an **Observatory that is dedicated to combatting the online illicit trade of products whose distribution and sale are regulated**.

This Observatory could be made up of police officers, gendarmes, DGCCRF (General Directorate for

<sup>58</sup> The principle of a “takedown” is to delete the illicit content on a website.

Competition Policy, Consumer Affairs and Fraud Control) officers, customs officers, representatives of the private sector and of any other necessary area of expertise that is dedicated to combatting illicit trade, in order to constitute a mixed, multi-disciplinary unit with a variety of expertise that is capable of combatting the phenomenon of illicit trade and the ramifications thereof (financing of organised crime, terrorism and other illegal activities).

Moreover, this Observatory, which should have **a formal method of functioning**, through the implementation of an information exchange system (digital and physical/vocal), must not neglect the **informal aspect** of such a project and the importance of human relations in information sharing and investigations.

#### **To sum up:**

**In terms of cooperation: the purpose of the Observatory, which will bring together all the stakeholders concerned, would be to exchange information and identify illicit channels, so that preventive, regulatory and law enforcement systems can then be implemented.**

NB: although there is a consensus and genuine motivation concerning these guidelines between the stakeholders involved, the precise operating methods of the Observatory in question still need to be detailed and formalised (how the existing structures will operate as a part of a network, the roles of

## **INTERVIEW**

**Philip Morris France SAS**

**Daniel Bruquel, Manager Illicit Trade Strategy & Prevention**

***Why are you involved in the discussions surrounding this Observatory as a representative of the tobacco industry?***

The tobacco sector is impacted by major online parallel market based on social networks or websites, most of which are European. This phenomenon, with which the public authorities are not familiar and that causes major losses of tax revenues, is likely to increase sharply with the rise in tobacco prices on March 1st 2018. The economic operators who are victims of online illicit trade have a duty to take firm action and to mobilise the public authorities, so that law enforcement is more adapted and effective. The Observatory and its online capabilities would be a novel solution and we have found its approach to be convincing.

***In your opinion, what are the strengths of such an Observatory?***

This initiative is a step towards greater flexibility in dealing with online traffickers, who are more skilful than ever. The aim is not to create a structure that is overly sophisticated, but above all to ensure greater fluidity in exchanges between companies and with public authorities. The approach must be efficiency-driven, for example by streamlining the procedures for complaints.

***What has been the reaction of manufacturers and service providers that are concerned by this problem?***

The fact that representatives of all the stakeholders in the value chain, from transport companies to manufacturers, including ISPs and payment service providers, have responded favourably to this initiative, on a voluntary basis, is a very positive point. Indeed, it is essential to share information between professionals from various sectors, in particular in anticipation of problems. A network-based collaborative approach is crucial when it comes to law enforcement. It will make it possible for us to have straightforward access to the right contact person, to pool our efforts and to share our field experiences.



## 2.b. The importance of “private-public” cooperation

The Observatory would be placed under the auspices of the public authorities.

The system for exchanges within the Observatory would be based on a multi-enterprise, private-public relationship.

This “private-public” cooperation would be organised using a balanced approach based on reciprocity of interest and joint efforts.

### Public-private operating methods

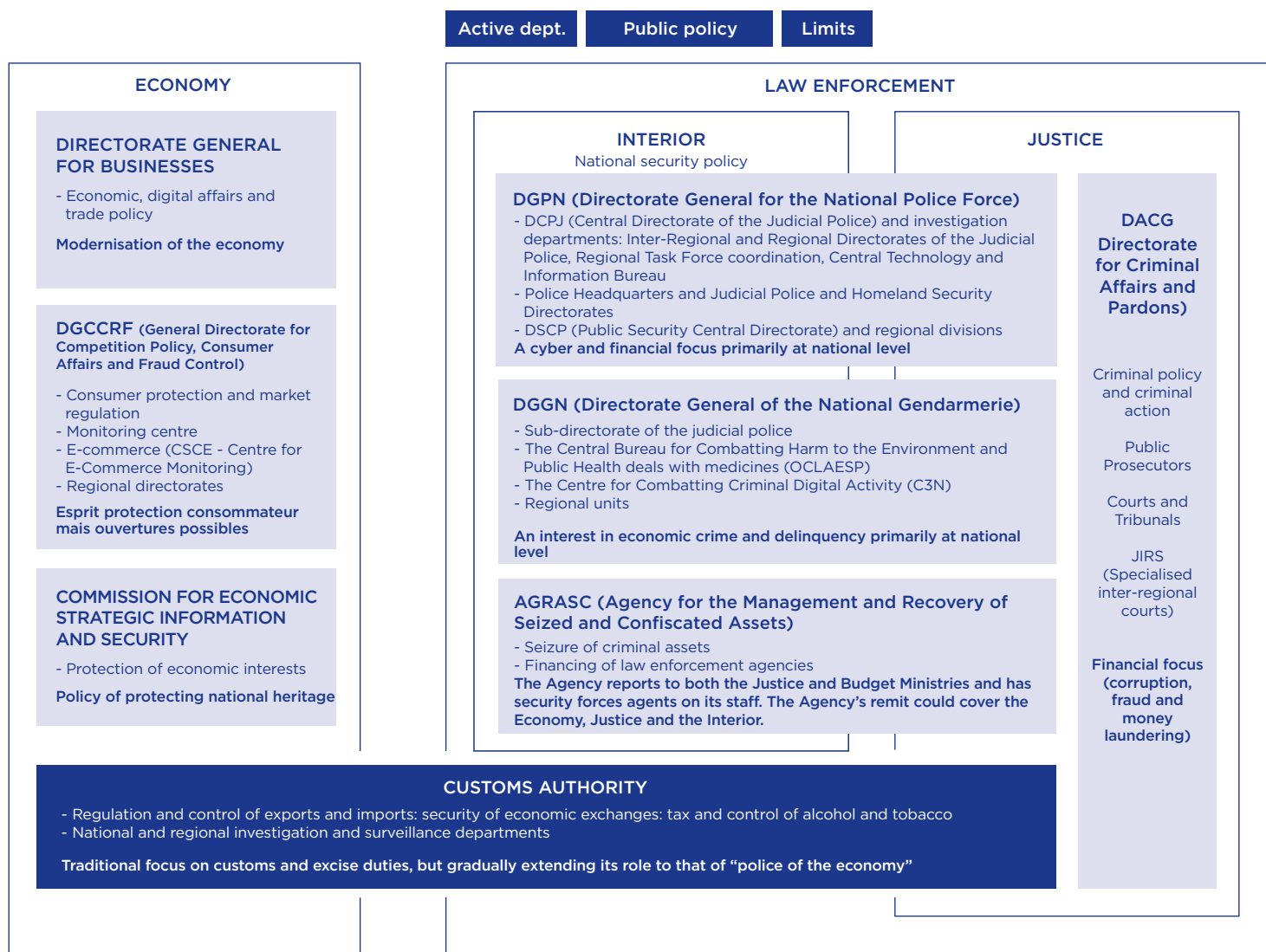
#### - The public sector:

A public authority that is in principle created on an ad hoc basis will supervise this “public-private” cooperation. Identifying illicit channels, thanks to information submitted by the private-sector stakeholders to the public-sector stakeholders, is one of the priority areas for the Observatory. Illicit websites and illicit accounts on social networks will be shut down under the aegis of this public authority, which will have **power to take action and will also be able to refer matters to the judicial authority**.

The terms of coordination between the public entities are still to be defined, with a view to join their efforts. The diagram below shows the obligations and limits of the public-sector stakeholders that could potentially be involved (“Economy”, “Interior” and “Justice”).

#### Focus on the public-sector stakeholders:

Source: Dominique Lapprand, ALCCI (Association for Combatting Illicit Trade)



## INTERVIEW

### Directorate General of the National Gendarmerie (DGGN)

Jean-Philippe Lecouffe, Major General, Deputy Director of the Judicial Police

#### *Could you describe your work?*

The aim of the gendarmerie is to dismantle networks and to seize criminal assets. We also participate in investigations and contribute to legal research and regulations for judicial police matters.

The gendarmerie handles 900 cases of illicit trade per year. The main difficulty is the choice of legal framework: as there is no criminal offence of illicit trade, the investigation needs to target a specific offence (such as theft, counterfeiting or smuggling). Two units are particularly committed to the fight against illicit trade: the C3N<sup>1</sup>, which focuses on digital crime, and the OCLAESP<sup>2</sup>.

#### *What is your perception of the problems of counterfeiting and illicit trafficking on the internet?*

This is a growing problem. The law enforcement agencies involved are aware of the reality and the seriousness of illicit trade. When they take this into account, their actions are still confined, as their capacities are limited and they must give their attention to other priorities (terrorism, unlawful immigration, financial crime and money laundering, in particular).

#### *To what extent does “public-private” cooperation appear to be relevant in your opinion?*

Despite the means for collecting and processing data at their disposal, law enforcement agencies need the information held by companies in order to be aware of the threat and act. The gendarmerie wishes to work with companies on the basis of the principle “heaven helps those who help themselves”. We expect companies to perform preparatory work prior to gendarmerie investigations by collating information that can answer at least two of the five questions: Who? What? How? When? Where? This public-private partnership can be useful for detecting illicit trade activities (targeting by the customs authorities when the risk analysis can incorporate information from companies) or for building investigation files (orientation of gendarmerie and police investigations)

#### *How do you view this Observatory?*

We are very interested in this project and are willing to support it. Having said that, in our opinion it is difficult to construct it around public officials, gendarmes, police officers and customs officers. On the contrary, we are waiting for companies that are victims of illicit trade to organise themselves and pool their efforts in order to detect and analyse the phenomenon, make connections and prepare, in liaison with us, the judicialization of their cases, then, during the criminal proceedings, with their counsels, to monitor the judicial outcome of the disputes.

In this respect, the work of ARGOS, which is an economic interest grouping set up by insurance companies, aiming at investigating on, identifying and recovering vehicles and other personal property reported as stolen, is a good example of cooperation between private-sector stakeholders and the gendarmerie, which we could use as inspiration for the illicit trade Observatory.

1 C3N: Centre for Combatting Criminal Digital Activity.

2 OCLAESP: Central Bureau for Combatting Harm to the Environment and Public Health.

## - The private sector:

The private sector functions on the **basis of voluntary actions by companies** that wish to participate in the Observatory, with the aim of collecting and sharing information. **The role of the private sector and, in particular the digital economy stakeholders, is to be at the forefront in terms of risk detection** and, at this level, it has a decisive role to play.

One person could be designated as the sole point of contact for each volunteer company. All the stakeholders in the value chain – transport companies, digital economy stakeholders, payment service providers or manufacturers – could be involved in order to identify illicit channels.

Moreover, many private sector stakeholders are adamant that **professional bodies**, which could contribute to the initiative, **should be involved**. This is the case in the pharmaceutical sector with the Ordre des Médecins (Physicians' Governing Body) or the French Chamber of Pharmacists.

**The role of the private sector is not to substitute government services, but instead, among other things, to provide suitable information to the law enforcement agencies concerned in a timely manner.**

## INTERVIEW

### ARJEL. French Online Gaming Regulatory Authority

#### Caroline Larlus, Head of the Department for Combatting Illegal Gaming, Legal Division

#### ***What is the specificity of your administrative authority?***

In order to combat illegal online gaming and advertisements for illegal online gaming (both of which are criminal offences), ARJEL investigators have the power to carry out online investigations under a pseudonym and to draw up official reports of offences.

On this basis, if requests to deny access to players residing in France that are made by the ARJEL to the publishers of illicit content and their website hosts are not heeded, the ARJEL President can ask the President of the Paris Court of First Instance, in an interlocutory ruling, to hand down injunctions to block access to the offending pages, which are implemented by the internet service providers.

Rather than being able to access the illegal content, internet users will instead be directed to a page published by the ARJEL, which details the reasons for the content being blocked and provides information on the types of online gaming that are authorised in France.

Indeed, we have found that it is necessary to make a major effort in terms of online education. These initiatives could serve as inspiration for your Observatory, the implementation of which we are monitoring with interest.

#### ***To what extent could the ARJEL be used as a model for other initiatives?***

In addition to exercising the specific powers of reporting offences and blocking content that the Law confers on the ARJEL, we are also looking to mobilise pragmatic, creative actions.

We are thus turning our attention to the service providers for illegal websites. These websites are often based abroad, outside of the European Union, whereas their service providers may have an establishment within the European Union.

The educational then more coercive actions that are taken with regard to online gaming publishers, which are major commercial partners of gaming operators, have convinced many of them to suspend access to their services from French territory. In addition to the fact that this puts an immediate end to the illegal behaviour, this type of “shut-down” has a negative impact on the illegal operators’ brand image with regard to players.

Moreover, the effects of the campaigns directed against payment service providers make the illicit activity appreciably slower and more complicated, then undermine the image of the gaming establishment, which can no longer accept payments and sometimes can no longer pay out winnings to its clients. This vector for action, which is largely based on the same rationale as anti-money laundering measures, in our opinion is probably one of the most effective ones. We are continuing to develop it, in particular with the ACPRI<sup>1</sup>, with which we are cooperating and whose action with regard to the establishments it regulates can be decisive.

1 ACPRI: Prudential Supervisory and Resolution Authority

## SECTION 4. RECOMMENDATIONS FOR EFFECTIVE ACTION

## 1. ONLINE REPORTING/ACTION

It is necessary to shorten and simplify the complaints procedures by introducing a **procedure that is simpler and faster**, in particular with regard to internet service providers.

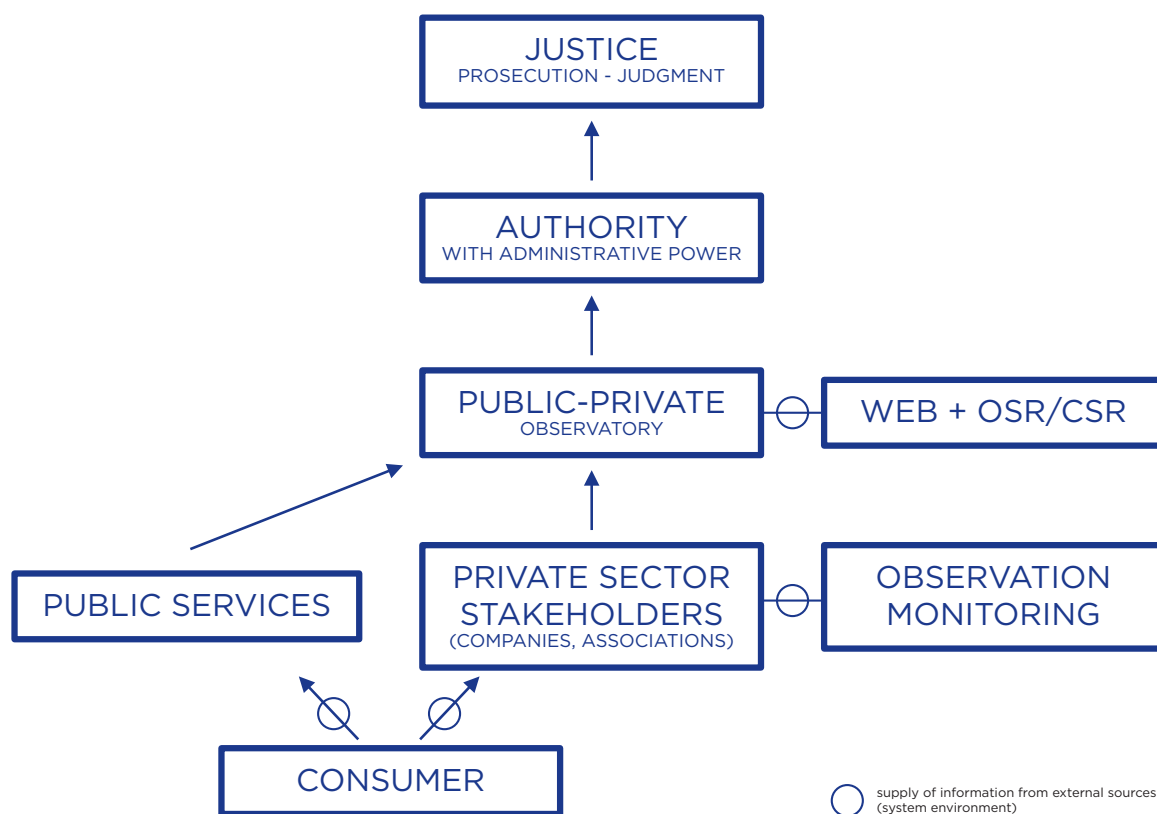
**A specialised, centralised reporting system will make it possible to process online reports of illicit trade through a single** (private sector or public sector) **point of contact** in the system.

These **reports will be passed on to the judicial authorities.**

The practical aspects of this system for processing reports are still to be defined.

The following diagram summarises the interactions between the various stakeholders involved.

The authority, which will be specialised in enforcement action against illicit trade of regulated products, will have the power to initiate criminal proceedings.



Reports can be filed by the private sector (consumers or companies) or by law enforcement agencies in the public sector (gendarmerie, police, customs or DGCCRF (General Directorate for Competition Policy, Consumer Affairs and Fraud Control) officers).

Reports by the public authority could have legal force after verification and formatting. Increased capacity to generate evidence is one aspect of the Observatory's added value and it is **therefore essential for the online reporting to be "trustworthy" and to have "legal force", with a single point of contact who will channel the information appropriately according to its nature.**



Direct contact with the stakeholders targeted by the Observatory for specific cases will also be possible. This strategy of reporting must also be used to **identify the risks upstream** in order to plan ahead for how to deal with them as early as possible.

A certain number of companies surveyed in fact emphasised the importance of the rapid notification of these new risks to a young population that is very much at ease with social networks.

## INTERVIEW

### OCLAESP<sup>1</sup> / National Gendarmerie

Eric Bayle, Head of the Strategy and Analysis Division

#### ***What is the current situation of the internet monitoring platforms in France?***

There is already a platform for declaring online illicit activity that is available to all internet users. This is the PHAROS platform (platform for the harmonisation, analysis, cross-checking and channelling of reports).

Moreover, the security forces each have a dedicated service for combatting cybercrime.

- Gendarmerie: C3N<sup>2</sup>.
- Customs: the Cyberdouane department of the DNRED<sup>3</sup>.
- Police: OCLCTIC.<sup>4</sup>

It would be appropriate to examine to what extent these platforms, each of which has its specificity, could complement your Observatory. Your monitoring system would be able to provide intelligence for law enforcement monitoring, taking into account the scope of authority of each entity:

- Dangers to public health - OCLAESP, police, gendarmerie.
- Counterfeiting and trademark infringements - Customs.

#### ***How do you view the integrated approach, which also aims to involve intermediaries in the management of the risks?***

Integrating the entire chain into the monitoring system would in practice make it possible to detect the weak points and to ensure better traceability. The pharmaceutical industry remains the benchmark in this field, as reflected in its “end-to-end” work.

#### ***Could the OCLAESP, for example, in principle, be part of this Observatory?***

Subject to approval by our management, we could indeed meet with the technical designers and the lawyers in order to define the expectations for such a system and how cases would be referred to law enforcement agencies.

1 OCLAESP: Central Bureau for Combatting Harm to the Environment and Public Health

2 C3N: Centre for Combatting Criminal Digital Activity

3 DNRED: National Directorate for Customs Intelligence and Investigations

4 OCLCTIC: Central Bureau for Combatting Crime linked to Information and Communication Technologies

## 2. LEGAL

### 2.a. Proposal for extended powers

In addition to the creation of this **Observatory**, there is in any event a need:

- **to incorporate the fight against illicit trade into the law enforcement authorities' performance indicators** in order to encourage them to act and to be involved in these cases;
- **to expand access to the existing databases** in order to improve information access and exchanges between the various stakeholders;
- **to extend the scope of undercover purchase operations**, which involve allowing the authorities to purchase or make products available to all the competent authorities, in order to be able to establish the existence of an offence and identify the perpetrators.
- **to expand the preliminary online complaint system to include purchases of products that come from illicit trade.** This preliminary online complaint service offered by the Interior Ministry<sup>59</sup> - which makes it possible for victims to make a declaration concerning offences against property (thefts, vandalism, scams, etc.), for which the identity of the perpetrator is not known – could be expanded to cases involving purchases of products that come from illicit trade. As the service is already operational, the administration could add an offence linked to illicit trade on the “facts” or “material loss” thumbnails. These reports could be redirected to the Observatory.
- **to increase the specialisation of the courts.**

There should be a specialised court: each specialised Court of First Instance should have a division that hears civil and criminal litigation involving online illicit trade.

- **to improve the training of magistrates.**

It is vital for magistrates and government law enforcement officers to specialise during their initial, ongoing and specific training, through awareness courses or dedicated modules.

- **to extend the techniques of “the procedure applicable to organised crime and racketeering”**

And in order to do so, to include counterfeiting in the main text of Article 706-73 or 706-74 of the French Criminal Procedure Code.

### 2.b. Proposal for formalising the legal framework for intermediaries

In addition to the proposal for judicial organisation, another initiative would make it possible to combat online illicit trade more effectively: **mobilise all the stakeholders involved in the value chain (internet service providers, sales platforms, social networks, banks, etc.)** so that they play a role in combatting online illicit trade.

In order to combat illicit trade more effectively, all the stakeholders (domain name registration offices, advertising agencies, market places, internet service providers, transport companies, payment service providers, etc.) must participate in this joint effort, by introducing **pro-active, appropriate and proportionate measures**. These stakeholders could only continue to benefit from liability exemption if they participate in this fight.

It should be stipulated that the **intermediaries commit themselves to use their best efforts, taking into account the general circumstances**. The administrative authorities could also play a role by ensuring these responsibilities are indeed fulfilled.

The judicial authorities, for their part, will be responsible for determining whether these reasonable measures were indeed adopted in a reasonable and sufficient manner by the intermediaries.

<sup>59</sup> <https://www.pre-plainte-en-ligne.gouv.fr/>

## 2.c. New legislation is necessary, as:

### - Soft law<sup>60</sup> has reached its limits

Soft law is a term used in English-speaking jurisdictions and refers to a set of non-binding rules that are applied on a voluntary basis.

In France, one example is the Charter for Combatting Counterfeiting on the Internet (the “Brochand-Sirinelli Charter”), that was signed in December 2009 between the rights holders and certain technical service providers that offer platforms for product sales.

In Portugal, the “Mapinet” (civic movement for combatting online piracy) **is worth mentioning**. This is an agreement between all stakeholders in the digital economy (rights holders, consumers, ISPs, etc.) to combat the online piracy of content (blocking of websites by the ISPs following notice, under the supervision of the General Inspectorate for the Creative Industries, the IGAC).

Soft law-type best practices are admittedly useful; however, the exponential, continual growth of the phenomenon of illicit trade in recent years has shown their limits. **While some stakeholders act responsibly, they are more the exception rather than the rule.**

### - Current legislation is obsolete

The private sector regularly observes that the regime of limited liability is no longer adapted to the reality of illicit trade as it exists today. Many intermediaries benefit from a privileged status, whereas the reality of their activity should render them ineligible for this. The difficulties, which result from the obsolescence of the liability regime for intermediary service providers, precisely illustrate the need to update the legal framework.

These limits can also be seen on a European scale:

**Directive 2000/31/EC** on e-commerce introduced special liability regimes for certain technical service providers (Articles 12 to 15):

- A service provider that acts as a **mere conduit** is **never liable** for the content transmitted, on the condition that the service provider ensured technological neutrality;
- A **hosting service provider is in principle not liable for the illicit content it stores at the request of a recipient of the service.**
- The **ISP is in principle not liable** for the illicit content to which it gives access, provided that it complies with the principles of technological neutrality.

To sum up, the favourable liability regime for the technical intermediary service providers is based on the **neutrality** and the **passivity** of these intermediaries. These **solutions** imposed by the European authorities **preclude domestic lawmakers from adopting legislative provisions that would be contrary to them.**

### - Case law is uncertain

Seeing as the current legal regime does not make it possible to respond to the reality of the activities performed by the intermediaries, it is up to the courts to judge each case individually in order to determine whether a stakeholder is liable. Yet, the outcome is extremely variable, and even uncertain, in particular when it comes to determining whether an intermediary market place will be classified as a “publisher” or “host”. All too often, the courts do not take into account all the intermediaries’ activities and, as a result, do not make it possible to attenuate the risks of distributing products that are derived from illicit trade.

**In short: a firm legislative response is required at this stage of tackling the problem. Re-balancing the burden of liability between the private sector and intermediaries in the fight against illicit trade, by introducing shared liability, is urgent.**

<sup>60</sup> <https://portail-ie.fr/resource/glossary/90/soft-law>

## CUSTOMS INTERVIEW

### Directorate General of Customs and Excise

Gil Lorenzo, Deputy Director of Legal Affairs and Anti-Fraud Measures

#### ***What action is being taken by the customs authorities against online illicit trade (counterfeiting, tax evasion and the parallel market)?***

In their fight against tax evasion and illicit goods that are ordered via the internet, the customs authorities take action at several levels:

- review of the customs declaration of the flows reported (subject to the threshold defined by the regulations above which there is an obligation to file a customs declaration), which primarily aims to combat tax evasion (under-declaring values), as well as prohibited goods (for which false declarations are submitted),
- physical inspection of the packages, in international airports and major postal sorting offices or sorting centres for express freight, with the aim of combatting prohibited goods, including counterfeits,
- searches for fraud on the internet (including on the darknet) and on the social networks.

#### ***Which factors make your actions increasing complex?***

Fraud is facilitated by the specificities of e-commerce: the anonymous nature of the transactions, sense of impunity, continual transformation of websites sites (name, URL, hosting country, etc.) and the extremely fragmented nature of shipments.

Moreover, consignments of negligible value (CNV) represent a major portion of the flows, namely more than 60% of express freight declarations in recent years, and are exempt from tax when their value is less than €22.

#### ***What are the characteristics of your Cyberdouane department?***

This department, which is part of the DNRED<sup>1</sup>, was set up in 2009 in order to facilitate the monitoring of goods that are sold on the internet. It is staffed by specialised analysts who track the sellers of counterfeits and smuggled products on the internet and all the social networks. The cyber customs officers have the means to subpoena internet operators in order to obtain all the information they hold on one of their clients, which makes it possible to start financial investigations or investigations with the aim of seizing goods that are prohibited on French territory. Moreover, under Article 67 bis-1 of the French Customs Code, which regulates undercover purchases, Cyberdouane can carry out investigations with added efficiency. In addition, this department was granted new legal powers by the Law of June 4th 2016, which makes it possible for cyber customs officers to search for and report offences using a pseudonym.

#### ***Are the customs authorities developing partnerships? How do you view the initiative of the UNIFAB-ALCCI Observatory?***

The customs authorities have in fact developed a strategy that aims to build partnerships with online sellers with the objective of cleaning up online trade and making users aware of the risks and consequences of these purchases/sales. Before contemplating the creation of an Observatory to combat the illicit trade of regulated products on the internet, in my opinion it is necessary to examine the scope of its remit with regard to the existing structures. The customs authorities will continue their action along these lines.

<sup>1</sup> DNRED: National Directorate for Customs Intelligence and Investigations



### 3. VECTORS WITH REGARD TO INTERMEDIARIES

#### Banks

- > In order to penalise traffickers financially, it is important to develop and structure the “single point of contact” tested by the gendarmerie. Each company that benefits from this individual “point of contact” would inform the banks quickly of frauds linked to illicit trade.
- > Monitoring and response times with regard to “risky banks”, especially European ones, should be improved. The banking establishments in certain countries, such as Cyprus, are clearly a problem in terms of ethics due to their choice of clientele.

#### INTERVIEW

##### Mastercard

**Ludovic Espitalier-Noël, Director of Public Affairs, France**

#### *What is your opinion regarding the launch of this Observatory?*

This is a highly relevant initiative. We have taken a certain number of initiatives ourselves and we currently have several partnerships with associations in order to identify and assist in combatting illegal sales of counterfeit products and services. Approaches such as these have made it possible for us to facilitate and strengthen our relationships with all the stakeholders concerned, regardless of their role and their place in the chain. This Observatory could also facilitate much closer cooperation with government agencies: for such a subject, we all need to work as partners. In general, our operating method is already well-established and is beneficial throughout the world. Moreover, this Observatory could also facilitate exchanges of best practices and be part of a more global initiative.

We should not forget, however, that we have no contractual relations with the rights owners who may be victims of counterfeiting, or with the cardholders (who are also victims of counterfeiting): our clients are still the banks.

#### *Which banking means of action can be used to curb this illicit trade?*

Due to the fact that our activities are those of a network (we do not issue any cards and we are not a banking institution or an account-holding institution), MasterCard cannot block a bank account that could be used for the sale of an illicit product. Having said that, we work with our clients – the banks – so that they implement suitable enforcement measures to prevent all illegal activity, which includes, among other things, sales linked to counterfeit products or services. French banks are very efficient in this area. We are convinced, on the other hand, that the actions of policy makers must not be limited to a given country: there are no borders for counterfeiting and counterfeiters regularly seek to identify the most vulnerable countries.

#### Digital economy stakeholders

**All of the professionals who are impacted by or unwittingly involved in illicit trade emphasise the major role of certain large corporations in the digital sector.**

The legislative tools previously described must make the retailers, in particular those that provide digital services, more accountable; however, **a strategy to attempt to influence them is complementary to this legal approach.**

It should be noted that while Price Minister was the digital economy stakeholder that was the most committed when it came to producing this White Paper, other digital economy stakeholders were informed of the project, but for the moment have shown themselves to be more reticent.

## Social networks

As already stated in this White Paper, **Facebook is particularly concerned** by the problem of illicit trade and its involvement is essential.

It is therefore vital for **Facebook France to comply with French law.**

If the online sale of a regulated product is prohibited, Facebook should take action and stop illegal advertisements from being displayed on its site.

Yet, sometimes this social network has shown itself to be reluctant to withdraw advertisements for counterfeit products, even after official requests had been made, as was the case in the UK, where National Trading Standards investigators recently criticised Facebook for this. This was reported as part of a major BBC undercover investigation into sales of counterfeit goods on Facebook Marketplace.<sup>61</sup>

**The rapid growth of Facebook Marketplace is also a major emerging risk** that public authorities should be concerned with. Traffickers who use Facebook as their main channel also use other social networks, such as Instagram or Pinterest, in order to promote their activities. These other social networks should also be taken into account.

Moreover, for some observers, Facebook also needs to be less demanding with regard to evidence to be provided by rights owners: a relationship of trust with regard to rights owners needs to be established.

## Search engines

We also need to **compel search engines, and in particular Google, to “delist” the numerous illicit websites that appear** on the first pages of the search results.

From a technical standpoint, it is complex for rights owners to combat this phenomenon for three reasons. The first is that the search engine has a commercial interest in selling traffic to a client, even an illicit one, who wishes to be listed. The second reason is that traffickers create specific powerful tools in order to generate website traffic. The third reason is due to the fact that these advertisements must also be delisted on the local versions of Google and that this process is costly and partially effective.

**Public pressure, combined with legislative measures, is therefore the best strategy for most of the observers who were surveyed.**

## Marketplaces

Marketplaces are still a problem, as some of them can distribute illicit regulated products.

**eBay** has clearly made progress in enforcement; however, more in-depth investigations could be made into the stores that are hosted and their suppliers.

**Amazon** bans traffickers when they are identified but could be more efficient in detecting them.

**Alibaba**, which is soon arriving in France, is somewhat controversial and presents a **genuine potential risk** when one realises the major importance of this platform in China for the distribution of illicit products, especially of French origin.

**For marketplaces, the situation is therefore variable depending on the website and it is important to have an appropriate strategy.**

As was seen in the legal section, **the question also arises on the status of these platforms, which should**

61 <http://www.bbc.com/news/uk-england-42267708>. Translator's note: the final sentence of this paragraph has been amended to reflect the contents of the article. The French original implied that the investigation was conducted by National Trading Standards.

**no longer be regarded as hosts, but have a greater role of surveillance and increased responsibility** with regard to the products distributed on their websites.

**The Observatory could monitor the risks linked to social networks, search engines and market places,** and even oblige these digital economy stakeholders to display banners or pop-up notices on illegal websites in France.

**As far as internet service providers are concerned,** it is necessary to implement faster, simpler procedures **in order to block access to certain websites.**

**The role of public prosecution is to stop the proliferation of illegal websites that are accessible to French consumers.**

## INTERVIEW

### Webdrone

#### Didier Douilly, Director of Business Development

***Your company specialises in monitoring and investigation on the internet; however, you seem to insist on lobbying as an enforcement method?***

Public affairs have a major role to play at this stage. Some American companies were able to make efforts in the past due to such an approach. This was the case for eBay, and for Google, which significantly reduced the presence of adwords for illicit counterfeiting websites. At present, the main vector for this plan should concern Facebook, which is a major network for illicit trade that has seen a higher increase in such traffic since its Marketplace opened in France a few months ago.

I am not sure that the authorities have fully understood the extent of the risk, or the economic impact of the illicit products that are available on this social network. The traditional means of response have been severely undermined due to the increasingly fragmented but nevertheless organised nature of the trafficking. For marketplaces, a potential risk concerns Alibaba, which is expected to set up shop in France in the near future, and we have in fact seen risks with AliExpress, which can already be accessed by French internet users.

***In your opinion, what are the main strengths of an Observatory in terms of combatting online illicit trade?***

I see two: the first is that of being able to anticipate new risks as early as possible and to ensure that they are shared between the various stakeholders concerned, as internet evolves very quickly and cybercriminals are in perpetual motion. Moreover, it is vital for the stakeholders to put a united front when lobbying. From this point of view, the pharmaceutical sector can serve as a reference.

## 4. INTERNATIONAL COOPERATION

### European Union

- > Even though the customs authorities are currently doing a remarkable job, they have **limited technical resources** (not many high-performance scanners or canine units). Numerous resources are available at the level of the European Union. For example, the **Hercule III Programme that was set up in May 2014 has a budget of hundreds of millions of euros**, among other things, for the purchase of scanners.
- > The aim is to find **vectors with regard to higher-risk countries** where online trafficking has an impact in France, and to ensure that cases with an international – or at least EU – dimension are comprehensively prepared, to avoid them being closed without charges being brought.

- > It is necessary to be able to **make a distinction between European Union websites that are lawful in their country but illicit in France, and foreign websites that are linked to criminal organisations.**
- > **Pooling police efforts at European level** could also be extremely relevant with regard to such an Observatory, in particular concerning Europol or Interpol. A step forward needs to be taken at this level.

## Improve investigations

- > As part of international cooperation, some express shipping companies have emphasised the need for **investigative capacity and foreign resources to be enhanced**, in particular in Asia and Africa. The Observatory must also be able to help with the development of informal networks on a European or even international scale.
- > Some **international companies** (such as Western Union, MasterCard and FedEx) are in principle willing to provide **support for international investigations** and already have some experience of sharing sensitive information between the private and public sectors.

### INTERVIEW

#### Fedex

#### Philippe Priolon, Security Expert

##### *How do you perceive the issue of enforcement?*

Illicit trade has become more sophisticated and increasingly uses highly fragmented traffic that is difficult for carriers to identify. It is vital to involve all the stakeholders in an enforcement-oriented approach. The express shipping sector already shares information between a few companies such as DHL, Chronopost and UPS; however, this approach needs to be expanded further. The initiative of this Observatory is therefore a move in the right direction. This would make it possible for us, for example, to build operational relationships with major stakeholders such as Amazon or eBay and to structure enforcement that is more adapted and faster.

##### *In your opinion, what are the areas where there is room for improvement in order for illicit trade to be tackled more effectively?*

Better information needs to be provided to the sector professionals, as sometimes not even police officers or gendarmes are aware of the stakes. Police forces should also be mobilised on a European scale, by enhancing relations with the departments concerned. The “human intelligence” factor should not be neglected, in particular internationally, even though at first sight the problem is fairly technical in nature.

## In order for the initiative to be strategic

- > **An initiative based on sectoral coalition is essential.**
- > **International shipping fraud** is a key area of the liability chain that is under-estimated and that should be integrated to a greater extent. **Profiling** in order to retrace shipments back to the countries from which they are dispatched is an area that warrants closer attention.
- > An international strategy should be implemented by targeting the most relevant illicit retailers and those that are responsible for most of the traffic. The aim is to be able to **identify the weak point of certain retailers** (cf. the ARJEL’s strategy).

Through such international initiatives, **France would position as a front runner in this area and would be a benchmark for the fight against illicit trade worldwide.**

## INTERVIEW

**Myriam Quémener**

**Advocate General at the Paris Court of Appeal, Doctor of Law and an Expert in digital law.**

***Do you think that there are international intermediaries that this Observatory would be able to leverage?***

Liaison magistrates and security attachés who are assigned to national security, and who are present in numerous countries, could be interesting intermediaries between the Observatory and the target companies. It could be useful to make contacts with the European Commission and the Council of Europe subsequently, as private-public cooperation also needs to be reinforced in this area.

***What legislative arsenal could be used for this project?***

Before making new legislative proposals, it would be appropriate to take stock of what already exists; the use of criminal investigations needs to be promoted by presenting the advantages (use of Europol, Interpol and Eurojust). Moreover, the procedure for using joint investigation teams could be simplified (authorisation by the Public Prosecutor and not systematically by the Directorate for Criminal Affairs and Pardons (DACG)).

***What is your comment on this initiative?***

The Observatory is fully consistent with the strategy of reinforcing public-private cooperation, which is vital in the fight against illicit trade. It could also be identified as an essential point of contact with regard to the social networks, the reporting obligation of which for illicit content could be accentuated.

## 5. EDUCATION / AWARENESS

### a. Specific actions to raise consumer awareness

#### - Customs/Post Office:

> When a product is inspected and then seized because it is found to be a counterfeit or an illegal import, the principle could be to send an information letter to the consumer to replace the illicit product. This is a cost-effective procedure that could have a clear educational or even dissuasive effect.

#### - On the internet:

On the basis of the US model: implementation of an alert system with a dedicated banner (or pop-up notice) stating that an illicit website was shut down and the reasons why.

> Possibility of integrating clickbait advertisements.

> Inform previous consumers of the illicit nature of their purchase.

### b. Actions to inform the public

#### - Consumers

Being pro-active in terms of communication requires a structured process.

> Action must be taken to inform the public, **to ensure external communication to the general public.** Consumers are not always aware of the illicit nature of purchasing certain regulated products online.



- > **Obtaining the official support of the gendarmerie/police** would have an impact on this communication.
- > Widespread communication should also be undertaken with regard to all companies and other chain stakeholders.
- > Companies and professionals are not always well-informed of the key issues surrounding illicit trade (within companies themselves, for intermediaries and also for healthcare professionals, magistrates, gendarmes, police officers, etc.).
- > Insist on actions to raise awareness so that these professionals adopt a **pro-active approach**.

### c. Intra-company education and information - KYC (Know your Customer)

- > **Improved knowledge on the part of suppliers and customers is necessary** in order to **make a system of “due intelligence”** more adapted to the illicit trade that targets them.

## INTERVIEW

Sanofi

**Geoffroy Bessaud, Associate Vice President, Anti-Counterfeiting Coordination**

### ***What do you think of this UNIFAB-ALCCI initiative for combatting online illicit trade?***

This is an excellent initiative in which we wish to participate. Sanofi has extensive experience in the fight against illicit trade and in particular the fight against counterfeit medicines. This initiative is all the more relevant as the counterfeiting of healthcare products is one of the main issues facing the public health sector in the 21st century and as the internet is a key distribution vector for fake, counterfeit or poor-quality products, in addition to their physical distribution in the field. Other laboratories could be associated with this Observatory. However, it is essential for such a project to have a strong operational dimension and it should probably be limited to a few targeted actions so that it can be launched and obtain concrete results, before its scope is extended.

### ***What risks do you think will emerge?***

In France, our physical distribution network is extremely solid and controlled. Along with dispensaries, which constitute a genuine bastion against fake medicines, and our reimbursement scheme, this ensures that patients receive safe products.

The danger comes from growing illicit trade on the internet. Young generations in particular are an at-risk sector of the population that is very much at ease with e-commerce and above all social networks. However, all sectors of the population are concerned, and the risk should be considered on a global scale.

### ***How do you think that illicit trade could be tackled more effectively?***

In my view, considerable emphasis needs to be placed on external communication and education. Healthcare professionals are paradoxically insufficiently informed of these issues. It would be extremely beneficial to use this Observatory for communication campaigns aimed at pharmacists and doctors. From an operational perspective, it is essential to be able to put a definitive stop to the current ease with which French consumers can access illicit websites. Moreover, the public authorities have an essential role to play, by adding their institutional legitimacy to this project.

## Conclusion

The fight against online illicit trade is a major challenge that requires a paradigm shift. It has become clear that, despite numerous initiatives, this fight against online illicit trade is still too fragmented and lacks strategic vision. Setting up a UNIFAB-ALCCI Observatory, which combines high-level monitoring, a pro-active approach to prevention and a coordinated approach to enforcement between the private and public sectors, is therefore a salutary and singular initiative. It would have the advantage of protecting industries and consumers from the complex challenges raised by internet.

It is important to note that this Observatory is completely consistent with the recent recommendations of the European Commission, which promote the idea:

- of fluid cooperation between all concerned stakeholders,
- of effective implementation of mechanisms for electronic notification,
- of an approach that emphasises prevention as much as enforcement, with increased responsibility of the digital economy stakeholders concerned.

Setting up this Observatory would thus demonstrate the capacity of the French State to provide leadership on a European scale for a novel, innovative initiative that is at the crossroads of industry, the digital economy and human security.

### **The European Commission's recommendations for combatting illegal online content<sup>1</sup>**

Early in March, the European Commission issued a series of recommendations for combatting illegal online content. These recommendations follow its communication of September 28th 2017<sup>2</sup> on the liability of platforms in the fight against illegal content. With this in mind, the Commission underlines the increased societal responsibility of internet service providers. The Commission reminded the major internet players of the desire to see illegal content (terrorist content, racist and xenophobic statements, content linked to child pornography, copyright violations and dangerous products) taken down within twenty-four hours of being reported. According to the Commission, fluid, effective, appropriate cooperation should be ensured between the relevant authorities and the hosting service providers in the fight against illegal online content. The implementation of electronic notification mechanisms that are easy to access and easy to use is also recommended.

Brussels now recommends that major internet corporations adopt a more “proactive” approach by making the automatic detection of illegal content systematic and by sharing this type of costly technology with small sites that have fewer resources, but to which the illegal content removed from Facebook or Twitter<sup>3</sup> often migrates. “We have seen that more than 90% of the illegal content taken down had already been reported and removed once. We really want to tackle this problem of content that reappears on smaller platforms”, emphasised the Bulgarian Mariya Gabriel, the European Commissioner for the Digital Economy and Society.

Brussels always prefers consultation but has implied that it could enact binding legislation if internet stakeholders do not face the problem head-on. “For the moment we are making these recommendations on a non-binding basis. However, we are not closing the door to other actions, including legislative actions”, warned Ms Gabriel.

<sup>1</sup> European Commission, Commission Recommendation on measures to effectively tackle illegal content online, March 1st 2018.

<sup>2</sup> COM(2017) 555 final of September 28th 2017.

<sup>3</sup> Cécile Ducourtieux, Bruxelles presse les géants du Web de mieux lutter contre les contenus illicites, Le Monde, March 2nd 2018.

The Observatory thanks all the representatives of the various manufacturing sectors (medicines, wines and spirits and tobacco products, digital sector stakeholders, service providers, logisticians, companies from the payment services sector and experts) and of the institutions (customs, gendarmerie, magistrates and associations) who participated in the writing of this White Paper.



Author of the Unifab-Alcci White Paper:

Eric Przyswa, [eric.przyswa@risk-05.com](mailto:eric.przyswa@risk-05.com), [www.risk-05.com](http://www.risk-05.com)

The logo for 'riskO5' is displayed on a yellow rectangular background. The word 'risk' is in a black sans-serif font, and 'O5' is in a bold, black sans-serif font.

With the participation of public institutions, intermediaries, (online sales platforms, payment service providers, etc.), members of UNIFAB and ALCCI.

With the support of Philip Morris France SAS