COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 8 June 2016
cdpc/docs 2016/cdpc (2016) 9

CDPC (2016) 9

EUROPEAN COMMITTEE ON CRIME PROBLEMS

(CDPC)

Concept note

MEDICRIME AND CYBERCRIME AS COE INSTRUMENTS:

WHAT ARE THEIR LINKAGES?

Document prepared by the CDPC Secretariat
Directorate General I – Human Rights and Rule of Law

CDPC website: www.coe.int/cdpc
CDPC e-mail: dgi-cdpc@coe.int

1. Introduction

The online selling of falsified medical products is a threat already identified by the Council of Europe in some of its legal instruments.

As early as 2001, the Committee of Ministers pointed out "the problems posed by distance sales of medicinal products and the development of this practice through the Internet", and that guarantees [regarding the quality, safety and efficacy of medicines on the market] "are jeopardised by certain practices related to the Internet, as well as by illicit importation and illegal distance sales"[1].

Furthermore, the Recommendation Rec(2004)17 of the Committee of Ministers[2] recognised that "the Internet has created a global health information community which transcends national borders and raises issues for states that go beyond their jurisdiction for Internet matters, making them profoundly difficult to regulate".

Moreover, the Committee of Ministers expressed its will to take into account that "mail-order trade in medicines is by and large marketed via the Internet, which is uncontrollable and used as a platform for many illegal offers of medicines, be they for prescription-only medicines or medicines available without prescription, stem from doubtful sources of supply, and be of substandard or uncontrollable quality […]"[3].

Following the Council of Europe Internet Governance strategy (2016-2019), "[t]he online safety and security of Internet users is a shared responsibility. This requires action to combat […] the sale of counterfeit medicines and drugs". Among other key priorities, the CoE decided to consider "ways to prevent the illegal sale of drugs and counterfeit medicines as well as illicit trafficking in drugs online, including the promotion of the MEDICRIME Convention"[4].

Activities foreseen under the Strategy include, inter alia, the drafting of a report on the links between the MEDICRIME Convention[5] and Cybercrime Convention[6].

2. The need of a report: objective and scope

The complementary action of the MEDICRIME and Cybercrime Conventions has long been recognised, even already at the drafting stage of the MEDICRIME Convention[7]. Interestingly, the Budapest Convention is also specifically mentioned in the Preamble of the MEDICRIME Convention.

A report is aimed at identifying the possible links and gaps, from a criminal law perspective, between MEDICRIME Convention and the Convention on Cybercrime.

The objective of this concept paper is to provide basic elements of understanding of the issues at stake, as well as to initiate a discussion on possible actions to be taken. It should not be understood as an in-depth and final analysis of the policy and legal aspects involved.

Under the MEDICRIME Convention, the following types of offences are covered:

---

[1] Resolution ResAP(2001)2 of the Committee of Ministers to member States concerning the pharmacist's role in the framework of health security, (§9).
[2] Recommendation to member States on the impact of information technologies on health care – the patient and Internet
[3] Resolution ResAP(2007)2 of the Committee of Ministers to member States on good practices for distributing medicines via mail order which protect patient safety and the quality of the delivered medicine.

[4] Internet Governance – Council of Europe Strategy (2016-2019), §10.e
[5] Council of Europe Treaty Series No.211, Council of Europe Convention on the counterfeiting of medical products and similar crimes involving threats to public health (MEDICRIME Convention), 28/10/2011.
[6] Council of Europe Treaty Series No. 185, Convention on Cybercrime, 23/11/2001.
[7] See for example the Workshop "Medicines on the web – risks and benefits" (UN Internet Governance Forum, Sharm El Sheik, 15-18 November 2009) co-chaired by the EDQM and the CoE's criminal law division, which stressed that the Medicrime Convention could be used "in conjunction with the Council of Europe's Cybercrime Convention to ameliorate some of the worst risks to the patient and to tackle crimes emerging from the abuse of the Internet" §32).
(See : https://www.edqm.eu/medias/fichiers/Workshop_report_Medicines_on_the_webrisks_and_bene.pdf)

- Manufacturing of counterfeits;
- Supplying, offering to supply, and trafficking in counterfeits;
- Falsification of documents;
- Similar crimes involving threats to public health.

Under the Convention on Cybercrime, the following types of offences are covered:

- Offences against the confidentiality, integrity and availability of computer data and systems;
- Computer-related offences;
- Content-related offences;
- Offences related to infringements of copyright and related rights.

Given the scope of the paper, some legal crossroads between the fight against falsification of medical products and Cybercrime are not examined. It is the case, among other issues, of the protection of medical data in the digital era. Such issues may be dealt with under other headings of the Internet Governance strategy[8].

Structure of the analysis

With a view to examining potential interactions between both the MEDICRIME and Cybercrime Conventions, a focus is given to the following issues:

a) **Internet as a platform for the advertising of counterfeited medical products**
b) **Internet as a market-place for the selling of counterfeited medical products and similar offences**
c) **Fake e-pharmacies as 'baits' to commit cybercrime offences**

These issues are examined below, from both a criminological and a criminal law viewpoint.

3. Internet as a platform for the advertising of counterfeited medical products

As the Explanatory Report to the Medicrime Convention stressed,

> "*Using the internet to advertise and supply their inherently dangerous products directly to patients and consumers around the world has proven to be a safe and easy modus operandi for the criminals involved and has given them a global reach*." (§6)

The Internet can be used in different ways to advertise counterfeited medical products and devices[9]:

- E-pharmacies (be they 'genuine' or fake)
- Marketplaces (e.g. Alibaba)
- DarkNets on the Deep Web
- Social networks (Facebook, Twitter, Instagram,…)
- Forums
- E-mailing, spamming and web manipulation

Among these different platforms of advertisements, "spamming" (the sending of unsolicited e-mail, for commercial or other purposes, to a large number of recipients) plays a crucial role. It provides an easy, cheap, and anonymous channel for the trafficking of counterfeit medical products and devices[10]. Web manipulation deserves also a particular attention.

[8] See especially, under the heading "Respecting and protecting the human rights of everyone in the digital world": Mobile health (mHealth) and electronic health (eHealth), including access to (quality) health and health care products, as well as the prevention of the illegal sale of drugs and counterfeit medicines").
[9] See the report FAKECARE.com, *Search and stop - Guidelines to tackle the online trade of falsified medical products*,
[10] See UNICRI, *Counterfeit Medicines and Organised Crime*, 2012, pp. 67-83.

Market places on DarkNets on the Deep Web" are also increasingly used as platforms of advertisement. Before it was shut down in November 2014, the most commonly advertised drug on Silk Road 2.0, formerly the largest Darknet market place, was prescription medicines[11].

An in-depth analysis of criminal offences covered by both conventions is needed[12].

4. Internet as a market-place for the selling of counterfeited medical products and similar offences

Whilst Internet has long acted as a market-place for the selling of counterfeited medical products and similar offences, the market continues to grow. In Europe, the online market in falsified medical products is even skyrocketing: in 2013, some studies reported that the trade has increased 90% since 2005, with an estimated turnover of $200 billon[13].

This trend raises many concerns, especially regarding the increasing presence of vital medical products and medical devices. "In a shocking development, it was discovered relatively recently that counterfeit versions of lifesaving prescription medicines for cancer and serious cardiovascular diseases are also being sold to consumers online," the European Alliance for Access to Safe Medicines reports[14].

Certain factors may lead to an expansion of this market:

- Low reimbursement rate of medical products and medical devices under the social security mechanisms of many States;
- Stricter regulation of the access to certain medicines in physical and online legal pharmacies;
- Persisting high gain/low risk ratio of the activity (compared, among others, to the selling of illegal drugs);
- New technologies (especially 3D printers, which may lead to a rapid surge of fake counterfeited medical devices).

The Darknet obviously facilitates the expansion of the selling of counterfeits, by providing anonymity to criminals – both in terms of online access, through anonymizing software such as P2P or Tor, and in terms of online payment, through crypto-currencies such as Bitcoin.

An in-depth analysis of criminal offences covered by both conventions is needed[15].

5. Fake e-Pharmacies as 'baits' to commit cybercrime offences

According to the figures of the USA accreditation centre 'LegitScript', the number of legal, licenced e-pharmacies online amounts to 0,7% of the web offer, in terms of number of sites[16]. The rest of the offer, according to many different independent studies is almost equally divided between fake and rogue websites.

Fake e-Pharmacies should be distinguished from rogue e-Pharmacies. Whereas rogue e-Pharmacies are websites that genuinely – but unlawfully – market medical products and devices, fake e-Pharmacies only *pretend* to provide such service in order to attract victims[17].

---

[11] Among the prescription medicines, the most commonly advertised therapeutic category was "Relaxants", where the main medicine type advertised was benzodiazepine. See INTERPOL, *Pharmaceutical Crime on the Darknet - A study of illicit online marketplaces*, 2015, p.9.

[12] Articles 5, 6, 7, 8 and 13 from the MEDICRIME Convention as well as Articles 2,3,4,5,7 under the Cybercrime Convention.

[13] Source: IRACM - Institut de Recherche Anti Contrefaçon de Médicaments.

[14] See WORLD HEALTH ORGANIZATION, *Growing threat from counterfeit medicines (Bulletin);* available at: http://www.who.int/bulletin/volumes/88/4/10-020410/en/

[15] Articles 5, 6, 7, 8 and 13 from the MEDICRIME Convention as well as Article 7 under the Cybercrime Convention.

[16] See https://www.legitscript.com/

[17] See UNICRI, *Counterfeit Medicines*…, op.cit.

The main goal of the creators of fake e-Pharmacies is to attract victims on the website, where they will:

- voluntarily provide personal data (ID or credit card details);
- click on links or download files, hence infecting their computer with viruses and similar devices (e.g. Trojan files) (again, with the purpose of obtaining ID or credit card details).

These websites are sometimes promoted through spam campaigns using keywords related to recent health crisis[18].

It should be taken into consideration that the setting-up of a fake e-Pharmacy may involve the commission of certain criminal offences set out in article 6 of the MEDICRIME Convention, inasmuch as the act amounts to offering to supply counterfeits. Other criminal offences might not be relevant.

The setting-up and functioning of fake e-Pharmacies appear to involve several offences set out by the Budapest Convention. Other cybercrime offences may also be committed in the preparation of, or as result of, the operation of a fake e-Pharmacy. A particular attention is deserved to offences against the confidentiality, integrity and availability of computer data and systems as well as to computer-related offences.

6. Conclusion

It is a fact that Internet is used as a platform for the advertising of counterfeit (falsified) medical products. Both CoE instruments cover, in various aspects, the advertising of counterfeited medical products. Further study should be undertaken to examine to which extent spamming should be criminalised as such by both instruments.

Moreover, Internet is a market-place for the selling of counterfeited medical products and similar crimes, which is an issue mainly dealt with by the MEDICRIME Convention. An important element to analyse is whether the *online* distribution of falsified documents is, or should be, directly incriminated

Fake e-Pharmacies as 'baits' to commit cybercrime offences is the other element to be analysed, in particular whether the setting-up of a fake e-Pharmacy is directly addressed by both legal instruments (or not).

[18] See the studies carried out by the Italian Pharmaceutical Agency (AIFA) and the Italian Ministry of Economic Development: D. DI GIORGIO, *Farmaci contraffatti: il fenomeno e le attività di contrasto*, 2010, AIFA-Tecniche Nuove, AIFA/EDQM ed. ; DI GIORGIO D. (ed.), *Counterfeit medicines* , 2011, AIFA/EDQM.

Criminal Law Division
Action against Crime Department
Council of Europe