

French LOPPSI 2 Law: The huge mess - Focus on some means to fight against cybercrime (cyber or not)

The so-called LOPPSI 2 law (law on guidelines and programming for the performance of internal security) sets the guidelines to safety for five years (2009-2013) and defines the priority operational objectives concerning terrorist threats, organisations and actions that harm national cohesion, organised crime, domestic violence, reckless driving, public health or environmental crisis and fight against cybercrime. This law, which had been under review for more than a year, was adopted by the Parliament on February 8, 2011.

We have chosen to look specifically at three initiatives intended to fight against cybercrime.

1. Creation of an online identity fraud offence

Article 2 of the LOPPSI 2 law creates a new article 226-4-1 in the Criminal Code providing that *“the use of someone else’s identity or of one or more personally identifiable data of a person with the purpose of disturbing this person or others’ peace or damaging their honour, respectability or interests, shall be punished by two years imprisonment and a fine of 20 000 Euros. This offence is punishable by the same penalties when it is committed on an online publicly available communication network”*.

The creation of an online identity fraud offence has been discussed for a long time. It was announced, on March 20, 2008 during the Cybercrime International

Forum, by Michele Alliot-Marie¹, when she was Home Secretary.

Patrice Calmejane, Member of Parliament, has expounded in front of the French National Assembly on February 11, 2010, during the LOPPSI 2 law parliamentary debates, that *“each year in France, more than 210 000 persons, i.e. 4,2% of the French adult population over the past ten years, were confronted with this crime”, which “is a more important phenomenon than home burglary – 150 000 - and car theft – 130 000”, and that shows “an increase by 40% each year”*².

Until then, a complaint for identity fraud could only be filed if the use of someone’s identity was likely to trigger criminal proceedings against the person whose identity had been used: Article 434-23 of Criminal Code provides that *“Assuming the name of another person in circumstances that lead or could have led to the initiation of a criminal prosecution against such a person is punished by five years’ imprisonment and a fine of €75,000.”* But, this provision does not allow punishing the many identity frauds that can be perpetrated through new technologies

The new Article 226-4-1 of the Criminal Code is therefore intended to punish every attack that can harm someone’s identity and should also enable to protect legal entities. Indeed, during the parliamentary debates, the reporting MP, Eric Ciotti, has declared that Article 2 of the law *“shall*

¹

http://www.interieur.gouv.fr/sections/le_ministre/interventions/archives-mam/forum-cybercriminalite

²

http://www.nosdeputes.fr/seance/3310#inter_dadf627de99edc709a689c0a3e035812

apply to both individuals and legal entities”³.

The element of intent of the offence is constituted by the intention to use someone’s logins and data for the purpose of causing harm to such person or any other person’s interests, peace, honour and reputation.

The wording of the provisions establishing this offence is broad enough to punish several behaviours: use of someone else’s banking data (credit card or bank account) to perform transactions without his/her knowledge, use of someone else’s login data to access information or perform transactions in his/her name, or to use an Internet user’s alias in such a way that it may harm his/her reputation, to use someone else’s name to defame and insult another person. During the second debate at the French National Assembly in December 2010, the scope of the identity fraud offence has been extended to “the facts causing harm to the interest of the victim” in order to include phishing.

The definition of identity or personally identifiable data is broad: IP address, alias, email address, social network account such as Facebook. Furthermore, all the elements used to make the stolen profile look more realistic are prohibited, such as photos and videos.

In the absence of clarification from the Parliament, , the scope of the definition and the solution to the many legal issues that will undoubtedly arise will be left to the Courts.

For instance, would the use of a person’s name and surname to create an account on a website be considered an identity fraud? Likewise, if someone uses a company

name such as “walmart.company” or “the.times” could it be judged unlawful?

Judges will have to decide whether or not, for legal entities in particular, this offence could be combined with trademark infringement.

In any case, we strongly advise you do not make such a joke to an acquaintance by creating for instance a fake Facebook profile with your friend’s name. You might have to pay a huge sum of money for doing so, up to 20 000 Euros to be precise!

2. Spyware : the collecting of remote data

Article 23 of the LOPPSI 2 law provides that “*when required by the investigation on any crime pursuant to Article 706-73, the investigating judge may, after hearing the Prosecutor’s opinion, allow by Court Order the police through a letter rogatory to settle, without the consent of the individual concerned, a technical device to access remotely to computer data, record, retain and transmit them, in the form displayed on the computer screen of the automated data processing system’s user or in the form programmed by such user . These operations are performed under the authority and the control of an investigating judge*” (future Article 706-102-1 of the Code of Criminal Procedure).

Article 706-73 of the Code of Criminal Procedure only deals with serious crimes and offences (such as murder committed by an organised group, drug trade, abduction, pimping, terrorism, currency counterfeiting, money laundering linked to the abovementioned offence). Criminal police is allowed to use spyware programs, such as keyloggers or screenshot programs, to determine and/or prevent crimes.

³ <http://www.assemblee-nationale.fr/13/cr/2009-2010/20100129.asp>

These devices could be installed for a period up to 8 months in a computer but also in a mobile phone or a table pad since the monitoring can concern computer data “*in the form as they are displayed on a computer screen*”. All the registered offences could be used by the police even if they have no link with the crime that triggered the monitoring since “the fact that these operations reveal offences different from those mentioned in these decisions does not constitute a ground for declaring accessory proceedings invalid. (Future Article 706-102-4 of the Code of Criminal Procedure)

Thus, contrary to what has been written in the newspapers, the use of this telephone tapping process is strictly framed and limited. And Big Brother is not going to spy systematically on your computer. This surveillance can be only prescribed in certain clearly defined cases connected to organised crime and companies should not be concerned by this provision.

However, publishers of security solutions are going to be confronted with several difficulties with this new legal tool. One can wonder if at first they will have to let an open door to investigating spyware programmes in the security software programmes they create.

In this case, a publisher who distributes a software programme on a worldwide scale will have to modify it especially for the French market, to incorporate features in order not to detect those investigating spyware programmes. How will it be possible to impose such obligations to software publishers, located outside of France and offering only online services?

Furthermore, during an audit, IT service providers will be able to find on the company’s server some investigating spyware programmes. However, since the

LOPPSI 2 law does not provide on this particular point and in the absence of legislative or regulatory provisions, IT service providers will be in a delicate position. He will have to choose between hiding the fact that an investigating spyware programme is installed, thus breaching the confidence of the cocontracting company or disclosing the presence of such programmes, thus risking to endanger the police investigation.

The implementation of such provisions might create some difficulties.

3. Blocking child pornographic websites.

Article 4 of the LOPPSI 2 law provides that “*when justified by the need to fight against the circulation of images or representations of minors pursuant to Article 227-23 of the Criminal code, the administrative body notifies the URL addresses of online publicly available communication services that violate the provisions of said Article to the Internet Service Providers, who must prevent access to such online publicly available communication services immediately*”.

The OCLCTIC (the Central Office for the fight against ICT-related crimes), an administrative authority under the supervision of the Home Office, will be in charged of performing the screening process of child pornographic websites. This Office may request from Internet Services Providers the blocking of child pornographic websites, by means of a Home Office decision, without recourse to prior judicial authorisation.

Despite several amendments imposing prior judicial control to every blocking measure, this provision stipulates that such

ensorship will not be subject to a judicial inquiry prior to the blocking process.

In its report dated September 28, 2010, the reporting MP of the law-making committee of the French National Assembly, Eric Ciotti, explains that Article 4 of LOPPSI law 2 sets out “*a system of administrative police*” and that “*having the blocking measure ordered by a judge is totally against the philosophy and efficiency of this system*”⁴. He justifies his view by the decision of the Constitutional Council on the Hadopi law, which made internet access a component of the principle of freedom of expression.

In his opinion, “*on a legal point of view, the recourse to Courts is not necessary since the situation is not the same as the one already judged by the Constitutional Council, in which the access to Internet was at issue*” especially since “*the decision that the administrative body will have to make on the reality of the child pornographic character will be controlled by the administrative judge, having jurisdiction to know of each appeal lodged against Home Office decisions*”.

But there are voices challenging all kind of abuses of the blocking system of websites. The action to combat child pornography justifies taking urgent measures, but as stressed by Christiane Féral-Schul, successor of the President of Paris Bar “*it can be feared that such automatic sanction spreads to other crimes, and steadily steps out from the control of an independent judge*”⁵.

⁴ http://www.assemblee-nationale.fr/13/pdf/amendements_commissions/cloi/2780-01.pdf

⁵ http://www.lepoint.fr/chroniqueurs-du-point/laurence-neuer/loppsi-2-les-points-qui-fachent-28-09-2010-1242300_56.php

Furthermore, such provisions do not take into account the failure experienced by our German neighbour. In June 2009, the German Parliament had enacted a law on Internet censorship for the purpose of fighting against child pornography websites with similar provisions as those set out in LOPPSI law 2. However, nine months after, the German government decided to move away from this system because of the risk of violation of public freedoms and because its implementation raised practical challenges.

In an email sent to its members, the Service Providers Association (AFA) explains the reason why this provision has been deleted: “*following German surveys, out of 8000 URLs contained in the police blacklists, only 110 websites were displaying some sexual abuse and sexually explicit pictures of children under 18 years of age, and following the notification to the hosting provider, only 7% of such illegal contents hosted in non-INHOPE country members (International Association of Internet Hotlines), were still online 14 days after the notification (while most questioned contents were deleted within 48 hours following the notification)*”⁶.

For instance, the police files had identified 8000 domain names that could have been blocked pursuant to the internet censorship law, only 110 addresses actually were child pornographic websites, i.e. a ratio of 1.37%.

This shows the risks of inefficiency and the reported abuses of the blocking system by several persons among which the Committee of National Defence and Armed Forces who in a parliamentary report signed by Marc Joulaud has expressed that “*if the blocking system*

⁶ <http://www.pcinpact.com/actu/news/53750-loppsi-afa-fai-allema-gne-blocage.htm>

appears to be appropriate, the related impact study does neither prove its efficiency nor evaluate precisely its global cost, both in terms of compensation for Internet Service Providers and means for States agencies”⁷.

On the basis of the abovementioned studies by the Service Providers Association (AFA), it seems more relevant to directly reach the hosting provider of child pornographic contents to request the deletion of the contents instead of proceeding to the blocking of this particular website. On the one hand, this approach avoids the negative impact on the networks neutrality and allows saving the cost that has not been assessed but will be particularly high. On the other hand, it enables to use a judicial system that already exists and, obviously, works efficiently. Indeed, Article 6 of the French law for the confidence in the digital economy (Loi pour la confiance dans l'économie numérique) of June 21, 2004 compels hosting providers to delete all the manifestly unlawful contents as off the first notification, otherwise they might be held liable.

Hence, in the abovementioned studies performed by the Service Providers Association, after sending the notification to the hosting provider, 93% of child pornographic websites have been removed within two weeks. The previous notification procedure to the hosting provider is more efficient and less costly than the creation and the setting-up of a police service entirely dedicated to screening child pornographic websites, which inefficiency and time length has been showed by the German example.

Last, it is much easier to directly get in touch with a hosting provider to request the deletion of contents than to send notifications to Internet Service Providers requesting the blocking of some websites from computers located in France.

The controversial provisions of the law have led to refer the case to the Constitutional Council on February 15, 2011, after the enactment of the law by the Parliament.

On March 11, 2011, the Constitutional Council judges released their decision regarding the LOPPSI 2 law. Qualified being “a sharp set-back to the government and the French President”, this decision supports the petitioner’s claim and censors more than thirteen key provisions of the LOPPSI law 2 (minimum sentence, video surveillance, change in the status of some municipal officers, etc.). The referral did not concern Articles 2 and 23; therefore, these provisions can be brought into force unchanged.

Furthermore, the provision referring to the screening of child pornographic websites provided by Article 4 of the law has not been censored. According to the Constitutional Council, “Article 4 guarantees a conciliation between the protection of public order and freedom of communication that is not disproportionate”. Judges thus consider that the possibility for an Internet Service Provider to challenge the administrative body’s decision and the fact that the power to screen is limited to a legitimate objective constitutes sufficient guarantees to allow the censorship of websites displaying child pornographic pictures

This law intends to lead the government policies on cybercrime until 2013. It limits some fundamental public freedoms and will inevitably cause enforcement

⁷ <http://www.assemblee-nationale.fr/13/pdf/rapports/r2271.pdf>

problems but, in the Government's opinion, this is the price to pay for

cybersecurity. This is the final "cyberstruggle"!

17th March 2011

By Annabelle RICHARD, Avocat à la Cour – Attorney at Law (New York State), and Oriane ZUBCEVIC, at Ichay & Mullenex Avocats

Ichay & Mullenex Avocats is a French law firm focusing on all legal issues related to the new technologies in France and abroad. They are considered experts in intellectual property and Internet law, e-commerce, online gaming and gambling, data protection. Ichay & Mullenex Avocats also assists its clients on all issues related to financing, mergers & acquisitions, restructuring, etc. and advises them on their litigation and arbitration procedures.

5, rue de Monceau 75008 Paris - France

Tel : +33 1 42 89 19 80

Fax : + 33 1 42 89 14 99

www.ichay-mullenex.com