Michel Toporkoff, Avocat à la Cour,
Maison de la Communication
114 rue Chaptal (92300) Levallois-Perret (France)
m.toporkoff@toporkoff-avocat.fr
(+ 33) 6 18 37 73 30

Cybersecurity : recent french courts cases

1) Applicable french law

2) EDF vs. AFLD, Greenpeace et autres (Cour d'appel de Versailles, february 6, 2013)

3) Sarenza vs. Jonathan L. et autres (Tribunal de grande instance de Paris 3ème section, 4ème chambre, february 21,2013)

4) Gautier vs SOCORPI, IMMOVAC et autres (Cour d'appel de Paris, 25 juin 2013)

Michel Toporkoff, Avocat à la Cour,
Maison de la Communication
114 rue Chaptal (92300) Levallois-Perret (France)
m.toporkoff@toporkoff-avocat.fr
(+ 33) 6 18 37 73 30

Recent publications

Print : Droit de la concurrence déloyale, Editions Lextenso, 2010

On line :

. Advertising law : Dictionnaire juridiques des allégations publicitaires (Stratégies, 2012) http://www.strategies.fr/actualites/marques/187490W/dictionnaire-juridique-des-allegations-publicitaires.html

. Computer law : various articles in «Journal du Net»

Suppression de la page Wikipedia d'un concurrent : la victime doit être particulièrement attentive à ses moyens de preuve (october 14, 2013)

http://www.journaldunet.com/expert/55409/internet-et-concurrence-deloyale---gare-au-parasitisme.shtml (october 7, 2013)

http://www.journaldunet.com/ebusiness/expert/55317/internet-et-concurrence-deloyale---comment-peuvent-reagir-les-sites-victimes.shtml (september 25, 2013)

Article 323-3

Unlawful introduction on a computer system or fraudulent alteration (or suppression) of data thereon is punishable by imprisonment of (up to) 5 years and a fine of 75 000 €

If a State-operated computer system running personal data was involved : (up to) 7 years of imprisonment and a fine of 100 000 €

Article 323-4

Participating in a group intending to commit any of the above actions is punished in the same manner as committing any of the above actions.

Cour d'appel de Versailles, 6 février 2013 (EDF vs/AFLD, Greenpeace et autres)

Facts

A sub-contractor of EDF was hacking a Greenpeace computer system

This was discovered by OCLCTIC by pure accident : while investigating on an illegal access on the computer system of AFLD (french agency responsible for «doping» testing), they went to cycle runner Floyd Landis, who had been using a person in Morocco hacking not only AFLD but also Greenpeace (who did not know being hacked) ; investigators obtained a «commission rogatoire internationale» and discovered this (they also discovered hacking of a Paris attorney)

Court judgments

On November 10, 2011 : Tribunal correctionnel de Nanterre sentenced 2 EDF employees to jail + fine and EDF to 1,5 M€ itself for unlawful access

On February 6, 2013, the Cour d'appel de Versailles overturned this judgment and sentenced one EDF employee (working in the nuclear safety department) to 6 months of emprisonment but neither his superior nor the sub contractor (because of lack of proof of EDF giving orders to commit unlawful actions)

The EDF employee and the sub contractor were also sentenced to damages (15 000 €)

Major factors of success in locating the source of unlawful access

Hard work of the part of OCLCTIC

Good international cooperation between french and moroccan authorities

Major problems for courts

What when no written orders appear to have been issued ?

What when orders may be implicit ? What when the employee or sub-contractor is only trying to please his manager (or client) ?

What when the (large) customer gives a great freedom of action to its sub-contractor ? Is the customer not liable for what the sub-contractor does ?

Tribunal de grande instance de Paris, 21 février 2013, Sarenza vs. Jonathan L. and others

Facts

Sarenza's (shoemaker selling on-line) access codes to its customer data base (including 4.7 million mail addresses) had been supplied to a third party (NA2J) by one of its employees, who gave NA2J the login account and the password of her manager ; NA2J used it for its own needs but also sold it to other corporations (Vivaki)

Court judment

The employee is fined ; the damage amount is estimated by the Court at 100 000 € but the award is reduced by 30 000 € as the Court finds Sarenza to have been negligent in not taking the appropriate safety measures to protect its data base

The login and password of the employee's manager were also used by 4 other persons

The Court also finds that Vivaki should have been alerted by the very low price it paid for the data base and should accordingly have wondered about the legality of the transaction

NA2J is now bankrupt

Cour d’appel de Paris, 25 juin 2013, Gautier c/ SOCORPI, IMMOVAC and others

Facts

Unlawful use of a data base : the data base of a real estate group of companies has been fraudulently used by the founder of the group (while selling its company which was a member of such group) for its new totally independent company

Courts judgments

Seller is sentenced (Tribunal de commerce de Paris, 12 octobre 2011) to damages amounting to 50 000 € for «unfair practices»

This is confirmed by Cour d’appel de Paris on june 25, 2013

A few final remarks

Very few «criminal» cases

. Many cyber attacks remain unknown

. French courts seem to feel somewhat uneasy about who to punish and about the appropriate punishment

. A serious propension to blaming the victim for failure in protecting its own data

A larger number of «busines cases»

. French courts feel more at ease in such cases