*Noëlle Lenoir**

DATA PROTECTION: EUROPE VS. THE UNITED STATES

Long before the term "uberisation" made its way into everyday parlance, the digitisation of means of payment had already turned practices in the world of finance, industry and commerce upside down. First, remote internet or mobile phone payments based on debit and credit cards, then Paypal payments linking electronic wallets and bank accounts and now contactless payments by card or mobile phone: the growth of e-commerce — like convenience shopping — is coming to rely more and more heavily on electronics, the new key to mass consumption.

The formation of the debit and credit card economic interest consortium in the 1980s clearly played its part in this development, though France remains relatively well placed in the world of digital finance, ranking sixth in the world after the United Kingdom in third place and Germany in fifth. In October 2015, the French government launched a "national payment means strategy" designed to further strengthen competitiveness in the payment sector through innovation. For this is where the challenge lies: electronic payment means are not just a way of making life easier for consumers; they also play a vital role in the finance and business sectors. Above all, they are vectors of innovation capable of exerting considerable influence. It does not take a genius to work out that whoever succeeds in defining the standards that govern how means of payment work, and the business model on which they operate, will have the power to shape all financial transactions and, thereby, the economics of trade as a whole.

* Member of the French Constitutional Court between 1992 and 2001, then Minister for Europe in Jean-Pierre Raffarin's government from 2002 to 2004, Noëlle Lenoir also took a keen interest in data protection issues during her stay at France's data protection agency, the *Commission nationale informatique et libertés* (CNIL). A lawyer by training, she is a partner in the law firm of Kramer Levin Naftalis & Frankel.

The interests of the Internet giants

It is no coincidence that Internet giants such as Google, Apple, Facebook and Amazon — always quick with an innovative solution to consolidate their market positions — are showing such interest in these payment means: Google with Google Wallet, Apple with ApplePay and Amazon with its selfie-based facial recognition payment system along the lines of those already launched by other operators such as La Banque Postale in France and MasterCard in the United States. If the European Union has been striving to create a genuine integrated payment services market for some years now, it is precisely because part of its programme to complete the single market includes developing its technological capabilities in order to compete with its US counterparts.

Although payment security has not thus far appeared to be a major preoccupation of our neighbours across the Atlantic, Europe, on the other hand, is keen to address the concerns of those consumers who are still mistrustful of online payments and, in so doing, consolidate its advance in terms of Internet transaction security — which remains far from perfect. Everyone knows that hacking has become a popular participation sport. Widely used to organise fraud on a huge scale, it can also be employed to serve more political ends by making the public aware of the vulnerability of certain systems, for example. A new paradigm, hacking is both a great danger and a formidable incentive to try and foil Internet pirates by inventing impregnable new security systems.

On this front, Europe is winning — both by virtue of its technology and thanks to its privacy culture, embodied in data protection legislation that is particularly restrictive for business. Indeed, the extraterritorial application of this legislation is affecting both business and political relations between the European Union and the United States to such an extent that the US has modified its own laws. We are used to the scenario in which the extraterritorial scope of US legislation causes Europe to amend its legal landscape, as in the case of the Sarbanes-Oxley Act of 2002 that forced European banks to deploy a complete compliance arsenal. It may have failed to prove particularly effective at the time of the systemic banking crisis in 2008, but has nevertheless brought about a profound change in the internal operation of lending institutions. This time, however, it is the US that is having to react and fall into line with data protection requirements resulting from a number of European Court of Justice (ECJ) judgments handed down in 2014 and 2015.

The internal payment services market: a strategic challenge for Europe

The European internal remote payment market was set up under legislation that leaves individual Member States very little room for manoeuvre. Indeed, the 2007 Payment Services Directive, revised in 2015, provides for full harmonisation, meaning that in all but a few limited cases Member States can neither permit exceptions to it nor adapt its provisions. The Directive has opened up national markets whilst at the same time making a dent in the monopoly held by banks, thereby allowing other accredited players — payment and electronic money institutions — to compete with them.

It is interesting to note that the EU Directive 2015/1794 amending the 2007 Directive concentrates primarily on payment security as being "fundamental in guaranteeing the protection of users and the development of a healthy environment for e-commerce". Indeed, experience has shown that though e-commerce is growing appreciably, it must still gain the complete trust of consumers by finding ways of combatting fraudulent intrusions.

The solution advocated by the Directive is encryption incorporated either in the payer's personal device (card reader, mobile phone) or provided by the payment service provider, by text message or email. European legislation prescribes "strong customer authentication" based on something known only to the user (the answer to a personal question) on one hand, and on something inherent to the user, on the other. The CNIL is becoming more and more vigilant on this issue. During recent discussions, it reprimanded businesses for allowing access to their systems via passwords that were too easily detectable, quite regardless of specific regulations such as those that exist, for example, in relation to electronic payments. Facebook experienced this to its cost in February 2016 when the CNIL issued a public warning about its alleged use of non-compliant passwords.

In parallel, payment service providers are now required to collect ever more detailed data at either end of the chain — on both those issuing and those receiving fund transfers — as part of current efforts to combat money laundering and the financing of terrorism. Indeed, a new 2015 directive, constituting a fourth "anti-money laundering package", requires all payments to be traceable. These providers are now responsible for processing sensitive data which requires enhanced security measures.

Payments and the challenge of hacking

A sort of latter-day Arsène Lupin (France's literary answer to Raffles), the hacker is seen as both a crook and a hero. Hero because he uses cunning rather than force to gain access to the systems containing the data that will eventually make his fortune; crook because the sums he diverts can be truly enormous. Apart from the specific case of payment service providers, there is no business, no government department that has not fallen prey to hackers. So much so that today it is true to say that there are only two categories of business: those that realise their systems have been hacked and those that do not.

One of the most spectacular cases of hacking, uncovered in 2014, was the theft of data from over 110 million debit and credit cards belonging to customers of the chain store, "Target", the second largest discount retailer in the US. The hackers used malware that was capable of intercepting data belonging to the store's customers as it passed through a computer's random-access memory. As the data was not encrypted, the task was easy.

Another case that gained a lot of public attention involved a Turkish hacker who was arrested in Germany in 2013, then extradited to the United States for trial. He managed to steal tens of millions of dollars from cash machines by cloning debit and credit cards, placing the money stolen in offshore accounts before converting it into electronic currency.

Europe a step ahead on security

These two examples amongst others have highlighted the somewhat archaic nature of the debit/credit card system in the United States, where data is stored on a simple magnetic strip rather than contained in computer chips that are much more difficult to duplicate. The proceedings of mafia-based hacking, for example, often carried out from the countries of Central and Eastern Europe, is said to amount to some 11 billion dollars per annum.

The scale of fraud would appear to be lower in Europe than in the United States. What is more, until recently the US did not possess a data protection agency comparable to the CNIL, capable of holding negligent operators (who are after all indirectly responsible for data theft) to account by carrying out unannounced audits, for example, and handing out penalties where appropriate. This

legal vacuum has recently been filled, in part at least. In 2015, a US court of appeals ruled that America's consumer protection agency, the Federal Trade Commission (FTC), had jurisdiction to prosecute and impose penalties on businesses that fail in their duty to guarantee the confidentiality of the personal data entrusted to them. The FTC had brought a negligence action against the Wyndham hotel chain for storing its customers" debit and credit card details without any safeguards whatsoever, with the result that in 2008 and 2009 hackers were able to access the personal data of over 600,000 people without any great difficulty.

In Europe, banks are currently testing a new generation of debit and credit cards equipped with "dynamic" — i.e. changing — CSC codes that are renewed at regular intervals (every 20 minutes, for example) to prevent fraudulent use.

Data protection law — a source of competitive advantage?

History goes some way to explaining the different approaches to IT security, and more generally to data protection, on either side of the Atlantic. Unlike the countries of continental Europe, the United States has never experienced dictatorship, whence the European sensitivity to privacy in relation to both their lives and their personal data. In addition, two recent events have strengthened Europe's will to ensure data protection anywhere in the world. The first is the Treaty of Lisbon and its EU Charter of Fundamental Rights. Previously, the European Data Protection Directive (which continues to apply until 2018) was based on the single market and the need to ensure the free movement of data within it. Data protection is now enshrined in the Charter as a fundamental EU right.

The second is the case of Edward Snowden, a former NSA (National Security Agency) contractor who leaked millions of items of classified information in a bid to reveal the Agency's global surveillance programme to the world. A few years ago, Snowden would simply have been considered a traitor to his country. Today, for some people at least, he is almost a god, legitimately entitled to give the US government lessons in democracy from Russia where he has sought asylum. The echo found by Snowden's actions in both public opinion and the European Parliament has translated directly into the decisions made by the ECJ, Europe's court of last resort and consequently an influence to be reckoned with.

These decisions, and in particular the Google Spain and Weltimmo rulings of 14 May 2014 and 1 October 2015, respectively, make it clear that all data (including banking information) relating to EU citizens that is processed or stored in the United States is protected under EU law if the operator has an "establishment" in the European Union. This is confirmed in the forthcoming General Data Protection Regulation set to replace the 1995 directive in 2018. It stipulates that, as far as commercial operations are concerned, the applicability of European legislation will be decided not in relation to the place where data is processed but rather whether or not the individuals whose data is being processed are resident in the EU.

Clearer still is the Schrems ruling of 6 October 2015 — named after the Austrian law student and disciple of Snowden who brought the case — by which the European Court of Justice quashed the European Commission's decision on the US/EU Safe Harbor agreement. This rendered all data transfers under its provisions illegal with immediate effect, on the grounds that it allowed US authorities to access the data stored in the United States by Internet companies such as Facebook, in breach of European data protection law. The fact that certain US operators (Google, Facebook, Microsoft, etc.) have now set up clouds in Europe is not unrelated to their desire to reassure European consumers whilst at the same time ensuring they do not lose out to European operators who have been quick to make a move into the US market where, they claim, data security is less rigorous.

Tensions between Europe and the US

Much has been left unsaid in the heightened tension between the US and Europe around these ECJ rulings. It is clear that Europe, which does not intend to apply the criteria set out in the Schrems ruling to stop data transfers between the EU and China, for example, sees them as a lever for bringing data centres equipped with all the most advanced security technology back to Europe. Its objective is to put European digital operators ahead in the data/systems security market.

The new Privacy Shield agreement, signed in February 2016 between the US government and the European Commission to resolve the dispute, strengthens the guarantees offered to EU citizens by giving them several potential means of redress for dealing with possible abuses by the US authorities. However, it is

already being vilified by MEPs and regarded with suspicion by the Art. 29 Working Party that brings together representatives from the EU's 28 data protection authorities.

The battle currently being waged by Apple, on one hand, and the US Department of Justice and the FBI, on the other, also offers a number of lessons. Apple's refusal to provide access to the data stored on the iPhone of the Islamist terrorist who killed 14 people in San Bernardino, California in December 2015 may not only be linked to Apple boss Tim Cook's (1) concern "not to jeopardise" the security of the countless users of his mobile phones around the world. After all, the dispute places Apple right at the centre of the debate about the challenges of data security and the protection of individual rights to privacy...

How can we reconcile data security and security *per se* in a world where terrorism is striking at the heart of our democracies? What will be the outcome of this "EU meets US chase" through the digital and data security market? How will either of them deal with hacking, a new vector for rapidly expanding cross-border corruption? The future remains uncertain, but one thing is sure. Once again, and contrary to our preconceptions, it is the law — in this case the tensions between data protection law and the protection of public security — that is shaping technology rather than the other way around. Our job is to make sure that the often nit-picking data protection constraints placed on operators do not hinder competitiveness in the industry, but rather strengthen it.

---

(1) See the interview with Tim Cook in *Time Magazine*, 17 March 2016.