Dutch Data Protection Authority - Annual Report 2013

Foreword

If there was one event in 2013 that attracted the attention of even the most inveterate adherent of the mantra 'If you've got nothing to hide, you've got nothing to fear', it was Edward Snowden's revelations about the practices of the NSA. The idea that the National Security Agency is using a gigantic trawl net to collect the data of citizens worldwide has outraged many people. And not just private citizens. Eight large American technology companies also voiced their objections to the NSA's practices in a joint letter to the U.S. President − amongst other things, about the large-scale surveillance of users of their internet services. These are the multinationals with which we as European data protection authorities are usually at odds with.

'You're no better than us,' is the reaction of the Americans when others criticise the working method of the American security services. We don't know whether they are right or wrong. Snowden's revelations did bring to light – albeit in the second instance – the fact that the Dutch intelligence services have also been collecting and are still collecting traffic data or metadata on a very large scale. Metadata – although the term suggests otherwise – can just as well be traced back to specific persons and can reveal a great deal about them. In late 2013, the Dessens Commission, which evaluated the Wet op de inlichtingen- en veiligheidsdiensten (Wiv) [Intelligence and Security Services Act], advocated an extension of the powers of the Dutch General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD): the Commission stated that the two organisations should also be authorised to investigate the transfer of personal data by cable.

Should the AIVD and the MIVD, like their American counterparts, be able to indiscriminately throw out a data trawl net? Although the intelligence services do not lie within the competence of the Dutch Data Protection Authority (Dutch DPA) [College bescherming persoonsgegevens (CBP)], these questions are so interlinked with the essence of personal data protection that the Dutch DPA does not want to stay silent on the matter. After all, the adage 'finders keepers' runs counter to the principles enshrined by the legislator in both the Wet bescherming persoonsgegevens (Wbp) [Dutch Data Protection Act] and the Wiv – that is, the principles of proportionality, subsidiarity and finality.

It seemed for a long time as if these principles would come off badly in the fight against terrorism. But that may soon change somewhat in the United States. In reaction to a critical report from the committee that the White House ordered to investigate the NSA, a number of checks and balances will be built in that may lead to reforms and greater control over the operations of the American security services. However, there is no concrete evidence that this will also signal the end of large-scale data collection. After all, the point of departure for the Americans – unlike for the European Union – is that the practice of collecting data is not worth protecting. It is only when that data is actually used that the Administration must comply with the restrictions issuing from the Fourth Amendment to the U.S. Constitution.

In the Netherlands, we should also be alert to the possibly excessive collection of data by our intelligence and security services. As already mentioned, the Dutch DPA is not authorised to investigate the AIVD and the MIVD. That is the task of the CTIVD, the Dutch Review Committee for the Intelligence and Security Services. Nevertheless, it would be wise to closely examine the abovementioned principles of the privacy legislation as well as the degree of transparency of these security services. Complete openness is out of the question, of course, given the possible threat to national security. But the Government rightly states in a memorandum issued in December 2013: "*The question we are facing is how, given the continued digitalisation of Dutch society, we can properly give substance to the transparency principle in the area of security. This is an important task, because transparency can increase the trust of citizens in the way the authorities collect and further process data in the security domain. That importance is increasing, because the average citizen will not be aware of all the modern technical possibilities in that area.*[1] I fully agree with this statement. But it will be interesting to see how the Government gives substance to this in the area of national security, also against the background of the continued digitalisation of our society.

In the Netherlands and in the European Union as a whole, we can try to uphold the fundamental right to the protection of personal data as effectively as possible, but the transfer of personal data does not stop at our borders. And notwithstanding increasingly frequent transatlantic contact, in the area of privacy the US and Europe are still in different worlds. In the EU, the protection of personal data is a fundamental right, and governments must stand surety for the protection of that data in their relationship with citizens and draw up regulations for the rights of citizens in their role as consumers in relation to companies. In the US, the initiative to act against the abuse of personal data primarily lies with the citizen.

To a certain extent, the abovementioned reaction of the high-tech companies in the US to Edward Snowden's revelations is significant. The companies feel that the trust of their customers is diminishing because their personal data prove to be unsafe at these companies. Partly as a result of this, Europe is gradually developing its own 'Silicon Valleys'. These developments may make it possible, given the wave of collective indignation, to take a pragmatic approach to the transatlantic differences between the methods used to protect privacy. After all, the American consumer and the European citizen want the same thing: to live the legitimate part of their lives without being spied upon.

Jacob Kohnstamm
Chairman Dutch Data Protection Authority

[1] Memorandum from the Minister of Security and Justice, the State Secretary of Security and Justice and the Minister of the Interior and Kingdom Relations entitled *Freedom and security in the digital society. An agenda for the future*, page 9.
(Notitie van de minister van Veiligheid en Justitie, de staatssecretaris van Veiligheid en Justitie en de minister van Binnenlandse Zaken en Koninkrijksrelaties getiteld *Vrijheid en veiligheid in de digitale samenleving. Een agenda voor de toekomst*, pagina 9.)

Introduction

The year 2013 was an exciting and successful year for the Dutch Data Protection Authority (Dutch DPA) [College bescherming persoonsgegevens (CBP)]. The Authority investigated a multitude of cases, enforced compliance, issued legislative opinions and maintained external contacts. In all of these activities, the main themes were the protection of medical data, data processing in the employment relationship and profiling. In addition, the legal principles of finality, consent, transparency and security were particularly prevalent in the work of the Dutch DPA.

Everybody should be able to trust that the personal data that they – consciously or unconsciously – provide to government organisations and companies is handled with care. For example, government organisations and companies must have a legal basis for processing data and may not use data for completely different purposes to those for which it was collected in the first place. For most people, it is no longer possible to keep track of what is happening with their personal data and how it is being used. That is why it is so important that companies and government organisations provide them with clear information.

Through its work, the Dutch DPA promotes compliance with the Wet bescherming persoonsgegevens (Wbp) [Dutch Data Protection Act]. In many instances, the actions of the Dutch DPA put an end to the detected violations. This often means not just that the investigated companies or institutions start complying with the law, but also that other companies or institutions and sector organisations start paying more attention to the way they comply with the legal requirements.

Patient data
Famous or unknown, rich or poor, every patient is entitled to the same degree of protection against unauthorised access to his or her medical data. However, protection against access to patient data is still inadequate, as shown by a major investigation carried out by the Dutch DPA into care institutions, after-hours clinics and pharmacies. Due to inadequate security measures, there is a risk of medical records being accessed by employees with whom patients have no treatment relationship. On the basis of the investigation as well as new signals and discussions with umbrella organisations, the Dutch DPA believes that these practices are widespread in the care sector.

Strict requirements have also been defined for the disclosure of patient data by one organisation to another in the chain, such as by a mental health institution to a health insurance company. The same applies to the provision of medical data to third parties, such as manufacturers of medical equipment. That is not permitted without the consent of the data subjects. The Dutch DPA investigated the supply of medical data to a manufacturer of incontinence materials and concluded that pharmacies had put insufficient safeguards in place to protect patient data and also had not asked all patients for permission to disclose their data to the manufacturer.

Employment relationship
It is completely unnecessary – and also prohibited – for employers to access the medical history of their employees. Health and safety service providers, such as 'absenteeism companies' and occupational health services, must therefore be aware that they may not disclose any data about the medical treatment of employees to the employer. In 2013, the Dutch DPA investigated two health and safety service providers. Both were found to be in violation of the law by supplying medical data of employees to their client, the employer.

Employees are entitled to the protection of their personal data on the work floor as well. For example, employers may not use images from security cameras to confront their personnel about their performances. The use of hidden cameras is only permitted in exceptional cases and definitely not for training purposes. The Dutch DPA's investigation into Media Markt, which focused on both of these issues, attracted a great deal of attention from the press and the public.

Online data and profiling

Data about the programmes people watch on television, the websites they visit and the apps they download reveal a great deal about their behaviour and preferences. What happens next with this data collected by telecom providers or app developers is usually not revealed. Many people are not aware that they are paying for many online services with their personal data. Companies and organisations must inform them properly about the use of their data and, where necessary, ask them for their consent.

In 2013, the Dutch DPA investigated unlawful data analysis (packet inspection) by four telecom providers. It found, amongst other things, that these companies were violating the law by retaining detailed data about the websites and apps visited by their customers and not notifying them (properly) about it. The Dutch DPA also investigated the collection and retention of data about online viewing behaviour, the use of apps and website visits of users of smart TVs. Parliamentary questions about the use of cookies on the websites of the Dutch public broadcasting services (NPO) prompted the Dutch DPA to refer the matter to the applicable legal framework. According to the Dutch DPA, visitors to the NPO websites who do not consent to have their web browsing patterns monitored may not be refused access.

Across the border

The ongoing review of the European privacy regulations is vitally important for citizens, companies, government organisations and the data protection authorities. The Dutch DPA has therefore worked hard, on a national and European level, to develop an EU Regulation that is consistent with the spirit of the times and that offers a sufficient level of protection. By late 2013, however, the Council of Ministers of Justice and Home Affairs of the European Union had not yet reached political agreement on a number of crucial components of the new privacy legislation. This is delaying the negotiations between the European Commission, the Council and the European Parliament.

Apart from the developments around a new EU privacy regulation, the Dutch DPA is actively working to achieve greater cooperation between the data protection authorities, not just inside Europe but also globally. This is indispensable in view of the cross-border character of many data processing operations. Amongst other things, the Dutch DPA worked with the Canadian data protection authority on an investigation into WhatsApp and with other European data protection authorities on an investigation into Google's new privacy policy.

The revelations about the surveillance programmes of the American and European intelligence services, particularly the NSA, have caused great controversy worldwide. In two letters to the European Commission, Jacob Kohnstamm, Chairman of the Dutch DPA and of the Article 29 Working Party of European data protection authorities, expressed serious concerns about the consequences for the privacy of European citizens on behalf of the working party. Furthermore, at the request of the European Commission Kohnstamm joined an ad hoc working party of the EU and the US that investigated the content and legitimacy of the various American surveillance programmes. In addition, in late 2013 the Dutch DPA and the Belgian data protection authority launched a joint investigation into possible unlawful access by third parties to the bank data of European citizens in the SWIFT organisation.

--

This publication only concerns a selection of the investigations and legislative recommendations made by the Dutch DPA in 2013. An extensive annual report has been published on http://www.cbpweb.nl/Pages/jv_2013.aspx More information regarding the work carried out by the Dutch DPA can be found on http://www.cbpweb.nl/Pages/home.aspx and on www.mijnprivacy.nl.
