MAGAZINE

DATA CYBERSECURITY & PRIVACY

The cookie has crumbled: custom audience to the rescue?

Data security: what about your IT-inventory?

Interview with Cecile Schut - Dutch Data Protection Authority

The Dutch DPA on data brokering

Interview with Ton Wagemans - Considerati

The Socratic approach to technology adoption

#07 | 03-2021 | DCSP.NL

DCSP
DATA CYBERSECURITY & PRIVACY

MAGAZINE
DATA CYBERSECURITY & PRIVACY

The cookie has crumbled: custom audience to the rescue?

Data security: what about your IT-inventory?

Interview with Cecile Schut – Dutch DPA
The Dutch DPA on data brokering

Interview with Ton Wagemans – Considerati
The Socratic approach to technology adoption

#07 | 02-2021 | DCSP.NL

A magazine for professionals in consultancies, law firms, scientific and educational institutions, corporate firms, government agencies and the business.

Advisory Board:
Christiaan A. Alberdingk Thijm (bureau Brandeis, Institute for Information Law, University of Amsterdam)
Serge J.H. Gijrath (C-Legal, e-Law Center for Law and Digital Technologies, Leiden University)
Wouter Seinen (Pinsent Masons)

Editors in Chief:
Claudia Zuidema
Robert Kreuger

Editor:
Frederique Ternede

Photography:
Manisha Ramsaran

Design:
rdesign, Amsterdam

Production:
RVV Grafisch

Website:
www.dcsp.nl

Subscription services:
info@dcsp.nl

Publisher:
deLex Media & Management B.V.
Barbara Strozzilaan 101
1083 HN Amsterdam
T: 020 345 22 12
E: info@delex.nl

Commerce & advertorial acquisition:
info@delex.nl

ISSN:
2666-058X

DELEXMEDIA

From the editor

A year that flew by and in which so much has happened at the same time. It seems as if the corona crisis has brought more and more to light. The importance of data, cybersecurity and privacy can no longer be underestimated. Think of the many digital shortcomings that have surfaced, data leaks, privacy violations and systems and technologies that are in need of improvement and (higher standards of) security. What a year.

In this seventh edition of DCSP we address the latest discussions and information in the context of the current state of the society. We kick off this edition with an article from the partners and lawyers of The Data Lawyers, Eliëtte Vaal and Vonne Laan, written in collaboration with Matthias de Bruyne, Senior Legal Counsel at the DDMA. They provide insight into the current situation of cookie-tracking. Has the cookie crumbled with social media and custom audience in the playing field or not?

In line with this article is the interview with the Dutch Data Protection Authority (DPA). Through their research, many faults and offences were revealed. We spoke with Cecile Schut, Director System Supervision, Security and Technology about data brokering. What does it mean, what is the DPA's perspective on this subject, how to tackle illegal data trafficking?

We all know IT-infrastructure is complicated. An essential component of this infrastructure is security. Flaws in IT-infrastructure are frequently caused by vulnerabilities in software. This time, together with two other cyber security experts, Petra Oldengarm and Rutger Leukfeldt, our cyber security columnist Bernold Nieuwesteeg wrote his column about the security of software and the responsibility that goes with it when an attack occurs. The three of them bundled their knowledge into two pages where they give us insight into vulnerabilities in software which could lead to cyber-attacks and who is responsible for the security.

Even though our interviewer Roel van Rijsewijk from our regular section 'at the kitchen table' moved to another kitchen table just outside Amsterdam, he again interviewed someone interesting. This time it was Considerati's founder and partner, Ton Wagemans' turn. They talked about the regulation of the Internet, the essence of testing policies and inventions, keeping up with technology as a company and as a country, and much more.

For this next article we have crossed borders in terms of content. We (metaphorically) went to Brazil! Greenberg Traurig's lawyer, Willeke Kemkers and CGM Brazil's partner and lawyer, Adriano Chaves, discussed Brazil's new privacy initiative, with their National Data Protection Authority just installed in November 2020. They gave us an overview of the national law with regard to global implications.

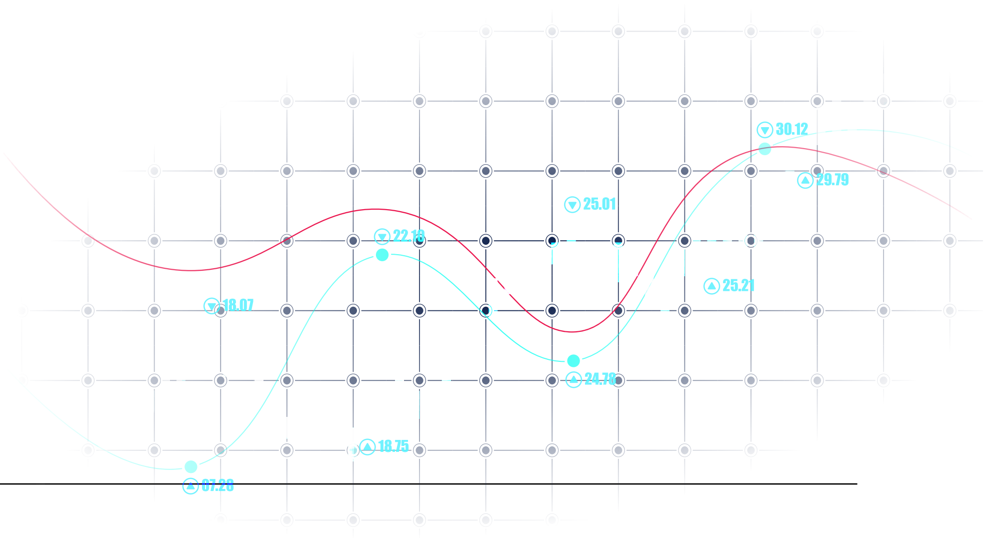
Further included in this edition are a column from Rob van den Hoven van Genderen about the corona vaccination passport. Will this be the start of a social partition? 'The Legal Look' by Victor de Pous where he provides us his point of view on the legal liability when it comes to digital shortcomings that make individuals, organisations and the society as a whole more vulnerable, Peter van Schelven with his column about data security where he emphasizes the importance of a central, up to date and complete IT-inventory to protect against cyber incidents and the column from Hans Schnitzler about the misleading metaphors of the information age. Why exactly do we use terms like 'smart' and 'intelligence'?

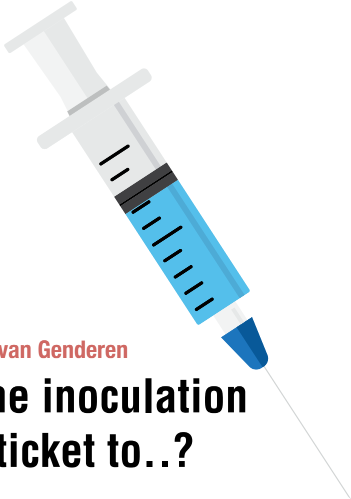
Do you as a professional in data, cybersecurity and/or privacy have more interesting information or ideas to share? Or do you want DCSP to be included in your business network as a company subscription? Contact us at any time.

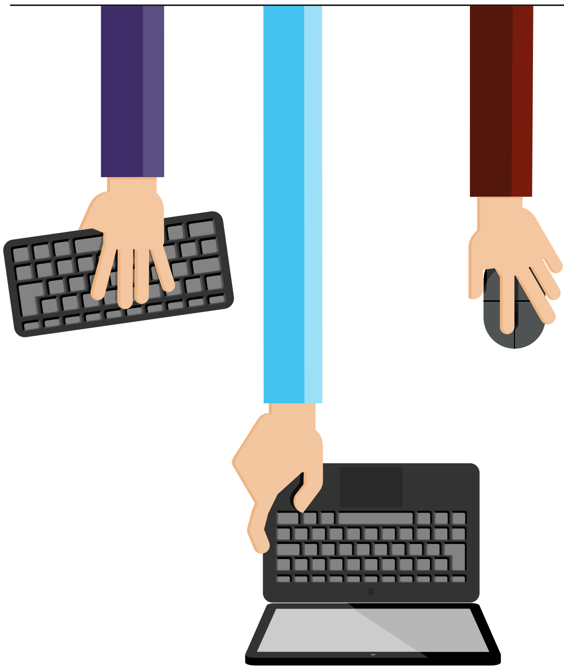
On behalf of the editorial board we hope you will enjoy this seventh edition of DCSP.

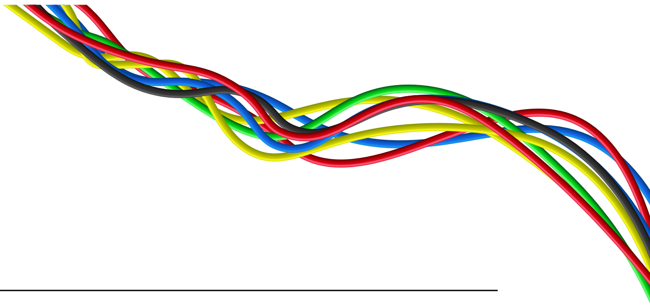
Robert Kreuger – *Editor in Chief*

CONTENTS









Eliëtte Vaal, Vonne Laan, Matthias de Bruyne

The cookie has crumbled: custom audiences to the rescue?

The digital marketing industry is in reform. For the past 25 years, third-party cookie-tracking has been one of the most important tools for online targeting and retargeting. How do things stand now? Are cookies future-proof or has the cookie crumbled, with custom audiences on social media platforms coming to the rescue?

Cookies and the applicable legal framework

We all know the standard phrasing in cookie statements. But cookies and similar technologies are in essence nothing more than small bits of data that can be placed on your laptop or other device and used to recognize website visitors. They are therefore ideal for marketing purposes, where recognizing who has clicked on your ad is essential. However, using cookies means facing tough legal challenges. In the Netherlands, two legal regimes apply to the online tracking of customers: the ePrivacy and the GDPR regimes. The current ePrivacy regime is based on the ePrivacy Directive (2002/58/EC, amended by Directive 2009/136/EC), implemented in the Telecommunications Act, while the GDPR has been transposed into the General Data Protection Regulation Implementation Act. The combination of the ePrivacy and the GDPR regimes determines whether an opt-in is required or an opt-out is sufficient.

> “Using cookies means facing tough legal challenges.”

When targeting practices involve the use of cookies (or similar technologies such as pixels, tags, or beacons), the main rule is that prior consent is required. Under the Dutch Telecommunications Act, the use of cookies for analytic purposes also requires an opt-in, except where they have limited or no impact on the privacy of end-users (so-called ‘privacy friendly’ analytic cookies). Strictly functional cookies do not require consent either. This is the case if their sole purpose is to facilitate communication over an electronic communication network, or if storage of or access to the data is strictly necessary for providing the information-society service requested by the website visitor.

Thus, under the ePrivacy rules, targeting and retargeting cookies requires consent. Consent is any freely given, specific, informed, unambiguous and advance indication of the data subject’s wishes. This implies a real choice as well as control when providing consent via cookie banners. The European Court of Justice has confirmed that pre-ticked boxes are not allowed (C-61/19). Furthermore, a regional court in Germany has held that misleading cookie banners that do not present consent to and refusal of cookies as equivalent options do not meet the requirements of German law. Excessive cookie banners and pop-ups would therefore appear to be inevitable. All hope is now vested in new legislation to resolve this issue. On February 10th, the Council of the European Union finally published a new proposal for an ePrivacy Regulation. It is the fourteenth in a long series of attempts by EU presidencies to find common ground following the European Commission’s 2017 proposal. Ambassadors from the Council of the European Union have agreed on this latest version for a negotiating mandate, finally leading to some movement in the legislative process of the ePrivacy Regulation. The next step in the process is the trilogue, in which the Parliament, Council and Commission of the European Union will come together to hammer out the final text.

Just like the GDPR, the ePrivacy Regulation is part of the EU Digital Single Market Strategy. Its aim is to update the current, outdated ePrivacy regime by safeguarding the privacy of the end-users, the confidentiality of their communications, and the integrity of their devices. And although this proposal does not explicitly mention the option of providing consent via browser settings as was the case in the proposal by the European Commission, it does seem to give a little ground in this regard. Having regard to the prevailing consent fatigue, the recitals state: “For example, an end-user can give consent to the use of certain types of cookies by whitelisting one or several providers for their specified purposes.” Thus, consent via browser settings seems to be allowed, but only if the browser settings offer the possibility of providing granular consent as regards the parties and purposes concerned. If they do not, then cookie banners and cookie pop-ups will continue to be a necessary evil. Unless you don’t use cookies. Recently, for instance, publishers such as the New York Times and the advertising platform STER announced that they have abandoned the use of third-party tracking cookies. With Google Chrome’s announcement that it will phase out all support for third-party cookies over the next year, thus joining Safari and Firefox who are restricting third-party cookies in their web browsers, the end of the third-party cookie era seems nigh.

Custom audiences and the related legal framework

In the absence of third-party cookies recognizing customers on their websites, organisations are looking for alternatives to targeting customers. One such existing and popular form of online targeting is known as 'custom audiences' or 'list-based' targeting. An advertiser uploads a list of email addresses, phone numbers, cookie-IDs or other identifiers of its own customers or prospects to a platform, such as Facebook. The platform then uses a process called matching to identify customers or prospects on its own platform. This enables the advertiser to either target its own customers and prospects with a personalized campaign or exclude them to save online advertising costs.

But what is the situation in the Netherlands? How are custom audiences used here? At our request, the Data Driven Marketing Association (DDMA) carried out a survey to find out more about the use of custom audiences in the Dutch market. Most commonly, custom audiences are being used to exclude current customers from marketing campaigns and to focus solely on prospects (most likely to reduce advertisement costs). The majority of the participants in the survey also use custom audiences to create so-called lookalike audiences, a group of new customers selected by the platform based on the advertiser's common parameters for current customers. In addition, the platforms most frequently used for custom audiences (by the respondents) are Google and Facebook, followed by LinkedIn and Instagram. However, the survey showed that there is still uncertainty about the rules that apply to custom audiences. When is consent required?

Direct marketing through electronic messaging (email/SMS/personal messages on social media) requires prior consent under the ePrivacy rules. Although the exact scope of this requirement is not clear, it does not necessarily apply to custom audiences, as it seems defensible that the majority of such advertisements do not qualify as electronic messages under the Telecommunications Act. It remains to be seen whether this will change under the new ePrivacy regulation. It will depend on the exact interpretation of electronic messaging. But how are consent requirements regulated under the GDPR?

> "The platforms most frequently used for custom audiences are Google and Facebook, followed by LinkedIn and Instagram."

If no consent is required under ePrivacy, then, under the GDPR, there may still be a requirement to obtain consent for the processing of the personal data. This depends on whether a so-called legitimate interest can be relied upon or not. The conditions for a legitimate interest to apply are: (i) the existence of a legitimate interest that is to be pursued; (ii) necessity and (iii) proportionality (whether the legitimate interest is overridden by the individual's fundamental rights and freedoms. Although this may sound like a rather theoretical exercise, the European Data Protection Authorities, united in the European Data Protection Board (EDPB), recently provided two practical examples in relation to custom audiences in their draft guidelines on the targeting of social media users.

In the first example, a Bank provides the email address of a prospect to a social media platform to enable the platform to match it with its users' email addresses and thus identify and target the individual on the platform. In the second example, the Bank provides the email address of an existing customer for the same purpose. According to the EDPB, this legitimate interest may be relied upon when targeting the existing customer in this example, on condition that; (i) the customer was informed that their contact details would be used for direct marketing by the company, (ii) the advertisement relates to the services similar of those provided to the customer, and (iii) the customer was given the opportunity to object when the contact details were collected. As regards the targeting of the prospect, however, consent is required according the EDPB, as the prospect does not have the reasonable expectation that their contact details will be used for targeting on social media. Consequently, targeting prospects seems to require the consent of the individual concerned. However, it remains unclear to which extent this has been influenced by the specifics of this case. This may be clarified in the final version of the guideline.

In practice, organisations rarely collect data for the purpose of targeting customers on platforms but, rather, they use their existing customer database. The use of personal data for subsequent processing for custom audience purposes, such as sharing email address, matching, selecting targeting criteria, displaying advertisements and ad reporting, needs to be compatible with the initial purpose of the processing. This is the principle of purpose limitation. It may be argued that the use of existing customers' email addresses to target those customers on social media and send them newsletters for marketing purposes is a purpose compatible with the collection of those email addresses. However, if personal data is collected for other purposes, such as in the course of customer service, processing for direct marketing purposes is probably not compatible and consent is required before the data can be used in the custom audience scenario.

Plan of action?

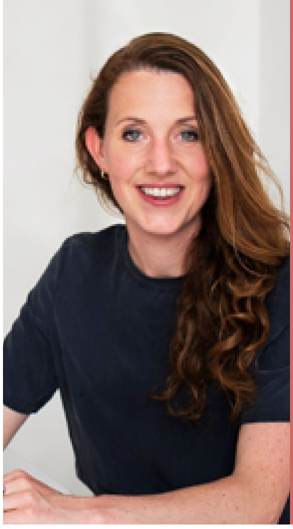
Until browsers provide the option to grant granular consent, there is no real solution to the problem of consent fatigue on the web. At this point, if you use tracking cookies, you still need to work with cookie banners or cookie pop-ups etc. Organizations wishing to investigate alternatives to tracking cookies can of course examine custom audience options. A Data Protection Impact Assessment (DPIA) is recommended to determine whether consent is required in that scenario, including with a view to the new purposes envisaged for an existing data set. Basically, a DPIA is a questionnaire that guides you through all the privacy elements that need to be considered. It provides a structured method for documenting and improving privacy compliance for a new version of a custom audience that you may want to use, for example. Regardless of the so-called purposes limitation, the chances are that you will need consent for the custom audience scenario if you target prospects rather than your existing customers. If you target existing customers, you may not need consent if you are able to substantiate your legitimate interest in the DPIA. Businesses may therefore need to complete a lot of DPIAs. Fun times ahead!

In short:

- Under the current (e)Privacy rules, targeting and retargeting cookies require consent;
- The new version of the ePrivacy Regulation has regards to the prevailing consent fatigue. However, it is expected that cookie banners and cookie pop-ups will continue to be necessary;
- 'Custom audiences' is an alternative to target customers online. According to the EDPB, this alternative does not always require consent when targeting existing customers;
- A Data Protection Impact Assessment is recommended to determine whether consent is required, including with a view to new processing purposes envisaged for an existing data set.

About the author

Matthias de Bruyne is Senior Legal Counsel at the DMMA, the main data-driven marketing association of the Netherlands. He contributed to this article by providing input on the use of custom audiences in practice.



About the author

Eliëtte Vaal is a lawyer and partner at The Data Lawyers. Eliëtte handles cases in relation to new technologies, e-privacy, e-commerce, copyright law and freedom of expression. Eliëtte advises on compliance and assists clients in enforcement procedures initiated by the Data Protection Authority.

About the author

Vonne Laan is a lawyer and partner at The Data Lawyers. She assists Dutch and international clients with various matters in the field of privacy, data protection and cybersecurity. Furthermore, she is a frequent speaker at conferences and guest lecturer at Nyenrode Business University and the Windesheim University of Applied Sciences.

Interview with Cecile Schut – Dutch DPA

The Dutch DPA on data brokering

"To hold grip on your personal data and knowing what others know about you is crucial" - Aleid Wolfsen

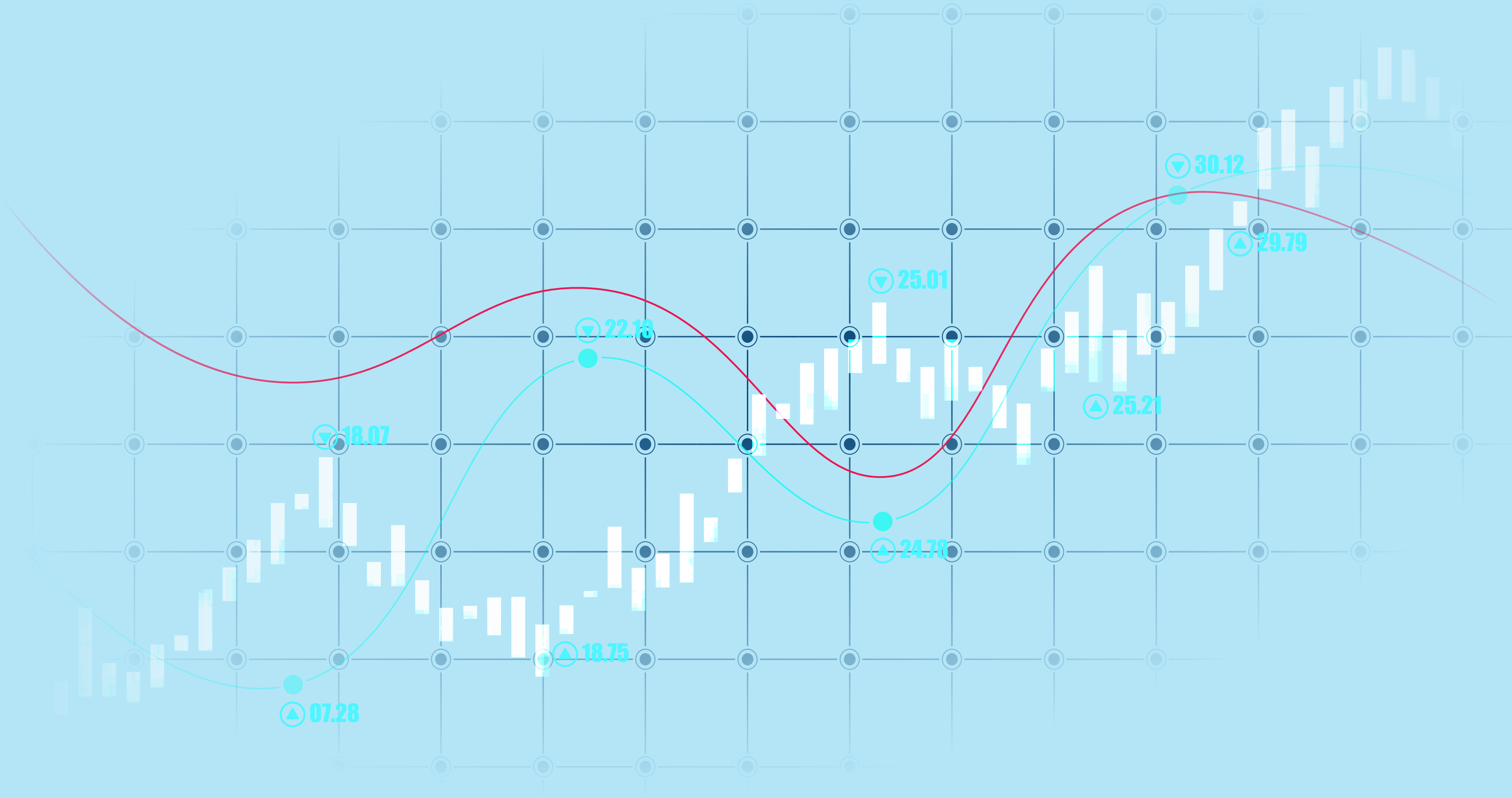
The Dutch DPA is the independent supervisor in the Netherlands that guards our constitutionally enshrined protection of personal data. One of the organisation's main tasks is to monitor companies and governments to determine whether they are complying with the applicable privacy legislation, by means of investigations. In addition to conducting supervision, the Dutch DPA advises on new laws and regulations and provides information. We spoke with Cecile Schut, Director of System Supervision, Security and Technology about the meaning of data brokering, the DPA's perspective on this subject, how to tackle illegal data trafficking, and more.

1. We're going to talk specifically about data brokering/trafficking, but first of all, I'm curious about your position within the Dutch DPA. You have been appointed Director of System Supervision, Security and Technology at the Dutch DPA since 2018, if I'm not mistaken. This, in view of the then new European privacy legislation that was going to come into force from May that year. Can you tell us a bit more about your career path and why you took this position?

Of course! My start at the Dutch DPA in January 2018 was closely related to the start of the new European privacy legislation. At that time, the Dutch DPA had decided to restructure its organisation in preparation for the GDPR (and for the Data Protection Directive for the police and justice sector, which also became applicable as of May 2018). At the time of my application for the job, I was Director Policy at the Dutch Statistical Office. One of the things I was working on was the implementation of the GDPR. For an organisation with the amount of data as a statistical office has, this project was taken very seriously.

Because I am originally trained as a mathematical engineer, one might not expect me to join a DPA. However, I think that my background adds a lot: I like to connect people and knowledge from different backgrounds and to try to make things clear for the widest possible audience.

In the years that I was responsible for statistics, I learned how important it is not only to know how to make reliable statistics, but also to have knowledge of what the figures are about, to understand them. And the same goes for data protection: only when you know and understand the context in which organisations work, it is possible to supervise in a meaningful way. Besides, I had learned in my work and during my executive MPA which



I completed in 2014, that my mathematical thinking fitted well with how people with a legal background think. The combination of leading the technical people within the Dutch DPA and being responsible for what we call 'ex ante' supervision makes my job very inspiring.

2. Data brokering is one of the three key points the Dutch DPA is focussing on. What exactly does this mean?

At the end of 2019, we published the Focus of the Dutch DPA 2020-2023 which outlined three themes that we have decided to prioritize in the upcoming years. The themes are data brokering, digital government, and Artificial Intelligence and Algorithms. We chose these particular themes, because we see a lot of potential risks regarding the protection of personal data in connection to these specific topics. And if these risks occur, the consequences for the daily life of citizens can be far-reaching. Data brokering is one of the themes, because we currently live in a society where data is used to make products and services 'smarter', and these same products and services subsequently create even more data. This growing and constant creation of data means that even more data can be gathered, processed and sold. While this has its advantages, the dark side of data brokering is lurking: unlawful data processing and the lack of transparency for individual citizens.

We notice that citizens are losing their grip on their personal data, are unable to control where their personal data ends up and who has access to it. The Dutch DPA wants to give citizens the control of their personal data back by ensuring that they can exercise their rights effectively. Data brokers are accountable to ensure lawful, fairly and transparent use of personal data. The Dutch DPA stimulates this accountability and will take action against organisations that violate the GDPR.

> "We notice that citizens are losing their grip on their personal data."

3. The Netherlands has about 200 data brokers. Can we say that the Dutch entrepreneur has adopted this way of doing business from abroad? Imagine that data was bought from a US broker. How does this work regarding consent, its legal basis and so on? How does the Dutch DPA view these matters?

The growth of data brokering as a business has been a consequence of several different trends in the past few decades. The creation of the Internet, increasing proces-

> “More and more ‘normal’ companies are also starting to sell data that they gather through their product or services.”

sing power and the declining costs of data storage have all facilitated the development of data brokering. And also, from the beginning of this era, a lot of people strongly believe in “data as the new oil”. This has encouraged a lot of entrepreneurs to collect and exploit data. Alongside the technological trend, there has also been a social and political trend of increasing importance of risk assessment and crisis prevention. Since 9/11 and the war on terror, there has been a significant interest in creating profiles of possible (future) criminals and diminishing the number of opportunities of such criminal behaviour. This all requires the gathering and processing of data. Therefore, I wouldn’t necessarily say that “the Dutch entrepreneur has adopted this way of doing business from abroad”, but rather: it is the consequence of several trends in our digitalizing society.

If a data brokering company wants to process data, it must be done in compliance with the GDPR. This process begins by establishing a legal basis as stated in Article 6 of the GDPR. A data broker can form its legal basis on consent, but other options are also possible. The data broker needs to determine which legal basis is most appropriate in the circumstance. Next to a legal basis, the data broker needs to ensure that the data is processed for specific purposes, is adequate, relevant and limited to what is necessary. Also, the data broker needs to ensure that the data is accurate and up to date. Another thing a data broker needs to think of is defining retention periods and ensuring proper security. In certain circumstances it also will be necessary to perform a Data Protection Impact Assessment and designate a Data Protection Officer.

If a data broker is able to comply with all the rules of the GDPR and continues to promote a culture of data minimalization, transparency and accountability, it should be possible for them to continue their work.

4. What is the definition of a data broker? When does an organsation meet the requirements to be appointed as a data broker? Are amongst these organsations also for example organsations that use payment platforms, collect information and sell this to other parties?

It is not our task to come up with a definition of a data broker. In our view, the core business of data brokers is to make use of personal data as a key ingredient for products and services that can be sold to other parties. The possibilities are endless in theory. A well-known type of data broker is for instance a company that collects and combines on - and offline personal data to be able to create a profile of a person and sell this profile to companies. These companies than can use such a profile to decide on a persons’ creditworthiness or to be able to determine which advertisement will be of interest to which person.

Besides, more and more ‘normal’ companies are also starting to sell data that they gather through their product or services.

5. One of DCSP’s regular columnists, Hans Schnitzler, once wrote in a piece ‘data trafficking is the same as human trafficking’. Those who reveal all their data on the internet and thereby reveal themselves as human beings to data brokers will sooner or later become objects of exploitation and manipulation. The government, in a way, facilitates the way of working for data brokers. Isn’t it a task for the government to stop this?

I understand the concern that the growing amount of personal data, especially when data is combined and exploited from different sources over a long period of time, can lead to manipulation. This may threaten our personal freedom. Our task is to ensure that these practices are executed in a manner that is compliant with the GDPR. The principles of the GDPR state that personal data must be processed lawfully, fairly and transparently in relation to the natural person to whom the data relates. Revealing information about oneself, whether it is on the internet or whether it is in real life, does not mean that this information is free to be collected by companies for other goals. Besides, there are a lot of data breaches where personal data gets ‘lost’. In some cases the data comes into the hands of criminal organisations, who use the data for instance for identity fraud or phishing.

6. What bottlenecks does the Dutch DPA face during investigating and monitoring illegal data trafficking? How do you deal with this?

Currently, the main challenge that the Dutch DPA has to cope with is the budget. At this moment the budget of the Dutch DPA is not sufficient for the amount of work the

Dutch DPA has to execute. We are only able to follow up a small amount of all complaints we receive from citizens. And the same goes for the data breaches that are reported to us. In 2019, we were only able to investigate and close 0,3 percent of about 27.000 reported data breaches. Besides, the amount of reported data breaches and complaints might be only the tip of the iceberg. Some data breaches are not noticed by organisations or not reported to us, and for individual persons it is often not at all clear how their personal data is used or traded. This does not mean that we are powerless. In the last year, we have shown that despite our lack of resources, we were able to achieve great strides in the protection and promotion of personal data. We assisted and provided advice for the controversial corona-app, warned about the deficiencies in the system of the Municipal Health Services (GGDs), and investigated and confirmed cases of discrimination in the recent benefits affaire at the Dutch tax department.

> “individuals have to be able to gain back control on their own personal data.”

7. The Dutch DPA works with supervisors of all EU countries together in the European Data Protection Board. What can the Dutch DPA learn from the other countries in terms of the supervision on data brokering? Or do you feel that the other countries can learn from the Dutch DPA? If so, can you give an example?

All supervisory authorities strive to a harmonised application of the GDPR. Therefore, there is an active cooperation between the supervisory authorities. If necessary, specific cases are discussed. Together, an approach is determined. Unfortunately, the Dutch DPA is not the only one who is understaffed. For the coming years it is key that we can develop our cooperation and grow in capacity as joint European guardians of data protection.

8. What is the ultimate goal for the Dutch DPA regarding data trafficking? Are there also positive sides to data trafficking. For example, can we learn something from data trafficking?

As mentioned in our Focus 2020-2023, our goal is to ensure that citizens have control over their own personal data. To achieve this goal, data brokering needs to develop in a specific way. This means that data brokers need to be fully compliant with the GDPR and citizens need to know what rights they have and how to exercise those rights. Therefore, transparency is a key issue: individuals have to be able to gain back control on their own personal data. We aim to supervise, to (where necessary) enforce the GDPR and to educate citizens on their rights. In this way, we will enhance and stimulate innovative use of data.

As far as the illegal trade of illegally collected data concerns, the ultimate goal is to ban this entirely. However, we are fully aware that that is not only in our hands: we need more attention and awareness from organisations in information security, national and international cooperations with e.g. organisations in charge of cybersecurity and organisations in the criminal justice system.

As this shows, we must not forget the citizens. If we only talk about data brokering between the closed circles of organisations, companies and governments, the citizen gets lost. In the end, the purpose of our work is to protect citizens and their personal data. They are the reason why we do what

we do.

About the author

Cecile Schut Msc. MPA has been Director System Supervision, Security and Technology with the Dutch Data Protection Authority since January 2018. She is responsible for offering guidance to organisations and their data protection officers, the assessment of requests for prior consultations, codes of conduct and other GDPR instruments that stimulate organisations to become privacy-proof. In addition, her unit is responsible for high-quality and up-to-date knowledge in the field of security and technology which is necessary for the different supervisory tasks of the Dutch DPA.

Hans Schnitzler

On the misleading metaphors of the information age

Perhaps the most apt definition of privacy comes from the Dutch artist and Internet critic Tijmen Schep: "privacy is the right to be imperfect," he argues. This view of privacy is at odds with an ideology also known as computationalism. This is a philosophy of life that reduces the human mind to an information-generating machine, that sees a data problem in every social problem and that has replaced the belief in higher values with a belief in mathematical values.

With this bits and bytes approach to reality, one chases absolute control and predictability of everyday existence. In his book New Dark Age, James Bridle, a computer scientist, characterizes computationalism as a 'cognitive hack': decision-making processes and responsibility are transferred to machines, automated thinking - i.e., computation - replaces conscious thought, with the ultimate result that we increasingly act like 'perfect' machines. At least, that is the suggestion.

According to Bridle, computational thinking has now penetrated into the smallest capillaries of daily life. And indeed: in order to optimize daily life, the art of peeping has risen to unprecedented heights. All kinds of digital surveillance - from individual track and trace applications to the prying eyes of the tax authorities - have nestled themselves in the fabric of society. But the denser the system of data pipelines, the greater the chance of leakage or sabotage.

Even more important is the blind spot underlying computational thinking: the dominant technology of our time (information technology) is used as the paradigm for the basic structure of reality as a whole. For this matter, history has an important lesson to teach us. Think about it: it is of course no coincidence that the most important technologies of the Antiques (their water works) led them to understand the functioning of man in terms of bodily fluids. Nor is it a coincidence that at the time of the Renaissance, when clockwork and timepieces became widespread, people began to compare the essence of man with the workings of an 'artful and ingenious cog'.

> "After all, who buys a stupid refrigerator or decides to move to a stupid house or stupid city?"

'The explanatory metaphors of a given epoch incorporate the devices and spectacles of the day and reflect, probably in more subtle ways, the predominant social forms and everyday practices,' observes computer scientist John G. Daugman in his treatise 'Brian Metaphor

and Brain Theory.' In this, Daugman criticizes the frequent use of computer metaphors in the neuro and cognitive sciences and even dismisses them as a bandwagon effect. That is, a fallacy caused by the enthusiasm with which a majority runs after an idea or innovation. The metaphors may be patient, but their effect is real. This is especially true for those of the information age, simply because their metaphorical application, their actual reach, is through technologies that are more comprehensive, intimate and invasive than ever before. The creation of the Internet of Things, a world in which all objects and subjects are connected by invisible data wires and are therefore crowned 'smart', is the result of an industry that has successfully deployed the metaphorical use of the word 'smart'. After all, who buys a stupid refrigerator or decides to move to a stupid house or stupid city?

However, anyone who takes note of the history of technology, and the misleading role that metaphors play in it, cannot rule out the possibility that this semantic success will eventually prove to be one of the most influential misfires of technoscientific discourse. 'Smart' systems may well generate a certain kind of (selective) knowledge or facts, a certain kind of knowing, but that is of an entirely different order than the task of making sense of something or giving meaning to something. That task requires effort, is precarious and more often ends without ready-made or perfect answers.

It seems to me that there is every reason to replace predicates such as 'smart' or 'intelligent' with less ambiguous terms. Instead of a 'smart city' it would be better to speak of a 'pre-programmed city', and for the term 'artificial intelligence' it seems to me that 'machine comprehension' would be more appropriate.

There is much to be done to sober the machine discourse; demythologizing the smart device universe is perhaps the most appropriate route to greater understanding, and thus ultimately to greater grasp.

About the author

Hans Schnitzler is philosopher, author, columnist and speaker. He is the author of 'Het digitale proletariaat' (2015) & 'Kleine filosofie van de digitale onthouding' (2017) at De Bezige Bij, columnist for Follow the Money, former columnist at de Volkskrant. His essays and columns are published in NRC, NRCNext, Trouw and more.

Photo: Michiel van Nieuwkerk

News

Cooperation between the Netherlands and Japan in smart industry

During a three-day virtual trade mission, the Netherlands and Japan agreed to work together to strengthen smart industry in both countries. The theme of the mission is Digital Economy and will offer both countries a lot of opportunities for jobs and income. The mission focuses on the utilisation of innovative, digital technologies in the industry.

https://www.rijksoverheid.nl/actueel/nieuws/2021/02/09/nederland-en-japan-gaan-samenwerking-aan-voor-versterken-smart-industry

EDPS wants to prohibit targeted advertising based on tracking

The prohibition is the reaction from the head of the European Data Protection Supervisor (EDPS), Wojciech Wiewiorowski, to the legislative proposal on digital services of the European Commission. Because of the risks of targeted advertising on the Internet, the EDPS advises to think about additional regulation. Such regulation must eventually lead to a strict prohibition.

https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opinions-digital-services-act-and-digital_en

Data breach: 3.2 billion stolen passwords

Cybercriminals have published all the stolen e-mail addresses and passwords on the Internet in a bundle named: Compilation of Many Breaches (COMB). This might be the biggest data breach ever. It is a collection of data that hackers have stolen from various websites in recent years, such as Netflix and LinkedIn.
Cybernews is the research and news-site that found out this leak. Check here if your data has been leaked:

🌐 https://cybernews.com/personal-data-leak-check/

🌐 https://www.rtlnieuws.nl/tech/artikel/5214415/groot-datalek-bundeling-wacht-woorden-accounts

Microsoft Attack by China leads to another Global Crisis

A Chinese hacking group has broken into private and government computer networks through a popular email software for months. The hack was initially meant for a small number of victims, but expanded rapidly and has so far claimed at least 60.000 known victims. The result is a second cybersecurity crisis. Cybersecurity experts that fight against hacks like these state that they are getting frustrated and tired.

🌐 https://www.bloomberg.com/news/articles/2021-03-07/hackers-breach-thousands-of-microsoft-customers-around-the-world

The Dutch Tax Authority will not comply with GDPR until 2024

The State Secretary of Finance mentioned, during a debate on fraud detection by the Tax Authority, that the Tax Authority still needs four years to comply with the GDPR. This was revealed by a question from the member of parliament, Pieter Omtzigt, about which laws the Tax Authority had violated during the benefits affair.

🌐 https://fd.nl/economie-politiek/1372498/belastingdienst-voldoet-pas-in-2024-aan-privacywet

250.000 euro fine for Swedish Police

The Swedish Authority for Privacy Protection (IMY) found out that the Swedish Police Authority has processed personal data in breach of the Swedish Criminal Data Act when using Clearview AI to identify individuals. The infringement will cost them 250.000 euros.

🌐 https://www.imy.se/nyheter/police-unlawfully-used-facial-recognition-app/

INTERVIEW

Roel van Rijsewijk

The Socratic approach to technology adoption

Inspiring conversations with Ton Wagemans- Considerati

My previous kitchen table discussion ended with Christiaan Alberdingk Thijm's call to empower citizens to regulate technological developments. As a society, we struggle to set the boundaries within we can make optimal use of technology. How do we balance regulation and innovation?
Today I'm going to talk about this with Ton Wagemans, a lawyer, tech policy expert, professional balancer and a freethinker. He helps organisations to increase adoption of new technology with dialogue and experiments.

I meet Ton at my kitchen table in Landsmeer, where one of my children occasionally rushes by as Chase of Paw Patrol. He is the first guest to sit down at this table after I moved from Amsterdam. Originally a lawyer, but an entrepreneur at heart. Ton, founder and partner at Considerati, wants to make technology work for everyone and get the most value out of it. With his organisation, he advises leading international organisations on the policy, vision and communication needed to achieve this. He develops and bases his advice on research, talking to consumers and stakeholders and by testing new policies.

The internet's regulatory holiday

With a big cup of tea, we start the conversation. I would like to know where his passion for this subject of technology regulation comes from.
Ton begins: "After law school, I started a webshop with some friends. The lawyer in me started looking for general conditions for doing business on the internet. After a lengthy search, I discovered that these just did not

exist. I did find a code of conduct from the Electronic Commerce Platform (ECP). I approached them with the question: Why are you working on this? The director thought this was an interesting question and invited me over for coffee. This meeting led to a job as a lawyer at ECP, where I became secretary of the legal working group." With a glint in his eye, he says, "I considered myself lucky to be offered this job, because the webshop would probably not have survived the dotcom bubble." "The ECP was set up to enable the Netherlands to rapidly develop in the field of digital business. The platform aims to develop codes of conduct and communication. In the more than four years at ECP, I represented the Netherlands as an expert in the United Nations and the European Commission. Here, I have seen a lot and also thought about the balance that is needed to achieve good legislation. You want to make the best use of technology and prevent abuse. Shortly after I started at ECP my friend and co-founder of Considerati, Bart Schermer, also started and since then we have been working together on this cool mission." Smiling, Ton shows his mobile phone and adds: "Bart's number won the top position in my favourites list on my phone: we have been talking and thinking about this for over 20 years now."

"Nobody could explain to me what self-regulation of the internet actually meant."

"After a few years I was ready for a new challenge. For years I had been working on internet policy and regulation, but nobody could explain to me what self-regulation of the internet actually meant. The internet started with a kind of 'regulatory holiday'; it was small, nobody understood it and was unregulated. Now it has a huge impact on our daily lives. When technology becomes so vital, you need policies and regulations. So, I decided to research internet self-regulation at Oxford University."

I wonder if anybody does anything at Oxford but dream and remember - William Butler Yeats

With some professional jealousy, I imagine being in Oxford to study and think about self-regulation of the internet. I ask Ton about his experiences.

The memory brings a big smile on his face: "The three months in this academic environment surrounded by the smartest people were magic. The rich history, the old libraries, the colleges, just the whole atmosphere certainly contributed to this. I had been living with my wife for years and here I was thrown back on my own. They were months of reflection and thinking about what's next. I returned with an extra suitcase full of books I had read and many new insights. At Oxford, the idea was born that you have to make sure technology fits into society, so society as a whole can benefit from it. I firmly believe that technology can take us forward, but at the same time I also recognise that technology can have

undesired consequences. That's why we need to think carefully about regulations and frameworks that enable technological innovation with the right safeguards."
"After Oxford, I helped some companies to develop their own vision, policy and communications to achieve this. That's when I decided to start my own company to help organisations with this. And I phoned Bart to ask if he would like to join me. The aim was to support companies and governments not only in managing the legal aspects of technology, but also in their vision, policy and communications to have society accept new technologies without fear. We were very lucky that we immediately had a number of visionary clients who believed in our story. We have continued to grow ever since," he says with pride.

> "If you look at how essential information technology has become in our society, you have to make sure that technology benefits humanity."

Technology is omnipresent

Digital technology is developing exponentially. So fast, that we as linear-thinking human beings can hardly keep up. If you look at how essential information technology has become in our society, you have to make sure that technology benefits humanity. I am curious how Ton sees this.

"Never before so much has happened in the field of technology as in the last 10 years. The absorption of so many new things at this speed is difficult. At the same time, quick adaptation of technology determines the success of a society. Also, hot topics such like the environment and migration have a technical dimension; solutions to these kinds of big issues are never easy, but we need smart technologies to make them manageable. It is therefore crucial for politicians and policymakers to gain more knowledge on technology and consult the experts. If you look at the current political programmes in the Netherlands, they are hardly about digital transformation at all. They talk about employment, healthcare and education. These are the important themes, but information technology is a dominant theme for all of them," Ton states with determination.

Catch me if you can

What Ton says triggers me. Cees Verhoeven made the same statement at my kitchen table. If digital technology is everywhere, you cannot grasp it. Or regulate it as such. "Politics and regulation are territorial, while cyberspace knows no borders.", I add another dimension.

Ton responds: "This makes it more difficult to draw up and enforce policy and global principle-based standards are needed. In addition, technology is constantly evolving. Restrictive legislation is not desirable. You do not want to hinder or stop the progress that technology brings by over-regulating it. At the moment, there is no global governance for setting standards for technology, such as the use of algorithms. The United Nations, for example, is global but also very political and cautious. In any case, it is necessary to take practical action and regulate global technological developments both ethically and legally."

The digital 'poldermodel'

Globally, we need to work together to make proper policies that ensure the benefits of technologies for everybody. The topic of collaboration leads me to an idea I've been toying with for a long time and I would love to hear Ton's opinion. I briefly tell him my idea about an expansion of the mandatory data breach notification within GDPR. As far as I'm concerned, the mandatory data breach notification should be extended so that all information should be shared on breaches, threats and vulnerabilities so that others can learn to better protect themselves. Currently, the mandatory data breach notification seems to be mainly used for naming and

shaming, or worse, issue fines, while knowledge about why things went wrong and what we have learned is not shared. Companies should in fact share this information with each other, without the risk of damaging their reputation. Security companies must also offer the information they have freely and no longer sell it to the highest bidder. Finally, this mandatory notification and information sharing should also apply for government and the intelligence services. In this way, our national digital infrastructure becomes more resilient so we can benefit from technology in a secure way.

"I think that would be very good," Ton replies, nodding in agreement. "But the tricky thing is of course: who is going to process this information? It's a lot of work to collect, analyse and distribute all that information. How we would organize this requires careful consideration."
In my opinion, the Netherlands is a good environment to experiment with this. "We learned to work together to protect us from water, the same 'poldermodel' should work for cyberspace. We could set this up as a distributed network using smart encryption and blockchain-like concepts. That way, information can be shared anonymous without some central authority having to do all the work."

Ton is not yet convinced: "It really does depend on the implementation. I think everyone is in favour of sharing such knowledge, but the question is how to organise it in a way it works. You don't want everyone to put effort into sharing information with no follow up or anything in return. Besides, not all data breaches are worth reporting, so it requires some human editing. In addition, there are already some good structures in place. For example, many other countries would like to have an institution like 'our' NCSC and the Ministry of Justice has recently started a team that is fully focussed on AI. The field is continuously developing," Ton continues.

The global technology arms race

But from another view we are far behind. In the media, China and the US are labelled as technology superpowers in competition. You often read about Europe's challenge to keep up. I am curious what to hear Ton's geo-political view of technology adoption and regulation.
Ton confirms the picture I paint: "America has of course marketed a lot of new technology and conquered the free world with Silicon Valley in a regulatory environment that fosters investments and innovation. China follows closely with many new developments in a more closed and highly regulated eco-system. The speed at which you implement technology is becoming increasingly important. Regulation is necessary in order to allow technology to take root. This is where Europe is particularly lagging behind; we are not known for our speed. We talk too long and lack pace. And yet that is necessary to maintain our position in relation to the other world powers. A good example is the introduction of the digital signature. It took us eight years to introduce it. In Singapore, it took only 1.5 years to implement. If that happens with every technology, at a certain point you fall too far behind. The countries that adopt technology faster will then also lead the discussion on its proper use."

> "This is where Europe is particularly lagging behind; we are not known for our speed."

Facebook's Supreme Court

I respond, "The GDPR is an example where Europe is leading the debate. We have set the standard on privacy for the rest of the world. What worries me is that most of the big tech companies are not from Europe and we are lagging behind. They determine what technology we use and their norms and values are programmed into it."
I see some frustration in Ton. "There is a lot of criticism on the big tech companies, but I believe they also want to do the right thing. For example, social media is now being judged for spreading fake news, but they never wanted to edit or filter content. Governments told them to take action against fake news and hate speech. They have long resisted this enormous responsibility. After all, it puts them in an impossible position. How do you set universal norms and values in a multi-cultural context, who has the moral authority to judge right from wrong? It's all new and nobody knows exactly how to do it."
I agree that you can't expect business leaders to make those decisions and Facebook is trying to solve this: "I read that Mark Zuckerberg wants to create some kind of independent Supreme Court, since they themselves do not want to determine what is or is not acceptable on their platform. Facebook is a global community of more than 2.5 billion global citizens, almost a country in itself with policies and regulations. Can this community, as a group, determine those norms collectively? The anarchist in me gets very enthusiastic about this form of community self-regulation. After all, the internet doesn't belong to anyone," I add to Ton.

Ton responds: “There is a lot of discussion about this amongst academics. The internet once belonged to no one, but we’re past that phase. The question is whether users should regulate themselves. In any case, good agreements must be made that are tenable and that take everyone’s interests into account. Don’t forget that your background often determines how you look at regulation. I notice this especially in my conversations with foreign students at Leiden University. They are all smart people, but they look at technology from their country’s perspective. They understand our individualism, but not everyone is a great supporter of it. Consensus is therefore difficult, if only within one country. And then you have to put it into practice.”

> “If you start forbidding everything and don’t dare doing anything, it won’t work either.”

Policy prototyping

And then we often learn that these regulations don’t work in practice and have unintended consequences. “The cookie law is a good example of good intentions, but everyone suffers from it and it does not work as intended. The user experience is compromised as a result.” I mention.

“That’s right,” Ton replies, “We are discovering it together, so you have to test and try. If you start forbidding everything and don’t dare doing anything, it won’t work either. At Considerati, we use policy prototyping. Based on all regulatory initiatives from different countries, we make a “red line law”. We then test this for a group of users in the product environment, like A/B testing. This provides feedback from people who have to work with it in practice with which you can adjust and optimise the rules.”

I am excited by this. This is the way to let the people decide. And information technology makes this feedback loop possible. “I think this is a great concept. By A/B testing legislation, we can renew the way we make all policies and information technology gives us the tools to do this. I can see that.”

> “Make your mistakes small, fast and cheap.”

Philosophising in the Twiske

Ton says he also belongs to the free thinkers. “It is important that everyone starts thinking and discussing technology and rules that work in practice. I notice that the choices are often simplified to yes or no, like you have to choose between for example privacy and security. But it is not a zero-sum game. It’s about learning to adopt technology with the safeguards you need so that it doesn’t harm anyone,” he argues passionately.
I fully agree with Ton, like the referendum on the ‘Sleepwet’ in 2018: “Yes or no is too simple, by presenting the problem in that way, you don’t get a good result. Few people fully understood it. It is not a yes or no choice, but about finding the right checks and balances. This also applies to the policies and legislation surrounding technology; finding the right balance is always a challenge. We have to keep discussing and learning here. By implementing and testing policies more quickly, you can learn and keep improving. Make your mistakes small, fast and cheap.”

Ton nods affirmatively: “We want to make the best use of the technology, but then there must be room for experimentation in terms of policy. Regulation is not easy. You have to find the balance to help society further. Testing policy helps us do this, which speeds up the adoption of technology.”

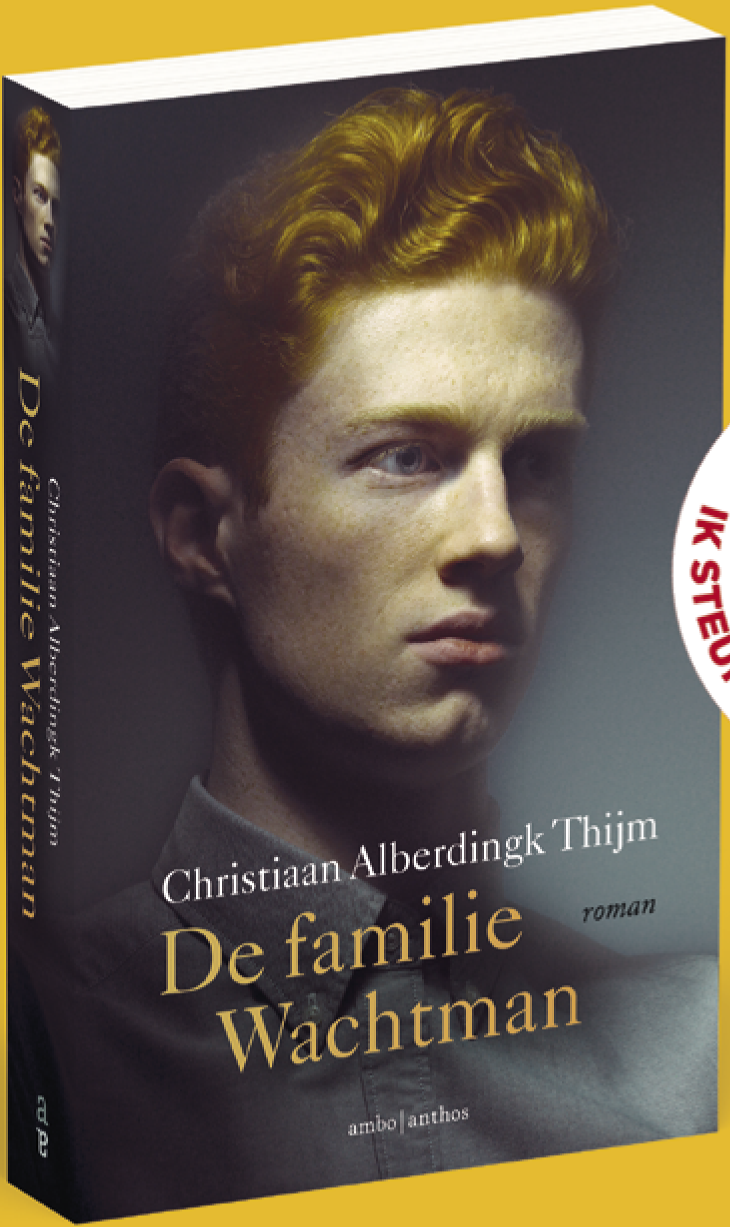
Ton doesn’t claim he has the answers, but the Considerati mission is to consider all the options. He calls for dialogue and experimentation to discover the answers. And on this Socratic ending, we agree to continue our philosophising on technology and ethics during a corona-proof walk in the Twiske.

About the author
Roel van Rijsewijk is a cyber security consultant and evangelist with over 20 years of experience helping organizations become cyber resilient. He is a key note speaker and author of ‘Cyberrisico als Kans’ (The Upside of Cyber Risk).

A current novel about identity and privacy

★★★★

‘Suspenseful, current
and urgent.’ – *De Telegraaf*



IK STEUN MIJN BOEKHANDEL

ambo|anthos

www.amboanthos.nl

Rob van den Hoven van Genderen

The vaccine inoculation passport, ticket to..?

On the initiative of Greece European, countries are discussing the enactment of a ‘vaccination passport for Covid-19’, in the first place to allow vaccinated person to visit the starving European tourist destinations. Will this be the start of a societal partition within Europe and the Netherlands between ‘free traveling’ vaccinated people and locked down ‘non vaccsers’?

The new chapter in the fight against Covid-19 has started, the vaccination, hopefully the beginning of the end, although there are not enough vaccines delivered by the producers because we wanted to have a bargain and are one of the last to be delivered to. The over-organized Netherlands is the last in Europe to begin with vaccination anyway. The Netherlands is so well organized that decision-making is stranded by the segmented organization. Who determines the policy: the Minister, the security region, the laboratories, the State Health institution (RIVM,) OMT or the Municipal Health Service (GGD)? Which group first: the elderly or start with the 1st line medical care staff?

In addition to these selection problems, which category of the population will be given priority in vaccination, social and constitutional problems will also arise. We are already accustomed to anti-corona regulations restricting our fundamental rights unequally: no freedom of demonstration, no family gatherings or free association and assembly except when it comes to religious events. In the latter case, the participants may infect each other unmasked and singing. The restrictions that may be imposed by the government, also constitutionally underpinned, to protect public health apparently do not always have the same objectives. The vaccinations that will have to stop corona can be considered also a violation of physical integrity and requires the consent of the person concerned and a firm formal legal basis. A vaccine is a weakened, artificial form of infection that triggers the production of antibodies if one is infected. It is currently estimated that about 70% of the Dutch will get vaccinated, 30% will not. The government portrays this group of non-vacs as negative, almost a-social. The opposition though, cannot be explained solely by mistrust in the effect of the vaccine, religious considerations, possible side effects or an a-social attitude of the population. There are now millions of people who already have been infected by corona and the majority have already developed antibodies in a natural way and for whom vaccination therefore has no added value. There has been a failure to register those healed persons (with permission). In addition, there is a large group of people who were not tested for corona in the spring - and also during the last wave - due to the lack of testing capacity but, given the symptoms, did have corona. This group cannot be found at all. It would therefore be wise to test for antibodies, as this is the goal to be achieved by vaccination. To vaccinate all these people as an embarrassment solution is a waste of vaccines - maybe welcomed by the pharmaceutical industry - and, moreover, contrary to the fundamental right to physical integrity. The policy is aimed at isolating the people who are potentially at risk of infection. A negative test statement is often required for entry to foreign travel. Not a watertight, but a logical and acceptable measure. But a vaccination statement or passport could also provide for this. The question is whether such an explanation could be required beyond touristic destinations for more general access to all kinds of social, cultural and commercial environments such as government institutions, theatres and shops, excluding unvaccinated individuals.

In principle, private parties may themselves determine which access requirements are set as long as this is not in

conflict with the law. Can we accept a dichotomy in society between people who have proof of vaccination and people who have not been vaccinated against Covid-19? Is this a form of discrimination that can be justified in the context of public health and therefore not in violation of the prohibition of discrimination, as laid down in Article 1 of the Constitution? When a vaccination certificate becomes necessary for access to cinemas, shops, concerts and travel abroad - and those who do not have the certificate are banned from doing so - there is a dangerous precedent. Who should issue such a statement? The Communal Health Services (GGD) and GPs? And what form should that statement take? Can it be securely linked to the digital identification? Already massive leaks of personal data were discovered within the Covid testing system (by GGD). In any case, if there were to be a registration, it requires a different approach than the simplistic distribution of a paper and easily falsified vaccination certificate in order to regain 'normal' access to society in all its aspects. An obvious requirement of catering and event organizations for such a vaccination certificate may not be accepted by the government without further ado. A careful and more carefully considered access policy for risk-free persons to public and enclosed spaces and activities is required in the return to a 'normally' accessible society. In doing so, the step of simply creating a dichotomy between a vaccinated and an unvaccinated part of society should be avoided. It is likely that the government will be happy to ignore this problem. I consider a careful policy based on yet another amendment to the corona emergency law to create a basis for both the registration of vaccinees and the exchange of sensitive data between health institutions and relevant third parties extremely unlikely. With a vaccination coverage of 60% with voluntary vaccination, the chance of further spread of the pandemic is extremely small in view of the foregoing, and a separation of society between vaccinated and unvaccinated becomes completely unnecessary and not acceptable. It is extremely important that a harmonized European position on this issue will be achieved so that not every country sets its own rules. Schengen will have to be applied again as it is intended. But that will turn out to be wishful thinking.

> "It is likely that the government will be happy to ignore this problem."

About the author

Robert van den Hoven van Genderen is professor AI Robotlaw at the University of Lapland, director of the Centre for Law and Internet at the Law Faculty of the Vrije Universiteit and president of the Netherlands Association for AI & Robotlaw. Before his academic positions he worked a.o. as director Regulatory affairs in the Telecommunications industry.

Bernold Nieuwesteeg

Secure software: a shared responsibility?

Today, many flaws in the security of an IT infrastructure are caused by vulnerabilities in software. Software vendors regularly release updates to address known vulnerabilities. Yet we still see many software developers for whom security is more of a closing item than a spearhead. At the same time, we see that software users do not always perform updates on time and are thus vulnerable to cyber attacks. And if an attack does eventually happen, whose responsibility was it to have security in order? Was it the software vendor who supplied an unsafe product? Or was it the customer who had to take measures to protect themselves better? And how long does a software vendor have to provide its software with security updates?

These are all issues to which there is no simple answer. Yet the answers are very relevant, because more and more discussions are being held about legally establishing responsibilities in this cybersecurity, in other words: software liability.

> “We see that software users do not always perform updates on time and are thus vulnerable to cyber attacks.”

Software liability is about the possibilities of recovering cybersecurity damage in a B2B relationship. An example of this is an organization that is hacked because it uses insecure software from a supplier and suffers damage as a result. For example, hackers could use the vulnerability in that software to gain access to sensitive company data. And who is responsible then? The software supplier who delivered an unsafe product? Or the buyer of the software?

Recent research showed that the legal and economic barriers are often too great to make redress practically possible. Some important barriers are:

The duty of care. Damage can only be recovered if there is a violation of a “standard”. In the case of cybersecurity liability, these are minimum cybersecurity requirements. For example, these requirements are laid down in the contract or are reflected in the nature of the B2B relationship.

Damage. Obviously there must be (quantifiable) damage in order to be able to recover it. Reputational damage, for example, is often difficult to quantify.

Causality. There must be a causal link between the incomplete provision of cyber security and the damage suffered by the purchaser.

Burden of proof. In principle, the burden of proof lies with the party that wishes to recover the damage. This makes the possibility of recovering damage enormously difficult because the purchasing party cannot simply look into the ICT systems of a supplying party.

Bargaining power. Large parties generally exclude liability completely and also limit their duty of care. At least in the perception of SME parties, there is little to no negotiation about this.

We have a few lines of thought to improve the system:

Clarify agreements on cybersecurity with the sector so that it becomes clearer when a supplier does not comply with the agreements regarding cybersecurity. For example, the development of a model SLA that can be used when entering into a contract with a supplier.

Simplify the burden of proof by making it easier to prove

both damage and the link between the damage and the deficient cybersecurity.
However, one could also think about more severe measures for large multinationals such as Google, Microsoft and Amazon. Within a B2B relationship, freedom of contract is important (and so the government should, in principle, be restrained in intervening in the market), unless, for example, there is such a difference in bargaining power that the strong party can abuse this. In those situations, we could build on the following mindset: mandatory offering of a form of liability by major international software providers, so that not all liability is excluded by default. Or, drawing up standard clauses that suppliers and therefore multinationals must adhere to.

As said, the discussion about the (distribution of) software liability does not have simple answers. It is not a very sexy topic either. However, in the end, cybersecurity is all about the proper distribution of responsibilities in order to give parties the right incentives and information that allows them to implement the most effective cybersecurity measures. And the discussion about responsibilities inevitably has a legal component. We hope that this important topic will be discussed in more depth in the upcoming years as the cybersecurity debate continues to mature.

About the author

Petra Oldengarm studied technical computing science at Groningen University. Petra is an independent strategic cybersecurity consultant and Director at Cyberveilig Nederland (Association of the Dutch cybersecurity sector). She previously worked as innovation team manager at KPN Research, department manager at the Ministry of the Interior, manager IT at ECN and as Director Cybersecurity at Hoffmann.

About the author

Bernold Nieuwesteeg is director of the Centre for the Law and Economics of Cyber Security at Erasmus University and partner at CrossOver. He regularly advises public and private actors on their cyber security strategy and studies methods to increase knowledge about sensible investments in cyber security.

About the author

Dr. Rutger Leukfeldt is Senior Researcher and the cybercrime cluster coordinator at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR) and Academic Director Centre of Expertise Cybersecurity of The Hague University of Applied Sciences. His work focuses on the human factor in cybercrime and cybersecurity.

Reports & Regulatory

The Cybersecurity Certification Landscape in the Netherlands after the Union Cybersecurity Act

The National Cyber Security Centre in the Netherlands recently published a study with the title "The Cybersecurity Certification Landscape in the Netherlands after the Union Cybersecurity Act". The research for the study was conducted by researchers of the Law, Technology, Markets, and Society (LTMS) department of Tilburg Law School and explored what the impact is of the new EU cybersecurity Act on the Dutch certification market. The study looked into the national and European legislation on cybersecurity, and gathered the views of government, industry and certification stakeholders. Also, the study inventoried potential roles for the NCSC in this evolving landscape.

🌐 **https://www.ncsc.nl/binaries/ncsc/documenten/rapporten/2020/oktober/2/the-cybersecurity-certification-landscape-in-the-netherlands-after-the-union-cybersecurity-act/NCSC_CYBERCERT_FinalReport__20200730.pdf**

Paper about Cybersecurity information in annual reports

This paper provides the disclosure of cybersecurity information in Dutch annual reports, such as cybersecurity measures and cyber incidents, from a financial law and economics perspective. The results of the study show that although there is no strict legal obligation to do so, 87% of the companies mention cybersecurity or similar words in their annual report in 2018. However, only 4 out of 75 companies disclosed more than six specific cybersecurity measures, while openness would generate the highest surplus for society from a social welfare perspective. The analysis aims to propel the debate on stimulation of selfregulation or possible obligations in financial law concerning cybersecurity in annual reports.

🌐 **https://www.sciencedirect.com/science/article/abs/pii/S0267364920301187**

WODC-report: Security-by-Design in the vital sector

This report describes the results of research into the possibilities of the Secure-by-Design design of Operational Technology (OT) for the Vital Infrastructure. The National Cyber Security Centre (NCSC) considers the disruption or sabotage of services and processes, on which governments and society depend, one of the main and real cyberthreats. The vulnerability of Industrial Control Systems (ICS) has the special attention of the NCSC, because they are so widely used in the Vital Infrastructure of the Netherlands. The report gives answers to how Design Thinking could be applied in the Vital Infrastructure when designing new operational technology and how, where and when Design Thinking can have a place in the design of systems.

🌐 **https://repository.wodc.nl/handle/20.500.12832/3007**

Adopted resolution on Digital Security

This resolution emphasises the core task of the Dutch city councils for Digital Security. This was initiated by the adoption of the resolution "Information security as a prerequisite for a professional municipality" in 2013. The essence of this resolution is to invest in increasing resilience and that municipalities must cooperate in prevention, in crisis situations and in the aftermath. Only if municipal administrators, councillors and civil servants are aware of their responsibility for digital safety, they can fulfil these tasks.

https://vng.nl/sites/default/files/2020-12/resolutie-digitale-veiligheid-versie-3-december-2020.pdf

Governments' reaction to international legal order in the digital domain

The Netherlands is actively working to improve the international legal order in the legal domain. The members of the VVD party think positively about this matter, but want to eliminate any ambiguity. They ask questions about the commitment of the Netherlands to the international protection of data relating to individuals, now that by collecting data that is currently distributed internationally, a person's entire life can effectively be mapped out, with all its consequences for the safety and freedom of individuals.

https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2021/02/09/antwoorden-op-vragen-over-kamerbrief-over-internationale-rechtsorde-in-het-digitale-domein/vragen+over+de+internationale+rechtsorde+in+het+digitale+domein.pdf

Governmental letter about Privacy by Design and open source

This letter contains a reply from the State Secretary for Home Affairs to a motion that was held during the debate of February 3 about the privacy leak from the Public Health Service's systems. The State Secretary pleads for privacy by design and open source in the context of the core principles that are fundamental to the functioning of the public sector: privacy protection, security and reliability.

https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2021/02/09/kamerbrief-over-privacy-by-design-en-open-source/kamerbrief-waardering-over-privacy-by-design-en-open-source.pdf

Supreme Court: Unlocking smartphone with suspect's thumb is permitted

Police officers may force a suspect to place his finger on the fingerprint scanner of his smartphone in order to gather evidence. They may use light, physical coercion. The Supreme Court sees no difference with, for instance, taking a blood or urine sample. The Supreme Court confirms the decision of the court.

https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2021:202

Peter van Schelven

Data security: what about your IT-inventory?

Do you know all the servers, desktop computers, software, networks and other IT-assets that are around in your company? In case your job is within a large organization it might very well be conceivable that an up to date and easily accessible inventory of the entire IT-infrastructure is lacking. If so, this will undermine the protection and security of systems and data. Without such an overall inventory it may be troublesome to respond to cyber incidents swiftly and effectively.

Cyber incidents become more commonplace. An example: Maastricht University. Just before Xmas 2019 the University was hit by a severe and high-profile attack of ransomware. The criminal attack and its severe impact were frontpage news in the media. Scientific research and education were blocked for several days. It took the University nearly 200.000 Euro to pay a ransom in order to receive the key that was necessary to decrypt the encrypted data files. Immediately after the attack management of the University set up an incident response program, in which a reputable external incident response provider was engaged.

Lessons learned: a central CMDB needed

The task of responding effectively to the severe cyber incident was felt to be 'gigantic', as we can read in the lessons learned, published by the University in a well-documented report from February 2020. The report makes clear that addressing the incident was impeded due to the fact that the University did not have an entire inventory of all IT-systems and backups. In IT jargon: a central Configuration Management Database (CMDB) was lacking. Investigations were first needed to find out that 1,647 Linux and Windows servers and 7,307 workstations were included in the IT-infrastructure of the University. Eventually, it turned out that 267 servers from the Windows domain had been affected by the ransomware attack.

> "For nearly every cyber incident new spreadsheets with relevant IT-assets have to be created."

The absence of a central and up to date CMDB is a deficiency we also can find in lots of other organizations. Because of this, for nearly every cyber incident new spreadsheets with relevant IT-assets have to be created. Reactive and ad hoc governance. Sometimes those organizations only have dozens of spreadsheets that attempt to be a CMDB-like administration; any central point for insight being absent. This may be the result of immature security practices.

Without a central, up to date and complete inventory of IT-assets, organizations may not be able to react adequately to cyber incidents. It delays finding the cause of incidents and it retards creating appropriate fixes. Besides that, the absence exposes the organization to the risk that the impact of a cyberattack cannot be fully understood. Cyber robustness implies that your organization has a clear overview of its IT-infrastructure. So, a well maintained central CMDB is a key element in managing cyber risks.

From that point of view the absence of an adequate central CMDB may be at odds with legal obligations in the field of information security. If your CISO, your IT department or your Board does not have a rapidly

available and detailed insight in the IT-infrastructure, causing any incident response hindrance, this may have ramification under article 32 of the General Data Protection Regulation (GDPR). This article covers information security in the processing of personal data. A central CMDB is needed to make a solid first step to restore the availability of IT-systems and the access to personal data. As article 32.1 sub b and c GDPR reads, ensuring the resilience of processing systems and related services is an essential obligation. In plain wording: computers must be able to continue to work and non-availability must be kept to an absolute minimum.

CMDB: not only paperwork

Making and maintaining a CMDB is more than just dull 'paperwork'. On the contrary, it is an important instrument as part of your cyber security strategy. Besides providing a clear inventory of your IT-assets, a CMDB may also be a useful tool for describing and monitoring which software and systems will be patched automatically and which security updates are installed only after human intervention. In organizations like Maastricht University, where the number of software updates may well exceed the 100,000 on a yearly basis, such a tool is of utmost importance. A CMDB may also detail active and inactive systems, links with other networks and systems, geographic locations of IT and backup facilities. Such information may be crucial for a compromise assessment, containment, root cause analysis and business impact analysis.

However, in day-to-day operations implementing and maintaining a central CMDB can be a very complex and tough job. Within organizations hardware and software are often purchased - in whole or in part - on a decentralized level, e.g. in branches, subsidiaries or business units. Various silos within an organization may prevent an entire central inventory. Another possible complication: using the services of one or more external Cloud Providers. One can see the IT-infrastructure of a Cloud Provider as a 'black box'. Trends like Bring Your Own Device and Internet of Things even more complicate matters. And even more basic: what exactly encompasses IT? Does it include stuff such as USB-sticks, digital cameras and mouses? All these things may be troublesome for making a perfect central CMDB.

The extreme complexity of and dependency on IT in organizations, the ever-evolving IT landscape and the increasing cyber security threats create challenges for IT departments, also in the light of meeting (legal) regulations and compliance needs. One cannot underestimate the importance of a CMDB as an instrument to operate in such an agile and dynamic context.

About the author

Peter van Schelven is a specialist in IT and IP law and the founder of his practice Bij Peter – Wet & Recht. As legal counsel, Peter deals with issues relating to data protection and cybersecurity. His area of expertise also extends to alternative dispute resolution and arbitrarion in IT.

Victor de Pous

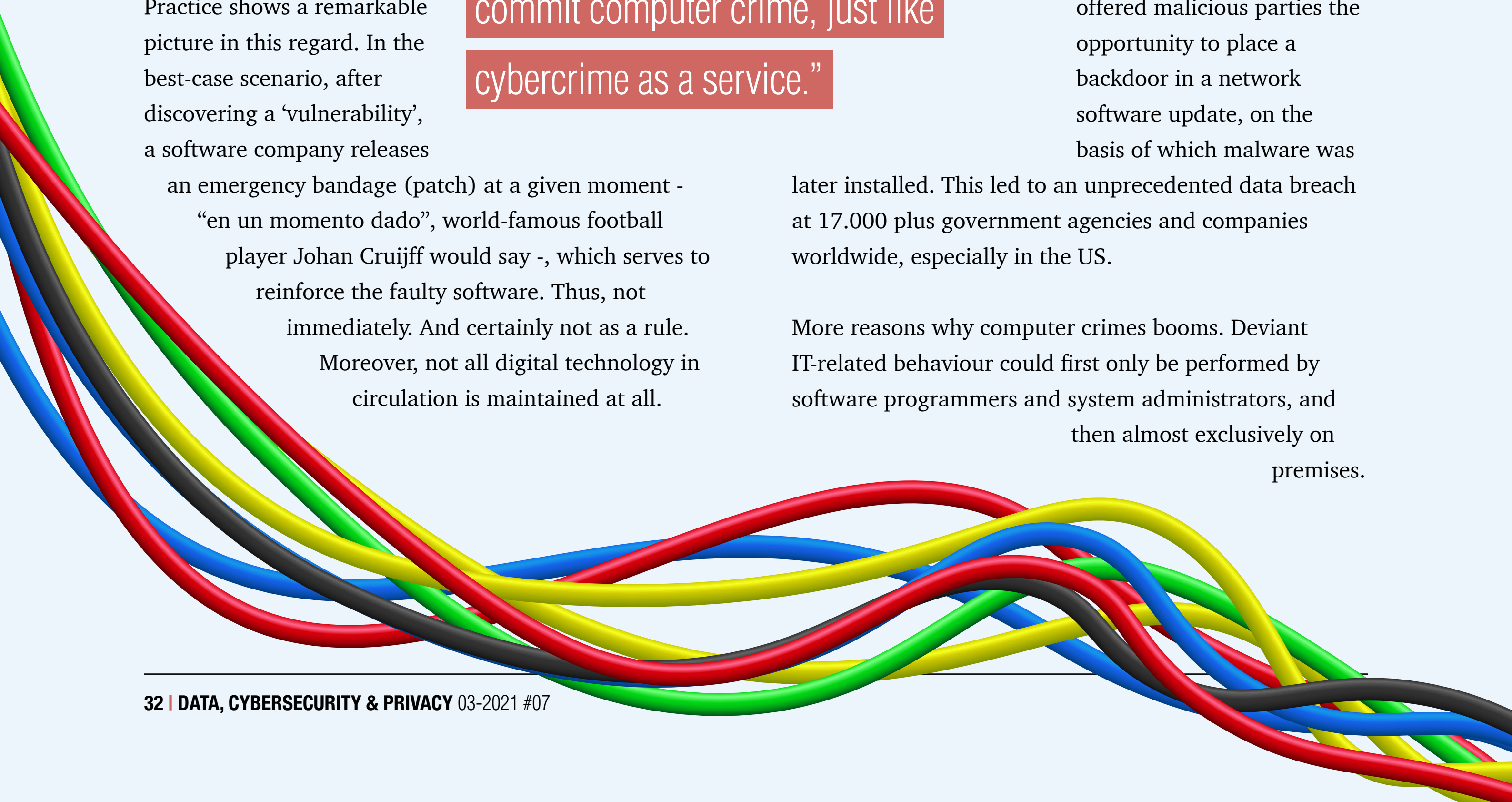
Digital shortcomings will lead to legal liability

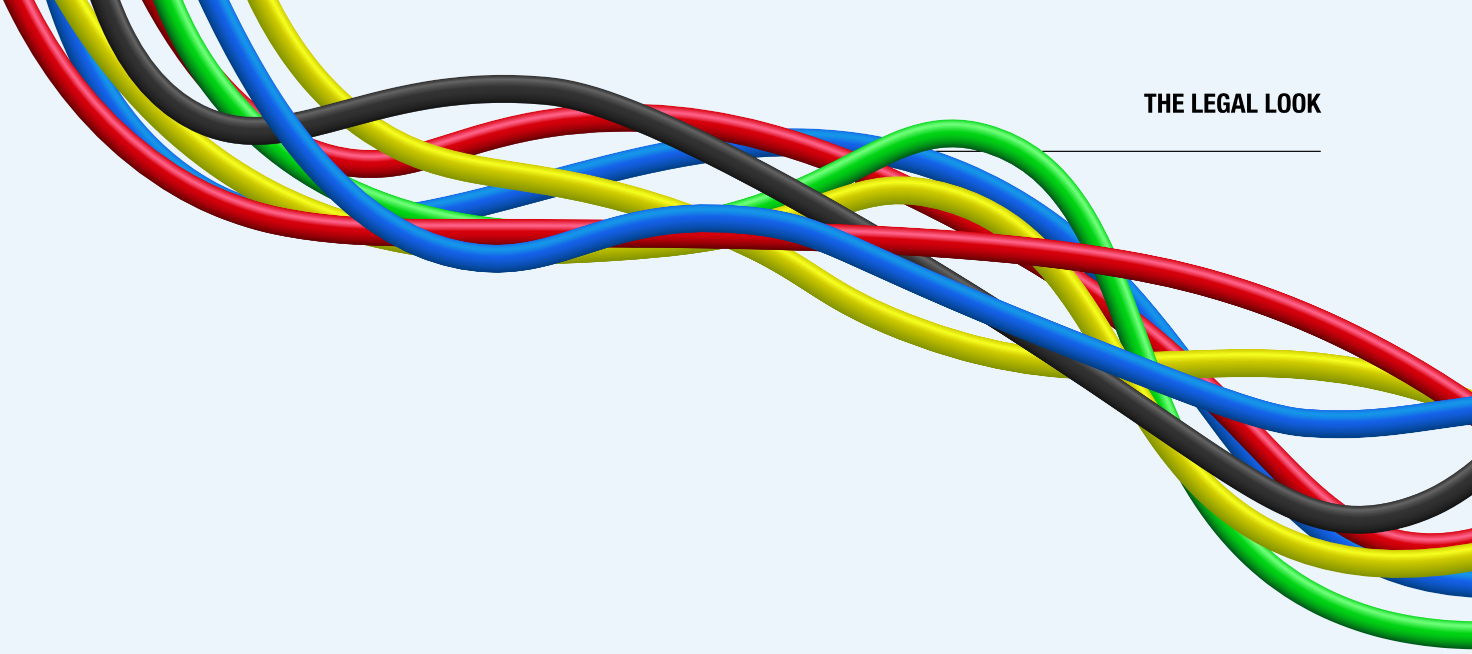
Five years ago, the Dutch Public Prosecution Service (Openbaar Ministerie) expected that by 2021 half of all crime in the Netherlands will be IT-related. Historical words. Hard data about what once and then reluctantly surfaced as 'computer crime' are barely available today. The cause remains largely unchanged. The willingness to report a digital crime to the police is still lacking, and this partly has consequences for the protection against this type of deviant behaviour. Nobody knows whether the tipping point will be reached this year. However, various signals from society give a strong indication that computer crime is rampant — and has profound consequences, such as caused by ransomware or digital espionage. First of all, the factor that IT became ubiquitous is important indeed. Subsequently, digital quality invariably falls short. Practice shows a remarkable picture in this regard. In the best-case scenario, after discovering a 'vulnerability', a software company releases an emergency bandage (patch) at a given moment - "en un momento dado", world-famous football player Johan Cruijff would say -, which serves to reinforce the faulty software. Thus, not immediately. And certainly not as a rule. Moreover, not all digital technology in circulation is maintained at all.

> "Anyone can buy technical resources to commit computer crime, just like cybercrime as a service."

That digital quality shortcomings are making individual users, organizations and society more vulnerable than necessary and computer crime much easier to execute, follows also from two major incidents. One relates to Citrix's security vulnerabilities in Application Delivery Controller and Citrix Gateway that became known in December 2019. More than a hundred Dutch healthcare institutions alone use Citrix and were vulnerable due to this leak. Some government and private sector organizations shut their systems down, because of active attacks. Six month later Home Affairs deputy Minister Knops wrote to Parliament that the national government has, as far as is known, the digital incident under control. The other incident is of even greater size: the Solarwinds hack, occurring mid-December 2020. In this case, poor security management offered malicious parties the opportunity to place a backdoor in a network software update, on the basis of which malware was later installed. This led to an unprecedented data breach at 17.000 plus government agencies and companies worldwide, especially in the US.

More reasons why computer crimes booms. Deviant IT-related behaviour could first only be performed by software programmers and system administrators, and then almost exclusively on premises.





Today, anyone can buy technical resources to commit computer crime, just like cybercrime as a service. Everything remotely thanks to the Internet, including the act itself. Add to that the circumstance that digital threats are no longer limited to the traditional malicious parties (individual criminals, organized crime and state actors), as the regular business community shows through the use of fraudulent software (code with hidden functionality) and for example activists with fake news.

But it all starts at the beginning. A society that has become largely or completely dependent on the availability, proper functioning and further development of IT should not neglect digital quality. Yet, that is exactly what has been happening for decades. One aspect of this concerns security, starting with the technology itself. Although the cabinet has so far failed to introduce a special legal liability for unsecure computer programs in Dutch law, as agreed in the coalition agreement of 2017, we also point to a ray of hope here. In response to the notorious Citrix vulnerability the Dutch Safety Board (Onderzoeksraad voor Veiligheid) has set to work. In doing so “special attention is given to the governance of digital security” in our country and the Board is also taking into account other incidents. “Which parties, public and private, have what responsibility and authority to safeguard digital security and how have they been used to limit the consequences of this leak?”

We repeat that the primary responsibility for — the assurance of — secure software lies with the software company. After all, the maker must work carefully. But the investigation can lead to more leads for legal liability. The Board will probably follow the line of shared responsibility. Then, all parties involved — manufacturer, reseller, user and government — have a task. Justice Minister Grapperhaus said in 2019 that he wants to be able to intervene at companies if the security patch made available by the supplier is not installed or not installed quickly enough. We previously called this failure to act as ‘digital neglect’. A last development. The Telecom Agency has rightly been concerned about embedded software for several years. On August 26, 2020, it published eight ‘simple requirements’ for the manufacturer and trader that can greatly improve the cyber security of smart equipment. Although the European Radio Equipment Directive (2014/53/EU) still does not contain legal minimum requirements for digitally secure IoT hardware, these and other criteria also currently provide tools for legal liability. The bottom-line: improvement of digital quality must apparently be primarily enforced by law.

About the author

Victor de Pous is an Amsterdam-based corporate lawyer, legal analyst and researcher since 1983. He has over thirty years of experience in the legal and policy aspects of digital technology, information processing and the information society.

Photo: Arvid de Windt

Willeke Kemkers, Adriano Chaves

Brazil's new privacy initiative; national law with global implications

An overview

On August 15, 2018 the text of the Lei Geral de Proteção de Dados Pessoais (LGPD) was published. After two years, during which the planned entry into force changed multiple times, the LGPD came into force on September 18, 2020. The provisions regarding administrative sanctions and penalties are however not yet in force. These will enter into force on August 1, 2021. The National Data Protection Authority (Autoridade Nacional de Proteção de Dados – ANPD), was only recently installed on November 6, 2020, when its directors took office.

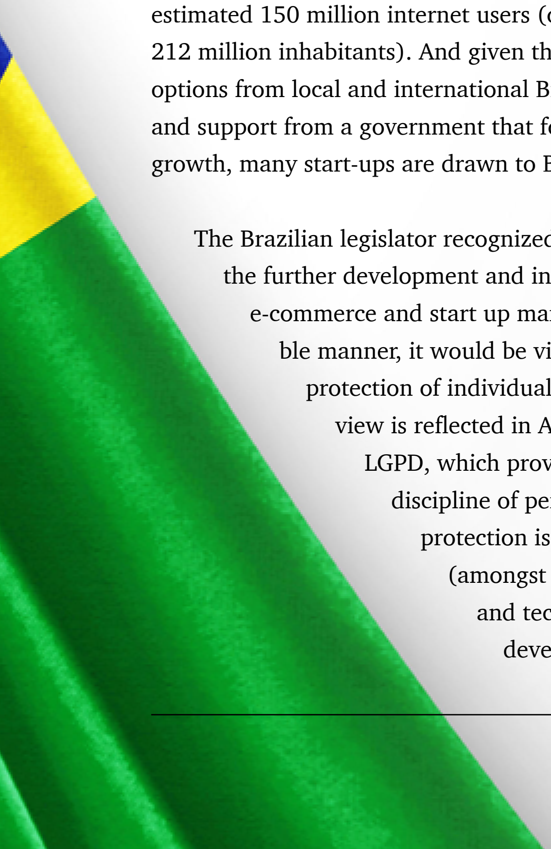
Background

Prior to the LGPD, Brazil had generic privacy provisions in several laws – such as the Brazilian Constitution, the Civil Code, the Internet Civil Act, and the Consumer Defense Code – but not an all-encompassing data protection law such as the EU General Data Protection Regulation, the GDPR. For many years, legislators and members of the civil society attempts to enact a broad data protection law were unsuccessful. However, the enactment of the GDPR in Europe and Brazil's goal to join the Organization for Economic Co-operation and Development (OECD) resulted in the LGPD finally being enacted.

> "Brazil is the fourth largest internet market in the world."

While some may be surprised to see Brazil enacting a law much like the GDPR, it is important to note that Brazil is the fourth largest internet market in the world, with an estimated 150 million internet users (of a total of around 212 million inhabitants). And given the investment options from local and international Brazil-centric funds and support from a government that focuses on business growth, many start-ups are drawn to Brazil.

The Brazilian legislator recognized that to support the further development and innovation of the e-commerce and start up market in a sustainable manner, it would be vital to ensure the protection of individuals' privacy. This view is reflected in Article 2 of the LGPD, which provides that the discipline of personal data protection is grounded on (amongst others) economic and technological development and innovation and free enterprise, free competition and consumer defense.



Who must comply

The LGPD applies to processing activities of personal data, carried out by a natural person or a legal entity of public or private law, irrespective of the means, the country in which its headquarter is located or the country where the data are located, provided that:
(i) the processing operation is carried out in Brazil; or
(ii) the purpose of the processing activity is to offer or provide goods or services or the processing of data of individuals located in Brazil; or
(iii) the personal data being processed were collected in Brazil.

Similar to the GDPR, the LGPD does not apply to data processing activities in specific situations, for example if a natural person processes personal data exclusively for private and non-economic purposes and if processing activities are carried out for purposes of public safety, national defense, state security, and investigation and prosecution of criminal offences. The LGPD provides, again similar to the GDPR, that processing activities for these purposes shall be "governed by specific legislation, which shall provide proportional and strictly necessary measures" in order to protect the legal interests and principles involved.

It is important to note that like the GDPR, the LGPD has an extraterritorial scope, and applies to global businesses that meet the above criteria even if the company does not have an establishment in Brazil.

What & who are protected

Similar to the GDPR, personal data is defined as "any information regarding an identified or identifiable natural person". Also similar is the definition of sensitive personal data, being: "sensitive personal data: personal data concerning racial or ethnic origin, religious belief, political opinion, trade union or religious, philosophical or political organization membership, data concerning health or sex life, genetic or biometric data, when related to a natural person".

In order to refer to the natural person whose data is involved, the LGPD also uses the term data subject, which is “a natural person to whom the personal data that are the object of processing refer to”.

The definitions of controllers and processors are in essence identical to those of the GDPR, as a controller is a “natural person or legal entity, of public or private law, that has the power to make the decisions regarding the processing of personal data”. A processor is a “natural person or legal entity of either public or private law that processes personal data in the name of the controller”.

Processing Obligations

Companies subject to the LGPD that process personal data must comply with data processing obligations similar to those under the GDPR:

1. Processing of personal data is subject to ten principles (such as purpose limitation and data minimization), which are partly similar or related to the GDPR’s principles. One principle is fairly new, which is the nondiscrimination principle (the impossibility of carrying out the processing for unlawful or abusive discriminatory purposes).

2. Processing of personal data must be based on one of 10 legal bases, which include the data subject’s consent, an obligation to comply with a regulatory obligation, the execution of a contract, legitimate interest, or the protection of credit. Different from the GDPR is the legal basis for the protection of credit. Processing of sensitive personal data (highly similar to the GDPR’s concept) can be legitimized on 8 legal bases, including consent and compliance with a legal or regulatory obligation (but not on legitimate interest).
The legal basis of the data subject’s consent must comply with several conditions, such as that if consent is given in writing, it must appear highlighted and that the burden of proof with regards to provided consent lies with the controller.

3. Different from the GDPR is the LGPD’s inclusion of explicit provisions concerning the duration of data processing activities. It must be ensured, for example, that data processing activities are terminated once it has been verified that the desired purpose has been achieved, that the processing period has ended or if a national authority has determined that there has been a violation of the LGPD. Data may be kept, however, if (amongst others) this is required for compliance with legal or regulatory obligations or if this is for the ‘exclusive’ use by the controller, provided that the data has been anonymized.

Data subject’s rights

Article 17 of the LGPD specifically refers to the right to ownership of data, providing that “Each natural person is assured ownership of her/his personal data, with the fundamental rights of freedom, intimacy and privacy being guaranteed, under the terms of this Law”.

Data subjects under the LGPD have rights which are very similar to data subjects under the GDPR. Under the GDPR, the data subject may request any of the following from the data controller:

- confirmation on the existence of processing activities;
- access to the data;
- correction of incomplete, inaccurate or outdated data;
- anonymization, blocking or elimination of unnecessary or excessive data, or data processed in breach of the provisions of the Law;
- portability of the data to another service or product provider;
- erasure of personal data processed with the data subject’s consent;
- information on the public and private entities with which the controller shared the data;
- information on the possibility of not giving consent and on the consequences of refusal; and
- withdrawal of consent.

Penalties

In addition to their (sometimes joint) liability for damages caused in case of breach of the law, controllers and processors will, as of August 1, 2021, be subject to the following penalties provided by the LGPD:

- warning;
- fine of 2% of the group’s turnover in Brazil (limited to R$ 50 million per violation);
- daily fine (limited to R$ 50 million per violation);
- public disclosure of the infraction;
- blocking of personal data related to the breach;
- elimination of the personal data related to the breach;
- suspension of operation of the database;
- suspension of data processing activities; and
- prohibition of data processing activities.

The ANPD shall define the methodologies for calculation of the fines mentioned above, which shall be objective and contain a detailed justification of their elements, in compliance with the criteria set forth by LGPD.

Data breaches

The LGPD also touches upon data breaches, though the related obligations are a bit less stringent than under the GDPR. Article 48 LGPD provides that a controller must communicate "the occurrence of a security incident that may create risk or relevant damage to the data subjects" to the ANPD and the data subject.

This communication shall be done in a 'reasonable' period of time and must contain the requirements as set out in the LGPD. After the notification, the national authority verifies the seriousness of the incident, and if needed for the protection of data subject's rights, it can order the controller to adopt additional measures. All this is expected to be further regulated by ANPD, as further commented below.

International Transfers

Article 33 of the LGPD lists the situations in which an international transfer is allowed, some of which are similar to those under the GDPR. These situations include transfers to countries and/or international organizations with a level of data protection adequate to the LGPD (the adequacy level shall be evaluated by the ANPD), and when the controller provides appropriate safeguards, such as standard contractual clauses and Binding corporate rules, certificates and codes of conduct which shall be defined/verified by the ANPD.

An important task of the ANPD is to provide clarity about countries which are deemed as offering an adequate level of protection. Until the ANPD takes the measures required to allow companies to perform international data transfers under the other legal bases provided by the LGPD (e.g. adequacy decisions, Binding Corporate Rules and standard contractual clauses), companies need to rely upon another basis, such as consent, to transfer personal data outside Brazil or assume some risk.

DPO

The role of the professional in Charge of Data Processing (encarregado pelo tratamento de dados pessoais – 'DPO') is similar to that of the data protection officer under GDPR. However, the LGPD establishes that all data controllers shall appoint a DPO, who may be an individual or a legal entity and whose identity and contact information shall be disclosed publicly, in a clear and objective manner, preferably at the controller's website. Also, in principle, the DPO cannot be held liable under the LGPD – the law sets forth liabilities and penalties only for controllers and processors.

Although the LGPD does not determine whether the DPO needs to be in Brazil, it is expected that such DPO must be able to provide information in Portuguese, based on the principles of the Brazilian consumer protection rights, and to interact closely with the ANPD and data subjects in Brazil. Moreover, it is reasonable to assume that ANPD (when installed) or Brazilian courts (when analysing cases under the LGPD) might require the DPO to be

"The first lawsuits are already being filed by individuals or state prosecutors."

resident in Brazil or consider the lack of a local DPO as a negative factor when establishing penalties.

Children and Teenagers

Important to point out is that processing of personal data related to children and teenagers must be carried out in their best interests and, if related to children, shall only be based on the consent of one of the parents or guardians, save for specific exceptions set forth by the LGPD. In the event of such processing, the controller must publicly disclose information about the collected data, how it is used, and the procedures for the data subject to exercise their rights under LGPD.

News / Lookout

On January 27, 2021 the ANPD issued its regulatory agenda for the next 2 years, providing that the main guidance and regulations must be issued on such two-year period. The agenda shows that the ANPD will first focus on certain items such as exemptions for small businesses and startups, regulations on data breaches and on the calculation and application of the administrative penalties. Issues such as international data transfers and further obligations of DPO's are expected to be regulated only in 2022. In this regard, the ANPD has already opened a procedure to receive contributions for its future regulation on exemptions for small businesses and startups, which will soon be subject to a public hearing.

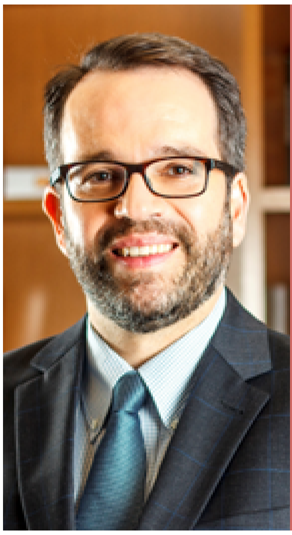
ANPD directors have been publicly stating that the authority will start with a more educative approach, without applying heavy sanctions initially.

Regardless of the ANPD actions, the first lawsuits are already being filed by individuals or state prosecutors. However, the number of data subject requests has been lower than expected, but this is likely to increase over time.

In short:

- The Lei Geral de Proteção de Dados Pessoais (LGPD) came into force on September 18, 2020. The National Data Protection Authority (Autoridade Nacional de Proteção de Dados – ANPD) was only recently installed on November 6, 2020, when its directors took office;
- The Brazilian legislator recognized that to support the further development and innovation of the e-commerce and start up market in a sustainable manner, it would be vital to ensure the protection of individuals' privacy;
- This article gives an overview of the most important rules and guidelines in the LGPD in comparison with the GDPR;
- ANPD can only issue administrative penalties as of August 2021, but the first lawsuits are already being filed by individuals or state prosecutors.

About the author
Willeke Kemkers is an associate at Greenberg Traurig Amsterdam. She specializes in Intellectual Property and Data Protection, and counsels national and global clients on a wide range of privacy issues such as data processing agreements, cross-border transfers of data, privacy policies and data breaches.



About the author
Adriano Chaves is a Brazilian lawyer and partner at CGM located in São Paolo. He specializes in M&A, Corporate Law, Technology and Data Protection. Adriano has been acknowledged by several important publications, such as Chambers Global, Chambers Latin America, LACCA, Leaders League, Best Lawyers.

DATA CYBERSECURITY & PRIVACY

An interdisciplinary platform for sharing knowledge and practical insights across multiple industries.

DSCP is the leading magazine for professionals working in the field of Data, Cybersecurity and Privacy.

A network for professionals in consultancies, law firms, scientific and educational institutions, corporate firms, and government agencies.

Sign up now for an annual subsription

One year for only € 37,50

(instead of € 75,-)

Check our website:

www.dcsp.nl and register!

Interested in the digital Company Subscription? Please contact marketing@delexmedia.nl

50% OFF!

DCSP
DATA CYBERSECURITY
& PRIVACY

CONSIDERATI

Legal and Public Affairs consultancy for the digital world

Fitting technology into society

Technology and data create opportunities for every organisation. Their application has become front-page news. However, such innovations also create legal issues and friction with interests in society. As an organisation, you want to remain in control. Considerati is the legal and public affairs consultancy for the digital world, with offices in Amsterdam and The Hague. In three specialised teams, we help organisations to innovate responsibly with digital technology and data.

Legal: Carefree innovation within the framework of privacy legislation
Responsible Tech: for an ethical compass when innovating with data and algorithms
Public Affairs: for societal and political support for technology and innovations

Over 15 years, we have built up our expertise with large companies and governments, as well as growing organisations

Considerati legal services

Advice

- Privacy advice
- Data breach & Incident management
- Privacy integration
- IT and telecom advice
- Data protection impact assessment
- Privacy awareness training
- Privacy compliance & maturity audit
- Studies on privacy impact of new technology

Interim

- DPO as a Service
- DPO coaching and support
- Privacy officers
- Legal counsel
- Tailored in-house privacy courses for all business functions and any type of organization (Dutch / English)

Academy

- Tailored in-house privacy courses for all business functions and any type of organization (Dutch / English)
- Full DPO course (Dutch)

Amsterdam
De Boelelaan 7
1083 HJ Amsterdam
+31 20 737 0069

M: INFO@CONSIDERATI.COM

The Hague
Anna van Buerenstraat 41 4DE
2595 DA The Hague
+31 20 737 0069

WWW.CONSIDERATI.COM