#28: Big brothers have responsibilities

The digitalization of our life leads to an enormous amount of data: e-mails, documents and exchange of information like SMS and WhatsApp. Digital data leaves its footprint. This footprint can be of great interest to, for instance, investigation or prosecutions services as they might lead to evidence of criminal offences. Consequently, in practice, large amounts of data are seized under criminal law. And the question is whether it is possible to communicate anonymously in a digital way. It seems Big Brother is always watching you. But Big Brothers have responsibilities. Dealing with this data in a careful manner is a responsibility of the investigating services in our opinion which comes along with this development. In an increasing amount of criminal investigations the seized data is of such an amount that the criminal defense can no longer see the forest for the trees. In our opinion a lot of progress can be made in data-structuring and transparency of the data investigation in the investigation process.

In Lawlunch #14 we concluded: we can hardly live without foreign storage- and communication services. This results in an increasing amount of legal discussions on how to deal with the seizure and the processing of this data. In Lawlunch #14 we explained whether the public prosecutor could order or seize data which is accessible in the Netherlands but is stored abroad. In this months' Lawlunch we also go into a case in which large amounts of data have been seized on a foreign server. However in this case questions come up such as how the investigation services structure the chaos of seized digital data. How do they structure it in order for the defense and judges to be able to verify the processing of this data? And how can we avoid biased data-investigation, leading to a one-

sided view of events? And more important, how can be established whether or not the data-investigation was biased?

Last week, media in the Netherlands frequently reported on a case concerning a decision based on data-related evidence. The evidence the court based its decision on was encrypted data. The Dutch Public Prosecutor's Office received this kind of information from Canadian authorities after an international request for mutual assistance. The Canadian authorities had access to information that was located on the server in Canada of the Dutch company Ennetcom. The court states: *'Ennetcom is a Dutch company that offered secured BlackBerry-cellphones, enabling its users to draft and send encrypted e-mails via so-called Pretty Good Privacy-cellphones (PGP-cellphones). These PGP-cellphones cannot be used for others purposes, such as making phone calls.'*

The 'million dollar question' was whether the Dutch Public Prosecutor's Office obtained the encrypted data in accordance with Dutch law and whether this kind of evidence was admissible in court. The Court of Amsterdam answered these questions in the affirmative in its decision of 19 April 2018. During the trial, the criminal defense repeatedly argued against both the Dutch Public Prosecutor's Office obtaining access to the encrypted data via the international request for assistance and its use by court. However, the court does not sympathize with the arguments of the defense.

One of the most important arguments the defense put forward concerned the fact that the criminal defense did not get enough time to verify the integrity and reliability of the results of the data-research. To do so, the defense got access to Hansken, the search engine of the Dutch Forensically Institution ("NFI"). This search engine is also used by Dutch investigation services. As appears from the conviction, neither the investigation team nor the defense had access to *all* Ennetcom-data that Dutch authorities had obtained via their international request for mutual assistance. Keywords

used in the search engine, were considered to be a proper basis for the investigation in question and consequently limited the amount of data that was selected on behalf of the investigation.

In order to verify the investigation results, the defense received a CD containing data-information. The defense argued that the information on the CD was neither complete nor accessible. Yet, the court dismisses the argument of the integrity and accessibility of the data-information by using very general and vague considerations. The court uses the following words: *"The court however, will adhere to the conclusion of the examining judge that the information on the CD is in fact well-upright and -accessible. The court considers any further investigation on this matter unnecessary."*

By using the previous phrase, the court conveniently avoids making comments on this crucial issue. The decision unfortunately does not really provide insight on the argument of the defense. A description by the defense of the encountered problems while accessing the data on the CD can be useful to argue that the defense is not able to verify the investigation results as presented by the investigating authorities. Other pressing issues which come up are why the Dutch Public Prosecutor's Office limited the total amount of obtained data to the results of several keywords? Did privacy reasons play a certain role in this decision? Did, consequently, exculpatory evidence get excluded from the data-investigation?

Verification of investigation is only possible when investigation authorities carefully and thoughtfully report their way of research. In our opinion this responsibility comes with the possibility of the investigation services to use this data in prosecution of individuals. As a result, we feel that the reporting obligations of the investigation authorities as laid down in article 152 of the Dutch

Procedural Criminal Code will become more important as the digital economy will further develop. During investigations, investigation authorities should define their actions and measures accurately. Whether this concerns the elaboration of keywords, the total amount of hits resulting from those keywords or a possible alternative course of events. Only in that case the defense and judge will have a clear perspective on the execution of investigation.

Only judges can truly ensure that investigation authorities respect the responsibility following from article 152 of the Dutch Procedural Criminal Code. This could help involved parties to see the wood for the trees again concerning data investigations. In order to trigger judges to come to a conclusion, it is also up to the defense to emphasize in court why we should take the responsibility following from article 152 of the Dutch Procedural Criminal Code seriously.

Do you have any questions about this subject, are you confronted with a related issue and would you like to discuss this with us? Please feel free to contact us via boezelman@hertoghsadvocaten.nl and boer@hertoghsadvocaten.nl.