Rob van den Hoven van Genderen

The criminalization of Doxing?

The use of the internet and modern media regularly results in new provisions. This applies in particular to criminal law. With the introduction of the Computer Crime Act, many existing criminal provisions were transformed by just adding the word 'computer' to the criminal provision such as computer trespassing instead of trespassing. Later, English-language oriented activities were also added under the regime of internet crime, such as spoofing, using other people's Wi-Fi without permission (which has since disappeared) and grooming, making contact via the internet and preparing to meet minors with the intention of having intimate (sexual) contacts.

Now a new (draft) article on the criminalization of 'doxing' in the penal code is added that nestles somewhere between insult, intruding on privacy, criminal intimidation, and terrorism. The explanatory memorandum indicates that this is an English hacker term: 'The term 'doxing' is a term used by hackers and is derived from the English word 'documents". In doing so, identifying personal data is disclosed with the aim of frightening a specific person, causing serious nuisance or hindering them in the performance of his function. The proposal, which was submitted for consultation on 13 July, is the result of a motion from the Lower House of parliament. What this means is that present or detectable identifying data is used or published on the internet to threaten people or organizations, put them in a bad light or expose them to potential danger. This new criminal provision could serve to avoid and criminalize situations that have a negative impact on the social and economic functioning of natural persons and organizations and companies. As an example of situations to be avoided and punishable by law, the Explanatory Memorandum refers to "people who are active on the online messaging platform Twitter and make a progressive political sound there, have a sticker of 'Vizier op Links' on their front door and as a result became victims of online bullying campaigns". At others a firework bomb was thrown in the garden. Police officers, opinion makers, journalists and politicians are also increasingly faced with online intimidation and threats. The GTPA (Violence Against Police Officers) annual figures show an increase in the number of online intimidating statements aimed at police officers. For example, attempts have been made for a while to reveal the identities of undercover agents. The question is whether fundamental rights such as freedom of expression and journalistic freedom are not endangered by this new criminal provision.

Article 298b paragraph 2 could provide for this, but one must be able to demonstrate that the act has been done in good faith, with the burden of proof on the 'suspect'? Can't activities in the context of doxing not be classified under the current criminal provisions such as threat, insult and defamation and also be subject to civil sanctions under civil law in the context of tort? The examples also indicate that reactions, such as throwing a fireworks bomb and threats, can be prosecuted fairly easily under existing criminal provisions. Care must be taken to ensure that activities such as 'deep research' journalism also have to be justified every time the reprehensible way of life of public figures or big tech (or energy) companies are raised. "Journalists and whistleblowers, who disclose news facts and abuses, are not punishable if the disclosure of data is necessary in the public interest. After all, the intention is then not to intimidate others," according to the ministry. It is all too easy for new (negative) activities as a result of new

technological developments, in this case to misuse generally accessible information, to resort to criminalization through the creation of a new staff provision. It is better to look for a solution within the current legal instruments and also to realize education, information and awareness of the unacceptableness of this behavior with an open eye for the positive aspects of the accessibility of public information for the promotion of transparency of behavior of companies and individuals with a major influence on society. There is a need for unveiling the behavior of the dark sit(d)e in times of technological cloacks and daggers of fake media and techno-giants.

Text of the proposed Article on Doxing

ARTICLE I After Article 285c of the Criminal Code, an article is inserted, reading:

Article 285d

1. He who provides identifying personal data of another or a third party, disseminates this data or otherwise makes it available with the intent to provoke or cause to be provoked, to cause serious nuisance or to cause to be caused to or to seriously hinder or cause to be hindered in the performance of his office or profession, shall be punished with a term of imprisonment not exceeding one year or a fine of the third category.
2. Not punishable is the person who has been able to assume in good faith that it is in the public interest to obtain, spread or otherwise making the data referred to in the first paragraph available.

ARTICLE II After Article 298a of the Criminal Code BES, an article will be inserted, reading:

Article 298b

1. He who provides identifying personal data of another or a third party, disseminates this data or otherwise makes it available with the intent to fear that other person inciting or causing instigation, inflicting serious nuisance or causing it to be caused to or seriously hindering or allowing him to be hindered in the performance of his office or profession, shall be punished by a term of imprisonment not exceeding one year or fine of the third category.
2. A person who has been able to assume in good faith that the public interest requires the provision, distribution or otherwise making available of the data referred to in the first paragraph shall not be punishable.

ARTICLE V This Act shall enter into force at a time to be determined by Royal Decree.

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.