ARTICLE:

Forced biometric authentication – on a recent amendment in the Norwegian Code of Criminal Procedure

By **Ingvild Bruce**

Introduction

In June this year, the Norwegian Parliament approved an amendment to section 199 a of the Norwegian Code of Criminal Procedure, allowing the Norwegian police to order anyone dealing with a data-processing system to open it by biometric authentication and to perform the authentication by use of force should the person refuse to comply with the order.

The amendment is the result of a practical situation in which the Norwegian police was, as on many previous occasions, outplayed by technology. In this case, the police had seized the mobile telephone of a person suspected of gross violence, because the police believed the telephone to contain video recordings of the incident, however the suspect refused to provide neither the code or his fingerprint, either of which was necessary to obtain access to the content of the device. After three rounds of court proceedings, the Norwegian Supreme Court decided unanimously that there was no legal basis in Norwegian legislation according to which the suspect could be forced to cooperate (the Biometric case).[1]

The Norwegian government, acting with unusual swiftness, distributed a consultative paper less than four months later,[2] followed by a legislative proposal, which was soon after adopted without amendments.[3] This article will outline briefly the lacunae in Norwegian legislation that caused the need for the amendment; set out the provision that permits the police to obtain access to biometric authentication by the use of force; the material and procedural conditions that apply, and finally present some of the objections that were put forward against the proposal and subsequent amendment.[4]

The legislative lacunae and the process of filling it

Criminal investigations are processes of information gathering with the aim of finding out whether a crime has taken place, and if so, whether anyone can be held criminally responsible for it. The police have different tools that may be used in these processes, some of which have such an effect on individual integrity that they are regulated by law. In the Biometric case, faced with a suspect of a serious crime and a telephone possibly containing evidence of the crime, the Norwegian police had legal grounds both for seizing the telephone, searching its content and storing any information that might have shed light on the crime. The question was not whether the police could legally obtain access to the information in question, but which procedure they could legally use to gain such access. As the phenomenon of biometric authentication had hitherto been beyond the imagination of the legislator and was not explicitly regulated, the question was whether the suspect could be forced to cooperate according to any existing legal provisions.

Within one year, three different cases were brought before the Norwegian courts,[5] all of which raised the question of whether the current section 157 of the Code of Criminal Procedure allowed the police to order the suspect to provide access to his or her

[1] Decision 30 August 2016 by the Norwegian Supreme Court (HR-2016-1833-A).
[2] Consultative paper of December 2016 issued by the Ministry of Justice and Public Security, *Høring – politiets adgang til bruk av tvang ved ransaking av datasystem for å få tilgang til datasystemet ved biometrisk autentisering*, (desember 2016) (https://www.regjeringen.no/no/dokumenter/horing---politiets-adgang-til-bruk-av-tvang-ved-ransaking-av-datasystem-for-a-fa-tilgang-til-datasystemet-ved-biometrisk-autentisering/id2524043/).
[3] Proposal Prop. 106 L (2016 – 2017) *Changes to the Code of Criminal Procedure (biometric authentication)* by the Ministry of Justice and Public Security (Prop. 106 L 2016 – 2017).
[4] It does not, however include a thorough examination of these objections or their validity, nor an in depth analysis e.g. of the practice of the European Court of Human Rights or the legislation of other countries.
[5] See decision 10 December 2015 by Nord-Troms District Court (TNHER-2015-196550), 29 March 2016 by Jæren District Court (TJARE-2016-43883) and 29 April 2016 by Halden District Court (THALD-2016-704812).

device that had been secured by biometric authentication. Section 157 states that suspects may be 'subject to physical examination when it is deemed to be of significance for the clarification of the case and does not amount to a disproportional interference'. This includes the taking of 'blood samples', or 'other examinations' if they can be done without risk or considerable pain. In all three cases, the district courts decided that the provision allowed forced biometric authentication. Also, in each case, the Court of Appeal affirmed the decisions in the lower court, arguing that although the wording of the provision indicated that only examinations of the body and not the use of the body in the examination of other objects were comprised, the provision was not clear cut and could also comprise the measure of forcing someone to put their finger on the telephone.[6] The court stressed that the enforced act strongly resembled the taking of fingerprints which was clearly comprised by the provision, and that it is much less intrusive than other acts comprised, such as search of bodily cavities. In two of the decisions,[7] however, a dissenting minority found that the wording of the legislative provision did not include forced biometric authentication, and thus that it should be left to the legislator to decide whether it should be allowed. The Supreme Court agreed with the dissenting judges, and found it evident that section 157 of the Code did not constitute a sufficiently clear legal basis for the use of biometric authentication to satisfy the requirement of precision and foreseeability that follows both from the Norwegian constitution and the European Convention on Human Rights.[8] The court based its conclusion on the fact that the wording of section 157 of the Code provides for examinations of the body or its content to be used as evidence, not to obtain access to evidence outside of the body. Considering this, the Supreme Court did not find that neither the low level of intrusion, nor the legitimate aim of obtaining access to important evidence could justify a different conclusion.

This was the background to the government's speedy initiative to provide a clearer and more precise legal basis for the ordering or forcing of individuals to give access to computer systems through biometric authentication.[9]

Forced biometric authentication – by whom to what?

The amended section 199a of the Code now allows the police to order 'anyone dealing with a data-processing system' to give access to it by 'biometric authentication' and to 'complete the authentication by force' should the person refuse to comply with the order. The wording of the provision is as follows (amendments in italics):

> Ved ransaking av et datasystem kan politiet pålegge enhver som har befatning med datasystemet å gi nødvendige opplysninger for å gi tilgang til datasystemet *eller å åpne det ved bruk av biometrisk autentisering.*
>
> *Dersom noen nekter å etterkomme et pålegg om biometrisk autentisering som nevnt i første ledd, kan politiet gjennomføre autentiseringen med tvang.*
>
> *Beslutning om bruk av tvang etter annet ledd treffes av påtalemyndigheten. Er det fare ved opphold, kan beslutning treffes av politiet på stedet. Beslutningen skal straks meldes til påtalemyndigheten.*
>
> When conducting a search of a data-processing system the police may order everyone who is dealing with the said system to provide the information necessary for gaining access to the system *or to open it by use of biometric authentication*.
>
> *Should anyone refuse to comply with an order of biometric authentication as mentioned in the first paragraph, the police may perform the authentication by force.*
>
> *Permission to use force according to the second paragraph is given by the prosecuting authority. If delay entails a risk that the investigation will be impaired, permission may be given by the police on the spot. The decision by the police shall be submitted to the prosecuting authority.*

The term *'data-processing system'* was chosen because it is a familiar term in Norwegian criminal

[6] See decision 16 December 2015 by Hålogaland Court of Appeal (LH-2015-198908), 26 April 2016 by Gulating Court of Appeal (LG-2016-62717) and 12 December 2016 by Borgarting Court of Appeal (LB-2016-72029).
[7] See decision LG-2016-62717 and LB-2016-72029.
[8] See section 113 of the Norwegian Constitution and Article 8 of the European Convention of Human Rights.
[9] Prop. 106 L (2016 – 2017) page 1.

(procedural) law, considered to comprise 'any device consisting of hardware and software which processes data by means of computer programs'.[10] It covers computers, mobile telephones and tablets as well as devices that are not used for normal communication such as printers, copiers etc. It arguably also covers applications, user accounts for email, message- and cloud services, etc.[11] The question of whether the provision should allow the ordering of persons to grant access by biometric authentication anything *other* than computer systems, such as buildings, rooms etc. was deferred to an on-going general revision of the Code of Criminal Procedure.[12]

The new provision may be used to order *'anyone dealing with'* a data-processing system, thus not only a suspect of the crime being investigated, but also, for example, witnesses or persons operating the system. The person is not required to have ownership of the system in question, and the fact that the person has *access* to the system is probably sufficient.

The act to which the person in question may be ordered or forced is called *'biometric authentication'*. The term comprises not only the reading of finger- or other prints, but also iris- and retina recognition, and according to the preparatory works, it can also include other forms of biometric authentication that are taken in use in the future, such as DNA-recognition.[13] The government aimed to find a term that was not limited to specific technological solutions, but that would adapt to future technological developments.[14] It did, however, recognize that not all kinds of biometric authentication can be enforced. An example of the latter is vocal recognition, as one cannot (in a civilized manner) force anyone to speak.[15] Moreover, it stated that the biometric characteristics that are enforced may only be used to gain access to the system, and may not be stored.[16]

The order of or forced biometric authentication is, like all coercive measures allowed in Norwegian Criminal Procedure, subject to a general requirement of proportionality according to section 170 a of the Code of Criminal Procedure. This implies that the order must be capable of facilitating the implementation of the search or seizure, and that the implementation of these measures cannot be achievable by less invasive means.[17] In general, coerced acts of biometric authentication were considered by the government as relatively minor and brief infringements on personal integrity compared to other infringements within the power of the police, such as examination of bodily cavities. It stated that such coercion would normally be proportionate, but that the proportionality would always have to be determined by the circumstances of the particular case.[18]

A significant question that is left unanswered both by the provision and the preparatory works is the kind of force the police may use if the suspect refuses to comply with an order of biometric authentication. This must be determined by the abovementioned principle of proportionality, as well as the general rules on police use of force. These rules allow the police to use physical force if 'necessary and appropriate' in light of the gravity of the situation, the consequences for the person in question and the circumstances in general.[19] Additionally, other measures must be presumed inadequate or inappropriate to enforce the order, and the use of force has to be adequate and commensurate with the gravity of the situation and the purpose of the action taken.

The decision to use force must be made by the Prosecuting Authority in the Police. This is the lower level of the Prosecuting Authority, which is in Norway directed by the Director of Public Prosecutions but also part of the police. In cases of urgency, the decision may be taken by police officers, although such decisions must immediately be reported to the prosecuting authority. The suspect may challenge the legality of the decision before the courts, but this will not necessarily lead to implementation being suspended.

[10] Prop. 106 L (2016 – 2017) page 10.
[11] The Norwegian Police Directorate stressed, in its response to the government's consultation paper, the need for the provision also to comprise such services, see Prop. 106 L (2016 – 2017) page 6. The government did not address this question in the final proposal, but stated that the term should be understood in the same way as when used in other parts of the Act. The term is also used in section 216o of the act, which regulates what is called data reading. This provision also allows for the interception of digital information from such services, but is not clear as to whether this is included by the term 'computer system' or follows from a separate part of the provision, see Prop. 68 L (2015 – 2016) page 270 – 271.
[12] Prop. 106 L (2016 – 2017) page 8 – 9.
[13] Prop. 106 L (2016 – 2017) page 4.
[14] Prop. 106 L (2016 – 2017) page 4 and 9.
[15] Prop. 106 L (2016 – 2017) page 11.
[16] Prop. 106 L (2016 – 2017) page 11.
[17] Prop. 106 L (2016 – 2017) page 11.
[18] Prop. 106 L (2016 – 2017) page 9 and 11.
[19] See section 6 paragraph 4 of the Norwegian Police Act and section 3-2 of the Norwegian Police regulation.

Possible objections

The right to not incriminate oneself was launched as an argument against allowing forced biometric authentication both in the public debate and the formal consultation process.[20] This objection however, relies on a (common) misunderstanding of the extent of that right. At its core is the suspect's right to remain silent, and thus a prohibition against forcing the suspect to give incriminating statements or to use such enforced statements as evidence. This is confirmed by the European Court of Human Rights (ECtHR) in the case *Saunders v The United Kingdom*[21] where the court held that the right not to incriminate oneself does 'not extend to the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect'.[22] Examples of acceptable compulsory powers are, according to the court, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing. In the preparatory works, the Norwegian government argued that forced biometric authentication does not conflict with the right not to incriminate oneself, as it constitutes exploitation of a physical characteristic that exists independently of the suspect's will, and does not force the suspect to choose between lying or incriminating him- or herself.[23] Rather, the government argued, it helps the police overcome a physical obstacle to information already legally available to them through the measures of search or seizure, not unlike the forcing of a suspect to give up the key to a lock. The government conceded that the right not to incriminate oneself could limit the access to and use also of incriminating physical evidence, among other things if their collection violates articles 3 or 8 of the European Convention of Human Rights, but stated that this would have to be decided in light of the circumstances of a particular case, and that the proposed rule was not problematic as such.

Some have argued that the provision allows for disproportionate interference with personal integrity and the right to privacy, not because the act to which the suspect is forced is very invasive in itself, but because of the potentially vast amount of information to which the act may give the police access, including sensitive information. It is, however, not the access to forced biometric authentication that gives the police the right to obtain access to the information, but the rules on search and seizure. The critique concerning the effect on privacy should thus be directed at these rules and the way they are practiced. In relation to biometric authentication, the argument might be more valid if it focused on the subjective experience of the order as more invasive for the person concerned when the information he or she is forced to give access to is significant or sensitive, or both. This may be a relevant argument in the determination of the proportionality of the measure in each individual case, but cannot mean that the provision as such must be considered disproportional.

Others have objected that the wording of the amended provision that allows biometric authentication is too vague to satisfy the constitutional and international requirements that measures interfering with individual rights must have a clear legal basis.[24] However, both the terms 'data-processing system' and 'biometric authentication', although open to interpretation in light of the technological development, are reasonably precise and meaningful, and not likely to be problematic in relation to such constitutional and international requirements. The vagueness-critique could more validly be directed at the lack of specification of the kind of force that may be applied to implement an order of biometric authentication. As noted above, this is not explicitly stated anywhere, and the limits that do apply are highly discretionary and can only be inferred from other regulations, most of them found in other statutes and documents. An illustration that the use of force to implement an order of biometric authentication could have been more strictly regulated is provided by the fact that the use of force to take someone's fingerprints requires a court order,[25] and that internal physical examinations and blood tests can only be conducted if they can be done 'without risk or considerable pain'.[26] It is probable, however, that the general framework of principles regulating and limiting the Norwegian police' use of

[20] Prop. 106 L (2016 – 2017) pages 7 – 8.
[21] Prop. 106 L (2016 – 2017) page 3.
[22] *Saunders v The United Kingdom* 17 December 1996 (app. no. 19187/91) para. 69.
[23] Prop. 106 L (2016 – 2017) page 10.
[24] See particularly the responses from the Norwegian Data Protection Authority and the Norwegian Bar Association to the government's consultation paper cited in Prop. 106 L (2016 – 2017) page on page 5 – 6.
[25] Section 11-4 of the Norwegian regulation of the Public Prosecution Service.
[26] Section 157 of the Norwegian Code of Criminal Procedure.

force will be considered to provide sufficient clarity and due process to satisfy constitutional and international requirements.

In conclusion, the Norwegian regulation of biometric authentication stands out as a modernization of the Code of Criminal Procedure necessary to bring the police up to speed with technology, which arguably does not give rise to serious concerns in relation to individual integrity and due process.

Ingvild Bruce is a research fellow at the Institute of Public and International Law, University of Oslo, writing a PhD titled 'Preventive use of surveillance measures in the protection of national security – a comparative study'. She was previously legal advisor to the Norwegian government and parliament, and a prosecutor.

Ingvild.bruce@jus.uio.no