Encryption from a Human Rights Perspective

The right to privacy as stated in Art. 12 UDHR not only protects against arbitrary interference with correspondence but also entitles to protection by law against such interference.

Applied to non-electronical communication there is a vast agreement that neither state agencies nor companies or individuals can lawfully read/hear and process your communication without explicit authorization to do so. Encryption, as encoding with the intent to hide the contents from other people than the intended recipient, in this case would consist in the use of another language, code words or other well-known basic encryption methods. This is rarely done in daily life because usually the laws that protect privacy of mail are considered to be effective. If done, it is not considered to be an illegal activity. This might be linked to the fact that almost all of the classical encryption methods can be broken within a reasonable amount of time and have the key exchange as weakest spot.

The picture changes drastically for electronic communication. Even constitutional states exercise mass surveillance of electronic communication, there are companies with mass data storage and trade as business model, with databases much broader and more detailed than it was the case in the pre-digital era. Laws governing the privacy of e-mails are not considered effective since an e-mail may cross borders several times before reaching its recipient and at each mail server in between it can be read and processed (and usually is, e.g. by spam filters) without leaving traces in the e-mail. Breaching electronic privacy can be and is done in a much more effective way than for non-electronic communication, affecting sometimes millions of users.

Encryption of e-mails comes in two flavors: encryption of the stored content and encryption while in transfer. Transfer encryption is nowadays widespread, however SSL/TLS-based end-to-end-encryption does not provide a safe solution, since the transfer between two mail servers only happens encrypted if both servers support this. Usually some mail servers of large ISPs and e-mail providers do not provide encryption. This way they can scan the e-mails for viruses but also assess the contents in quite different ways. The safe solution, DANE TLS, is at the moment much less in use, e.g. in Germany only by a few smaller e-mail providers. User based content encryption via PGP or S/MIME is quite rare since there is need of some technical understanding and of a “critical mass” in order to be useful. The encryption methods rely on openly documented mechanisms. Nevertheless, with our current mathematical knowledge, some of them are virtually impossible to break. For public/private key encryption also the key exchange is difficult to interfere with. Apart from e-mails there are many more applications of software-based encryption: websites, chats, clouds, file/volume encryption. To all of them similar comments apply.

In all these cases, software-based encryption provides privacy protection where national laws or practices prove inefficient or inconsistent with Art. 12 UDHR. Amnesty International, for example, uses encryption to communicate with human rights defenders all over the world. On the other hand, encryption can also be used for criminal offences. Due to it being virtually unbreakable a state has limited means in dealing with this problem.

The question is: Is encryption, apart from being a practical means to maintain the right to privacy, a universal right or may a state in principle prohibit some encryption methods in general if it is able to protect its inhabitants' privacy by other means? The free use of encryption technologies is suggested by Art.11, Art.12, Art. 19 and Art.27 UDHR, i.e. the rights to be deemed innocent, to privacy, to freedom of expression and the right to participate in scientific progress. A general prohibition of an encryption method would need very strong arguments to counter this, e.g. a structural increase in the risk of being killed or bodily harmed in the absence of a ban. Since encryption in itself cannot inflict bodily harm, in case of a ban punishment for using it is not expected to deter anybody who plans to inflict bodily harm to another person or group from doing so. The effect of a ban would consist in being able to use encryption as indication for other unlawful behaviour and to stop criminal intents already at the stage of using encryption in electronic communication. The latter, however, can also be achieved by more specific measures than a general ban on encryption and can only work in an international framework including the stakeholders of internet governance. The relation of such a wide violation of fundamental rights to the benefit of reducing crime seems grossly inappropriate.

Moreover, the current state of affairs teaches that the absence of (widespread) encryption encourages more criminal activity and enables groups and states to violate fundamental human rights more easily. In the light of this discussion encryption standards are not only vital to maintain fundamental rights - hence the free use of encryption constitutes a derived universal right -, but by Art. 12 UDHR (and also Art. 19 and Art. 27) the state members of UN are obliged to ensure the availability of encryption techniques whenever personal data are sent or received electronically inside their territory.

Dr. habil. Marco Kühnel, Hanover/Germany
Sebastian Schweda, Attorney-at-law, Saarbrucken/Germany
Steffen Härting, Heidelberg/Germany