The criminalisation of abusive and offensive communication in German law¹

INTRODUCTION

- 1.1 The internet "revolution" and the phenomenon of content distribution and communication through social media, including the borderless nature of such technology, has raised concerns about harmful contents in Germany just as it has in the United Kingdom.
- 1.2 The effectiveness of criminal speech offences in the German Criminal Code (Strafgesetzbuch - StGB) has been questioned since the development of the internet and social media. Such debate was grounded in the view that social media companies were reluctant to take down content notified by the police and other authorities quickly and efficiently. This was one of the political motivations for the Netzwerkdurchsuchungsgesetz (NetzDG), passed in 2017.
- 1.3 The German Government observed in the NetzDG Bill explanatory notes that the increase of hate crimes and other content-related offences on social media platforms required legislative action.² While the Government had already established a task force to address the problem informally, in collaboration with social media platform representatives, it found that the obligations social media platforms imposed on themselves were insufficient. These companies had committed themselves to establishing user-friendly mechanisms to allow for the flagging of critical content, the majority of which was to be assessed by linguistic and legally trained teams within 24 hours.
- 1.4 Nevertheless, too little illegal content was removed. A study conducted in early 2017 showed that while YouTube managed to remove 90% of criminal content, Facebook only removed 39% of such content, and Twitter only 1%. The Bill was passed on 30 June 2017, and has caused much controversy between those that hail the NetzDG as an assertion of state power over irresponsible internet giants, as well as those that consider it a serious infringement of freedom of speech.

by Julia Hörnle, Professor of Internet Law, Queen Mary, University of London, and Dr Maria Schmidt-Kessen, Queen Mary University of London.

The Explanations of the German Government for the NetzDG of 5 April 2017 can be found at https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_NetzDG.pdf?_blob=publicationFile&v=2.

³ Explanations of the German Government for the NetzDG of 5 April 2017.

For press coverage along these lines, see for example Der Spiegel, 'Das Facebook-Gesetz ist erst der Anfang', 30 June 2017, http://www.spiegel.de/netzwelt/netzpolitik/heiko-maas-und-facebook-das-netzdg-ist-erst-der-anfang-die-analyse-a-1155222.html. The critique continued after the entry into force of the NetzDG on 1 January 2018, see, for example Die Zeit, 8 January 2018 https://www.zeit.de/digital/internet/2018-06/netzdg-netzwerkdurchsetzungsgesetz-klage-fdp. June 2018, https://www.zeit.de/digital/internet/2018-06/netzdg-netzwerkdurchsetzungsgesetz-klage-fdp.

- 1.5 German criminal law doctrinally defines the legitimate interests which each criminal offence protects. It makes a clear distinction between individual interests (such as, in this context, individual dignity, liberty or privacy, or an individual's reputation) and public interests (such as public order and public peace). Thus, offences are categorised more clearly (compared to English law) as to the specific legitimate interests they protect.
- 1.6 The starting point for developing new laws is identifying how, and to what extent, these protected legitimate interests are affected by (in this instance) new social and technological developments. While generally speaking there should be functional equivalence between offline and online criminality, in practice, new ways of interacting and communicating online have changed social behaviours and therefore the need to protect legitimate interests. This will become obvious in the discussion below, for example in relation to the protection of privacy in §201a (prohibition on transmission of highly private images and prohibition on sale/acquisition of nudist images of children⁵), the definition of insults in §185, the new stalking offences or the changes to the "hate" public order offences.

How is the German Criminal Code (Strafgesetzbuch - StGB) applied to criminal offences committed online?

- 1.7 §§ 3 to 7 of the StGB determine the applicability of German criminal law. In relation to offences that have a cross-border dimension, which can regularly be the case with internet-related offences,⁶ German criminal law is applicable if the place where the event giving rise to the harmful event, and/or the place where the harm occurred, are within German territory.⁷ The simple fact that a website can be accessed from Germany would be too broad a criterion to establish the applicability of German criminal law.⁸
- 1.8 If a person uploads privacy-infringing pictures to a social media website from a German IP address, for example, the location of that person and the device from which she uploaded the picture would trigger the application of German criminal law. In other words, Germany would be the place where the event giving rise to harm occurred. If a person uploaded such a picture from another jurisdiction, it would become more difficult to establish the applicability of German criminal law. If the victim were a German citizen or resident, however, the place where harm occurred could be within the German territory, rendering German criminal law applicable. Unrisdiction also depends on the nature of the offence and the specific legal interests it protects and whether these interests (such as public order) are harmed on German territory.

Publicly discussed in Germany in the light of the Edathy scandal, see for example https://en.wikipedia.org/wiki/Sebastian_Edathy.

⁶ J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 7.

⁷ § 3 in conjunction with §9 StGB.

⁸ J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 9.

⁹ As above.

¹⁰ As above.

BGH 1 StR 184/00 Urteil Auschwitzlüge.

- 1.9 While the provisions of the German Criminal Code are updated and amended from time to time see for example the new provisions on stalking the starting point is that the criminal law is applied to the online space as it is applied to the offline space. So, no conceptual legal difference is made in terms of the statutory provisions. However, technologies such as the internet, as in other countries, have changed both the way crimes are being committed, how people interact and the scale of offending, with the ease of peer-to-peer communication and user-generated content. However, this is primarily an enforcement problem, which is reflected in the new law on network enforcement, discussed in the next section.
- 1.10 The adaptation of the German criminal law to crimes committed online has taken place through direct amendments to the StGB, as well as amendments to related legislation, such as the Copyright Act (Gesetz über Urheberrecht UrhG) and the Data Protection Act (Bundesdatenschutzgesetz BDSG).¹² The impetus to reform German law in light of the rise of cybercrime has not only come from the German legislature, but also from European and international law makers.¹³

NETZWERKDURCHSUCHUNGSGESETZ

- 1.11 Politicians have blamed social media providers for contributing to the dissemination of hate speech online and have called on them to "do more" to prevent the spread of hate speech, abuse and extremist content on their platforms. In this vein, the German Minister of Justice, Heiko Maas published a draft Bill¹⁴ on 17 March 2017 which was passed on 1 September 2017¹⁵ and came into force on 1 October 2017.
- 1.12 This Act obliges social media companies with a user base of at least two million users in Germany¹⁶ to take down content infringing a list of certain provisions of the StGB¹⁷ within 24 hours (for obviously infringing content) or seven days (where infringement is not immediately obvious)¹⁸ and provide an accessible and efficient notice and take down procedure for German users.¹⁹ Failure to do so can lead to a fine of up to 50 million euros.²⁰ This proposal was motivated by the perception of an unacceptable avalanche in hate crime, online abuse and fake news not being countered effectively by social media companies ("SMC"). In the speech introducing the Bill to Parliament, the German Minister said:

Sven Krischker, Das Internetstrafrecht vor Neuen Herausforderungen (Logos Berlin 2014).

For example, the Council of Europe Convention on Cybercrime, the UN Convention on the Rights of the Child (which contains provisions on combatting child pornography) as well as a range of European Union Directives and Regulations.

Final version of government draft 5. April 2017 see http://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/NetzDG.html (in German).

¹⁵ BGBI I 3352.

¹⁶ §1 (2).

¹⁷ §1 (3).

¹⁸ §3 (2) No. 2 and 3.

¹⁹ §3 (1).

²⁰ §4.

the self-regulation by the relevant companies has had some success, but has been insufficient. New figures (...) show: not enough criminal content is taken down and the processes are too slow. The biggest problem remains that social networks do not take seriously the complaints of their own users. Therefore, it is clear to us that we have to increase the pressure on social networks. In order to engage these companies in removing illegal content we need legislative measures²¹

PRIVACY OFFENCES

Personal data

- 1.13 With the entry into force of the new General Data Protection Regulation ("GDPR"),²² a new German Act on Data Protection (*Bundesdatenschutzgesetz* BDSG) came into force.²³ Under German data protection law, serious violations of the provisions of the BDSG and GDPR can constitute a criminal offence.²⁴
- 1.14 In the new version of the BDSG, § 42 (1) stipulates that any person who, for economic benefit, consciously transfers personal data²⁵ of a high number of individuals without authorisation to a third party, or makes it available in another form, can be punished with a fine or a prison sentence of up to three years.²⁶ The concept of economic benefit is defined broadly and can constitute any reward of economic value.²⁷
- 1.15 Under new § 42 (2) BDSG, any person who processes personal data without authorisation, or illegitimately acquires it through false statements, and does so for an economic benefit, in order to enrich herself or another, or does so to harm another person, can be punished with a fine or a maximum jail sentence of two years.²⁸ The aim of enriching oneself or another person include any possible means to increase personal wealth/assets.²⁹ The intention of harming another person covers any type of

For the speech see (in German)
http://www.bmjv.de/SharedDocs/Artikel/DE/2017/03142017 GE Rechtsdurchsetzung Soziale Netzwerke.html.

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Bundesdatenschutzgesetz (BDSG) v. 30. 06. 2017 (BGBI I S. 2097).

^{§§ 42} BDSG (new version, applicable since 25.5.2018). Previously, § 44 BDSG (old version, applicable before 25.8.2018). Less serious violations of provisions of the BSDG can constitute administrative offences (§43 BDSG (new), § 43 BDSG (old)).

Article 4 (1) GDPR defines personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is on who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

²⁶ § 42 (1) BDSG (new).

²⁷ § 11 (9) StGB, J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013), 87.

²⁸ § 42 (2) BDSG (new).

J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013), 88.

- negative consequence for the victim, including pecuniary and non-pecuniary damages.³⁰
- 1.16 The violations of the BDSG that constitute criminal offences are only prosecuted upon complaint.³¹ A complaint can be made by the victim, the responsible person, the Federal Commissioner for Data Protection and Freedom of Information, or the data protection authorities of the Federal States (the *Länder*).³²
- 1.17 A lex specialis to the criminal offences found in the BDSG can be found in the German Criminal Code, when the data breach is committed by a person belonging to specific professions that are subject to a duty to confidentiality, such as doctors, lawyers, and public office holders.³³ If persons belonging to these professions reveal secrets regarding a person's private life or a business secret with which they have been entrusted, they can be subject to a fine or a prison sentence of up to one year according to § 203 StGB. "Revealing" a secret can be forwarding th relevant information via email or storing it insecurely in the cloud.³⁴ It is clear that confidential data can be stored in the cloud but must be encrypted or anonymised in order not to violate § 203 StGB.³⁵
- 1.18 A potential challenge under § 203 StGB has been the growing practice within the relevant professions to outsource to external companies providing cloud services handling of data for administrative, billing, or storing purposes.³⁶ Anonymisation or encryption of data is often not a practicable way to protect the personal data and secrets of clients because the administration of such data often requires it to be accessible to the third-party service providers (for example, an external company processing and sending out a doctor's bills to patients).³⁷ There could be criminal liability of professionals subject to confidentiality obligations if they do not take sufficient care that there are safety and control measures in place to prevent unauthorised parties having access to personal data or other secrets of clients.³⁸ A way of avoiding criminal liability under § 203 StGB would be to obtain the consent of the person to her data or secrets being processed by a third party.³⁹
- 1.19 Given the economic need for most of the above-mentioned professions to outsource activities that involve confidential data, the German legislature recently amended §

³⁰ J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 88.

³¹ § 42 (3) frist sentence BDSG (new).

^{32 § 42 (3)} BDSG (new).

³³ J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 89. § 203 StGB.

³⁴ J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 68.

³⁵ Kristian Kühl and Martin Heger, *StGB Kommentar* (29th edition, Beck 2018), § 203, Rn 25.

³⁶ J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 68.

³⁷ As above, 69.

³⁸ As above, 69.

³⁹ As above, 70-71.

203 StGB.⁴⁰ § 203 (3) StGB now provides that members of a profession subject to a duty of confidentiality are not liable under § 203 (1) StGB when sharing confidential data with third parties providing support services for their work. The allowed sharing of confidential data is limited to the essential amount of information needed by these third parties to provide their respective services in the case at hand.⁴¹

- 1.20 § 204 StGB provides for more severe sanctions in case where an offence under § 203 StGB is committed for commercial exploitation. It therefore only covers secrets that are capable of being commercially exploited. 23 § 204 StGB explicitly mentions business or trade secrets as one of the category of secrets covered. An example would be a patent attorney that has been entrusted with the application for a software patent and instead uses this knowledge to produce her own software. It is decisive for the offence under § 204 StGB that commercial exploitation occurs at the cost of the victim whose data or secrets are being used. The sanctions for an offence committed under § 204 StGB can be a monetary fine or up to two years imprisonment.
- 1.21 Offences under §§ 203 and 204 StGB are only prosecuted upon complaint.⁴⁵

Violation of highly personal/intimate privacy through the taking of pictures

1.22 §201 a StGB was introduced in the German Criminal Code in 2004, ⁴⁶ as a reaction to technological developments in photography and image registration that allowed for new and more severe forms of intrusion into a person's privacy. This included very small web and spy cams, as well as the camera function of the ever-more pervasive mobile phones. ⁴⁷ This new provision is also a reaction to the increasingly aggressive intrusion in peoples' privacy through distribution and use of private photographs on mass media and the internet (including such new phenomena as revenge porn). ⁴⁸ Consequently, further sections were added to §201 a StGB in 2015, to increase the scope of the provision in order to catch the rise of cyber bullying through the use of denigrating, degrading and embarrassing photographs, particularly among younger people on social media platforms. ⁴⁹ The legislature recognised that cyberbullying can be more harmful than offline bullying since it is not limited to specific situations (such as school), and can occur constantly and publicly. ⁵⁰

See justification of the German legislator for the new wording of § 203 (3) (BT-Drs. 18/11936 of 12 April 2017).

⁴¹ Kristian Kühl and Martin Heger, StGB Kommentar (29th edition, Beck 2018), § 203, Rn 25.

⁴² J Eisele, *Computer- und Medienstrafrecht* (Verlag C.H. Beck, München, 2013) 72.

⁴³ As above.

⁴⁴ As above; see also T Fischer, *StGB Kommentar* (64th edition, Beck 2017), § 204, Rn 3.

^{45 § 205} StGB.

The official gazette reference is BGBI I, Nr. 41, S. 2012 of 30 July 2004.

⁴⁷ J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 145.

⁴⁸ T Fischer, StGB Kommentar (64th edition, Beck 2017), § 201 a, Rn 2.

See justification for the amendment of § 201 a StGB by the German legislator (BT-Drs. 18/2610, 36-37).

⁵⁰ See justification for the amendment of § 201 a StGB by the German legislator (BT-Drs. 18/2610, 36-37).

- 1.23 §201 a (1) StGB stipulates that whoever unlawfully creates or transmits photographs of another person located in a dwelling or room protected from view,⁵¹ or takes and transmits photographs showing a person in a situation of helplessness,⁵² and thereby violates the person's highly personal/intimate privacy, shall be subject to a fine or a prison sentence of up to two years. The same sanctions apply to anyone who makes available to third parties images that were created under the previously stated circumstances.⁵³ The notion of "making available" covers any form of making the image available to third parties,⁵⁴ including putting it on a website.⁵⁵ It is irrelevant whether any third party actually takes notice of the image.⁵⁶
- 1.24 For §201 a (1) StGB to apply, the photograph of the person must have been taken in a protected area. Personal images taken in a public space, for example during an accident on a public road or at the beach, are not covered by the provision.⁵⁷ Images taken in a person's home will always be covered, provided they violate the person's highly personal/intimate privacy.⁵⁸ An obvious example would be images taken inside a private home without the consent of the home owner through a Trojan Horse (a piece of malware)⁵⁹ that records images through a Personal Computer ("PC")'s webcam on the victim's PC.⁶⁰ Other premises are only covered by the provision if they are protected from view, such as bathrooms, changing rooms, and doctor's examination rooms.⁶¹
- 1.25 There are difficulties in establishing the exact meaning of "highly personal/intimate privacy".⁶² The scope of protection of highly personal privacy is narrower than the general protection of one's private life. Highly personal/intimate privacy is limited to the core of one's private life, covering, but not limited to,⁶³ sexuality, illness, and death.⁶⁴ This will be regularly the case with unauthorised photographs taken of users

⁵¹ § 201 a (1) para 1 StGB.

⁵² § 201 a (1) para 1 StGB.

⁵³ § 201 a (1) para 3 StGB.

⁵⁴ J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 149.

⁵⁵ T Fischer, StGB Kommentar (64th edition, Beck 2017), § 201 a, Rn 16.

⁵⁶ J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 149.

⁵⁷ As above, 146. The definition of a person's home includes also the home of another person, as well as hotel rooms.

J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 146.

For an overview of different types of Trojans, see e.g. https://www.kaspersky.co.uk/resource-center/threats/trojans (accessed 3 October 2018).

J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 147.

⁶¹ As above.

⁶² As above, 148.

T Fischer, *StGB Kommentar* (64th edition, Beck 2017), § 201 a, Rn 3 clarifies that the highly personal private sphere is not only related to what is understood as intimate sphere such as "illness, death, and sexuality". He nevertheless makes clear that personal assets (*Vermögen*) are not covered by this provision.

J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 148.

in bathrooms or changing rooms.⁶⁵ It will not cover every image taken of persons in private homes, since these images could also cover banal situations, the creation and sharing of which would not violate the person's highly personal/intimate privacy.⁶⁶

- 1.26 Incurring criminal liability under §201 a (1) StGB can be avoided if the person whose image is created or made available consents to it.⁶⁷ There will not be consent, however, if the victim consented to the photograph being taken without being able to foresee how the photographs would be used in the future.⁶⁸ For example, a man who shared nude pictures of his ex-girlfriend on an online platform as revenge was liable under §201 a StGB irrespective of whether the girlfriend agreed to the pictures being taken at the time.⁶⁹
- 1.27 § 201 a (2) StGB provides the same sanctions as § 201 a (1) StGB for anyone who takes and makes available an unauthorised photograph of a person that is capable of significantly damaging that person's reputation. The offence is worded in a vague and possibly overbroad manner since what constitutes significant damage to a person's reputation lends itself to subjective interpretation.⁷⁰ Nevertheless, the provision was introduced by the legislature in response to the phenomenon of taking and posting certain types of mobile phone snapshots on social media platforms, ⁷¹ and intended as a signal against cyber bullying.⁷²
- 1.28 § 201 a (3) StGB prohibits the taking of nude photographs of minors to sell them to third parties, as well as obtaining these photographs against payment. Sanctions for violations of § 201 a (3) StGB can be a prison sentence of up to two years or a fine. The introduction of this provision in the Criminal Code has been repeatedly criticised as paternalistic and overbroad.⁷³ Since partial nudity is sufficient to trigger § 201 a (3)

^{48.} J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 148.

As above. This interpretation of § 201 a StGB is, however, criticized by Fischer (2017), § 201 a, Rn 21, who thinks that any unauthorized photograph taken of an individual in a home should be considered as a violation this individual's highest personal sphere of privacy under § 201 a StGB.

⁶⁷ J Eisele, *Computer- und Medienstrafrecht* (Verlag C.H. Beck, München,2013) 149. § 201 a (3) provides an exception to this rule: "unlawfully and knowingly makes available to third parties a picture that was created with the consent of another person located in a dwelling or a room especially protected from view and thereby violates his intimate privacy shall be liable to imprisonment not exceeding one year or a fine." Note, however, that this offence requires knowledge or intention of taking a picture and sharing it in view of violating another's intimate privacy.

⁶⁸ Fischer (2017), § 201 a, Rn 22. § 201 (1) para 4 StGB covers these types of situations.

⁶⁹ Judgment of the Regional Court of Kiel of 27 April 2006 (LG Kiel NJW 2007, 1002).

T Fischer, StGB Kommentar (64th edition, Beck 2017), § 201 a, Rn 23; Kühl and Heger (2018), § 201 a, Rn 9a

T Fischer, StGB Kommentar (64th edition, Beck 2017), § 201 a, Rn 24.

Justification for the amendment of § 201 a StGB by the German legislator (BT-Drs. 18/2610, 37) that was eventually implemented in the 49th amendment bill of the Criminal Code (49. StÄG) in 2015.

⁷³ T Fischer, *StGB Kommentar* (64th edition, Beck 2017), § 201 a, Rn 26; Kühl and Heger (2018), § 201 a, Rn 9b.

- StGB, advertisements for children's beachwear, for example, could be caught by the provision.⁷⁴ No court cases have been brought under § 201 a (3) StGB to date.⁷⁵
- 1.29 § 201 a StGB has no explicit exception for the creation or use of images violating highly personal privacy by the press. Exceptions could apply in individual cases, for example in the case of investigative journalism that helps to uncover a crime. 77
- 1.30 Offences under §201 a StGB are only prosecuted upon complaint, unless the prosecution office decides that it will prosecute on its own motion in a case of special public interest.⁷⁸

The right to one's own image

- 1.31 §33 together with §22 of the Artistic Copyright Act (Kunsturheberrechtsgesetz KUG) provides for criminal sanctions in case of dissemination or public display of personal images without the consent of the photographed person. This applies where the picture does not amount to a violation of the subject's highly personal/intimate private sphere. The sanctions for this offence can be a monetary fine or a jail sentence of up to one year. Offences under §33 in conjunction with §22 KUG will only be prosecuted upon complaint.⁷⁹
- 1.32 §23 (1) KUG provides for exceptions to the general prohibition of disseminating or displaying publicly images without a person's consent. These exceptions include images of contemporary history,⁸⁰ images of landscapes or other spaces on which persons appear only as a by-product,⁸¹ images of conferences and similar events at which the photographed persons participated,⁸² and images that have not been commissioned and whose dissemination or display serves higher artistic interests.⁸³
- 1.33 §23 (2) KUG stipulates that the exceptions will not be applicable in cases where there is a legitimate interest of the photographed person not to have the image publicly displayed or disseminated. This provision will be applied on a case-by-case basis.

⁷⁴ T Fischer, StGB Kommentar (64th edition, Beck 2017), § 201 a, Rn 27; Kühl and Heger (2018), § 201 a, Rn 9b.

The author conducted a search of the term "§ 201 a Abs 3 StGB" on the German case law platform Juris, and the search hit no results in respect of case law.

⁷⁶ J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 149.

⁷⁷ As above.

⁷⁸ § 205 (1) StGB.

⁷⁹ §33 (2) KUG.

^{§23 (1)} para 1 KUG. This exception is in place to protect the freedom of the press, freedom of information, and artistic freedoms. Eisele (2013), 150.

⁸¹ §23 (1) para 2 KUG, Eisele (2013), 150.

⁸² §23 (1) para 3 KUG.

^{83 §23 (1)} para 4 KUG.

HARASSMENT AND STALKING

- 1.34 §238 (1) StGB prohibits stalking and thereby seriously limiting the victim's way of conducting their daily life by either:
 - (i) seeking the victim's proximity;84
 - (ii) trying to establish contact with the victim by means of telecommunication, other means of communication, or third parties;⁸⁵
 - (iii) abusing her personal data for the purpose of ordering goods and services for the victim or causing third parties to make contact with her;⁸⁶
 - (iv) threatening her or a person close to her with loss of life or limb, damage to health or deprivation of freedom; or
 - (v) "similar acts".87
- 1.35 This final paragraph does justice to the many different possible forms stalking can take⁸⁸ and allows new technological developments to fall within the meaning of the law.⁸⁹
- 1.36 § 238 StGB was introduced in 2007,⁹⁰ after a perceived rise in stalking cases among the general population. It is estimated that around 11% of the German population has experienced some form of stalking.⁹¹ Nine months after the introduction of § 238 StGB, 11,500 complaints of incidents in violation of § 238 StGB had already been filed with the police.⁹²
- 1.37 The sanctions for an offence under §238 (1) StGB are monetary fines or a prison sentence of up to three years. §238 (2) StGB provides for tougher sanctions if the offender places the victim, a relative, or another person close to the victim at risk of death or serious injury. In this case, the prison sentence shall be between three months and five years. If the offender causes the death of the victim, a relative or another person close to the victim, the prison sentence shall be from one to ten years.⁹³

^{84 §238 (1)} para 1 StGB.

^{85 §238 (1)} para 2 StGB.

⁸⁶ § 238 (1) para 3 StGB.

⁸⁷ § 238 (1) para 4 StGB.

⁸⁸ J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 155.

⁸⁹ T Fischer, StGB Kommentar (64th edition, Beck 2017), § 238, Rn 6

⁹⁰ See 40th StGB amendment of 22 March 2007 (Gesetz zur Strafbarkeit beharrlicher Nachstellungen (40. StÄG) vom 22.3.2007, BGBI I, 354).

⁹¹ T Fischer, StGB Kommentar (64th edition, Beck 2017), § 238, Rn 3.

⁹² T Fischer, StGB Kommentar (64th edition, Beck 2017), § 238, Rn 3a.

^{93 § 238 (3)} StGB.

- 1.38 In the online world, §238 (1) StGB applies to situations of cyberstalking, including stalking via email and on social media platforms. 94 The most relevant subsection of §238 (1) StGB is paragraph 2, which prohibits stalking in the form of harassing the victim through repeated contacts via means of telecommunication. 95 Means of telecommunication include SMS, telephone, email, as well as messengers on social medial platforms or chat windows in chat rooms. 96
- 1.39 For § 238 (1) StGB to apply, the offender's behaviour needs to be persistent and incessant. At times, it can be difficult to draw a line between normal social behaviour and stalking, since repeated telephone calls and the sending of several emails can constitute adequate social behaviour.⁹⁷ This is why for the application of § 238 (1) StGB the actions of the offender need to be highly persistent and contrary to the will of the victim.⁹⁸
- 1.40 Lastly, the actions of the offender must lead to a serious limitation of the victim's conduct of life. These limitations must go beyond normal and acceptable interferences of another person's day-to-day life. Serious limitations of the victim's daily life can manifest, for example, in the victim changing her home or her work against her will, only to escape the stalker.⁹⁹ In contrast, switching off a telephone or ceasing to use an answering machine would not constitute a serious limitation.¹⁰⁰ In light of this, shutting down an email address or social media profile by the victim would probably not, by itself, amount to a serious limitation of the victim's daily life.¹⁰¹
- 1.41 At the same time, social media has been used as one tool for committing stalking offences in combination with other means that ultimately led to victims having to change jobs and cities, ¹⁰² or even attempting suicide. ¹⁰³ In this context, social media allows stalkers to easily identify friends and family of victims and to harass the victim through contacting the victim's close persons. ¹⁰⁴

⁹⁴ J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 152.

⁹⁵ As above, 153.

⁹⁶ As above, 154.

⁹⁷ As above, 155.

⁹⁸ As above. See also judgment by the German Federal Supreme Court of 19 November 2009, BGHSt 54, 189-202.

⁹⁹ J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 156; Fischer (2017), § 238, Rn 22-24.

J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 156.

T Fischer, *StGB Kommentar* (64th edition, Beck 2017), § 238, Rn 24. In addition, social media platforms and email services allow for the blocking of certain users and senders.

LG Dortmund (Regional Court Dortmund), judgment of 22 November 2012 – 44 KLs - 110 Js 720/11 - 33/12 –, juris.

¹⁰³ BGH, NJW 2017, 2211-2214.

This was the case, for example, in LG Dortmund (Regional Court Dortmund), judgment of 22 November 2012 – 44 KLs - 110 Js 720/11 - 33/12 –, juris.

INSULTS & DEFAMATION

- 1.42 Insults and defamation are dealt with under §§ 185 to 187 StGB. Under §185, an insult may be punished with a prison sentence of up to one year or a fine. If the insult is committed by means of an assault, it shall be punished with a prison sentence of up to two years or a fine. The content of an insult must show disrespect for another person regarding her ethical value determined by her outer appearance and behaviour, or her social value determined by qualities or responsibilities to fulfil a certain public role or profession.¹⁰⁵
- 1.43 To determine whether something amounts to an insult, the situational context needs to be considered in its entirety and evaluated on a case-by-case basis. ¹⁰⁶ This includes, in particular, taking into account opinions and customs of the parties involved, and the linguistic and social environment in which a remark was made. ¹⁰⁷ Changes in the meaning of linguistic expressions or symbols, as well as divergences in meaning due to social class, age, membership of certain subcultures, nationalities, and regional particularities (including dialects) need to be considered. ¹⁰⁸ This assessment has to be undertaken objectively, from the perspective of a reasonable third party would understand the remark in context. ¹⁰⁹ It has been noted that language used publicly on the internet tends to be more provocative and extreme than ordinary language, which might require a readjustment in the substantive interpretation of what constitutes an insult. ¹¹⁰
- 1.44 § 185 StGB is applicable to insults made via emails, on websites, social media and other internet platforms, as well as in the press.¹¹¹ § 185 StGB has the purpose of protecting a person's honour, and applies when the offender attacks the victim by denigrating her or by falsely attributing deficiencies to her that would harm her reputation if they were true.¹¹² § 185 StGB only covers negative value judgments, and not untruths about a person communicated to a third party. The latter scenario would qualify as defamation, which falls under §§ 186 and 187 StGB.¹¹³
- 1.45 Insults not against individuals, but against groups of persons are only punishable in limited circumstances under § 185 StGB. In order for the provision to apply to insults made against groups of persons, three conditions must be fulfilled: the group must be clearly defined, it must fulfil a legally recognised social or economic function, and it

T Fischer, StGB Kommentar (63rd edition, Beck 2016), § 185, Rn 8.

T Fischer, *StGB Kommentar* (63rd edition, Beck 2016), § 185, Rn 8. This definition is usually used by German courts, for a recent case see, for example, OLG Karlsruhe (Higher Regional Court Karlsruhe), judgment of 22 Mai 2018 – 2 Rv 4 Ss 193/18 –, juris.

T Fischer, StGB Kommentar (63rd edition, Beck 2016), § 185, Rn 8.

¹⁰⁸ T Fischer, StGB Kommentar (63rd edition, Beck 2016), § 185, Rn 8.

¹⁰⁹ Kühl and Heger (2018), § 185, Rn 4; Fischer (2016), § 185, Rn 8.

¹¹⁰ T Fischer, StGB Kommentar (64th edition, Beck 2017), § 185, Rn 12a.

¹¹¹ J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 110.

¹¹² As above.

¹¹³ As above.

must have a collective decision-making capacity or uniform will. 114 Generally, family honour is not protected under § 185 StGB; 115 that is, a family is not a group of persons which can be the victim of an offence under § 185 StGB. Insulting the police in general, for example, would also not be caught under § 185; 116 while the police as a whole fulfils a social function recognised by the law, it does not have a uniform decision making-capacity, since there are many independent units within the police at federal and regional level that differ in tasks, significance, and organization. 117 Insulting one specific police unit of a municipality, in contrast, would be caught under § 185, since this would constitute a clearly defined group of individuals. 118 The military, too, would be considered as a clearly defined group of persons, due to having a social function recognized by the law (under Article 87a of the German Constitution) and a uniform will or decision-making capacity held by the Defence Minister. 119 Another group that has been recognized as a sufficiently clearly defined group under § 185 StGB has been, for example, the Qatar Football Association. 120

1.46 § 186 StGB covers defamation, that is, negative false statements made about a person to a third party. 121 § 186 StGB stipulates that:

whosoever asserts or disseminates a fact related to another person which may defame him or negatively affect public opinion about him, shall, unless this fact can be proven to be true, be liable to imprisonment not exceeding one year or a fine and, if the offence was committed publicly or through the dissemination of written materials (§ 11(3) StGB), to imprisonment not exceeding two years or a fine. 122

1.47 A defamation is public when a large number of persons not necessarily in a relationship with each other can take notice of it.¹²³ A defamatory statement on a website will always be considered as public whenever a website's access is not

J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 112; BGH 6, 186 Kapitalgesellschaft.

¹¹⁵ T Fischer, *StGB Kommentar* (64th edition, Beck 2017), Vor § 185, Rn 11a.

Insulting the collectivity of "soldiers" has also not been found contrary to § 185 StGB, see judgment of the Federal Constitutional Court of 10 Ocober 1995 (BVerfG, Beschluss vom 10. Oktober 1995 – 1 BvR 1476/91 –, BVerfGE 93, 266-319).

Bayerisches Oberstes Landesgericht (Highest Regional Court of Bavaria), judgment of 22 Dezember 1989 – RReg 1 St 193/89 –, juris.

Eisele (2013), 113. See also Klaus Geppert ,Zur Frage strafbarer Kollektivbeleidigung der Polizei oder einzelner Polizeibeamter durch Verwendung des Kürzels "a.c.a.b.", *NStZ 2013*, 553-559.

¹¹⁹ LG Frankfurt (Regional Court Frankfurt), judgment of 20 Oktober 1989 – 5/29 Ns 50 Js 26112/84 –, juris.

LG Düsseldorf (Regional Court Düsseldorf), judgment of 19 April 2016 – 6 O 226/15 –, juris.

¹²¹ J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 114.

^{§ 11(3)} StGB clarifies that audio-visual media, data storage media, illustrations and other depictions shall be equivalent to "written material" referred to in different sections of the Criminal Code. It essentially provides an update to the Criminal Code for the digital age, where large numbers of people are no longer reached through written materials only, but all kinds of other media distributed over mass media and the internet.

¹²³ T Fischer, StGB Kommentar (64th edition, Beck 2017), § 187, Rn 16.

controlled or restricted.¹²⁴ A defamatory statement made in an email will generally not be considered to be public.¹²⁵

1.48 § 193 StGB provides a defence to liability under §§ 185 and 186 StGB in cases of fair comment. According to § 193 StGB:

critical opinions about scientific, artistic or commercial achievements, utterances made in order to exercise or protect rights or to safeguard legitimate interests, as well as remonstrations and reprimands by superiors to their subordinates, official reports or judgments by a civil servant, and similar cases shall only entail liability to the extent that the existence of an insult results from the form of the utterance and the circumstances under which it was made.

- 1.49 "Legitimate interests" generally covers all legitimate interests recognised in a legal system, such as public and private interests, fundamental rights, and economic interests. 126 § 193 StGB is applied on a case-by-case basis in the light of the principle of proportionality, that is, the interest of the offender (for example, freedom of expression or press freedom) must override the interest of the victim. The interest of the victim can never be overridden in cases of attacks against the victim's human dignity or in the case of abusive criticism. 127
- 1.50 § 187 StGB covers intentional defamation, ie the dissemination or assertion of a fact that the offender knows to be untrue (§ 186 StGB covers situations in which the untruthfulness of a fact cannot be proven). The sanctions under § 187 StGB are higher than under § 186 StGB, the prison sentences being up to two years, or five years in cases of public dissemination. No defence for intentional defamation is available under § 193 StGB.¹²⁸
- 1.51 The criminal offences in respect of insults and defamation protect personality rights and individual dignity. By contrast, the public order offences in respect of hate speech and incitement, which we consider below, protect group interests and harmony between different groups of the population (public order, public peace).

PUBLIC ORDER OFFENCES AND HATE SPEECH AND INCITEMENT

1.52 The criminal offence of "Volksverhetzung" (incitement of the people to hatred) comprises several public order offences, aiming to protect public order and public peace, as well as individual dignity.

¹²⁴ T Fischer, StGB Kommentar (64th edition, Beck 2017), § 187, Rn 19.

T Fischer, StGB Kommentar (64th edition, Beck 2017), § 187, T Fischer, StGB Kommentar (64th edition, Beck 2017)19.

¹²⁶ J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 118.

¹²⁷ As above.

¹²⁸ As above, 117.

1.53 § 130 (1) No 1 of the German Criminal Code (StGB) contains an incitement to hatred offence: 129

whosoever incites hatred or abuse or violence against a national, racial, religious, or ethnically defined group, or against certain parts of the population or against an individual because of his/her belonging to such a group or, to a particular part of the population, if this has the potential to disturb the public peace.

- 1.54 "Abuse" ("Willkürmaßnahmen") refers to acts which are discriminatory or inhumane. 130
- 1.55 A second offence is contained in § 130 (1) No 2 StGB:¹³¹ "whosoever attacks the dignity of others by maliciously sowing contempt or defaming such a group, parts of the population or an individual because of his/her belonging to such a group or, to a particular part of the population", if this has the potential to disturb the public peace. There is a high threshold before a statement amounts to an attack on human dignity: the persons attacked must be treated as less-valued or second-rate beings.¹³²
- 1.56 This offence is wider than just hatred against persons based on their nationality, religion, ethnic group and so forth it covers any sub-grouping of the population in Germany, 133 such as "dark-skinned people", 134 "asylum-seekers" 135 or "punks". The group has to be sufficiently defined. A group is sufficiently defined if it is clear who belongs to it and who does not, based on external or internal distinguishing factors (for example, ideology, profession, or socio-economic status). 136 The fans of a football club, for example, would not count as a relevant part of the German population, 137 and nor would "lefties and the anti-fascism mob". 138 The group can be wide, however, as long as it is sufficiently defined and an attack on an individual can be representative for an attack on the group thus hate speech against disabled persons or the LGBT community would be covered. 139
- 1.57 Both these offences attract a sentence ranging from three months to five years.

¹²⁹ Translation by the authors.

J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 126.

¹³¹ As above.

¹³² As above.

J Eisele, *Computer- und Medienstrafrecht* (Verlag C.H. Beck, München,2013) 125; T Fischer, *StGB Kommentar* (63rd edition, Beck 2016), §150, Rn 5.

OLG Zweibrücken NStZ 1994, 490.

¹³⁵ BayObLG NJW 1994, 952.

¹³⁶ T Fischer, *StGB Kommentar* (63rd edition, Beck 2016), § 130, Rn 4; Kühl and Heger (2018), § 130, Rn 2.

¹³⁷ J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 126.

¹³⁸ BGH NStZ-RR 2009,13.

¹³⁹ J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 126.

- 1.58 The potential to disturb the public peace is more likely if the material is likely to come to the attention of a broad range of the public, for example on the internet. 140
- 1.59 § 130 (2) StGB provides for a number of offences in relation to the distribution and dissemination of documents (written materials, but widely defined, to include electronic documents, storage media and images (such as a PDF)).¹⁴¹ For these dissemination offences, no evidence that the public peace is disturbed is required, but the dissemination must be public (or to a minor).¹⁴²
- 1.60 In relation to dissemination online, a distinction could be made between forms of online communication which are clearly limited to a small and restricted number of recipients (such as an email sent to a limited number of persons, or a chatroom open only to a limited number of participants, or a Facebook group limited to a handful of persons) and forms of online communication with a potentially wide reach, such as a website, public blog, social media with a large number of followers, or a YouTube video which is made generally available. The former is less likely to count as dissemination to "the general public", and the following dissemination offences would be applicable to the latter only.
- 1.61 § 130 (2) No 1 StGB contains an offence concerning the distribution of documents: "whosoever disseminates or makes available, or offers to make available to, the general public, or gives to a minor, a document which:
 - (1) incites hatred against the person(s) mentioned in §130 (1) No 1; or
 - (2) calls for violence or abuse against the person(s) mentioned in § 130 (1) No 1; or
 - (3) attacks the dignity of such persons by insulting them, by maliciously sowing contempt, or defaming them";

may be sentenced to a fine or a maximum sentence of three years".

- 1.62 This includes making available on the internet. 143
- 1.63 Secondly, § 130 (2) No 2 contains an offence concerning the broadcasting or online distribution of such content (eg streaming) to either the general public, or a minor, which also attracts criminal penalty of a fine or a maximum sentence of three years.
- 1.64 Thirdly, § 130 (2) No 3 contains an offence concerning the production, obtaining, supply, storage for supply, offering, advertising, or importing or exporting for dissemination or broadcasting of such content, which attracts the same criminal penalty of a fine or a maximum sentence of three years.

As above, 127; BGHSt 46, 212 (219) Holocaust denial website.

^{§ 11 (3)} of the German Criminal Code has been updated to clarify that the expression "document" includes other media, such as storage media for sound and images, data storage media, images and other representations (for example in electronic format).

¹⁴² J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 127.

¹⁴³ BGH NStZ 2007, 216.

- 1.65 Finally, § 130 (3) and (4) contain offences concerning the approval, denial or the playing down of (certain) crimes committed during the National Socialist ("NS") era, in particular Holocaust denial. The approval, denial or the playing down of certain NS crimes in public or in a public assembly, if this is liable to disturb the public peace, is punishable with a sentence of up to five years or a fine. To condone, glorify or justify the NS totalitarian and violent regime, if done publicly or in an assembly and if it actually disturbs the public peace by violating the dignity of the victims is punishable with a sentence of up to three years or a fine. The distribution offences in § 130 (2) No 1-3 also apply in respect of such NS content.
- 1.66 Recent changes to these public order offences followed from the implementation of the EU Framework Decision 2008/913 and the Protocol to the Cybercrime Convention.¹⁴⁴
- 1.67 Thus, for the hate speech public order offences, while amendments have been made to ensure new technologies are captured by these offences, no separate offences have been created for the internet.
- 1.68 According to the Federal Criminal Statistics (Federal Police), in 2017 4,763 cases of incitement to hatred (§ 130 StGB) have been registered by all police forces, out of which 3,190 have been solved by the police (67%), involving 3,086 suspects. ¹⁴⁵ A separate statistic (part of the Federal Criminal Statistics of the Federal Police) shows that 2,384 of the cases registered with the police related to the internet as a means of committing the crime (in 2017 around 50%) and out of these 1,609 have been solved (67.5%), involving 1,437 suspects. ¹⁴⁶ Because of the increase of hate speech most local police forces have created specific portals which allow internet users to notify the police of hate speech online. ¹⁴⁷
- 1.69 An example of a well-publicised prosecution in November 2017 was against a soldier of the German army who had made postings on his Facebook account attacking asylum-seekers and immigrants, equating them with monkeys and vermin and suggesting that they should be put on a plane and dropped from mid-air and similar comments. He was convicted under § 130 (1) and sentenced to a fine of Euro 3750. The appeal court found the fact that these comments were made publicly by a serving soldier to be one element for finding that these comments endangered public peace and upheld the sentence. 148
- 1.70 Another relevant offence in this context is § 111 StGB, public incitement to the commission of a criminal offence: whoever publicly incites, in an assembly or through

Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

PSK available from https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2017/Standardtabellen/standardtabellenFaelle.html?nn=96600.

¹⁴⁶ As above, Table 5.

Online Portal
https://www.bka.de/DE/KontaktAufnehmen/Onlinewachen/onlinewachen_node.html;jsessionid=593C86FCB
B26A3D623FE152CB7572CB7.live0601.

¹⁴⁸ OLG Hamm (Beschluss vom 07. September 2017, Az. 4 RVs 103/17).

the dissemination of documents others to commit a criminal act, will be punished for incitement. If the incitement is not successful, the maximum penalty is up to five years' imprisonment or a fine. The punishment must not be more severe than if the crime incited had in fact been committed. The crime is committed even if the incitement was not the only reason for the addressee to commit the crime, but it must be a way of trying to influence others and motivate them to commit a crime. ¹⁴⁹ The incitement must be specific, focusing on a particular type and form of crime, but need not be specific in terms of its time, place and the victim. This offence is particularly relevant for incitements communicated over the internet. The addressees of the incitement appearing, for example, on a social media site are frequently not specified or determined, since the incitement may exhort "the world at large". This includes incitement published, for example on a website or social media site. ¹⁵⁰

- 1.71 In 2017, the German police forces registered 522 cases of public incitement to commit a crime, which were committed using the internet. Out of these, 356 (68.2 %) were solved, involving 341 suspects. ¹⁵¹ In total there were 793 cases of public incitement, so that the internet cases constitute 65.8%.
- 1.72 A further public order offence is § 131 StGB, representations of glorification of violence. This offence is to protect public order and public peace (rather than individual freedom from being exposed to such materials). Its purpose is to limit the representation of extreme aggression as trigger for public violence and to protect society from individuals who might develop in this direction, however, endangering the public peace is not part of the actus reus of this provision. The offence relates to written materials and images (documents) which express cruel or other inhumane violence against human beings (or beings similar to humans) in a manner which glorifies or belittles such violence or which represents the cruel or inhumane treatment in a way infringing human dignity. Thus, the representation of violence is not sufficient as such. Additionally, there must be a glorification or belittling of violence and the representation must infringe human dignity.
- 1.73 The criminal offences encompass:
 - (1) dissemination or making publicly available; or
 - (2) offering, giving or making it accessible to a minor or
 - (3) broadcasting it or making it available online (for example by streaming) to minors or the public; or
 - (4) producing, obtaining, supplying, storing, offering, advertising or importing/exporting for the purpose of dissemination.

¹⁴⁹ J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 134.

¹⁵⁰ As above, 135.

Available at:
https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2017/pks2017
s2017 node.html;isessionid=477E24151C780D4E3D14AC307FDCA2AF.live2302.

J Eisele, Computer- und Medienstrafrecht (Verlag C.H. Beck, München, 2013) 131.

- 1.74 There is an exception for reporting temporary or historical events in paragraph 135 (2).
- 1.75 The total number of cases registered with the police for representations of glorification of violence in 2017 was 364, of which 327 (89.8%) were solved involving a total of 367 suspects (with 18.8% of foreigners as suspects).190 of these cases were committed using the internet in 2017 (52%).¹⁵³
- 1.76 Finally, it should be noted that these offences must be interpreted in accordance with Article 5 of the German Constitution (freedom of expression, freedom of art).

¹⁵³ See no. 122