F. The Intelligence Act of 2015\textsuperscript{56}

The Act governs the activities of the intelligence services concerning their fight against terrorism, while maintaining the secrecy of correspondence. The Act authorizes the automatic analysis of data with the goal of detecting online patterns of behavior typically displayed by terrorists. Telecommunication operators are involved in the process and will be reported to the Prime Minister under the control of the National Commission for the Control of Intelligence Techniques. The act clarifies the concept of “national security” and the limits of usage of the surveillance measures. It prohibits monitoring of political parties, trade unions and peaceful protest. The Act provides that intrusion into privacy may be deemed necessary “in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”\textsuperscript{57} Under this law, internet providers are required to install “black boxes” to track a suspect’s online behavior. The Constitutional Council deemed the law a fair balance between public safety requirements and fundamental rights guarantees.\textsuperscript{58}

G. Code of Internal Security of 2012, as Amended up to 2016\textsuperscript{59}

According to Article L212-1 of the Code Associations and groups are dissolved by Order of the Council of Ministers if they among other reasons cause armed demonstrations in the streets, lead to discrimination, hatred or violence against a person or a group of persons because of their origin, membership (non-membership) in an ethnic group, nation, race, religion; or propagate ideas or theories tending to justify or encourage such discrimination, hatred or violence.\textsuperscript{60}

\begin{table}
\centering
\begin{tabular}{|l|l|l|l|}
\hline
\textbf{QUESTION} & \textbf{ANSWER} & \textbf{SOURCE OF LAW/ INFORMATION} & \textbf{ADDITIONAL RELEVANT INFORMATION / DEFINITIONS} & \textbf{COURT RULINGS} \\
\hline
Where is online hate speech established as a criminal offence? & The Criminal Code prohibits incitement to hatred, which may be carried out via “written materials” which is defined as including media storage and audiovisual media. Therefore, hate speech committed online is punishable. & Sections 11, 130, 130a, 131 of the Federal Criminal Code \textsuperscript{6}\textsuperscript{a} &  &  \\
\hline
What is the punishment for online hate speech? & For inciting to hatred - Imprisonment from three months to & Sections 11, 130, 130a, 131 of the Federal Criminal Code \textsuperscript{6}\textsuperscript{a} &  &  \\
\hline
\end{tabular}
\end{table}


\textsuperscript{57} http://www.gouvernement.fr/en/parlement-adopts-the-intelligence-bill

\textsuperscript{58}http://www.constitutionnet.org/news/france-under-mass-surveillance-french-constitutional-council-and-limits-intelligence-services


\textsuperscript{60} By a Presidential Decree of 14 January 2016 three associations, “Back to Basics”, “Returning to Muslim sources” and “Muslim Associations of Lagny-sur-Marne”, were dissolved in accordance with the Convention for the Protection of Human Rights and Fundamental Freedoms, in particular Articles 10 and 11 and Article L. 212-1 of Code of Internal Security. The Decree is available at http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025498645&categorieLien=id.
<p>| <strong>Is there a law-based obligation for intermediaries to monitor hate speech?</strong> | Teleservice Providers, including internet website companies, are not obligated to monitor content provided by third parties. | Sections 3 and 5 of the Teleservices Act c | “Teleservice Provider” is a person or company who provide access to the use of teleservices, which includes internet services. | Some regional courts and higher regional courts have imposed obligations on access providers like internet cafes or hotels, including port blocking. (Source: International Comparative Legal Guides, Telecoms, Media and Internet, 2017, available at <a href="http://www.iclg.co.uk/practice-areas/telecoms-media-and-internet-laws/telecoms-media-and-internet-laws-and-regulations-2016/germany">http://www.iclg.co.uk/practice-areas/telecoms-media-and-internet-laws/telecoms-media-and-internet-laws-and-regulations-2016/germany</a>.) |
| <strong>Who is responsible to remove/block access to hate speech?</strong> | Telecommunications operators, including internet service providers, are not obligated to disconnect customers who infringe upon third-party rights. Internet service providers are expected to block access to content after being made aware of the illegal content. According to the German State Treaty on Media Services the government through Internet Providers may restrict access to the websites with criminal content. (It is unclear whether this treaty is applicable to all news websites). | Sections 3 and 5 of the Teleservices Act c | German State Treaty on Media Services |  |</p>
<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is the required timeframe, if any, for removing hate speech?</td>
<td>Facebook, Twitter and Google have made an agreement with the German government to remove hate speech within 24 hours after notification.</td>
<td><a href="https://www.cnet.com/news/germany-is-putting-an-end-to-hate-speech-on-the-internet/">https://www.cnet.com/news/germany-is-putting-an-end-to-hate-speech-on-the-internet/</a></td>
</tr>
<tr>
<td>Is the intermediary liable for hate speech posted on a website?</td>
<td>Even though case law is not entirely consistent with respect to this question, in general, internet service providers are not liable for illegal content made available via their networks. They are only responsible for their own content, not the content of third parties unless made aware of the illegal nature of the content.</td>
<td>Act on the Utilization of Teleservices, Section 5 (Teleservices Act)²  (Source: <a href="http://www.iclg.co.uk/practice-areas/telecoms-media-and-internet-laws/telecoms-media-and-internet-laws-and-regulations-2016/germany/">http://www.iclg.co.uk/practice-areas/telecoms-media-and-internet-laws/telecoms-media-and-internet-laws-and-regulations-2016/germany/</a>)</td>
</tr>
<tr>
<td>Are there any online mechanisms for anyone to report about hate speech content?</td>
<td>There are no online reporting mechanisms.</td>
<td></td>
</tr>
</tbody>
</table>
| When is the offence considered to have been committed within the territory under the country’s jurisdiction? | The offer and the provision of tele media by a service provider who is established in another state shall be subject to the restrictions of domestic law, to the extent that this serves to protect: public security and order, especially with regard to the prevention, investigation, detection, prosecution and punishment of crimes and administrative offences, including protection of young people and the fight against incitement to hatred on grounds of race, sex, religion or nationality, and of violations of human dignity concerning individual persons, etc. | According to a Mannheim district court ruling of 2000, if the offence is committed abroad either by a German national or foreigner, it can still be pursued as a domestic offense, if it is determined that the offense affected the public peace in Germany or violated the human dignity of German citizens.  
For example, if the criminal content on the internet may be accessed from within the German territory. Hence the jurisdiction of German courts can be applied to the offences committed abroad.  (Source: [BGH 1 StR 184/00 – Urteil vom 12. Dezember 2000 Landgericht Mannheim (BGH 1)](https://www.bgh.de/wp-content/uploads/2021/06/BGH_1_StR_184_00_Urteil_vom_12._Dezember_2000_Landgericht_Mannheim_(BGH_1).pdf)) |

**GERMANY APPENDIX**


Section 11

"(1)-(2) (…)

(3) Audiovisual media, data storage media, illustrations and other depictions shall be equivalent to written material in the provisions which refer to this subsection."

Section 130 - Incitement to hatred

"(1) Whosoever, in a manner capable of disturbing the public peace

1. incites hatred against a national, racial, religious group or a group defined by their ethnic origins, against segments of the population or individuals because of their belonging to one of the aforementioned groups or segments of the population or calls for violent or arbitrary measures against them; or
2. assaults the human dignity of others by insulting, maliciously maligning an aforementioned group, segments of the population or individuals because of their belonging to one of the aforementioned groups or segments of the population, or defaming segments of the population, shall be liable to imprisonment from three months to five years.

(2) Whosoever

1. with respect to written materials (section 11(3)) which incite hatred against an aforementioned group, segments of the population or individuals because of their belonging to one of the aforementioned groups or segments of the population which call for violent or arbitrary measures against them, or which assault their human dignity by insulting, maliciously maligning or defaming them, (a) disseminates such written materials; (b) publicly displays, posts, presents, or otherwise makes them accessible; (c) offers, supplies or makes them accessible to a person

---

under eighteen years; or (d) produces, obtains, supplies, stocks, offers, announces, commends, undertakes to import or export them, in order to use them or copies obtained from them within the meaning of Nos (a) to (c) or facilitate such use by another; or

2. disseminates a presentation of the content indicated in No. 1 above by radio, media services, or telecommunication services shall be liable to imprisonment of up to three years or a fine.

(3) Whosoever publicly or in a meeting approves of, denies or downplays an act committed under the rule of National Socialism of the kind indicated in section 6 (1) of the Code of International Criminal Law, in a manner capable of disturbing the public peace shall be liable to imprisonment not exceeding five years or a fine.

(4) Whosoever publicly or in a meeting disturbs the public peace in a manner that violates the dignity of the victims by approving of, glorifying, or justifying National Socialist rule of arbitrary force shall be liable to imprisonment of up to three years or a fine.

(5) Subsection (2) above shall also apply to written materials (section 11(3)) of a content such as is indicated in subsections (3) and (4) above.

(6) In cases under subsection (2) above, also in conjunction with subsection (5) above, and in cases of subsections (3) and (4) above, section 86(3) shall apply mutatis mutandis.”

Section 130a - Attempting to cause the commission of offences by means of publication

“(1) Whosoever disseminates, publicly displays, posts, presents, or otherwise makes accessible written material (section 11(3)) capable of serving as an instruction for an unlawful act named in section 126(1) and intended by its content to encourage or cause others to commit such an act, shall be liable to imprisonment not exceeding three years or a fine.

(2) Whosoever

1. disseminates, publicly displays, posts, presents, or otherwise makes accessible written material (section 11(3)) capable of serving as an instruction for an unlawful act named in section 126(1); or

2. gives instructions for an unlawful act named in section 126(1) publicly or in a meeting, in order to encourage or cause others to commit such an act, shall incur the same penalty.

(3) Section 86(3) shall apply mutatis mutandis.”

Section 131 - Dissemination of depictions of violence

“(1) Whosoever

1. disseminates written materials (section 11(3)), which describe cruel or otherwise inhuman acts of violence against humans or humanoid beings in a manner expressing glorification or which downplays such acts of violence or which represents the cruel or inhuman aspects of the event in a manner which violates human dignity;

2. publicly displays, posts, presents, or otherwise makes them accessible:

3. offers, supplies or makes them accessible to a person under eighteen years; or

4. produces, obtains, supplies, stocks, offers, announces, commends, undertakes
to import or export them, in order to use them or copies obtained from them within the meaning of numbers 1 to 3 above or facilitate such use by another, shall be liable to imprisonment not exceeding one year or a fine.

(2) Whosoever disseminates a presentation with a content indicated in subsection (1) above by radio, media services, or telecommunication services shall incur the same penalty.

(3) Subsections (1) and (2) above shall not apply in cases of reporting about current or historical events.

(4) Subsection (1) No 3 above shall not apply if the person authorized to care for another person acts; this shall not apply if that person grossly neglects his duty of education by offering, giving, or making them accessible.”

B. German Code of Criminal Procedure

Section 100a - Conditions Regarding Interception of Telecommunications

“(1) Telecommunications may be intercepted and recorded also without the knowledge of the persons concerned if

1. certain facts give rise to the suspicion that a person, either as perpetrator or as inciter or accessory, has committed a serious criminal offence referred to in subsection (2) or, in cases where there is criminal liability for attempt, has attempted to commit such an offence or has prepared such an offence by committing a criminal offence; and

2. the offence is one of particular gravity in the individual case as well; and

3. other means of establishing the facts or determining the accused’s whereabouts would be much more difficult or offer no prospect of success.

(2) Serious criminal offences for the purposes of subsection (1), number 1, shall be:
1. pursuant to the Criminal Code:
   d) crimes against public order pursuant to sections 129 to 130;
(3) Such order may be made only against the accused or against persons in respect of whom it may be assumed, on the basis of certain facts, that they are receiving or transmitting messages intended for, or transmitted by, the accused, or that the accused is using their telephone connection.
(4) If there are factual indications for assuming that only information concerning the core area of the private conduct of life would be acquired through a measure pursuant to subsection (1), the measure shall be inadmissible. Information concerning the core area of the private conduct of life which is acquired during a measure pursuant to subsection (1) shall not be used. Any records thereof shall be deleted without delay. The fact that they were obtained and deleted shall be documented.”

Section 100b - Order to Intercept Telecommunications

“(1) Measures pursuant to Section 100a may be ordered by the court only upon application by the public prosecution office. In exigent circumstances, the public prosecution office may also issue an order. An order issued by the public prosecution office shall become ineffective if it is not confirmed by the court within three working days. The order shall be limited to a maximum duration of three months. An extension by not more than three months each time shall be admissible if the conditions for the order continue to exist, taking into account the information acquired during the investigation.
(2) The order shall be given in writing. The operative part of the order shall indicate
1. where known, the name and address of the person against whom the measure is directed;
2. the telephone number or other code of the telephone connection or terminal equipment to be intercepted, insofar as there are no particular facts indicating that they are not at the same time assigned to another piece of terminal equipment;
3. the type, extent and duration of the measure specifying the time at which it will be concluded.
(3) On the basis of this order all persons providing, or contributing to the provision of, telecommunications services on a commercial basis shall enable the court, the public prosecution office and officials working in the police force to assist it (section 152 of the Courts Constitution Act), to implement measures pursuant to Section 100a and shall provide the required information without delay. Whether and to what extent measures are to be taken in this respect shall follow from the Telecommunications Act and from the Telecommunications Interception Ordinance issued thereunder. Section 95 subsection (2) shall apply mutatis mutandis.
(4) If the conditions for making the order no longer prevail, the measures implemented on the basis of the order shall be terminated without delay. Upon termination of the measure, the court which issued the order shall be notified of the results thereof.
(5) The Länder and the Federal Public Prosecutor General shall submit a report to the Federal Office of Justice every calendar year by the 30th June of the year following the reporting year, concerning measures ordered pursuant to Section 100a within their area of competence. The Federal Office of Justice shall produce a summary of the measures ordered nationwide during the reporting year and shall publish it on the Internet.
(6) The reports pursuant to subsection (5) shall indicate:
1. the number of proceedings in which measures were ordered pursuant to Section 100a subsection (1);
2. the number of orders to intercept telecommunications pursuant to Section 100a subsection (1), distinguishing between
   a) initial and follow-up orders, as well as
   b) fixed, mobile and Internet telecommunication;
3. in each case the underlying criminal offence by reference to the categories listed in Section 100a subsection (2).”

Section 100g - Information on Telecommunications Connections

“(1) If certain facts give rise to the suspicion that a person, either as perpetrator or as inciter or accessory,
   1. has committed a criminal offence of substantial significance in the individual case as well, particularly one of the offences referred to in Section 100a subsection (2), or, in cases where there is criminal liability for attempt, has attempted to commit such an offence or has prepared such an offence by committing a criminal offence, or
   2. has committed a criminal offence by means of telecommunication,
then, to the extent that this is necessary to establish the facts or determine the accused’s whereabouts, telecommunications traffic data (section 96 subsection (1), section 113a of the Telecommunications Act) may be obtained also without the knowledge of the person concerned. In the case referred to in the first sentence, number 2, the measure shall be admissible only where other means of establishing
the facts or determining the accused’s whereabouts would offer no prospect of success and if the acquisition of the data is proportionate to the importance of the case. The acquisition of location data in real time shall be admissible only in the case of the first sentence, number 1.

(2) Section 100a subsection (3) and Section 100b subsections (1) to (4), first sentence, shall apply mutatis mutandis. Unlike Section 100b subsection (2), second sentence, number 2, in the case of a criminal offence of substantial significance, a sufficiently precise spatial and temporal description of the telecommunication shall suffice where other means of establishing the facts or determining the accused’s whereabouts would offer no prospect of success or be much more difficult.

(3) If the telecommunications traffic data is not acquired by the telecommunications services provider, the general provisions shall apply after conclusion of the communication process.

(4) In accordance with Section 100b subsection (5) an annual report shall be produced in respect of measures pursuant to subsection (1), specifying
   1. the number of proceedings during which measures were implemented pursuant to subsection (1);
   2. the number of measures ordered pursuant to subsection (1) distinguishing between initial orders and subsequent extension orders;
   3. in each case the underlying criminal offence, distinguishing between numbers 1 and 2 of subsection (1), first sentence;
   4. the number of months elapsed during which telecommunications traffic data was intercepted, measured from the time the order was made;
   5. the number of measures which produced no results because the data intercepted was wholly or partially unavailable.”

**Section 100b - Taking of Photographs; Technical Devices for Surveillance**

(1) Also without the knowledge of the persons concerned
   1. photographs may be taken or
   2. other special technical devices intended specifically for surveillance purposes may be used

outside private premises where other means of establishing the facts or determining an accused’s whereabouts would offer less prospect of success or be more difficult. A measure pursuant to the first sentence, number 2, shall be admissible only if the object of the enquiry is a criminal offence of substantial significance.

(2) The measures may only be directed against an accused person. In respect of other persons,
   1. measures pursuant to subsection (1), number 1, shall be admissible only where other means of establishing the facts or determining an accused’s whereabouts would offer much less prospect of success or be much more difficult;
   2. measures pursuant to subsection (1), number 2, shall only be admissible if it is to be assumed, on the basis of certain facts, that they are in contact with an accused person or that such contact will be established, the measure will result in the establishment of the facts or the determination of an accused’s whereabouts, and other means would offer no prospect of success or be much more difficult.

(3) The measure may be implemented even if it unavoidably affects third persons.”

**Section 100i - IMS I-Catcher**

“(1) If certain facts give rise to the suspicion that a person, either as perpetrator or as inciter or accessory, has committed a criminal offence of substantial significance, in the individual case as well, particularly one of the offences referred to in Section 100a subsection (2), or, in cases where there is criminal liability for attempt has attempted to commit such an offence or has prepared such an offence by committing a criminal offence, then technical means may be used to determine
   1. the device ID of a mobile end terminal and the card number of the card used therein, as well as
   2. the location of a mobile end terminal, insofar as this is necessary to establish the facts or determine the whereabouts of the accused person.

(2) Personal data concerning third persons may be acquired in the course of such measures only if, for technical reasons, this is unavoidable to fulfill the objectives of subsection (1). Such data may not be used for any purpose beyond the comparison of data in order to locate the device ID and card number sought, and the data is to be deleted without delay once the measure has been completed.

(3) Section 100a subsection (3) and Section 100b subsection (1), first to third sentences, as well as subsection (2), first sentence, and subsection (4), first sentence, shall apply mutatis mutandis. The order shall be limited to a maximum period of six months. An extension of not more than six months in each case shall be admissible if the conditions set out in subsection (1) continue to exist.”

**Section 100j - Request for Information**

“(1) Insofar as necessary to establish the facts or determine the whereabouts of an accused person, information on data collected pursuant to sections 95 and 111 of the Telecommunications Act may be requested from any person providing or collaborating in the provision of telecommunications services on a commercial basis (section 113 subsection (1), first sentence, of the Telecommunications Act). If the request for information pursuant to the first sentence refers to data by means of which access to terminal equipment, or to storage media installed in such terminal equipment or physically separate
therefrom, is protected (section 113 subsection (1), second sentence, of the Telecommunications Act), information may only be requested if the statutory requirements for the use of such data have been met.

(2) The information pursuant to subsection (1) may also be requested by reference to an Internet Protocol address assigned to a specific time (section 113 subsection (1), third sentence, of the Telecommunications Act).

(3) Requests for information pursuant to subsection (1), second sentence, may be ordered by the court only upon application by the public prosecution office. In exigent circumstances the order may also be issued by the public prosecution office or by the officials assisting it (section 152 of the Courts Constitution Act). In this case a court decision is to be sought without delay. The first to third sentences shall not apply if the person concerned already has or must have knowledge of the request for information or if the use of the data has already been permitted by a court decision. The fulfilment of the conditions pursuant to the fourth sentence shall be documented.

(4) In the cases referred to in subsection (1), second sentence, and subsection (2), the person concerned shall be notified of the request for information. Notification shall take place insofar as and as soon as this can be effected without thwarting the purpose of the information. It shall be dispensed with where overriding interests meriting protection of third parties or of the person concerned himself constitute an obstacle thereto. Where notification is deferred pursuant to the second sentence or dispensed with pursuant to the third sentence, the reasons therefor shall be documented.

(5) On the basis of a request for information pursuant to subsection (1) or (2), any person providing or collaborating in the provision of telecommunications services on a commercial basis shall transmit without delay the data required for the provision of the information. Section 95 subsection (2) shall apply mutatis mutandis.”

C. Teleservices Act of 1997 (Teledienstergesetz, TDG) 63

Section 2 - Scope

"(1) (…)

(2) Teleservices within the meaning of § 2 (1) shall include in particular:

1. services offered in the field of individual communication (e.g. telebanking, data exchange),
2. services offered for information or communication unless the emphasis is on editorial arrangement to form public opinion (data services providing e.g. traffic, weather, environmental and stock exchange data, the dissemination of information on goods and services),
3. services providing access to the Internet or other networks,
4. services offering access to telegames,
5. goods and services offered and listed in electronically accessible data bases with interactive access and the possibility for direct order.

(3) § 2 (1) shall apply irrespective of whether the use of the teleservices is free of charge either wholly or partially.

(4) This Act shall not apply to

1. telecommunications services and the commercial provision of telecommunications services under § 3 of the Telecommunications Act of 25 July 1996 (Telekommunikationsgesetz , Federal Law Gazette BGBl. I, page 1120),
2. broadcasting as defined in § 2 of the Interstate Agreement on Broadcasting (Rundfunkstaatsvertrag),
3. content provided by distribution and on-demand services if the emphasis is an editorial arrangement to form public opinion pursuant to § 2 of the Interstate Agreement on Media Services (Mediendienste-Staatsvertrag) signed between 20 January and 7 February 1997.

(5) Legal provisions concerning press law remain unaffected.”

Section 3 - Definitions

“For the purposes of this Act

1. the term "providers" means natural or legal persons or associations of persons who make available either their own or third-party teleservices or who provide access to the use of teleservices,
2. the term "users" means natural or legal persons or associations of persons requesting teleservices.”

---

Section 5 - Responsibility

“(1) Providers shall be responsible in accordance with general laws for their own content, which they make available for use.
(2) Providers shall not be responsible for any third-party content which they make available for use unless they have knowledge of such content and are technically able and can reasonably be expected to block the use of such content.
(3) Providers shall not be responsible for any third-party content to which they only provide access. The automatic and temporary storage of third-party content due to user request shall be considered as providing access.
(4) The obligations in accordance with general laws to block the use of illegal content shall remain unaffected if the provider obtains knowledge of such content while complying with telecommunications secrecy under § 85 of the Telecommunications Act (Telekommunikationsgesetz) and if blocking is technically feasible and can reasonably be expected.”

<table>
<thead>
<tr>
<th>QUESTION</th>
<th>ANSWER</th>
<th>SOURCE OF LAW/ INFORMATION</th>
<th>ADDITIONAL DEFINITIONS</th>
<th>INFORMATION/ DEFINITIONS</th>
<th>COURT RULINGS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where is online hate speech established as a criminal offence?</td>
<td>Hate speech, or incitement to hatred, made available to the &quot;public at large&quot;, including on the internet, is prohibited in Hungary's Criminal Code. Media content may not incite to hatred against any nation, community, national, ethnic, linguistic or other minority or any majority as well as any church or religious group.</td>
<td>Sections 77, 332, and 459 of the Criminal Code (^{A}) Articles 17 and 21 of the Act on the Freedom of the Press and Fundamental Rules on Media Content (^{F}) &quot;Public at large&quot; as defined in Section 459 of the Criminal Code, is when a crime is committed through publication in the press or other media services, by way of reproduction or by means of publication on an electronic communications network. (^{A}) “The meaning of the term ‘general public’ has been interpreted by the Supreme Court of Hungary, which found that a crime can be said to have been committed in front of the general public if, during its perpetration, a bigger group of people was present, or there is a chance that a group of a bigger number of people will learn about the result of the crime. In the meaning of the provision a group should contain a large number of people (where the number cannot be specified, it should be at least 20-30 people”). (^{64})</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>What is the punishment for online hate speech?</td>
<td>Imprisonment of up to three years (^{A})</td>
<td>Section 332 of the Criminal Code (^{A})</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>