

Counter-Intelligence

Trans- national Repression

Guidance for people affected



Federal Ministry
of the Interior

Contents

What is transnational repression?	3
How can transnational repression be reported?.....	4
1. Immediate danger	5
2. Possible criminal offense	5
3. Tip line of the Federal Office for the Protection of the Constitution (BfV)	5
4. Misuse of INTERPOL Notices.....	5
What can people affected by transnational repression do to protect themselves?.....	6
1. Cybersecurity	7
2. Personal safety and security.....	9
3. Travel advice	10
4. Support services.....	11

What is transnational repression?

The German Federal Government has set itself the goal of effectively countering transnational repression by authoritarian states in Germany.

Transnational repression (TNR) refers to any action taken by a foreign state to persecute, oppress and/or intimidate individuals living abroad whom it classifies as opponents.

The actions of foreign states range from espionage and intimidation to the most serious threats to life and limb. TNR can take the following forms, amongst others:

- Physical attacks, which can range from physical assault and abduction to the murder of the person
- Spying, threats, harassment, stalking, etc., often used to exert psychological pressure
- Digital forms of transnational repression such as online intimidation, online defamation, doxing, and cyberattacks against the targeted person

- Abuse of multilateral and bilateral law enforcement mechanisms such as INTERPOL Red Notices, extradition proceedings, notices about travel documents and other forms of intergovernmental legal assistance
- Abuse or denial of consular services by the foreign state
- Threats to family members

Those particularly affected include opposition figures living abroad, human rights activists, journalists and members of diaspora communities.

*How can
transna-
tional
repression
be reported?*

1. Immediate danger

People who are in **immediate danger** and/or wish to report a crime should call the **police emergency number** (110).

2. Possible criminal offense

If there is no imminent danger but a crime may have occurred, the **local police station** or the relevant **state criminal police office** (Landeskriminalamt) should be contacted. Contact information (telephone numbers and email addresses) is available on the internet. These police authorities are also responsible for individual threat assessments and for taking any (protective) measures that may be necessary.

3. Tip line of the Federal Office for the Protection of the Constitution (BfV)

Those affected can also confidentially contact the tip line of the Federal Office for the Protection of the Constitution (BfV) at any time if they suspect that government agencies or even intelligence services are behind the actions in question:

Telephone numbers:

+49 228 99792-6000

+49 30 18792-6000

Email: hinweise@bfv.bund.de

Or you can use the contact form on the website of the Federal Office for the Protection of the Constitution: https://www.verfassungsschutz.de/DE/service/kontakt/formulare/Kontakt_HinweisGeben/kontakt_node.html

Your tip will be investigated in all cases, although in most cases you will not receive a response from the Federal Office for the Protection of the Constitution. In individual cases, you may be contacted if further information is required. Every tip is helpful, and there are no consequences to worry about if a tip turns out to be incorrect.

4. Misuse of INTERPOL Notices

If you are a victim of the misuse of INTERPOL Notices, or suspect that you have been, you can directly contact the Commission for the Control of INTERPOL's Files (CCF). The Commission has three functions, in which it handles individual's requests for access to, correction of or deletion of data in the INTERPOL Information System. To perform its functions, the Commission directly consults the INTERPOL General Secretariat, National Central Bureaus and other relevant entities.

<https://www.interpol.int/en/Who-we-are/Commission-for-the-Control-of-INTERPOL-s-Files-CCF>

*What can
people af-
fected by
transna-
tional re-
pression do
to protect
themselves?*

1. Cybersecurity

Potential threats in cyberspace by foreign state actors range from intimidation and the spying on personal networks and communications to preparatory actions for repressive measures in the real world. The measures outlined below illustrate steps which could be taken to increase your level of security against cyberattacks and thereby to potentially reduce the damage done by such attacks:

Private data

- Be cautious about sharing your personal information, especially on social media.
- Do not reveal any personal information on websites which are not trustworthy.
- Demonstrate a healthy amount of mistrust.

Cloud services

- Make a conscious choice about which cloud services you use and what you save in the cloud.
- Deactivate automatic uploading and synchronisation.

E-Mail

- Protect yourself from phishing.
Be suspicious of emails, and check with the sender in cases of doubt.
- Do not click on links or open attachments without examining them carefully.
- Email clients should be configured in such a way that they do not automatically interpret any HTML code or other active elements in emails. Setting email to be displayed as “text only” (rather than e.g. HTML) reduces the risk of deception.

- Preview functions for attached files should be configured in such a way that they do not automatically interpret files.

Mobile devices

- When communicating via messenger services, only use services with end-to-end encryption that are suitable for secure sharing of information (e.g. Signal, Threema). Block any messages you receive from unknown senders and deactivate link preview functions.
- Only obtain apps from trustworthy sources (e.g. pre-installed app stores).
- If you are an iPhone user: Check whether you have activated “lockdown” mode. This mode was developed by Apple specifically for protection from sophisticated cyber threats such as those in the area of transnational repression.
- Shut off your mobile device entirely to prevent tracking or interception of communications or leave it at home when you go to sensitive meetings.
Be aware that wearables such as smart watches and smart glasses also contain the same functions.
- App stores offer apps that can detect unauthorized tracking via smart tags.
- Do not leave your mobile device unattended.
- Always keep the operating system of your mobile device up to date.
- Back up your data regularly.

Social media

- Customise your privacy settings.

- If possible, use pseudonyms on online platforms.
- Keep professional profiles and personal profiles separate.
- Only allow your friends access to your personal profile.

Passwords:

- Use a unique password for each application.
- A password manager can help you to generate and manage secure passwords.
- Use multifactor authentication.

Software:

- Use up-to-date operating systems and integrated protection programs (e.g. Microsoft Windows Defender).
- Carry out any needed security updates to your operating systems, programs and apps without delay.
- Back up data regularly on external storage media.

Wi-Fi:

- Free, openly accessible Wi-Fi hotspots are not secure.
- Use a VPN service to encrypt your data when connecting to a Wi-Fi network.

Additional recommendations for cybersecurity are available from the **Federal Office for Information Security (BSI)**:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/cyber-sicherheitsempfehlungen_node.html

For additional **questions concerning the security of your IT systems**, the BSI offers support through its service centre: https://www.bsi.bund.de/DE/Service-Navi/Kontakt/kontakt_node.html

You can also **report an IT security incident** there to receive advice and assistance in assessing the incident accurately, and you can contact a digital first responder there: <https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Buergerinnen-und-Buerger/buergerinnen-und-buerger.html?pos=1>

2. Personal safety and security

People affected by transnational repression who are concerned about their personal safety can take the following steps to protect themselves:

- Protect your contact information and other personal information (do not post live, do not share your live location or your home address, and only give your phone numbers and email addresses to familiar and trustworthy people).
- Adjust your activities (speaking engagements, posting online, professional activities, etc.) temporarily (see below) and/or temporarily reduce high-profile public appearances.
- Contact your local police; they may be able to take case-specific steps to avert the danger. These are measures to directly protect those affected by transnational repression.

Those affected can also protect themselves in their daily lives:

- Try to vary your routines and schedules (such as your commute to and from work) to make it harder for people to harm you.
- If possible, have other people accompany you to visits and meetings and when you travel.
- When you go to appointments, tell people you trust when you will arrive at the appointment, when you will be back, and what they should do if you do not show up to the appointment or do not return from it.
- Pay attention to any unusual individuals or situations in your surroundings.

- If you feel that you are being followed or watched, do not go home; instead, go to a crowded place and ask for help.
- If somebody approaches you, remain polite and try to extricate yourself from the situation.
- If you experience suspicious activities or behaviour, document everything in the greatest possible detail (date, time, location, description of any people or vehicles involved, etc.). This documentation will be useful for the police.
- If you have already spoken to the police about indications of a threat against you, and you notice that you are being followed or watched, contact the police via the contact number they gave you or the emergency number 110. Explain your situation and make it clear that you are a person at risk.
- Assess the steps you have taken to date to protect your own safety and consider whether additional steps are necessary – for example, improving door and window locks, installing surveillance cameras, varying your daily routines or consulting a private security firm.

3. Travel advice

Before travelling:

- Inform yourself in advance about the threat environment, security and legal situation in the country you are travelling to.
- Travel and safety advice for various countries is published on the website of the Federal Foreign Office (in German only) and should be consulted before travelling: <https://www.auswaertiges-amt.de/de/reiseundsicherheit/reise-und-sicherheitshinweise>.
- Ask other travellers about their experiences.
- Compile a list of emergency contact details (embassies, consulates, medical services, etc.) and register with the Federal Foreign Office's crisis preparedness list (Krisenvorsorgeliste): <https://krisenvorsorgeliste.diplo.de/signin>.
- If possible, do not bring along any IT devices (smartphones, tablets, laptops, smart-watches, etc.) that you use here in Germany. Instead, acquire devices specifically for your trip (e.g. "burner phones") and save only the minimum amount of necessary information and numbers on these devices.
- Bring along only the documents that you absolutely need for your trip. To be on the safe side, make photocopies of these documents and store them in a safe place.
- When completing entry and registration forms, be honest but keep your answers as general as possible.

While travelling:

- When entering your country of destination, expect security checks as well as luggage searches.
- Plan in advance what means of transport you will use in your country of destination and what routes you will take.
- Be sceptical of contact attempts and gifts from previously unfamiliar individuals. If possible, travel in the company of others.
- Wherever possible, stay away from potentially dangerous situations (e.g. demonstrations).
- Keep conversations about confidential matters to a minimum.
- Avoid open Bluetooth connections and Wi-Fi networks, especially when they are sponsored by your country of destination. If you cannot avoid using such networks, connect to them via a VPN.
- Only use your own chargers; do not use public USB ports or unfamiliar chargers or devices, especially in hotel rooms.
- Exercise caution in your interactions with service providers and service staff.

After travelling:

- Discuss your trip with fellow travellers or trustworthy people in Germany.
- Reset the devices you brought with you to the factory settings and delete all data from them.
Or consider disposing of the devices (e.g. a "burner phone") entirely.

- Without delay, check for suspicious activity on any online user accounts which you accessed during your travels (e.g. which devices users have logged in from, whether any new users/devices have been added, any expanded data back-ups on unfamiliar systems) and change your login data.
- Note any unusual or conspicuous observations, events or irregularities and report these, if potentially relevant, to your local police station or the Federal Office for the Protection of the Constitution.

4. Support services

A variety of support services for victims of crimes are listed on the website www.hilfe-info.de. The Federal Ministry of Justice and Consumer Protection has established this website as a central source of information for people affected by crimes. The website has information on victims' rights following a crime, including on the process of the investigation and criminal proceedings; on available forms of support and counselling; and on financial, practical, psychological and forensic aid. Victims can use the advice centre finder to search for a victim support organisation in their area.

Publisher

Federal Ministry of the Interior, 11014 Berlin

Website: <https://www.bmi.bund.de/en>

Date

May 2026

Article number

BMI26016

Additional publications of the Federal Government can be downloaded or ordered here:

<https://www.publikationen-bundesregierung.de/pp-en>

This publication is issued by the Federal Government as part of its public relations work. It is distributed free of charge and is not intended for sale. It may not be used by political parties, election campaigners or campaign workers during an election campaign for the purposes of campaign advertising. This applies to elections to the Bundestag, Landtag and local elections as well as to elections to the European Parliament



www.bmi.bund.de

-  bsky.app/profile/bmi.bund.de
-  [instagram.com/bmi_bund](https://www.instagram.com/bmi_bund)
-  [linkedin.com/company/bundesinnenministerium](https://www.linkedin.com/company/bundesinnenministerium)
-  [@bmi](https://www.facebook.com/social.bund.de)
-  [threads.com/@bmi_bund](https://www.threads.com/@bmi_bund)
-  x.com/BMI_Bund
-  [youtube.com/@BMIBund](https://www.youtube.com/@BMIBund)