

India state assembly elections 2022: Journalist safety guide

India is scheduled to hold legislative assembly elections in the states of Uttar Pradesh, Punjab, Goa, Uttarakhand, and Manipur in February and March 2022.

Media workers covering any of these elections should be aware of the potential risk of physical attack, intimidation, and harassment; online bullying; arrest and detention; and government restrictions on reporting, including access to the internet. Five journalists in India died as a result of their reporting in 2021, topping CPJ's global records for the year; seven were imprisoned in relation to their work as of December 1, 2021. Hundreds in India's media fraternity have died after contracting COVID-19, according to a database compiled by the Network of Women in Media India. Amid sectarian tensions journalists have faced reprisals for their religion, gender, and identity and been accused of spreading communal disharmony for reporting on religious violence.



Passengers wearing face masks wait to get tested for COVID-19 at a railway station in Mumbai on January 5, 2022. The virus is one of many obstacles facing journalists in India as they prepare to cover legislative assembly elections in five states in February and March. (AP/Rafiq Maqbool)



Contents

Editor's Safety Checklist	3
Digital Safety: Online harassment and misinformation campaigns	4
Digital Safety: Basic device preparedness	6
Digital Safety: Securing and storing materials	7
Digital Safety: Safer communications	8
Physical Safety: COVID-19 considerations	10
Physical Safety: Reporting from election rallies and protests	10
Physical Safety: Reporting in a hostile community	14

As Vijay Vineet, a former *Jansandesh* newspaper editor now freelancing for the website *Newsclick* in Uttar Pradesh, told CPJ via phone, "No organization in Uttar Pradesh provides any safety training or does enough for protection of their reporters."

"In a closely fought election, as we are realizing it has become, there is a potential for violence." he said.

CPJ Emergencies has updated its safety guide for journalists covering the elections, containing information for editors, reporters, and photojournalists on how to prepare for the legislative assembly elections, and how to mitigate digital, physical, and psychological risk.

Contacts & Resources

Journalists requiring assistance can contact CPJ Emergencies via emergencies@cpj.org or CPJ's Asia program via researcher Sonali Dhawan at sdhawan@cpj.org or India correspondent Kunal Majumder at kmajumder@cpj.org.

In addition, CPJ's resource center has additional information and tools for <u>pre-assignment preparation</u> and <u>post-incident assistance</u>.



Editor's Safety Checklist

Editors and newsrooms may assign journalists to stories at short notice in the run-up to, during, and after the legislative assembly elections. This checklist includes key questions and steps to consider to reduce risk for staff.

Staff Considerations

- Are selected staff experienced enough for the assignment?
- Do any selected staff fall into the <u>COVID-19 vulnerable categories</u> or have family members/dependents who rely upon them?
- If reporting from a potentially hostile event (e.g. an election protest), does the profile, sex, religion, or ethnicity of any staff member make them a possible target?
- Are selected staff fit enough for the assignment, and have you discussed any health issues that could affect them during the assignment?
- Does the specific role of any selected staff put them at more risk? For example, photojournalists who work closer to the action.

Equipment & Transport

- Have you discussed the risk of COVID-19 exposure with selected staff, and provided them with good quality face masks and alcohol-based hand sanitizer?
- If violent protests are likely, have you made available special protective equipment such as safety helmets, safety goggles, body armor, tear gas respirators, and medical kits? Do staff know how to use such equipment properly?
- Are selected staff driving themselves, and is their vehicle roadworthy and appropriate?
- Have you identified how you will communicate with the team and how they will remove themselves from a situation if necessary?

General Considerations

- Have you recorded and securely saved the emergency contact details of all staff being deployed?
- Do all selected staff have the appropriate accreditation, press passes, or a letter indicating they work for your organization?
- Have you considered the level of risk attached to the story that your team may be exposed to? Is the level of risk acceptable in comparison to the editorial gain?
- Is the team correctly insured and have you put in place appropriate medical cover?



- Have you identified the local medical facilities in case of injury and made team members aware of the details?
- Have you considered and discussed the possibility of long-term trauma-related stress?

For more information about risk assessment and planning, see the **CPJ Resource Center**.



A man wearing a facemask as a preventive measure against the Covid-19 coronavirus speaks on his mobile phone at a market in New Delhi on January 11, 2022. (AFP/Sajjad Hussain)

Digital Safety: Online harassment and misinformation campaigns

Online harassment, including targeted online campaigns, are likely to increase during the election period, especially in Uttar Pradesh, India's biggest state. Recent, sophisticated examples include the app, Tek Fog, which encouraged mass distribution of offensive messages about specific journalists. Hate speech in English, Hindi and Bengali spiked on Facebook during the pandemic, The Wire reported, with women and minorities as popular targets, some being offered for sale through demeaning fake auctions. Media workers are often targeted by online attackers who want to discredit the journalist and their work. This can often involve coordinated harassment and



misinformation campaigns that leave the journalist unable to use social media, essentially forcing them offline. Protecting against online attacks is not easy, however there are steps that journalists can take to better protect themselves and their accounts.

To better protect yourself:

Account security

Online harassers will often use personal information from your social media accounts to target and harass you. Take the following steps to better protect your accounts and your data:

- Create long and strong passwords for your accounts. These should be 16 characters or more, and unique for each account. Consider using a password manager, which is currently the most secure way of managing passwords. This will help to prevent accounts from being hacked.
- Turn on two-factor authentication (2FA) for accounts.
- Review your privacy settings for each account and make sure any personal data, such as
 phone numbers and date of birth, is removed. Check who has access to your personal data
 on social media sites and tighten your privacy settings.
- Look through your accounts and remove any photos or images that could be manipulated and used as a way to discredit you. This is a common technique used by online harassers.
- Monitor your accounts for signs of increasing harassment or for indications that a digital threat could become a physical threat. Be aware that certain stories are likely to attract higher levels of harassment.
- Speak with family and friends about online harassment. Abusers often obtain information about journalists via the social media accounts of their relatives and social circle. Consider asking people to remove photos of you from their sites or lock down their accounts.
- Speak with your media outlet about online harassment and have a plan of action in place if abuse becomes serious.

During an attack:

- Try not to engage with online harassers as this can make the situation worse.
- Try to ascertain who is behind the attack and their motives. The online attack may be linked to a story you have recently published.
- Journalists should report any abusive or threatening behavior to the social media company.
- Document any comments or images that are of concern, including screenshots of the activity, the time, the date, and the social media handle of the abuser. This information may be useful at a later date if you need to show it to your news organization, editor, organizations that defend freedom of expression, or the authorities.



- Be vigilant for signs of hacking. Ensure that you have strong, long passwords for each account, and that two-factor authentication is on.
- Inform your family, employees, and friends that you are being harassed online. Adversaries will often contact family members and your workplace, and send them information/images in an attempt to damage your reputation.
- You may want to block or mute those who are harassing you online. You should also report
 any abusive content to social media companies and keep a record of your contact with these
 companies.
- Review your social media accounts for comments that may indicate that an online threat is about to turn into a physical threat. This could include people posting your address online (known as doxxing) and calling on others to attack you and/or increased harassment from a particular individual.
- Consider coming offline until the harassment has died down.
- Online harassment can be an isolating experience. Ensure that you have a support network to assist you. In a best case scenario, this will include your employer.

Digital Safety: Basic device preparedness

While covering an election, journalists are likely to be using their mobile phone for reporting and filing stories as well as being in contact with colleagues and sources. This has digital security implications if journalists are detained and their phones are seized or broken. Before going out on assignment it is good practice to:

- Know what information is on your phone or computer and how that could put you or others at risk if you are detained and your device is taken and searched.
- Before going out to report, back up your phone to a hard drive and remove or limit access to any sensitive or personal data, such as family photos, from the device you are carrying.
- Log out of any accounts and apps that you will not be using while reporting and remove them from your phone. Log out of browsers and clear your browsing history. This will better protect your accounts from being accessed should your phone be taken and searched.
- Password protect all your devices and set up your devices to remote wipe before going out
 to report. Remote wipe will work only with an internet connection. Avoid using biometrics,
 such as your fingerprint, to unlock your phone as this can make access to your device easier
 should you be detained.
- Take as few devices with you as possible. If you have spare devices, then use them and leave personal or work devices behind.



- Consider turning on encryption for your Android phone. New iPhones have encryption as standard. Please check the law with regards to encryption use.
- Where possible use end-to-end encrypted messaging services, such as Signal or WhatsApp, to communicate with colleagues and sources. Set messages to delete after a certain timeframe.
- Install a VPN to help access sites if they become blocked. Research the law around using a VPN and also look into which VPN provider has previously worked best during a partial internet shutdown.
- Have a plan for how and when you will contact others should there be a complete internet shutdown.
- Be aware that <u>spyware</u> including <u>Pegasus</u> has allegedly been used against journalists in India, according to research by Citizen Lab and <u>CPJ interviews</u>. Once installed on your phone, sophisticated spyware will monitor all activity, including encrypted messages. [Israel-based NSO Group says it markets Pegasus as a surveillance tool only to governments for law enforcement purposes, and has repeatedly <u>told CPJ</u> that it <u>investigates reports</u> that its products were misused in breach of contract.]

For more information about digital safety, please see CPJ's <u>Digital Safety Guide</u>.

For more information about Pegasus spyware see CPJ's Safety Advisory.

Digital Safety: Securing and storing materials

It is important to have good protocols around the storing and securing of materials during election times. If a journalist is detained, their devices may be taken and searched, which could have serious consequences for the journalist and their sources. Devices can also be broken or stolen while out covering the election, which may lead to the loss of information if it is not backed up.

The following steps can help protect you and your information:

- Review what information is stored on your devices, including phones and computers.
 Anything that puts you at risk or contains sensitive information should be backed up and deleted. There are ways to recover deleted information, so anything that is very sensitive will need to be permanently erased using a specific computer program, rather than just deleted.
- When reviewing content on a smartphone, you should check information stored on the phone (the hardware) as well as information stored in the cloud (Google Photos or iCloud).
- Check the content in messaging applications, such as WhatsApp. Journalists should save and then delete any information that puts them at risk. Be aware that WhatsApp backs up all content to the cloud service linked to the account, for example iCloud or Google Drive.



- Think about where you want to back up information. You will need to decide whether it is safer to keep your materials in the cloud, on an external hard drive or on a flash drive.
- Journalists should regularly move material off their devices and save it on the back up option of their choice. This will ensure that if your devices are taken or stolen then you have a copy of the information.
- It is a good idea to encrypt any information that you back up. You can do that by encrypting your external hard drive or flash drive. You can also turn on encryption for your devices. Journalists should review the law in the country in which they are working, to ensure they are aware of any legalities around the use of encryption.
- If you suspect that you may be a target and that an adversary may want to steal your devices, including external hard drives, then you should keep your hard drive in a place other than your home.
- Put a PIN lock on all your devices. The longer the PIN, the more difficult it is to crack.
- Set up your phone or computer to remote wipe in advance. This function allows you to erase devices remotely, for example if authorities take them. This will only work if the device is able to connect to the internet.

Digital Safety: Safer communications

Knowing how to communicate more securely with others is an important part of your digital safety, especially as more journalists are working remotely due to COVID-19. Journalists and editors are increasingly using conferencing platforms instead of meeting in person, and taking steps to secure who can access these calls or webinars is essential for protecting employees and sources.

- If needed, ensure that you protect your account with a long and unique password and have two-step verification turned on.
- If you are able, use your work email to sign up for an online conferencing account instead of using your personal email. This protects your personal data, such as your contact lists, from being revealed either by the online conferencing service, or by other attendees.
- Do not publish information about online conferencing events on social media unless these are public events and you are happy to have no control over who attends.
- Ensure you are using the latest version of the conferencing platform service.
- If you need to speak to only a small number of people over video, less than 10, consider using WhatsApp or Signal instead.

Using Zoom

To better protect yourself when using Zoom, consider the following guidelines:



- Zoom creates a personal ID number for each user which you should not make public; for example, do not post it on social media.
- Set up a password for people to access your meeting.
- Enable the waiting room function. This will ensure that only people who have been invited will attend your event. You will also be able to view who is waiting and remove anyone that has not been invited or who is unknown.
- Lock the meeting room once all your invitees have arrived.
- You can manage the participants in the room by turning off video and sound and controlling who can share their screen.
- You can remove anyone at any time from the Zoom call and also block them from returning to the room.
- Ensure that you are using the latest version of Zoom and have enabled end-to-end encryption.

For more information, see CPJ's digital safety advice for journalists working from home.



Rakesh Tikait, a leader of Bharatiya Kisan Union, one of the largest farmers' unions, holds the Indian national flag as farmers vacate a protest site, at Ghazipur near the Delhi-Uttar Pradesh border, India, on December 15, 2021. (Reuters/Anushree Fadnavis)

Physical Safety: COVID-19 considerations

Maintaining physical distancing at any election event or related protest will be challenging. Large crowds are commonplace, members of the public may not wear face coverings/face masks, and media workers could be confined to a particular area in close proximity to other journalists. Such confinement could potentially expose them to virus droplets, as well as verbal or physical attack from hostile members of the public, who could deliberately cough or sneeze over them.

Be aware that people shouting or chanting can result in the spread of virus droplets, therefore increasing media workers' level of exposure to coronavirus infection.

- COVID-19 restrictions on public gatherings in India vary according to each state, and may
 change with little or no notice. Always research any restrictions in place, noting that
 numerous journalists were attacked or detained by police for allegedly violating restrictions
 in 2020.
- If travelling internationally or from another state to cover the elections you may be required to provide evidence of a recent COVID-19 test, and/or need to quarantine on arrival. A useful state by state guide can be found here
- The use of a good quality face mask is essential at any crowded event or protest (i.e. N95 / FFP2 standard or higher). Be aware that <u>fines</u> can be levied by the authorities for not wearing a face mask.
- Ensure you wash your hands regularly, properly, and thoroughly as often as feasible
 throughout the assignment. Ensure hands are dried in the appropriate way. Use alcoholbased hand sanitizer regularly if you can't wash your hands, but try not to make this a
 substitute for a regular hand washing routine.
- All clothing and shoes should be removed before re-entering your home and washed / cleaned with hot water and detergent where possible.
- All equipment should be thoroughly cleaned post-assignment.

For further detailed COVID-19 reporting guidance, see CPJ's safety advisory.

Physical Safety: Reporting from election rallies and protests

During elections, media workers frequently attend crowded rallies, campaign events, live broadcasts, and protests.



To help minimize the risks at such events, media workers should consider the following safety advice:

Political Events and Rallies

- Ensure that you have the correct accreditation or press identification. For freelancers, a letter from the commissioning employer is helpful. Have it on display only if safe to do so. Avoid using a lanyard around your neck, but clip it to a belt or in a transparent velcro pouch around your bicep instead.
- Wear clothing without media company branding and remove media logos from equipment/vehicles if necessary.
- Avoid wearing sandals or slip-on shoes. Instead wear sturdy footwear with hard soles, laces, and some kind of ankle support.
- Park your vehicle in a secure location facing the direction of escape, or ensure you have an alternative guaranteed mode of transport.
- Have an escape strategy in case circumstances become hostile. You may need to plan this on arrival, but try and do so in advance. Ensure you identify all available exits from the location.
- Gauge the mood of the crowd. If possible, call other journalists already at the event to assess the mood. Consider going with another reporter or photographer if necessary.
- Inside the event, report from the allocated press area unless it is safe to do otherwise. Ascertain if the security or police will assist if you are in distress.
- If the crowd/speakers are hostile to the media, mentally prepare for verbal abuse. In such circumstances, just do your job and report. Do not react to the abuse. Do not engage with the crowd. Remember, you are a professional even if others are not.
- If spitting or projectiles from the crowd are a possibility and you are determined to report, consider wearing a hooded, waterproof, discrete bump cap.
- If the atmosphere becomes hostile, avoid hanging around outside the venue/event and do not start questioning people.
- If the objective is to report from outside the venue, working with a colleague is sensible. Report from a secure location with clear exits, and familiarize yourself with the route to your transportation. If an assault is a realistic prospect, consider the need for security and minimize your time on the ground.
- If the task was difficult/challenging, do not bottle up your emotions. Tell your superiors and colleagues. It is important that they are prepared and that everyone learns from each other.

Protests

Planning:

- Across India the police have used live ammunition, rubber bullets, pellet guns, tear gas, lathi
 sticks, and truncheons to quell protesters in the past. If violence is anticipated, the use of
 protective safety goggles/glasses, helmets, tear gas respirators, and protective body vests
 should be considered. For more information see CPJ" s personal protective equipment (PPE)
 guide here.
- Know the area you are going to by researching the layout of the location in advance. Work
 out in advance what you would do in an emergency and identify all potential safe escape
 routes.
- Individuals should not be expected to work alone at protest locations. Try to work with a colleague and set up a regular check-in procedure with your base, family, or friends. Working after dark is riskier and should be avoided if possible. For more information please see CPI's advice for journalists reporting alone.
- Take a medical kit if you know how to use it and ensure you have a full battery on your mobile phone.
- Avoid wearing loose clothing, political slogans, media branding, military patterns, politically affiliated colors, and flammable materials (e.g. nylon).
- Wear footwear with hard soles, laces, and some kind of ankle support.
- Tie long hair up to prevent individuals from pulling you from behind.
- Limit the number of valuables you take. Do not leave any equipment in vehicles, which are likely to be broken into. After dark, the criminal risk increases.

Awareness & Positioning:

- Consider your position and maintain situational awareness at all times. If feasible, find an elevated vantage point that might offer greater safety.
- Always plan an evacuation route as well as an emergency rendezvous point if you are working with others.
- Identify the closest point of medical assistance.
- If working in a crowd, plan a strategy. Keep to the outside of the crowd and avoid being sucked into the middle, where it is hard to escape.
- Continuously observe and read the mood and demeanor of the authorities in relation to the crowd dynamic. Police can become more aggressive if the crowd is agitated (or vice versa). Visual cues such as the appearance of police dressed in riot gear or throwing of projectiles



are potential indicators that aggression can be expected. Pull back to a safe location, or plan a quick extraction when such "red flags" are evident.

- Photojournalists generally have to be in the thick of the action so are at more risk. Photographers in particular should have someone watching their back and should remember to look up from their viewfinder every few seconds. To avoid the risk of strangulation, do not wear the camera strap around your neck. Photojournalists often do not have the luxury of being able to work at a distance, so it is important to minimize the time spent in the crowd. Get your shots and get out.
- All journalists should be conscious of not outstaying their welcome in a crowd, which can turn hostile quickly.

If tear gas is likely to be used by the police:

The use of tear gas can result in sneezing, coughing, spitting, crying, and the production of mucus that obstructs breathing. In some cases, individuals may vomit, and breathing may become labored. Such symptoms could potentially increase media workers' level of exposure to coronavirus infection via airborne virus droplets. Individuals who suffer from respiratory issues like asthma, who are listed in the COVID-19 vulnerable category, should therefore avoid covering crowd events and protests if tear gas is likely to be deployed.

In addition, evidence suggests that tear gas can actually increase an individual's susceptibility to pathogens such as coronavirus, <u>as highlighted by NPR</u>.

For further guidance about dealing with exposure to and the effects of tear gas, please refer to CPJ's civil disorder advisory.

Physical Assault:

Protesters have previously <u>assaulted journalists</u> in India and in October 2021, CPJ documented the death of freelancer <u>Raman Kashyap</u> from injuries sustained while covering a protest by local farmers that turned violent. When dealing with aggression, consider the following:

- Assess the mood of protesters toward journalists before entering any crowd, and remain vigilant for potential assailants.
- Read body language to identify an aggressor and use your own body language to pacify a situation.
- Keep eye contact with an aggressor, use open hand gestures, and keep talking with a calming manner.
- Keep an extended arm's length from the threat. Back away and break away firmly without aggression if held. If cornered and in danger, shout.
- If aggression increases, keep a hand free to protect your head and move with short deliberate steps to avoid falling. If in a team, stick together and link arms.



- While there are times when documenting aggression is crucial journalistic work, be aware
 of the situation and your own safety. Taking pictures of aggressive individuals can escalate a
 situation.
- If you are accosted, hand over what the assailant wants. Equipment it is not worth your life.



Paramilitary troopers and Punjab Police personnel patrol in a market area, ahead of the state assembly elections in Amritsar, India on January 10, 2022. (AFP/Narinder Nanu)

Physical Safety: Reporting in a hostile community

Journalists are on occasion required to report in areas or communities that are hostile to the media or outsiders. This can happen if a community perceives that the media does not fairly represent them or portrays them in a negative light. During an election campaign, journalists may be required to work for extended periods among communities that are hostile to the media.



To help reduce the risk:

- If possible, research the community and their views in advance. Develop an understanding of what their reaction to the media will be, and adopt a low profile if necessary.
- Secure access to the community in advance. Turning up without an invitation or someone vouching for you can cause problems. If you are not familiar with the area or are perceived as an outsider, consider hiring or obtaining the input of a local facilitator, community leader or person of repute in the community who can accompany you and help coordinate your activities. Identify a local power broker who can help in case of emergency.
- If there is endemic abuse of alcohol or drugs in the community, be aware that the unpredictability factor increases.
- Ideally, work in a team or with back up. Depending on the risk levels, the backup can wait in a nearby safe location (shopping mall or petrol station) to react if necessary.
- Think about the geography of the area and plan accordingly. Consider the need for security if the risk is high. A local hired back watcher to protect you/your kit can be attuned to a developing threat while you are concentrating on work.
- Park your vehicle ready to go, ideally with the driver in the vehicle.
- If you have to work remotely from your transportation, know how to get back to it. Identify landmarks and share this information with colleagues.
- Know where to go in case of a medical emergency and work out an exit strategy.
- Always ask for consent before filming / photographing an individual, particularly if you do not have an easy exit.
- When you have the content you need, get out and do not linger longer than necessary. It is helpful to have a pre-agreed cut off time and to depart at that time. If a team member is uncomfortable, do not waste time having a discussion. Just leave.
- Wear clothing without media company branding, which should be appropriate and respectful. Remove media logos from equipment/vehicles if necessary.
- Take a medical kit if you know how to use it.
- Be respectful to the individuals and their beliefs/concerns at all times.
- Limit the amount of valuables/cash that you take. Will thieves be attracted by your equipment? If you are accosted, hand over what they want. Equipment is not worth your life.
- Avoid working at night: the risk increases dramatically.
- Before broadcast/publication consider that you may need to return to this location. Will your coverage affect your welcome if you return?