7

FENDING OFF CYBER-SHARKS

Karnika Seth

It was a Monday evening. I was preparing for the hearing the next day in a court case, when the phone began to ring frantically. The voice on the other end was both urgent and nervous – it was a client. She was desperately in need of some legal advice. She said that her phone was being tapped, that she was being persistently harassed by someone writing offensive mails to her.

Law has a term for her situation – she was being cyber-stalked! I gave the young woman an appointment and told her to bring her cell phone and laptop along. Her phone was scanned by our forensic team for spyware. Indeed, keyloggers were found to have infected her mobile. Keylogger installation is a serious issue – it makes every keystroke on the phone visible to the person who sent the spyware. Undoubtedly, all data on the phone and her online activity had been compromised! It was evident that the stalker had been following all online activity on her smartphone. The content of the emails received by her was obscene, with her very personal pictures attached, pictures she had no intention to share with anyone and were only saved on her personal phone.

Scared, clueless about the predator, the woman almost broke down talking of the harrowing time she had been going through. 'I have not slept for the past four-five days,' she said, recalling how the invisible stalker had been weighing her down. She was traumatized. The intimidating emails had pushed her into a state of panic – she was on the edge of a nervous breakdown. The young woman feared her reputation was at stake and life in danger. She worried that if the offender was not caught immediately, he could harm her further by creating a fake profile on social media or posting the pictures on adult websites.

Her fears were not unfounded. In many cases that I have handled as a cyberlawyer, the usual modus operandi of the offenders is to hack the phone, stalk, resort to identity theft, and ultimately distort the victim's image on the internet. Cyber-stalking is an offence under Section 354D of the Indian Penal Code, 1860 – punishable with imprisonment up to three years and fine. Section 509 of the IPC makes any word, gesture, or act intended to insult the modesty of a woman an offence punishable with a term of up to three years and fine. Anyone who follows a woman or contacts her despite her clear indication of disinterest or monitors her use of the internet and content of her emails can be accused of stalking. Hacking is an offence punishable with imprisonment up to three years and fine under Section 66 of the Information Technology Act, 2000; it includes offences such as unauthorized access and copying of any data. Section 507 of the IPC punishes a man with a two-year jail term if he intimidates or threatens a woman by anonymous communication.

In this client's case, a legal complaint was immediately drafted to report the crime. On our advice, the victim lodged a complaint at the police station nearest to her residence.

Ghosts at work

The police began to investigate the case. The investigators promptly called for the relevant data from the concerned social-media website. The website, in compliance with the law, made available the required information to the law-enforcement authorities, and in no time, the IP address of the stalker was found. The IP address of a computer identifies its status on the internet and its location. This location happened to be a cyber café in this case, and after a couple of days, the stalker was caught red-handed when he came to use the internet. Knowing he had been caught, he confessed to having stalked our client.

Our client was lucky as the accused was identified and nabbed, but some criminals on the internet can be smarter than this offender. The savvier ones use spoofing tools to hide their real identities and locations. They use software and browsers in private or anonymous mode. The internet has revolutionized communication, razing the silos and bringing the world closer. Entertainment, like any other field of activity, can be a curse when misused. Predators take advantage of the anonymity of cyberspace and its borderless expanse to commit innumerable illegal acts in many countries simultaneously and almost with impunity. Almost – because at times, they get caught. Lawyers like me play a role there. Hackers in China might wreak havoc in Europe or India, Russian jocks pose a serious threat to computer users in the US. In terms of the quantum of damage, a major cyber-attack is equivalent to a seven-day conventional war.

Crimes that once took place on the physical plane – blackmail, defamation, tampering with identity-proof documents, theft of records, intimidation, and even extortion – are now happening in the virtual world. As a lawyer, I have had the experience of dealing with all such crimes, representing the victims before the legal fora of the country.

I recall an interesting case of a woman in the US being harassed online by an ex-friend from years ago. At the time of the incident they were estranged, their relationship having ended long ago. The accused set up a fake website in her name and created several fictitious social-media profiles. He created 15 websites and posted her personal letters, greeting cards she had sent him long ago, photos, her passport details and other sensitive personal data to malign her, destroy her reputation.

This client was an Indian national who had settled in the US with her family. Defamatory information about her on the internet was intended to destroy her reputation as much in India as in the US. She had a large number of relatives, friends and acquaintances in India. Anyone could type her name in the Google search engine and access the 15 defamatory websites created in her name or land up on a fake profile of hers! This was a typical case of identity theft and defamation. Identity theft is an offence under Section 66C of IT Act, 2000 with similar terms of punishment – three years. Defamation is punishable under Section 500 of the IPC with a two-year jail term and fine. In defamation cases, criminal action is instituted and claims for compensation are also filed.

One pertinent point to note here is that the damage caused by defamation online is more extensive than if committed offline, simply because the reach and pace of the internet are phenomenally superior to that of the conventional routes of information dissemination. Keeping this in mind, response to any act of cyber assault needs to be both prompt and effective.

In this case, legal notices were drafted overnight and served on the registrars of the domains/websites and their hosting company. The effect was electrifying. Within 36 hours of receipt of the notice, they suspended the offensive websites. The social-media platform examined the reported abuse and blocked the fake profiles. According to Indian IT laws, if any aggrieved person writes to a service provider, with proof, about the misuse of its service platform to target them, the provider is obliged to remove and block the relevant content on its platform within 36 hours. We advised our client to claim compensation for the damage caused to her reputation, and she accordingly filed a civil suit before the appropriate court and lodged a complaint with the police to trace and punish the accused. Because of many tangles and procedural logjams, it took time to receive compensation. For the prosecution case, a delay occurred because the identification and tracking down of the accused take time in these cases. The client was, however, persistent, and after a couple of years of legal proceedings, she finally succeeded on both fronts. Handling such litigation is certainly not a simple task, knowing that electronic evidence is fragile and easily destroyable and must be collected, preserved and produced in a manner legally admissible in a court of law. Such cases often involve complex legal issues of jurisdiction, applicable laws (in the case of trans-border crimes), the identification and tracking of data, servers, and electronic evidence, and other substantive and procedural law issues.

When these crimes are committed against celebrities, an extra dimension is added in the form of public image and reputation. I learned this in depth when I recently represented a high-profile spiritual leader, who was being defamed through blog posts that made allegations of ulterior motives. He was being hounded by trolls on social-media platforms.

At first, all electronic evidence was preserved by taking prints and saving electronic copies in a folder. Quickly, a suit for defamation was filed before the appropriate court and compensation of ₹1 crore claimed against the offender. A police complaint was filed, and investigations began in right earnest. It did not take much time for the investigators to trace the man behind the defamatory posts. This was crucial for our claim of compensation.

As a next step, the service providers were served legal notices to block the offensive posts, and these pages were blocked within 36 hours after the receipt of our legal notice. An intermediary/service provider, such as BlogSpot, is only liable if, upon actual notice, it does not remove the defamatory content from its platform. This provision is made by Section 79 of the IT Act, 2000 which grants exemption from liability to intermediaries, except liability in cases where, for instance, the platform has colluded with the accused in posting defamatory content or has not complied with its due-diligence norms.

When a person posts offensive sexual remarks on social media, they are liable under Section 354A of the IPC and can be punished with a year's imprisonment and fine. The provision also covers posting or messaging content related to pornography and demand or request for sexual favours, which are punishable with three years' imprisonment and fine. I recall a case in which a woman employee was sexually harassed by her senior colleague through emails and on social media. A case for sexual harassment was lodged, and the accused was terminated from his services as such acts amount to misconduct. An internal probe confirmed that he had breached the company's policies for employee conduct. A police complaint was also lodged and a compensation claim for damage followed.

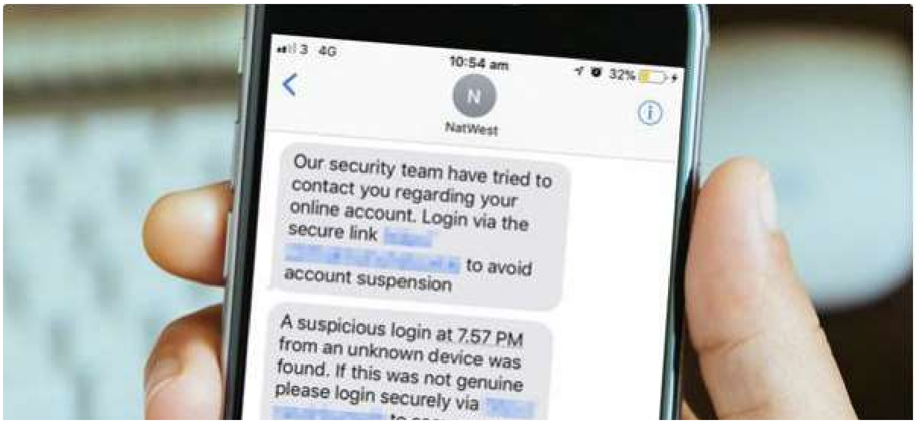
When a client walks into our office, they are often unaware of the legal rights and remedies available to them under the law and are tormented by the fact that they have been targeted by cybercriminals. Most of them very vaguely recall the sequence of the attack or facts related to it; therefore, the matter requires professional handling so that facts needed to draft the required pleadings or complaints are verified and clearly spelt out. It is somewhat like solving a jigsaw puzzle. Each case poses an interesting challenge and needs a different strategy to seek legal redress. The most important challenge, as I mentioned before, is to find the right evidence that can lead to the perpetrator of the crime. This, carefully done, can make or break a case.

Some cybercrime cases arise out of completely innocuous situations, where a client least expects to become a victim of a concerted attack. Once, an employee of a famous apparel store – without the knowledge or consent of his employer – installed a hidden webcam in a changing room. A woman who used the changing room was shocked to learn later from a social-media clip that she had been secretly filmed and her personal video and pictures had gone viral on internet. The woman was in a panicked state when she contacted us for professional help. A police complaint was lodged and investigations followed. The accused was caught from his home after interrogations at the store led to a finding that he was the only person in charge of security in the concerned part of the store. The service providers of social-media platforms were contacted by the police, and they were served legal notices to stop circulation of the relevant content. Some platforms blocked the clip from public access within 36 hours of receiving the complaint.

The

The law of the land stipulates that if a man captures an image of a woman engaged in a private act without her consent, it is punishable under Section 354C of the IPC, which holds the man liable to minimum one-year imprisonment, extending to maximum three years along with fine. Publishing a visual image of a person in electronic form, which violates the privacy of that person, is held punishable with three years' imprisonment or a ₹2 lakh fine under Section 66E of the IT Act, 2000. Here 'private act' means any act committed in a space where the woman has the legitimate right to privacy. This is different from a situation where a woman consents to her private images being clicked, but they are then published on internet without consent. Such acts are punishable under Section 67 and Section 67A of the IT Act, 2000. Section 67 and Section 67A make publishing and/or transmitting sexually explicit material in electronic form a punishable offence with a similar term of punishment.

While some social-media portals block streaming, circulation or publication of objectionable materials, a few others bluntly state that since the data shared on their platforms is between users, they have no control over its further circulation. In other words, such replication or forwarding cannot be stopped. However, there are techniques such as photo DNA that can create a hash value for every image, and with such unique numerical value, such content can be identified and stopped from replication or circulation.



Smishing: The hacker's bites and baits

In the face of an outcry about the risk and consequences of such exposure, the government took steps to urge social-media platforms such as WhatsApp and Facebook to appoint a public-grievance officer in India to address public grievances within 36 hours of receiving a complaint. It also proposed that such portals localize their servers and storage of content for Indian users in India. This will facilitate the legal process by speeding up the process of evidence collection, thus expediting investigation in cybercrime cases. This debate started around the time when the Justice Srikrishna Committee had just submitted its recommendations and drafted a Personal Data Protection Bill. The Indian legal regime is currently undergoing a transformation, particularly in the area of personal data protection, privacy and freedom of speech. These are fundamental rights guaranteed by Article 19(2) of the Constitution – it can only be curtailed in accordance with the procedure prescribed by law. This article provides exceptions for the protection of national security, national integrity, or friendly relations with other states; for public order, decency, morality; and in relation to contempt of court, defamation, or incitement to an offence.

In the past two decades, cybercrime has risen exponentially – in India and across the globe – taking on new forms, from phishing (stealing sensitive financial information using fake messages sent by mail) to

SMiShing (SMS for phishing). Phishing is a deceptive security attack, in which the user is hoodwinked into downloading a virus or a malware onto their mobile or another electronic device. Yet another vicious form of cyber-assault is vishing – phishing using Voice over Internet Protocol, or VoIP.

Given the technical impediments of tracing identity, tracking data, morphing and spoofing, law enforcement in general and cyberlawyers like me in particular are facing increasing challenges. It is important for me to state here that the dynamics of our cybercrime law practice have radically changed in recent times to handle complex incursions by the predators. Gone are the days when we would draft simple contracts for B2B or B2C platforms; today, we draft blockchain contracts, food aggregator agreements, social-media network agreements, hedge fund and cryptocurrency offshore-fund agreements, and so on. We deal with ransomware and man-in-the-middle attacks, trolling, hacking, defamation, blackmail and cyberstalking.

Tomorrow is another day with another set of issues, more opaque in nature and with scarier names. Our law offices buzz with new learning each day, and our success stories multiply as each year goes by. Each case reads like a bestselling John Grisham novel and offers useful tips about how to protect your sensitive data, digital assets and reputation online. ■

Dr Karnika Seth, a Supreme Court lawyer, specializes in cyber law. She is the author of *Computers, Internet & New Technology Laws*.