CAMBODIA'S LAW ON TELECOMMUNICATIONS

A LEGAL ANALYSIS

LICADHO Briefing Paper
March 2016

សម្ព័ន្ធខ្មែរសំរ្សាប់ការពារសិទ្ធិមនុស្ស លីកាដូ

LICADHO

CAMBODIAN LEAGUE FOR THE PROMOTION
AND DEFENSE OF HUMAN RIGHTS

Introduction

The new Law on Telecommunications ("Telecoms Law") poses a severe threat to freedom of expression in Cambodia, targeting not only online public expression but also any private communications made using telecommunications devices.

Its most egregious provisions allow the government to secretly intrude into the private lives of individuals, destroy evidence before criminal trials, and seize control of the entire telecoms industry if arbitrarily deemed warranted.

Its excessive measures, particularly those creating new criminal offences, reveal the true intent of the law: to intimidate individuals, punish the exercise of fundamental rights and freedoms and quash individual and group dissent. With a year to go until the next commune elections and two years until the next national election it would seem that the Cambodian government has equipped itself with a whole new arsenal with which to threaten and obstruct civil society.

The following analysis details the most serious threats posed by the law, under themes of surveillance powers; restriction of fundamental freedoms; risk to fair trial rights; policing and enforcement; and excessive state control. [1]

Surveillance powers

The law's stated purpose is regulation of the telecommunications industry and yet it contains provisions that give the government powers to secretly monitor the telecommunications of individuals without any accountability and to punish those individuals if their communications are deemed to be criminal. The law contains no reference to the right to freedom of expression or its protection, as guaranteed by the Constitution and international law,[2] nor to the right to privacy of correspondence by means of telecommunications which is expressly protected under the Constitution.[3]

- Article 97 of the law permits the secret surveillance of any and all telecommunications where it is conducted with the approval of a "legitimate authority."[4] There is no definition of what constitutes a "legitimate authority," or the means by which such an authority is competent to approve surveillance. This appears to create a power to secretly eavesdrop without any public accountability or safeguards to protect individuals' right to privacy. This means that any individual holding a phone conversation, sending a text message, email or communicating via social media might secretly be under observation at any point in time without their knowledge. Any private speech via telecommunications can no longer be considered truly private.

- Article 6 requires that, "All telecommunications operators and persons involved with the telecommunications sector shall provide to the Ministry of Post and Telecommunications the telecommunications information and communication technology service data."[5] In practice, this gives the Ministry unfettered rights to demand that all telecommunications service providers provide data on their service users and could even operate as an obligation for companies to surrender data without the requirement of a judicial warrant or other safeguards protecting the

[1] This analysis is based on an unofficial English translation of the Law on Telecommunications and the official Khmer language Law on Telecommunications published on the Ministry of Post and Telecommunications' website.
[2] Cambodian Constitution Article 41; International Covenant on Civil and Political Rights Article 19 – while Article 19(3) contains permissible limitations on the right to freedom of expression (so far as they are provided by law, necessary and proportionate), including national security and public order grounds, within the Cambodian context the willful and abusive misinterpretation of expression by the authorities means legitimate expression is often falsely labelled as a threat to national security.
[3] Cambodian Constitution Article 40
[4] Telecoms Law Article 97
[5] Telecoms Law Article 6

right to privacy. This is a clear violation of Cambodia's obligations under constitutional and international law. The Constitution guarantees the right to confidentiality of correspondence;[6] far-reaching and unchecked discretionary powers to seize data regarding individuals' telecommunications activities amount to a violation of this right. Additionally, the Constitution recognizes Cambodia's obligations under the International Covenant on Civil and Political Rights to protect individuals against arbitrary and unlawful interference in their privacy and correspondence and explicitly requires the law to protect individuals against such attacks.[7]

Criminalisation of expression and restriction of rights

Alongside the comprehensive surveillance powers, the law also creates new criminal offences relating to the use of telecommunications devices that are punishable with imprisonment and heavy fines. The combination of surveillance powers and the new offences means that all public or private expression by means of telecommunications devices could potentially be observed and interpreted as a crime. There is a strong possibility that this will bring about a chilling effect on individual expression of opinion and association through telecommunications. Furthermore, the provisions could be used to spy on high profile-individuals and selectively interpret the content of their communications as criminal activity.

Below is an analysis of some of the provisions that constitute the greatest threat to the rights and freedoms of individuals:

- Article 80 states that "Establishment, installation and utilization of equipment in the telecommunications sector, if these acts lead to national insecurity, shall be punished by sentences from seven to 15 years imprisonment."[8] No telecommunications activity appears to be excluded. This means any form of expression, public or private and conducted by any electronic means of communication, could be criminalized if it is deemed to create "national insecurity". This could heavily punish legitimate expression via radio shows, television, online and even through private messages and phone conversations between individuals, should the authorities determine it to be a threat. This offence appears to carry strict liability; no intention to cause national insecurity is necessary yet an individual could face up to 15 years' imprisonment and excessive fines of 140 million riels to 300 million riels.[9] The vagueness of the law also means the legality of an activity is not clear to the individual at the point of commission and is only clearly determined later on the basis of its perceived consequences. This makes this provision and its open-ended definition of "national insecurity" easily exploitable by Cambodia's politically partisan judiciary.

- In addition to the new offences created, Article 66 includes a general prohibition on telecommunications activity which merely "*may* affect public order or national security,"[10] without the requirement of actual harm. Essentially, an act with no tangible consequences could subsequently be deemed to have violated this law and incur penalties.

- The law creates new telecommunications "expression" offences that replicate existing Criminal Code provisions while imposing higher penalties, particularly those relating to threats expressed via telecommunications means. These offences add nothing new to the body of criminal law other than arbitrarily increased financial penalties and added risk of conflict between laws.[11]These

[6] Cambodian Constitution Article 40
[7] Cambodian Constitution Article 31; International Covenant on Civil and Political Rights Article 17
[8] Telecoms Law Article 80
[9] Telecoms Law Article 81
[10] Telecoms Law Article 66
[11] Telecoms Law Article 93 is broadly equivalent to Criminal Code Articles 231 (Threats); 232 (Threats with extortion) 233 (Death threat); 234 (Death threat with extortion). Telecoms Law Article 95 broadly replicates Criminal Code Articles 423 (Threats to cause damage) and 424 (Threats to cause damage followed by an order); however, Telecoms Law Articles 94 and 96 enact higher penalties for these offences than for their Criminal Code counterparts. The Telecoms Law also expressly permits additional penalties under Article 168 of the Criminal Code concurrent to those levied under the Telecoms Law.

provisions also contain unclear conditions that a threat must be "repeated" via a telecommunications means in order to incur criminal liability, leaving individuals unclear as to when they may be in violation of the law and at risk of substantial prison sentences.[12]

- Article 99 introduces sentences of six months to two years' imprisonment and heavy financial penalties for "any act of producing, installing or distributing software or hidden audio recorders for recording dialogue" without approval from the authorities. This unclear provision could potentially criminalise the basic use, sharing or development of software such as smartphone apps. These are disproportionate penalties that excessively include ordinary and legitimate usage of telecommunications equipment, software and networks. Again, this offence appears to carry strict liability.[13]

- Article 107 establishes the vicarious liability of leaders of organisations for the professional acts of individual staff members. This provision also affirms that individual criminal liability is not extinguished and both an individual staff member and the leader with ultimate decision-making responsibility within an organisation may be held dually criminally responsible for the same alleged telecoms offences. Additionally, organisations could face consequences if their staff representatives or leadership are found criminally liable for offences. This potentially poses a serious threat to advocacy work by individuals and groups and civil society at large. It could also allow for the targeting of groups and organisations through the acts of individuals. In the context of the upcoming elections, this is extremely worrying, for example it could allow opposition parties be targeted for the political speech of their members, candidates and activists. It also raises serious concerns over free expression by the media if individual reporters and senior staff can be convicted for expression of opinion.[14]

- Article 65 (b) claims to enshrine the right to privacy for individuals using telecommunications services.[15] However, this protection of privacy and correspondence carries no substantive value in practice due to the inclusion of an exception clause permitting this right to be overridden should it be, "Otherwise determined by other specific laws." This exception clause is unconstitutional. The right to confidentiality of correspondence is enshrined in the Constitution,[16] the highest source of domestic law and one that cannot be derogated from by ordinary national law.[17] The remainder of the Telecoms Law itself also severely undermines this flimsy protection and the powers it gives to government bodies amount to constitutional violations in their own right**.** Nevertheless, Article 65 (g) provides for the right to freedom of association through telecommunications, with explicit reference to the Constitution.[18] There is no explanation as to this inconsistency in the entrenchment of rights and protections.

- Article 65 (c) establishes a right for individual telecommunications service users to participate in consultation on the policies and regulations for the telecommunications sector. Yet the law itself was passed with little warning and no meaningful consultation, lacking any transparency and excluding input from service users.[19]

---

[12] Threats must be issued "again and again" under Articles 93 and 95.
[13] Telecoms Law Article 99; also Article 100
[14] Telecoms Law Article 107
[15] Telecoms Law Article 65(b)
[16] Cambodian Constitution Article 40
[17] Cambodian Constitution Article 150
[18] Telecoms Law Article 65(g); Freedom of association and peaceful assembly is protected under Cambodian Constitution Articles 41 and 42 while Article 31 also domestically recognizes and respects international standards including ICCPR Article 22
[19] Telecoms Law Article 65(c)

Destruction of Evidence

The Telecoms Law includes specific powers for the destruction of evidence that could preclude a fair trial for any individual charged under this law. This procedure is an outrage to fair trial rights, and dispatches with any notional respect for the burden of proof and the rule of law within the Cambodian criminal justice system. The destruction of evidence could amount to a state-sanctioned crime and could prevent any individual charged under this law from mounting a complete defence.

- Article 76 creates a procedure whereby telecommunications inspection officials can apply to the prosecutor for the right to destroy evidence "in line with applicable procedures", should it be declared a "prohibited or dangerous product."[20] It is unclear what would amount to applicable procedures – pre-existing and extremely limited Criminal Procedure Code provisions ban the destruction of evidence, only permitting the disposal of dangerous or unlawfully held items in circumstances where they are not required as evidence – these are not referenced by the Telecoms Law. Protections relating to the relevance of exhibits do not exist within the Telecoms Law itself. The Criminal Procedure Code does not accommodate a role for policing officials to request the prosecutor to destroy evidence and precludes the prosecutor from disposing of items during a judicial investigation or trial. Conversely, the Telecoms Law appears to create competence to carry out exactly such acts. Application to the prosecutor in this manner both conflicts with the provisions of the Criminal Procedure Code and suggests that relevant evidence could be destroyed at a pre-trial stage. Further, the definition of dangerous and unlawful items under the Criminal Procedure Code is strictly limited, another feature absent from the Telecoms Law. There are no safeguards in the Telecoms Law, leaving this provision extremely open to abuse. [21]

- As noted, these powers could be used to prevent a complete defence through the destruction of exculpatory evidence. Additionally, handing prosecutors powers to destroy the very evidence they are legally obliged to present to satisfy the burden of proof, in accordance with the constitutional presumption of innocence of the defendant, demonstrates the authorities' lack of commitment to the rule of law and genuine justice. This article simply increases the potential for the courts to be used as a political tool against free expression, association and democratic activism. Under the Criminal Code, destruction of evidence is an offence in its own right.[22] Without safeguards, this provision is simply state-sanctioned impunity for a criminal offence in order to subvert the criminal justice system.

- The law also permits the authorities to pass the financial cost of the destruction of evidence on to the accused. In addition to jeopardizing fair trial rights, the destruction of evidence belonging to an individual is arguably a violation of the right to property, particularly where an accused party is subsequently exonerated and the items cannot be considered dangerous or unlawfully held.

[20] Telecoms Law Article 76

[21] Code of Criminal Procedure Article 119 permits the prosecutor to dispose of dangerous or unlawfully held items only where such items are not required as evidence. The definition of "dangerous" under this article establishes an objectively high threshold through reference to weapons or explosives capable of harming persons or property. This article also prevents the disposal of items by a prosecutor during a judicial investigation or trial proceedings and contains an appeal procedure against decisions to dispose of items; Article 161 permits the disposal of items at a pre-trial stage, only by the investigating judge and only if they are dangerous and unlawfully held - disposal is only permitted where it does not impact "ascertaining of the truth" by the court – precluding the destruction of relevant evidence; Article 354 vests power to dispose of dangerous or unlawfully held items considered as evidence with the court as part of the judgement at the conclusion of a trial.

[22] Criminal Code Article 533;534

Telecommunications policing and enforcement

The Telecoms Law contains inspection and enforcement provisions exceeding those of previous drafts.[23]

- Chapter 13 creates a new unit of "telecommunications inspection officials", in effect a telecommunications policing force with duties to, "monitor, study, check and strengthen the enforcement of this law." While inspection of infrastructure and industrial regulation could be considered a legitimate function, in light of the numerous criminal offences the primary mandate of telecommunications inspection officials appears to be to "prevent and crack down on telecommunications offences." This permits the monitoring and penalizing of online content and potential investigation of any interaction between individuals. In addition, telecommunication inspection officials are authorized to conduct any other discretionary tasks ordered by the Minister of Post and Telecommunications.[24]

- This force will hold full judicial police powers in accordance with the Criminal Procedure Code.[25] As part of their investigatory powers, telecommunications inspection officials appear competent to seize and copy data and conduct "checks" on telecommunications equipment.[26] In worrying escalation, telecommunications inspection officials may call in support from the Royal Cambodian Armed Forces, "to join in cracking down on offences stated in the law," including the enforcement of the Telecoms Law's unlawful restrictions on individuals' fundamental freedoms.[27] This specific mandate for telecommunications inspection officials and the armed forces to "crack down" on instances of free expression and association by individuals is neither proportionate, nor necessary and simply represents legislative permission for the government to intimidate and crush any activity via telecoms that it disagrees with. Telecommunications inspection officials also hold powers to temporarily suspend telecoms firms' services and suspend or fire their staff.[28]It is foreseeable that these powers could be misused to disrupt democratic expression and assembly in the run up to an election.

Excessive state control

Chapter Two and Article 24 of the law place the entire telecommunications industry, its infrastructure and all telecommunications-related activity under the competence of the Ministry of Post and Telecommunications.[29]

- Article 8 of the law elevates the existing Telecommunications Regulator of Cambodia (TRC) to a statutory footing while under Article 9 the TRC chairperson gains equal status to a secretary of state within the Ministry of Post and Telecommunications.[30]

- The TRC is responsible for the practical implementation of the Telecoms Law and is granted far reaching powers under Article 12, including competence to authorize investigations and take action against telecoms operators it deems to be in violation of the law.[31]

- Article 7 of the Telecoms Law provides that in the event of "force majeure", the Ministry of Post and Telecommunications or other relevant ministries may order private telecommunications operators

[23] Telecoms Law Article 70 (c)
[24] Telecoms Law Article 70 (b); 70 (e)
[25] Telecoms Law Article 71; Criminal Procedure Code
[26] Telecoms Law Article 70 (a); (c); (d)
[27] Telecoms Law Article 72
[28] Telecoms Law Article 74; 78 (2)
[29] Telecoms Law Chapter 2; Article 24
[30] Telecoms Law Article 8; 9
[31] Telecoms Law Article 12; in particular 12 (k)

to "take necessary measures."[32] This article is ill-defined and does not specify the force majeure circumstances compelling discretionary government powers to direct the operation of private companies, or what "necessary measures" may entail. This leaves this provision extremely vulnerable to misuse. It is foreseeable that this provision could be abused to temporarily shut down social networks and other internet-based services, such as messengers, as a means to inhibit social mobilization as has been the case in other repressive regimes.[33] There is precedent for such a shutdown within Cambodia; in 2007 prior to the second nationwide commune elections, the government imposed a days-long suspension of SMS services in the Kingdom to interfere with the work of election observers.[34]

- The existing licensing regime under government control is further entrenched and the Telecoms Law adds no appeal procedures or improvements to safeguard against arbitrary licensing decisions. Unlicensed activity is punishable by custodial sentences and extremely high financial penalties.[35] While a licensing regime is not an unusual regulatory practice in itself, within the Cambodian context the government can use these provisions to maintain control over traditional media outlets and internet service providers. Article 110 requires telecommunications operators to reapply for licenses within one year of the Telecoms Law entering into force.[36] This means the government will decide on the continued operations of television stations, radio stations and internet service providers in the run up to the 2017 commune election.

- Although the TRC is obliged to provide written justifications for its decisions, the total lack of transparency over telecommunications infrastructure, for example bandwidth capacity, means there is no way of independently verifying whether TRC grounds for denial of a license are legitimate.[37]

- Under Article 89, any act of basic telecommunications operation[38] without a license could incur custodial sentences and heavy fines of up to 5 million riels.[39] The Telecoms Law Annex establishes an extremely broad definition of "telecommunications devices" to include any electronic device capable of communication,[40] meaning that small-scale unlicensed sale or repair of items as basic as a mobile phone or a computer could be punished by a custodial sentence. Under Article 91 the construction or operation of telecommunications infrastructure and services without a license is punishable by custodial sentences of up to three years.[41] As such, the Telecoms Law reinforces government constriction and discretionary licensing control over the use of telecommunications from an individual level up to major telecommunications infrastructure providers.

Government interference and private property rights

The Telecoms Law gives government bodies far reaching powers to interfere in the internal operations of private telecoms operators. There is a real risk that the provisions discussed below could be misused to convert notionally independent private firms into government proxy companies and vehicles for repressive action.

---

[32] Telecoms Law Article 7
[33] http://www.theguardian.com/world/2011/jan/26/egypt-blocks-social-media-websites; http://www.ibtimes.com/thailand-internet-censorship-government-orders-service-providers-block-criticism-take-1770220
[34] http://www.washingtonpost.com/wp-dyn/content/article/2007/03/30/AR2007033000944.html
[35] Telecoms Law Articles 14; 15; 16; 17; 18; 20; 78; 89; 91
[36] Telecoms Law Article 110
[37] Telecoms Law Article 20 (c) requires the TRC to provide a reasoned decision; however, there is no substantive mechanism for appeal against a refusal to license.
[38] Telecoms Law Article 15
[39] Telecoms Law Article 89
[40] Telecoms Law Annex
[41] Telecoms Law Article 17; 91

- The TRC is mandated to suspend or terminate the employment of senior staff of telecommunications operators for breach of the Telecoms Law.[42] It is unclear whether a final court judgement would be required to invoke this power or whether the TRC could declare a breach to justify interference in the internal operations of a company.

- The TRC is also authorized to recruit staff to replace private companies' employees punitively suspended or terminated under the Telecoms Law in order to coordinate and "check" the activities of firms deemed to have violated the law.[43] Additionally, the TRC can order restrictions on the activities of telecoms operators, irrespective of compliance with licensing conditions.[44] The lack of clarity over the status or permanence of government recruited staff within telecommunications companies means there is a genuine concern over the longevity and nature of government control over private companies and their assets.[45]

- Article 69 contains inconsistent provisions as it appears to authorize both the TRC and the courts to order compensation in disputes between telecommunications operators.[46] TRC powers to order compensation encroach on judicial competence[47] and amount to a violation of the constitutionally-guaranteed separation of powers.[48]

[42] Telecoms Law Article 78 (2) (a)
[43] Telecoms Law Article 78 (2) (b)
[44] Telecoms Law Article 78 (2) (c)
[45] Cambodian Constitution Article 44; Telecoms Law Articles 7; 78
[46] Telecoms Law Article 69
[47] Cambodian Constitution Article 39
[48] Telecoms Law Article 69; separation of powers is collectively established under Cambodian Constitution Articles 51, 128, 129 and 130