ARTICLE 19

Computer Crimes in Iran: Online Repression in Practice

2013

ARTICLE 19
Free Word Centre
60 Farringdon Road
London
EC1R 3GA
United Kingdom
T: +44 20 7324 2500
F: +44 20 7490 0566
E: info@article19.org
W: www.article19.org
Tw: @article19org
Fb: facebook.com/article19org

ISBN: 978-1-906586-72-0

© ARTICLE 19, 2013

This work is provided under the Creative Commons Attribution-Non-Commercial-ShareAlike 2.5 licence. You are free to copy, distribute and display this work and to make derivative works, provided you:

1) give credit to ARTICLE 19;
2) do not use this work for commercial purposes;
3) distribute any works derived from this publication under a licence identical to this one.

To access the full legal text of this licence, please visit:
http://creativecommons.org/licenses/by-nc-sa/2.5/legalcode.

ARTICLE 19 would appreciate receiving a copy of any materials in which information from this report is used.

Table of contents

Glossary and abbreviations

Basij = paramilitary volunteer militia, established in 1979 by order of the Islamic Revolution's leader, Ayatollah Khomeini.

DCI = Data Communication Company of Iran.

Etteraz = to protest.

Gooder = Google reader application.

Hashtag = A word or a phrase prefixed with the symbol #, providing a means of grouping messages.

ISP = Internet Service Provider.

IRGC = Army of Guardians of the Islamic Revolution.

Kafir = non-believer [in God].

MEK/MKO = *Mojadedin-e Khalq* organisation.

Meme = An idea, style or action which spreads, often as mimicry, from person to person via the Internet, as with imitating the concept..

Moharebeh = perpetrator of the crime of "waging war against God", or "enmity against God".

Parvadehye akhlaghi = A legal case brought against a victim using questionable "un-Islamic" social and cultural behaviour as evidence.

TCI = Telecommunications Company of Iran.

UNHCR = United Nations High Commission for Refugees.

Velayat-e-Faghih = Guardianship of the Jurist, in the Iranian context meaning that the supreme leader has custodianship over all Iranians, and in some cases all Shias.

VPN = Virtual Private Network.

Islamic Revolutionary Court = A special court established after the 1979 Islamic Revolution, designed to try people suspected of smuggling, blaspheming, inciting violence or trying to overthrow the Iranian government.

Executive summary

Iran's Computer Crimes Law was approved by parliament in January 2009. Many believe it has been instrumental in the prosecution and repression of cyber-activists and bloggers. Its 56 articles concerning internet usage and online content are ambiguous, vague and therefore dangerous. The Computer Crimes Law appears to be the latest addition to the Islamic Republic of Iran's vast censorship apparatus.

This report presents a collection of narratives from Iranian civil society activists who have become victims of the Iranian regime's sophisticated censorship apparatus and its suppression of digital activism. These activists had built prominent online presences over the years, and faced the strong hand of the regime because of their legitimate online critiques of the regime's control of civil society and/or politics.

This report also hints at the contentious relationship between the growth of the internet in Iran over the past two decades and the regime's response to it. This will help readers to appreciate and put into context the importance of the Computer Crimes Law, a relatively new element in the Iranian regime's vast apparatus of tools for the methodical suffocation of civil society and online expression.

Our research shows that the Iranian leadership has, up to now and on the pretext of "national security", sacrificed an open internet and a thriving civil society in order to ensure its own survival. The Iranian leadership fears the benefits of openness and transparency. Its policies and positions demonstrate its desire for increased control of the internet and for greatly enhanced monitoring. In fact, the Iranian regime does not need the Computer Crimes Law to repress activists, because it will be able to continue relying on the traditional existing legal apparatus, particularly the Penal Code, to intimidate and punish digital activists for expressing their views publicly. However, the Computer Crimes Law provides the regime with an additional legal tool, and an important one. It contributes to a larger orchestrated campaign aimed at effectively minimising or eliminating the freedoms which online fora provide for legitimate discussion and criticism and for any challenges to the Iranian government's control of society and politics.

The Computer Crimes Law and the Iranian regime's overall approach to censoring freedom of expression on the internet are in many ways contrary to international norms, human rights laws and interpretive standards. ARTICLE 19 believes that restoring the right to freedom of expression in Iran requires wholesale reform in order to redress the conceptual failure signified by the Computer Crimes Law and other legislation. The protection and promotion of freedom of expression must be reasserted as the norm and limitations on free expression must be the exception.

ARTICLE 19 hopes that the most recent steps taken by President Rouhani will pave the way for more progressive policies that enshrine freedom of expression and human rights, rather than demonising them, and that these will lead to more constructive relationships amongst all of the stakeholders who are interested in advancing human rights globally.

Methodology

Background and objectives

Iran's Computer Crimes Law was approved by parliament in January 2009. Many believe it has been instrumental in persecuting and repressing cyber-activists and bloggers. Its 56 articles have seldom received much public attention or scrutiny. ARTICLE 19 therefore conducted a thorough legal analysis of the law in 2011, illustrating its ambiguous, vague and catch-all provisions concerning internet usage and online content.

This report follows up on that analysis and presents a number of narratives from Iranian civil society activists who, because of their vocal critique of the regime's control of civil society and political affairs, have become victims of the Iranian regime's suppression of the online space. Their narratives help highlight some of the ways in which Iran's Computer Crimes Law has been applied to civil society activists working in the digital sphere, and illustrate how the vague, opaque and subjective interpretations of the law systematically undermine inherent human rights such as the right to freedom of speech.

The report also aims to help mobilise a coalition of like-minded non-governmental organisations and private sector partners who value the advocacy of the defence of internet freedom and freedom of expression and the provision of information to Iranian citizens unjustly affected by the institutionalisation of this law.

Methodology

This report presents a collection of narratives from Iranian civil society activists who have suffered collateral damage because of the Iranian regime's sophisticated censorship apparatus and its suppression of digital activism. These activists built prominent online presences over many years and faced the strong hand of the regime because of their online critiques of the regime's control of civil society and/or politics.

The report incorporates a diverse range of primary and secondary sources, obtained both in interviews and by using search techniques in both Persian and Pinglish (Persian written with the Latin alphabet).

Interview questions were created to reflect trends and insights garnered via secondary research, particularly changes in Iran's political environment and evolution in the online space. All interviews were conducted using Skype.

Additional interviews were conducted with authors, experts, opinion formers, practitioners and generators of online content (bloggers and social media users), both in order to bring a new layer of context to primary narratives and secondary data and also to clarify outstanding information.

Section I - The politisation of the internet and the Iranian regime's response

"People are scared, and the online space, which was once a sanctuary, is turning into a hunting ground."

– Sara (Pseudonym)

Iran's Computer Crimes Law

In January 2010, the Iranian parliament approved the Computer Crimes Law. Many believe it has been instrumental in prosecuting and repressing cyber-activists and bloggers. However, its 56 articles have seldom received much public attention or scrutiny. ARTICLE 19 therefore carried out a thorough legal analysis in 2011 illustrating the law's ambiguous, vague and catch-all aspects concerning internet use and online content. ARTICLE 19 found that the 2010 Computer Crimes Law of the Islamic Republic of Iran flagrantly violates international human rights law and is an affront to the principle of freedom of expression. ARTICLE 19 urgently advocates extensive legal reform, including the repeal of the Computer Crimes Law, in order to protect the right to freedom of expression in Iran.

The report reveals that the Computer Crimes Law is saturated with provisions that criminalise legitimate expression. Offences such as "crimes against public morality and chastity" and the "dissemination of lies" are engineered to ensnare all forms of legitimate expression. The provisions of this law include broad definitions of criminal defamation and obscenity that are antithetical to the right to freedom of expression. Essential elements of various offences are also described ambiguously, in vague and overly broad terms. No defence is available to individuals acting in the public interest. The Government is given unlimited discretion to pursue its own aims and to put these before the interests of the public and the imperatives of international human rights law.[1]

The Computer Crimes Law mandates severe sentences that penalise legitimate expression and offend the proportionality principal that is fundamental to human rights protection. ARTICLE 19 is particularly appalled at the fact that the death penalty can be ordered for crimes committed "against public morality and chastity". Other sanctions on legitimate expression include lengthy custodial sentences, draconian fines, and judicial orders for the closure of organisations and the banning of individuals from using electronic communications. These penalties also apply to internet Service Providers (ISPs) that fail to enforce content-based restrictions, thus incentivising the private sector to promulgate Iran's culture of censorship.

ARTICLE 19 notes with concern that the Computer Crimes Law is the latest addition to the Islamic Republic of Iran's vast censorship apparatus. It demonstrates the resolve of the Iranian Government to pursue the human rights defenders, bloggers and journalists who use electronic media, which was formerly the last available sanctuary for freedom of expression and political dissent in the country. ARTICLE 19 believes that wholesale reform is needed in order to restore the right to freedom of expression in Iran and redress the conceptual failure signified by the Computer Crimes Law. The protection and promotion of freedom of expression must be re-established as the norm and limitations on free expression as the exception.

The following sections elaborate on the relationship between the growth of the internet in Iran and the regime's response to this phenomenon over the past two decades. This will help readers to appreciate and put into context the importance of the Computer Crimes Law, a relatively new element in the Iranian regime's vast apparatus of tools for the methodical suffocation of civil society and online expression.

The rise of the internet in Iran

Since its inception in 1993, the internet has grown exponentially in Iran, at an average annual rate of approximately 48%, increasing from under one million internet users in 2000 to around 23 million by 2008.[2] As of September 2012, the BBC reported approximately 42 million internet users in Iran, comprising more than 50% of the population (InternetWorldStats.com).[3] The internet penetration rate sits at approximately 35% of the population, considerably higher than the average across neighbouring countries of 26%.[4] The web is the main forum for dissident voices, providing an alternative space for public discourse, away from the state-controlled media, and allowing anonymity and freedom of expression for political interaction – something that is otherwise denied under the prevailing conservative regime. Iran's online space boasts tens of thousands of weblogs, with bloggers active within Iran and outside among the diaspora. In fact, the Persian blogosphere has gained an international reputation as one of the largest and most active in the world, with an estimate of more than 60,000 blogs.[5] Despite the obstacles, access can be arranged to enable a certain amount of unfettered expression of opinions online.[6] The surge in internet usage can be attributed to Iran's technologically savvy youth demographic, who have benefited from increasing access to higher education over the last 13 years.[7]

The internet and other communications technologies have created unprecedented opportunities to share information, opening up paths for pro-democracy groups, activists, journalists and individuals inside Iran to organise themselves and hold their government accountable.[8] It has also allowed for the consolidation of the conservative ideology, whereby the state, through both sophisticated and pervasive censorship strategies and opaque regulation, actively closes down websites that it objects to and filters out any pro-secular, anti-Islamic and reformist political perspectives that threaten the prevailing conservative logic.[9]

The consolidation of conservative ideology and the fight to control discourse on the internet have also affected the renowned Persian blogosphere. Social networking analysts at Harvard's Berkman Center found that four different categories of bloggers exist in Iran, only one of which seeks secular reform and uses blogging as a tool for communicating grievances against the Iranian regime.[10]

According to the Berkman Center, the secular/reformist bloggers, of whom a high proportion are women, lead ongoing discussions in online fora about Iranian politics, the separation of religion and state in Iran, and current affairs in the world. However, a strong and rising contingent of conservative bloggers actively contributes content counter to this secular/reformist logic in order to gain supremacy of discourse and control the narrative on the internet.[11]

The Iranian state's response to the rise of the internet

The growth of the internet has not been an entirely positive phenomenon. It remains vulnerable to exploitation by the Islamic Republic of Iran, which aims to crush dissent and deny people their human rights, as evidenced by some of its most recent postures and actions against digital activists. Without exception, governments struggle to balance issues such as security, hate speech, and child safety for their citizens against the protection of freedom of expression, information and thought. In Iran, however, as in other states with repressive agendas, these tensions and concerns serve as convenient pretexts to engage in censorship or surveillance of the internet which violate the rights and privacy of users and threaten the free flow of information.

The following section describes how different Iranian Presidents have balanced the natural tensions between, on the one hand, support for civil and political rights, freedom of expression and the rise of an open internet and, on the other, national security and regime survival. Unfortunately, over the years the Iranian leadership has sacrificed the former in favour of the latter.

Socio-Political developments

Until 2000, the private sector was the main driver of internet development.[12] According to the International Telecommunication Union (ITU), there were 625,000 internet users in Iran at the beginning of 2000.[13] By the end of Khatami's presidency in 2005, that number had increased to several million, spurred forward by the country's increasingly youthful demographic profile.[14] During Khatami's presidency (1997-2005), civil society organisations enjoyed a much more open and tolerant political climate. At the end of Khatami's second term as president in 2005 there were 6,914 registered non-governmental organisations (NGOs), a number unprecedented under any other presidency or period of contemporary Iranian history.[15]

That said, during Khatami's second term in office, conservative forces gradually began gaining greater and greater dominance in their political struggle with reformists. Ahead of the 2004 parliamentary elections, the Guardian Council disqualified an unprecedented 3,600 candidates, many of them reformists.[16] More than 100 sitting members of parliament resigned in protest.[17]

The election of Mahmoud Ahmadinejad as President in 2005 signalled the arrival of a new conservative force. Many conclude that he was voted in with the support of Revolutionary Guards, the Basij and the Supreme Leader Ayatollah Khamenei.[18] Under Ahmadinejad's presidency, the attitude of the government shifted from one of cautious encouragement towards NGOs to one of suspicion and open hostility.[19]

Between 2005 and 2009, the government increasingly applied a "security framework" to NGOs in Iran, limiting their freedom of association, often accusing them of being "tools of foreign agendas".[20] The authorities regularly suppressed NGOs and denied them permits to operate, often even refusing to provide them with written explanations when rejecting applications, as is normally required by Iranian law.[21] This logic and approach also extended to secular and liberally-minded civil rights activists or bloggers.

In the lead-up to the 2009 Presidential elections, this tone of open hostility evolved into a more formally orchestrated crackdown on reformist agents of any kind, particularly bloggers and civil rights activists. The nature and size of the crackdown dramatically reduced the space available for civil society and independent or critical voices in Iran. According to an organisation defending civil society, Arseh Sevom, activists, dissidents, and critics of the government faced a stark choice: either risk arrest, detention and conviction or leave the country.[22] Many chose the latter option. In fact, since 2009, there has been a marked increase in the number of civil society activists who have applied for asylum and resettlement in third countries.[23] According to statistics compiled by the UN High Commissioner for Refugees (UNHCR) and collected from 44 industrialised countries that conduct individual asylum procedures, there were 11,537 new asylum applications from Iranians to these 44 countries in 2009; 15,185 in 2010; and 18,128 in 2011.[24] The largest number of new asylum applications was lodged in neighbouring Turkey, which saw a 72 per cent increase in the number of Iranian asylum seekers between 2009 and 2011.[25]

According to recent reports, there have been 436 arrests, 254 convictions, and 364 cases of students being deprived of education since March 2009.[26] Reports also allege that the judiciary summoned at least 144 students for investigation, while officials closed 13 student publications.[27] As a result of these pressures, dozens of students and student activists, many of whom had been deprived of the opportunity to continue their education, have left Iran to pursue education elsewhere.

According to the NGO Reporters Without Borders, more than 76 journalists have been forced into exile and the authorities have shut down at least 55 publications since 2009.[28] In fact, as of August 2012 there were at least 44 journalists and bloggers in prison, making Iran one of the countries imprisoning the most journalists.[29] The judiciary has imposed harsh sentences on journalists and bloggers, based on vague and ill-defined press and security laws, for crimes such as "acting against the national security", "propaganda against the state", "publishing lies", and insulting the Prophet or government officials such as Supreme Leader Ayatollah Khamenei or President Ahmadinejad.[30]

ARTICLE 19 expresses cautious optimism about Iran's more moderate tone under President Rouhani. ARTICLE 19 applauds the Iranian leadership's gesture of good will in releasing more than 80 prisoners, including a dozen political prisoners (in particular the prominent human rights lawyer Nasrin Sotoudeh), ahead of its visit to the United Nations General Assembly.

ARTICLE 19 encourages the Iranian leadership to continue demonstrating a greater degree of flexibility, reflected not only in a shift in the country's diplomatic policy, but in its domestic approach towards civil society actors and human rights defenders.

ARTICLE 19 encourages the government to cease its sophisticated crackdown on and intimidation of activists, journalists, and human rights defenders who exercise their right to peaceful dissent and requests the leadership to pursue a more enlightened and progressive approach to this issue.

Developments in Iranian internet infrastructure and policies

The desire of the Islamic Republic of Iran to control the internet very strictly follows a long tradition of state-sponsored censorship of freedom of speech.[31] For example, speech in the Islamic Republic is regulated through Iran's constitution, which states that "the media should be used as a forum for healthy encounters between different ideas, but they must strictly refrain from the diffusion and propagation of destructive and anti-Islamic practices".[32] Though the constitution does, in principle, provide for limited freedom of opinion and expression, numerous haphazardly enforced laws restrict these rights in practice. Since the internet provides a medium for relatively unfettered communication in comparison with the tightly controlled print media, radio and television in Iran, controlling access to the internet and regulating its use has become a strategic priority for the state.

As a first step, in 2001, the state issued regulations through the Telecommunications Company of Iran (TCI) requiring internet Service Providers (ISPs) to filter out all materials presumed immoral or contrary to state interests.[33] This decree also required all commercial ISPs to connect to the global internet via the state-controlled Telecommunication Company of Iran (TCI), effectively creating an internet infrastructure based around a government-managed gateway that offered a central point of control to facilitate the implementation of internet filtering and the surveillance of internet use. All traffic from the dozens of ISPs serving households was thereafter routed through TCI.[34]

The first ISPs began operating in Iran in 1994 and, as of 2013, many believe their number has grown to over 150.[35] Though many ISPs have been privatised, they are not fully independent of the government. The leading firms are still very closely linked to the government and remain ultimately accountable to it.[36] In terms of policy, all private ISPs must be vetted by both the Data Communication Company of Iran (DCI) and the Ministry of Culture and Islamic Guidance (MICG) for approval before being issued a licence to operate. The Data Communication Company of Iran (DCI) is today the largest ISP in the country, and the provider through which most other ISPs get their internet connectivity. The DCI is a subsidiary of TCI, owned by the Islamic Republic Revolutionary Guards and run by the newly re-named Ministry for Information and Communication Technology (MICT), which is responsible for TCI policy.[37] This level of centralisation allows the government to monitor, filter, slow or shut off all internet use in the country.[38]

Most recently, the new Computer Crimes Law aims to institutionalise this regressive posture by making ISPs criminally liable for all their content. Article 18 of this law makes ISPs responsible for making sure that "forbidden" content is not carried on their servers. If any objectionable content is detected, they must immediately inform law enforcement agencies of the violation, retain the evidence and then block access to the prohibited content.[39] As a result, ISPs are forced to monitor and filter content closely and constantly or risk losing their licence to operate (or worse).

The most recent revisions to the Press Law deem that blogs and websites are equivalent to written "publications". Therefore, if websites do not obtain licences before making content available, they become ipso facto subject to stricter "General Laws". In these cases, the Iranian Penal Code can be applied, placing harsher restraint on speech. The Penal Code sanctions "content-based crimes", such as propaganda against the state. Likewise, Article 513 of the Penal Code allows a

sentence of death or a prison term of up to five years for any speech considered an "insult to religion".[40] Also, Article 698 of the Penal Code deems a two-year sentence, or seventy-four lashes, to be an appropriate punishment for intentionally creating "anxiety and unease in the public's mind", spreading "false rumours", or writing about "acts which are not true".[41] Article 609 of the Penal Code makes it a crime to criticise state officials who are carrying out their duties, calling for punishments of either a fine, seventy-four lashes, or three to six months in prison.[42]

ARTICLE 19 maintains that the Iranian regime's overall approach to censoring freedom of expression on the internet is contrary to international norms, human rights laws and interpretive standards in a number of ways. Such severe penalties for legitimate expression offend the proportionality principal that is fundamental to human rights protection. ARTICLE 19 believes that restoring the right to freedom of expression in Iran demands wholesale reform to redress the conceptual failure that lies behind these policies.

According to the non-governmental organisation Reporters Without Borders, state authorities have significantly slowed down the internet's speed in Iran to a crawling 56 Kbps since the June election in 2009.[43] Following recent reports of slow speeds and the disruption of specific services such as Google, Ali Tavasoli, a member of the Supreme Council of Cyberspace, claims that the poor internet performance is because of the infrastructure requirements needed to protect Iran's network against "cyber-attacks", and not due to the incompetence or malicious policies of the state.[44] Research by Small Media Inc. into Iran's internet infrastructure and policies, however, found that internet connectivity and the accessibility of uncensored information continues to deteriorate, despite official posturing about the root causes of intermittent access and slow connectivity.[45] Many experts report that communicating with external platforms from inside Iran is becoming progressively more difficult as online services continue to be heavily filtered.[46] The slow speed and excessive filtering is a significant barrier to the free access to information.

Recent policy speeches from key officials corroborate these trends. In July 2011, the deputy director of the Ministry of Communication and Information Technology declared that linking to filtered websites in an online post could be considered "against the spirit of the law", and therefore punishable by a fine or imprisonment.[47] The Iranian Cyber Police seconded this warning in November 2011, stating that exchanging information on foreign social-networking sites could constitute a criminal act and lead to prosecution.[48] Speaking from a different perspective in January 2012, an Iranian cleric declared Facebook to be un-Islamic, and said that membership constituted a sin.[49] Most recently, on 4 January 2013, Esmaeil Ahmadi-Moghadam, Iran's Chief of National Police, announced plans to develop software and strategies to control social networking sites better.[50] In a similar vein, in early 2013, Mehdi Akhavan Behabadi, Secretary of the Supreme Council of Cyberspace, announced several significant policy changes to restrict access to the internet further in an interview with *Khabar Onlin*e, an online news agency. These included:[51]

1. Mandatory VPN registration: Akhavan Behabadi announced that all Virtual Private Networks (VPNs) in the market at this time are illegal and that internet users will soon be able to buy state-approved VPN connections. The pretext for this registration is that it will benefit the security of users and protect their online banking and corporate transactions. However, state-approved VPNs provided

under the pretext of enhanced security may also have the potential to undermine users' privacy, allowing government actors to monitor user content. From now on, the use of VPNs will have to be deemed legitimate by the Ministry to be legal and the provider will have to register on a dedicated website, www.vpn.ir.[52]

2. More Access to Domestic Hosting: Akhavan Behabadi also announced that the government will begin sponsoring domestic hosting services for websites, undercutting competitors in price, reducing costs at national data centres, and providing other incentives to encourage administrators to move their website hosting to a domestic location. This push will begin with news sites and then progress to other sorts of sites.[53] Again, this initiative poses a grave risk to users' right to privacy, allowing the government to monitor and filter user content very easily.

3. Content Filtering Needs Enhancement: Finally, Akhavan Behabadi claimed that Iran still needs to filter illegal content, but that the content filtering currently used is inefficient and requires significant revision.[54]

According to Small Media Inc., these broad policy developments, when put together with key policy speeches by decision makers, hint at the possibility of more sophisticated filtering technology coming online and at changes in the software and hardware that drive the censorship apparatus.[55]

Other notable and regressive developments in both infrastructure and government policy positions regarding internet usage in Iran include:

– The IRGC forming a "Cyber Defence Command" in 2009. This body is effectively responsible for monitoring potentially subversive internet activity and for hacking in to various well-known platforms and websites that are perceived as threats to the regime's stability.[56]

– The monitoring and filtering of the internet has become enshrined in law; new regulations mandate that all users' browsing data must be stored for three months by their servers.[57]

– In January 2012, the authorities unveiled new regulations that oblige cybercafé owners to record customers' personal details and browsing histories.[58]

– Iranian officials involved in influencing the future of internet policy continually reiterate that they are developing a "national internet" in the hope of severing the country from the global web. According to a study published by *Reporters Without Borders* in March 2013, "The construction of this parallel internet, with a high connection speed but fully monitored and censored, is supposed to be completed in the very near future".[59]

– The regime has upgraded its filtering technology and has begun using it to block particular types of traffic, hacking into two international firms' digital certificates in order to undermine user privacy. It is also filtering the internet to prevent access to specific types of information by identifying specific keywords, domain names and web addresses deemed to be subversive; intercepting email to identify and monitor dissidents; and hacking blogs and websites, disrupting and shutting down sites, and taking the first steps towards establishing a national internet.[60]

Low-tech repression is used as a complement to high-tech tactics to punish and intimidate bloggers, journalists, and ordinary users. According to the non-governmental organisation *Freedom House*, over the past two years Iranian judicial authorities have meted out some of the harshest sentences in the world for online activities, including imposing the death penalty on three bloggers and information technology (IT) professionals.[61] At least 50 bloggers and online activists were arrested in 2009 and 2010.[62] Although the number of new arrests decreased in 2011, many individuals who had been detained during the previous two years were sentenced, often harshly. Three bloggers and IT professionals – Saeed Malekpour, Vahid Asghari and Ahmad Reza Hasempour – were sentenced to death between October 2011 and January 2012 on various questionable charges.[63] Malekpour, for example, was prosecuted because a software program he had designed was used to upload pornography, although this was done without his knowledge.[64] The non-governmental organisation Committee to Protect Journalists speculated that the three were targeted because of their technical knowledge and ability to assist in the building and hosting of independent websites.[65] Other bloggers have been sentenced to prison terms of up to 20 years. Blogger Hossein Ronaghi-Maleki continues to serve a 15-year sentence imposed in December 2009 for "spreading propaganda against the regime" and "insulting the Supreme Leader".[66] In June 2011, Hossein Derakhsan, who is considered the father of the Iranian blogosphere, lost his appeal against a 19-year sentence imposed on charges of "cooperating with hostile countries", "spreading propaganda against the regime", and "insulting Islamic thought and religious figures".[67] In February 2011, the Ministry of Intelligence arrested eight bloggers who had been critically discussing Islamic doctrine over the internet. In January 2012, they were all sentenced to prison terms ranging from five to nine years.[68] In another round of arrests in early 2012, security forces detained at least six journalists and bloggers in what appeared to be a pre-emptive measure to thwart protests surrounding the March parliamentary elections.[69] Most recently, in November 2012, Sattar Beheshti, a 35-year old blogger, died while in police custody. The head of Tehran's cybercrimes unit was subsequently fired after allegations surfaced that Beheshti died under interrogation.[70]

Collectively, these developments reflect the government's desire to control the internet further and multiply their monitoring activities. They also signal a continuation of the harassment and intimidation of activists, journalists, and human rights defenders who exercise their right to peaceful dissent.[71]

Regulatory bodies

In addition to these developments, a number of new regulatory bodies have been founded with mandates to restrict free access to and use of the internet. ARTICLE 19 believes that all of these regulatory bodies are in one way or another ultimately accountable to and supervised by Iran's Supreme Leader. Since 2009, the number of these regulatory bodies has been on the rise. Though the chain of command is extremely opaque and difficult to ascertain, ARTICLE 19 believes the institutions are arranged in tiers according to the following hierarchy:

- The highest layer includes major policy making bodies, such as the Supreme Council on Cyberspace (SCC) which develops Iran's domestic and international cyber policies. Major members include Iran's President and the Head of the Judiciary. Also on this tier is the Supreme Cultural Revolution Council (SCRC), which oversees committee members from the Ministry of Culture and Islamic Guidance, the Intelligence and Security Ministry, and the Sound and Vision Organisation (Islamic Republic of Iran Broadcasting).[72] The Supreme Cultural Revolution Council (SCRC) is a body dominated by conservatives and based in Qom. It was set up in the time of Ayatollah Khomeini and its decisions can only be overruled by Iran's Supreme Leader. Most of its founding members were originally appointed by Ayatollah Khamenei, Khomeini's successor. The President of Iran is the ex officio chairman of the Council.[73]

- The next layer down includes executive decision-making bodies such as the Committee Charged with Determining Offensive Content (CCDOC), which identifies sites that carry prohibited content, communicates the standards to be used in identifying unauthorised websites to the TCI, other major ISPs and the Ministry of Information and Communication Technology (MICT) and also decides which sites will be blocked. The CCDOC is headed up by the Prosecutor General and its other members are representatives from 12 governmental bodies. Significant members include the Chief of Police and representatives of the three ministries of Intelligence, Islamic Guidance and Science, ICT. The SCC and the CCDOC have seven members in common, which allows for effortless policy diffusion and institutional alignment. Also included in this layer is the Ministry of Information and Cultural Guidance (MICG) which is the chief governmental body responsible for leading the effort to control internet activity, mainly balancing the protection of individual rights against the safeguarding of Islamic, national and cultural values. The MICG is actively engaged in the creation of infrastructure to manage "illicit and immoral content".[74]

- Layer three has a policing function, taking action against offenders. Included in this layer is Iran's Cyber Police unit (FATA), which fights digital criminals. The High Council for National Security is also in this layer; it has a mandate to censor official journalists, forbidding them from covering certain topics, such as gay rights and the opposition or women's movements.[75] These restrictions also apply to citizen journalists. Also included here is the Press Authorisation and Surveillance Commission, which issues licences allowing citizens to publish content online.

The Computer Crimes Law, enacted in 2009, upgraded the mandate of the CCDOC. The authorities claim that there are procedures for appealing against filtering decisions. However, the process of appealing is highly inefficient, and the dispute process requires the website owner to disclose his or her personal information and to accept responsibility for any misconduct in the future, a commitment that few are willing to make, given the risk of severe punishment.[76] In practice, little information is available about the inner workings of the CCDOC, and censorship decisions are often arbitrary and not at all transparent.[77] According to the law, this committee should meet twice a week to decide on any website bans, but a TCI vice president said in 2010 that the rate of filtering was 200 to 300 websites per day, meaning the bulk of filtering decisions are probably made immediately upon discovery of "objectionable" content or by a small technical team.[78]

This has led to the suspension of blogs or shutting of news websites hosted on platforms inside Iran under orders from government officials. Blogfa, one of the main blogging platforms inside Iran, reportedly receives orders to shut down an average of 50 blogs each week, though on some occasions this figure has reached 10,000 blogs per week.[79] According to Alireza Shirazi, the founder and manager of Blogfa, such massive censorship has damaged the Iranian blogosphere by discouraging users from blogging.[80]

The result of this opaque chain of command, the severe sentences and penalties and the added layers of regulation is that self-censorship has become the norm for internet users in Iran, particularly on political matters.

The following timeline provides a historical overview of the Iranian state's ambivalent relationship with the internet.

Timeline – A historical overview of the Iranian state's relationship with the internet

1993

January – Iran becomes the second country in the Middle East, after Israel, to be connected to the internet.[81] From the time of its inception, the internet becomes the most powerful form of ICT used for political dissent in Iran, despite the prevailing tightly controlled press. The internet is an innovation that is originally welcomed by the regime, illustrating the supposed affinity between scientific technology and faith that allows the regime to project an aura of modernisation and engagement with advancing global technology, as well as providing a forum for the online dissemination of revolutionary propaganda.[82] Furthermore, the internet provides the state with opportunities for religious proselytising and the promulgation of Shi'ite Islamist ideology.[83]

2001

May – An order entitled "Overall policies on computer-based information-providing networks" is issued by Ali Khamenei, the leader of the country. It urges the authorities to "make access to the global information-providing network possible only through authorised entities". Following this order, the Cultural Revolution High Council passes a set of laws over six successive meetings to put control of the internet into the hands of the government. The new legislation also states that all ISPs must install and use filtering systems to "block access to forbidden immoral and political websites and other undesirable sites", and record the internet activities of their users in order to provide this data to the Ministry of ICT.[84]

2002

31 December – The Committee Charged with Determining Offensive Content is established to identify unauthorised websites and block specific domains without recourse to the judiciary.

2006

November – Iran is among 13 countries branded "enemies of the internet" by the human rights NGO Reporters Without Borders. YouTube, Amazon, Wikipedia and IMDb are all blocked in Iran.[85]

2009

February – Facebook is unblocked to encourage engagement with the presidential elections. It is subsequently blocked again in May just before the elections.[86]

13 June – Opposition candidates reject as fraudulent the official election results, which declare Ahmadinejad the winner by a landslide.[87] Opposition internet activists launch DDoS (distributed denial-of-service) attacks against Tehran government websites and use Twitter to encourage others to do the same.[88] Twitter, Facebook and other social media are used by activists to spread information about protests.[89 / 90] The government responds by shutting down the internet for 45 minutes on 13 June (later reopening it with reduced bandwidth), increasing filtering and blocking proxies.[91] Even text messaging and mobile phone networks cease functioning properly.[92]

16 June – The U.S. State Department urges Twitter to postpone its scheduled network upgrade that would briefly put the Twitter service offline.[93] Twitter delays the network upgrade from midnight American time/morning Iran time to afternoon American time/midnight Iran time, "because events in Iran were tied directly to the growing significance of Twitter as an important communication and information network", but at the same time denies that the State Department had "access to our decision-making process".[94]

19 June – The use of social networking has become so important that reports from Iran encourage the Prime Minister of the United Kingdom, Gordon Brown, to state that the democratisation of communication has forever changed the way foreign policy is carried out.[95]

20 June – Neda Agha Soltan is shot dead while observing a protest. Her death is graphically captured on video and goes viral on the internet, being seen all over the world.[96]

29 June – During the protests, Anonymous, a loosely associated and decentralised international network of activists and hacktivists, and The Pirate Bay establish the Iranian Green Party support site, Anonymous Iran.[97] The site draws over 22,000 supporters world-wide, and provides several tools and covert resources to circumvent the Iranian regime's censorship of the internet. Anonymous posts a short video about Iran and releases a message to the Iranian government, also publishing manifestos declaring its reasons for supporting the protest movement.

4 July – Austin Heap, an IT professional, and Daniel Colascione announce their preparations for the release of Haystack, a program designed specifically to bypass the Iranian authorities' internet monitoring and censorship mechanisms in order to allow the Iranian population to access an unfiltered internet.[98] The global advocacy group Avaaz.org donates $15,000 for the ongoing project.[99] Independent reviews, however, show the software to be dangerously insecure, as it fails to encrypt secrets properly and could reveal its users' identities and locations.[100] The disclosure of the security issues with Haystack lead its sole programmer, Dan Colascione, to resign and culminate in the September 2010 announcement that the software has been withdrawn due to security concerns.[101]

November – The Iranian government launches a Web Crimes Unit, tasked with policing the internet for "insults and lies". Activists see this as an attempt to restrict still further the flow of information about the government's brutal post-election crackdown.[102]

18 December – Iranian hackers, known as the Iranian Cyber Army, bring down the micro-blogging website Twitter for around two hours. The main Twitter homepage is replaced with a black and red screen featuring an image of a green flag and a page carrying the message: "This site has been hacked by the Iranian Cyber Army."[103]

2010

January – The Computer Crime Act becomes law (having first been proposed as a law for Computer Crime Act Enactment on 19 November 2008 with 176 yes votes, 3 opposing votes and 2 recusant votes in the Parliament of Iran).[104] The Computer Crime Law (CCL) identifies punishments for spying, hacking, piracy, phishing, libel and publishing materials deemed to damage "public morality" or to consist of the "dissemination of lies". Punishments mandated in the CCL are severe. They include the death penalty for offences against public morality and chastity, as well as long prison sentences, draconian fines, and penalties for service providers who fail to enforce government content restrictions. It also obliges ISPs to record all the data exchanged by their users for a period of six months.[105]

At least 50 bloggers and online activists are arrested in 2009 and 2010; three bloggers and IT professionals—Saeed Malekpour, Vahid Asghari and Ahmad Reza Hasempour— are sentenced to death between October 2011 and January 2012 on various questionable charges.[106]

2011

January – The Iranian Cyber Police unit (FATA) is founded to "confront internet crimes and protect national interests".[107]

February – The Iran Cyber Army (a group under the control of the IRGC) hijacks the new website of *Voice of America*. Until early 2012, similar digital attacks continue against other government critics' websites, such as the *BBC*, and opposition organisations' websites, such as the Association of Combatant Clerics led by former president Mohammad Khatami. Access to the *BBC Persian Service* is also disrupted.[108]

14 February – A series of demonstrations is staged in Iran, beginning on 14 February 2011, called "The Day of Rage". The protests come in the wake of the 2009–2010 Iranian election protests and are influenced by other concurrent protests in the Middle East region (the Arab Spring in Tunisia). After 10 February, the keyword *Bahman*, the name of the current month in the Persian calendar, is blocked on mobile phones. This results in slower internet connection speeds in some Iranian cities.[109 / 110]

16 March – Comodo, a major American certificate authority, advises Microsoft that nine fraudulent SSL certificates have been issued by one of its affiliates in Southern Europe. The domains concerned are:

- login.live.com
- mail.google.com
- www.google.com
- login.yahoo.com (3 certificates)
- login.skype.com
- addons.mozilla.org
- "Global Trustee"

Microsoft subsequently releases an emergency update to revoke the fraudulent certificates, which could lead to spoofing attacks[111], while Mozilla blacklists the fraudulent certificates.[112] According to Comodo, both attacks originate from IP addresses assigned to ISPs in Iran, and may come from government agencies interested in monitoring dissident activity.[113]

2012

January – New guidelines are issued for internet cafés, requiring users to provide personal information that will be retained by café owners for six months alongside a record of the websites the users have visited. The rules also require café owners to install closed-circuit television cameras and store the resulting recordings for six months.[114] Tests for a countrywide, internal national network (dubbed the "Halal internet") are carried out. Users and observers fear that Iran wants to cut itself off from the World Wide Web. Some experts cite cyber-attacks on Iranian nuclear and banking industries as the impetus for the move; others see it as the government tightening its grip even further on the flow on information.[115]

February – In the days leading up to 14 February 2012 protests, internet access to specific sites, such as Facebook, Twitter, and "other foreign sites", along with email access, are blocked throughout Iran, affecting more than 30 million people.[116] The sites are replaced with a message reading, "In accordance with computer crime regulations, access to this website is denied". As reported by *The Washington Post*, a number of Iranian bloggers fear this outage to be a precursor to the implementation of the "National internet", also known as the "Halal internet", which will allow the Iranian government to "block 'damaging' Western Web sites".[117] On 13 February 2012, it is reported that email access has returned, though other sites remain blocked.[118]

March – Iran's Supreme Leader sets up a body to oversee the internet. "The Supreme Council of Virtual Space" includes the president, the information and culture ministers, and police and Revolutionary Guard chiefs, and is tasked with defining policy and co-ordinating decisions on the internet.[119]

November – The Cyber Police become mired in scandal when an arrested blogger, Sattar Beheshti, is found dead in his prison cell. Human rights watchdog Amnesty International says he may have died under torture.[120]

2013

March – Most VPNs (Virtual Private Networks), which are used by Iranians to bypass government filters, are blocked in the run-up to the presidential elections. Skype and Viber (Internet services used to make telephone calls) are also blocked.[121]

5 May – In the run-up to the presidential elections, internet connection speeds slowed to a crawl and popular, unblocked sites, such as Gmail and Google, become difficult to access. In addition to this, circumvention tools become increasingly unreliable.[122]

14 June – Hassan Rouhani, a moderate cleric, is elected President with 50.88% of the vote. Rouhani promises to minimise online censorship, calling filtering "futile" and describing social networking sites, such as Facebook, as a welcome phenomenon. Internet users report a relative easing of online censorship after his victory, though the extent of his reforms is yet to be seen.[123]

Section II - The Damage caused by the Computer Crimes Law

Expert contributions

This section presents a series of curated viewpoints highlighting some of the challenges posed by the application of the Computer Crimes Law to the advancement of Iranian civil society and the enhancement of basic freedoms. These points of view come from a number of prominent activists for human rights and civil society and from political and legal practitioners.

- Dr Ahmed Shaheed, United Nations Special Rapporteur on the situation of human rights in the Islamic Republic of Iran
- Mr Collin D Andersson, Internet censorship and electronic surveillance expert
- Ms Gissou Nia, Executive Director of the Iran Human Rights Documentation Centre
- Ms Tori Egherman, Director at Arseh Sevom
- Mr Arash Abadpour, Prominent Iranian journalist and blogger
- Mr Mohammad Nayyeri, Iranian attorney at law, human rights lawyer, legal adviser to Iran Human Rights Documentation Centre, UK Foreign Office Chevening Scholar
- Mr Mehdi Saharkhiz, Activist and art director

The call for free expression and access to information in Iran

Dr Ahmed Shaheed[124]

March 2013 marked the 37th anniversary of the International Covenant on Civil and Political Rights (ICCPR). This treaty was adopted in March 1976 and has been ratified by 167 countries, including the Islamic Republic of Iran. Core principles promulgated by this document relate to individual liberties, such as the rights to freedom of expression, opinion, belief, and to information. It is arguable that when governments resist encroaching on these fundamental rights, a given society will be equipped with the tools for promoting a free society, predicated on notions of human dignity through the advancement of civil, political, social, economic, and cultural rights.

In his seminal report on freedom of expression and the internet to the United Nations Human Rights Council in 2011, the Special Rapporteur on freedom of opinion and expression, Frank La Rue, explores censorship and underscores the "unique and transformative nature of the internet, not only to enable individuals to exercise their right to freedom of opinion and expression, but also a range of other human rights that promote the progress of a society".[125] He also concluded that unreasonable limits to the internet access violate international law.

The fact is that no country has absolute expression rights, and all governments exert some level of influence and control over the flow of information. However, these

limitations should not be abused by political forces to limit public dissent or criticism of policies and government actions that impact the integrity of governance. Thus, a healthy balance between legitimate national security interests and democratic imperatives must prevail.

I believe that several aspects of the Computer Crimes Law passed by the Iranian Parliament in 2009, as well as other policies governing content and internet access, are incongruous with protections provided by the Article 19 of the ICCPR.

The 2009 Computer Crimes Law appears to determine permissible expression and information for Iranian audiences in light of the Government's political, religious, or cultural standards; making limits on expression the rule, rather than the exception. In my 2012 report to the General Assembly I reported that websites deemed to promote "terroristic, espionage, economic or social crimes", insult Islam or Government officials, proselytize unrecognised religions, or establish anti-government political groups are effectively blocked in Iran. I noted that the Iranian government had announced its action to block some ninety "anti-religion, anti-culture and anti-public chastity" websites, and that they reported that "documents and confessions were obtained from a number of those individuals involved", demonstrating the Government's belief that the accused "enjoyed the security support of foreign nations", for the purposes of "advancing the goals of the enemies [sic] in parts of the soft overthrow project".[126] I also reported that authorities banned domestic news outlets from reporting on the impact of economic sanctions imposed on the country, which is a deeply concerning development, as this impairs the international community's awareness of possible emerging humanitarian issues that may result from certain aspects of economic sanctions in Iran.[127]

These laws have reportedly resulted in arrests, detentions and even death sentences against individuals accused of developing and maintaining such websites, and Iranian citizens who speak out against the Government on the internet. Today, it is reported that at least 29 bloggers and online activists are detained in Iran; mostly for national security charges relating to the dissemination of "propaganda" and the "disruption of public order".

When freedom of information and press freedoms are undermined, democracy is compromised. However, the good news is that the ever-expanding development of internet circumvention tools and the increasing availability of inexpensive, user-friendly communications technologies have the potential to turn every Iranian into a journalist on *YouTube*, *Twitter*, *Facebook*, or through an email to human rights organisations around the world; rendering government censorship unsustainable and often impractical.

In the weeks leading up to his election, President Hassan Rouhani expressed his desire to eliminate obstacles to free expression, including in the arts and media. I believe that persistent vigilance on the part of Iranians, international human rights organisations, the media, netizens, and the United Nations' human rights machinery remains instrumental in mobilising support for the advancement of President Rouhani's pledges to improve protections of rights guaranteed by those treaties Iran has ratified. It is vital for the country's future that the ongoing crackdown against dissenting voices should cease and that, instead, the State should allow those voices to play their rightful part in crafting an inclusive future for Iran in the coming years.

New Surveillance Math

Collin D. Anderson[128]

The disclosure of clandestine mass surveillance programs coordinated by the United States National Security Agency went relatively uncovered by an Iranian press preoccupied with one of the most significant elections since the creation of the Islamic Republic. Even the few translations of wire services pieces on *Boundless Informant*, whose focal revelation was the extent of data collection on Iran, were quickly drowned by exhortations to the public to create a political epic that would disappoint foreign powers. It took only a day after the establishment had secured electoral legitimacy for attention to shift. Mohammad Hassan Asafari, the head of the Majlis's Commission on National Security and Foreign Policy, was amongst the first to address the reports as evidence of the West's disregard for the basic privacy rights of its own citizens. Asafari was quoted by the government-aligned Fars News Agency as claiming that the programs demonstrated that "Facebook and Google are at the service of the US security bodies and the US uses the cyberspace to its interests."[129] In the subsequent weeks, the subject had gained substantial momentum with Persian-language media, with papers such as *Hamshahri* producing original analysis on the NSA programs and even carrying a profile of Snowden. What followed was the rapid re-appropriation of the discussion of privacy and security by State actors, using sovereignty and culture to legitimise the domestic Computer Crimes Law against the backdrop of unchecked intervention by historical foes. Understanding this narrative, and the actors in play, is critical to the ability of international civil society to advocate and build tools to resist the further deterioration of the online rights of the Iranian public, particularly when global policies are perversely symbiotic to the corrosion of domestic freedoms.

In the midst of the localised sensation, American press and social media picked up, with a self-assured sense of irony, a *Fars* report about an Iranian organisation named 'Justice Seekers Without Borders' that had invited Snowden to come to Iran to elaborate on American espionage on the country. The interest of the organisation, founded by hard-line activists Massoud Barati and Mohammad Saleh Meftah, in gaining access to Snowden and the dialogue surrounding the disclosures was no coincidence. Seven months earlier, expounding on the threats and opportunities facing the foreign policy of the Islamic Republic, Barati wrote on the blog Teribon Mostazafin advocating a "clarification" strategy against international accusations of human rights violations by the Iranian state.[130] It was incumbent, therefore, on the Ministry of Foreign Affairs to abandon its "passive defensive" position in favour of aggressively reporting on allegations of human rights violations by the United States. The *Prism* programs had provided exactly such an opportunity to undermine criticisms of Iran's protection of privacy rights by ignoring civil society and maligning the failures of other states.

Justice Seekers and Asafari were quick to accuse the same companies, Google and Facebook, of violating the trust of the Iranian public by allowing the 'illegitimate spying of the American government'. Predictably as well, Morteza Barari, at the time Deputy Minister of Information and Communications Technology, was quick to announce that the Iranian government and domestically-hosted services had no email surveillance policies, unlike foreign companies. Responding to questions on the security of the nationalised information offerings, Barari sought to offer reassurance in promising

that government-run services would be privatised and that, more broadly, Islamic custom did not permit the spying that others conducted. Barari naturally omitted the lawful interception requirements placed on internet Service Providers under Article 48 of the Computer Crimes Law, the known mandates for massive interception placed on telecommunications firms,[131] and cases of electronic records being used in the interrogation of political prisoners. Privacy in Iran had become about nationalism and culture, juxtaposing religious mandates and an illusory firewall of a private sector against a faceless and foreign zeitgeist.

Asafari and Barari operate by challenging credibility and trust, appropriating legitimate fears and dark history to influence the public into moving their private correspondence within the domain of Iranian intelligence services. Moreover, between the imposing presence of states and corporations, civil society's voice is comparatively meek and completely ignored by others when it is not considered useful. Relativism, equivocation and nationalism are the hallmarks of the regulation and administration of Iran's communications infrastructure. Evidence of this lies in the three-year history of the maligned filtered site page, peyvandha.ir. Peyvandha has changed themes like seasons of the year, cycling through floral design elements with the ambition of tempering frustration while encouraging morally upright behaviour. Across every redesign, one link, "Nezarat Bar Internet Dar Deegar Keshvarha", has remained fixed and prominent, directing users to an unchanged 6,546 word treatise: "Internet Monitoring in Other Countries".

Sermonising on the role of internet filtering in promoting political stability, social well-being, national security and public morality, the article extends into discussing the privacy of *Google* services, sanctions on Iran, the United States' Communications Decency Act and Patriot Act, BT's Cleanfeed child pornography blocking, cyber-warfare between Pakistan and Iran, imprisonment of Syrian online activists and filtering during Thailand's coup d'état. Peyvandha even goes as far as quoting criticisms of Australia and China by Reporters Without Borders' "Enemies of the internet" report, naturally excluding Iran from the list of violators. Minimising Iran's filtering in comparison to the collective international precedent, the page concludes by finding limitations justified, as unrestricted access across all segments of society would threaten the mental and spiritual health of the public. Should the Ministry of Culture and Islamic Guidance take the time to update the Peyvandha page, they may appreciate how much the internet has changed in three short years. The rapid decline of freedoms of independent, online media in states such as Egypt, Pakistan, Russia and Jordan have paralleled flirtations by the West with direct censorship in the name of securing intellectual property, restricting extremist content and 'protecting children and their innocence.'[132]

Within the public discourse of Iran, particularly from state media and government representatives, the ambiguous provisions on criminal defamation, obscenity and national security within the Computer Crimes Law increasingly show little difference from actions of states purporting to defend the global online free flow of information. To the depoliticised, few legal or technical differences exist between Vezarat-e Ettela'at and the National Security Agency; in effect the question of who is allowed to spy on an individual becomes an expression of national sovereignty. Barati and Meftah seize on this point in the Justice Seekers' letter, noting that "the United States government claims to be the defender of human rights while at the same time it has been spying and controlling its own civilians", adding that the disclosure

"becomes even more severe and ugly as we learn that this very government, which claims to support human rights so vigorously, commits these criminal acts against the civilians of other countries".

The perception of a lack of oversight in American and European intelligence programs creates a powerful basis for domestic and international justification of the actions of Iran's judiciary and security services, particularly when it appears that foreign persons are denied even the basic privacy expectations of the International Covenant on Civil and Political Rights. Complicit in the repression of bloggers and journalists,[133] Asafari's comments are not merely pernicious due to his disregard for fundamental rights of expression, but rather the un-ignorable element of truth that Google and Facebook had actually become inseparable components of foreign surveillance. Furthermore, Meftah, regardless of personal history or political opinions, should be difficult to dismiss, considering his own harassment and persecution under Article 21 for publishing an article criticising the judicial system.[134] Protection of privacy and due process applies as much to foreign governments as it does the security services most likely to kick down one's door, particularly for a country with such a sense of national pride.

When the United States and Europe impose mass surveillance and mandatory restrictions on content at home, they create new international norms that legitimise the actions of illiberal regimes. These standards and behaviours are then formalised within the constitution and processes of the International Telecommunication Union, providing the Iranian government with both the sovereign right to surveillance and the perception of comparative restraint. It is clear from a historical perspective that Iran's persecution of media and restrictions on critical debate have existed, in scope and outcome, independently of the legal framework used as justification. However, the Computer Crimes Law, directly appropriating language found in the United States' Electronic Communications Privacy Act, Communications Decency Act, Computer Fraud and Abuse Act, and the Patriot Act, provides the government with a crucial mechanism of legitimacy through a facade of a rule of law that is missing in nebulous charges regarding *Moharebeh*, national security and anti-government propaganda.

The Iranian government continues its aggressive domestic campaign, through coercion and propaganda, to nationalise the country's internet, putting private communications within the reach of the state. Internationally, it seeks, with a questionably-intentioned set of allies, to legitimise its own implementation of these norms by pushing language on the "right of access of Member States to access international telecommunications services" within standards bodies such as the World Conference on International Telecommunications.[135] Once even minimally accepted, these norms become rights of sovereignty and security that dubious hardware vendors liberally cite to wave off culpability for providing the latest generation of surveillance infrastructure. The simple choice of Gmail.com or Chmail.ir becomes the full manifestation of how the failure of policies in the West and opaque international bodies materially endanger the public by forcing it to choose the authority to which it will sacrifice its autonomy.

Whether legally justifiable, domestically popular, or core to national security strategies, infringements on the privacy of the Iranian public by Western intelligence services undermine the moral authority of freedom of expression advocates and subvert the trust relationships with international companies. It is now the responsibility of civil society to resist the encroachments of surveillance norms globally, so that they do not

proliferate to Iran through technology and law, and of private companies to re-prove their integrity, so the intimate moments of individuals' lives are not a simple search away from *ershad*[136]. Failing to do so internationally will irreparably undermine the position of domestic civil society regarding the fate of the Computer Crimes Law and contribute to the further erosion of privacy in Iran.

Imprisoned for a meme? Same repression, different tools

Gissou Nia[137]

In the Islamic Republic of Iran (IRI), any form of disloyalty to the *velayat-e faqih* – or the system of Shi'a Islamic rule governed by the country's Supreme Leader who holds absolute power in government – can be met with arrest, imprisonment and, in some cases, death.

But could these penalties be meted out for something as innocuous as an internet meme?

Under Chapters Four and Five of the Computer Crimes Law of the IRI, technically, yes.

Memes – or "mimicked themes" in the form of an image, video or hashtag that spreads via the internet – are often associated with such harmless fodder as cute cats, political gaffes or questionable art. But in the IRI, the creation or distribution of such online content – if deemed to be against public morality and chastity or to disseminate lies – could be met with criminal punishment.

Just as disloyalty, or perceived disloyalty, to the Supreme Leader is penalised for actions taken offline, those penalties can apply equally for similar actions in the online space.

In the case of Arash Sigarchi, a journalist, editor and blogger who was arrested in August 2004 for blogging about the 1988 prison massacre, a sensitive and controversial topic for the Iranian regime, the acts imputed to him resulted in a punishment vastly disproportionate to the alleged crime. In describing a search that the Iranian authorities conducted of the office of *Gilan-e Emrooz*, a regional newspaper where Sigarchi was editor-in-chief, he recalls:

When they confiscated the newspaper's computers they found a series of photo-shopped pictures, such as Khomeini's head on Jennifer Lopez's body. The interrogator said that this was insulting to Imam Khomeini.

At that time, the interrogator's lack of knowledge about the functions of a shared network drive further complicated matters:

I pointed out to him that they weren't my pictures. In our newspaper, 12 people had user IDs and could log into any computer. The pictures were not necessarily mine.

While Sigarchi's case predated the codification of the laws explicitly penalising online expression, adopted in January 2010 in the form of the Computer Crimes Law, it was

an ominous sign of the online repression to come. Even as the Iranian authorities have become more sophisticated in their approach towards combating cyber-crime, technological advances have continued to outpace user knowledge among less tech-savvy members of the IRI's law enforcement apparatus. The lack of understanding of how online tools and software work, coupled with the enormous breadth and vague language of the Computer Crimes Law, has led to persistent confusion over who bears the ultimate individual responsibility for online content.

According to Foad Sojoodi Farimani, a university student who was arrested and imprisoned in Ward 2-Alef of Evin prison in 2010 for allegedly insulting Islam, his interrogators had little knowledge of the functions of an RSS feed aggregator, and targeted him for his activities on the now-defunct *Google Reader*:

After they were able to access my Google Reader posts, they told me that I have insulted Islam. I told them that I had only reposted the material, but they wanted me to confess to writing them myself.

Unfortunately for Farimani, this faulty evidence pool formed the main thrust of his forced confessions:

The interrogators really didn't have any evidence against me and I would say about 80 per cent of what [they forced me to] confess to was related to what I had posted on Google Reader. The other 20 per cent was for taking part in protests.

While the Iranian authorities appear to have come a long way in understanding the online space from the days in which imprisoned bloggers claim that their interrogators did not even know what an email was, it remains to be seen what impact the codification of laws expressly penalising certain activities on computer networks and in the online space will have on criminal penalties for forms of expression, both online and off.

Ultimately, when the computers, internet connections and social media platforms are stripped away, the traditional forms of repression against any form of expressed dissent or non-conformity – however minimal – remain intact. In the days immediately following the Iranian Revolution of 1979, the possession of contraband, leftist literature could land a person in jail; now, an individual's "anti-Revolutionary" weblog writings can.

It's the same repression, just with different tools.

The Intersection of Cybercrimes and National Security

Tori Egherman[138]

Early on during our stay in Iran, my husband and I often found ourselves in the company of a judge who worked in Iran's criminal court system. The man wore all black, all the time, made a show of averting his eyes if I entered the room without a headscarf, and spoke often of "a dialogue of civilisations". His father, he told us, called him a *kafir* (unbeliever) because he had spent time studying the Torah and the New Testament.

One evening, my husband Kamran asked him, "If I see a policeman accepting a bribe and take a picture of it, what will happen?"

"That's complicated," he answered. While the officer is clearly doing something wrong and illegal, so is the witness taking the photograph. That witness would be likely to be charged with a crime. *The officer might never even be charged! Clearly the cop taking the bribe should be the one charged, right? Who charges a witness?* I wondered.

At that time, Iran had no cybercrimes bill. In fact, the lack of legislation was a concern in the business community, with more and more of their transactions moving online. There is no doubt that societies need to redefine laws to address the changing way that we engage with each other online and through electronic transactions.

The situation we discussed with the judge is one we see played out all over the world. The logic, however convoluted, of punishing the witness rather than the perpetrator is inescapably a feature of this era of easily shared data. Those few individuals who dare to expose the illicit activities of organisations and governments often find themselves facing charges for sharing protected and classified information. This is the case even when the information they share reveals unlawful activities or threats to public safety.

All over the world, governments, civil society and concerned individuals are battling out the definition of cybercrime and, importantly, national security. **When cybercrime and national security meet, the ferociousness of prosecution seems out of balance with the reality of the infraction.** "Governments don't like to be embarrassed", says security expert Peter Bagnall of *Surface Effect*. "Security forces are vindictive when they feel humiliated. There is a possibility that they think if they slam down hard, others will be less likely to follow suit".

Defining and protecting "national security" is a challenge that taxes a society like the United States, which sets a premium on protecting free speech. The recent treatment of high profile whistle-blowers Edward Snowden and Bradley [Chelsea] Manning illustrates the challenges.

Even in a country like the United States, with a legal system that presumes the innocence of the accused, whistle-blowers are often treated as pariahs: losing their livelihoods and facing prison sentences that seem completely out of whack with the nature of their actions.

As any judge or lawyer in Iran can tell you, so much of law is open to interpretation. This can be said of democratic countries with a basis in the rule of law. In the Islamic Republic of Iran, judges, prosecutors and interpretation can feel arbitrary at times. Laws are vague and ill-defined, leaving far too much room for prosecutorial overreach.

When it comes to the treacherous intersection of cybercrime and national security, the system in Iran has come down hard, targeting all forms of dissent and difference. Rights have been sacrificed. Laws have been bent and twisted. Iran's own constitution has been violated. What the government of Iran identifies as a threat to its power is broad and often private and personal: religion, education, identity, language.

It is unlikely that the judge we met in Iran would ever even be allowed to preside over a case involving cybercrime since those crimes are often linked with national security.

The very judiciary in Iran has been circumvented, with most cases ending up in front of revolutionary tribunals that have no accountability to the general population at all.

The ill-defined charge of violating national security has been used liberally to prosecute many political opponents, leaders of the Baha'i community, other ethnic and religious minorities, lawyers defending the rights of their clients, computer-programmers and journalists.

What constitutes national security in Iran is unclear and arbitrary. Without an open forum for discussion and dissent, it will remain that way.

Thoughts on the Iranian internet question

Arash Abadpour [139]

With any new development in Iran, the "Iranian internet Question" pops back into the domain of conversations on the web and elsewhere. What is known is that the internet is one of the only remaining functional platforms for public discourse in Iran. Communication and collaboration on the web is still possible in Iran, as long as individuals and organisations are willing to make the effort to connect and communicate. Fortunately, evidence shows that this is still the case. In effect, it is fair to say that **Iranians are online and that this is no doubt an asset for the community of Iranian activists, many of whom are now based outside the geographical borders of the country.** For this group, the internet is one of the only channels to receive information in order to stay relevant, and to transfer content in order to remain active, and to communicate in order to stay in touch with the motherland.

While no significant argument seems to exist against the claim that the internet is an important component in the socio-political evolution of the Iranian society, the jury is still out on the optimal way of utilising cyberspace in order to yield the best results and cause the least harm. The big question is how the internet could be a contributing factor to the improvement of life for Iranians in particular. The internet, the filtering regime and the Cyber Army are the reality on the ground. The question is, what is the strategy to fight back and gain some ground?

When governments fight, it is called war

Activism requires financial support and monetary transactions bring strings. In fact, it takes a significant amount of time and resources to find a funder for a project, to convince them that the project is worthy of the dollars spent on it, and to provide bi-monthly and annual progress reports. While many activists have got used to this process and know how to accelerate and optimise it, with the first wire transfer comes the early symptoms of the "is-funded-by-X-and-Y" illness. In reality, work is often reduced to the political agenda of its sources of funding, inadvertently or consciously. Through this process relationships become sour and energy is wasted on the peripheries. The fact of the matter is that one must never underestimate the machinery of oppression and its efficiency in utilising subtle separation lines in the

activist community. The haze of questionable financial support is the optimal working environment for the dissemination of disbelief and depression.

Psychological concerns over sources of funding are obviously neither a misconception nor ahistorical. Many western governments have a history of meddling in the affairs of other countries by financing programs that were planned for, or were hoped to become a contributor to, the undermining and destabilisation of non-cooperating governments. In the case of Iran, one needs only a minimal background in the recent history of the country to be wary of American and Western involvement in non-democratic activities. The bottom line is that governments are bad at doing many things, including supporting activists. Government agencies, however, are good sources of funding. This creates a dilemma that needs further attention and pondering.

One could suggest that governments should use proxies, i.e. large NGOs and endowments. These proxies would allow activists to function without the need to exhaust their resources on communicating with gigantic inefficient bureaucratic machines and their changing political agendas. The suggested layer of separation would also keep the activist community within arm's reach; close enough to keep the activists accountable for the tax money channelled in and far enough away to give them room to function independently and avoid becoming puppets of an international rivalry.

Crowdsourcing freedom

Size does matter when it comes to the dimensions of bodies that plan to perform activist work. In essence, activists do in society what start-ups do in the realm of business and innovation. To be effective, the group needs to be close at a personal level and to have an intimate relationship both within the group and with the cause. Agility and spontaneity are critical factors for an organisation that intends to cause change in a society. Only through a lean organisational structure can a body of activists tackle well-entrenched social norms and political structures.

While it is imaginable that larger-scale projects require more funding and demand a more elaborate level of organisational structure, many ideas materialise when a well-knit group of like-minded individuals starts a project in a basement-style environment. In the age of the internet, it is all about finding niches and planning to exploit possibilities in society. Such operations require small-scale funding, in the range of $50,000 to $100,000. More money brings the need to establish extensive accounting, employer-employee relationships, and organisational weight. One may argue that the efficiency of an activist group increases along with its access to financial resources only up to a certain point, after which it plunges.

The point is not that larger NGOs and activist-supporting organisations are useless. Such a claim would in fact be contrary to the first point made above. The assertion here is that larger organisations are indeed required, because they can support smaller groups and sole individuals who are the actual agents of change and producers of new ideas. The important point is that the pile of money has to be distributed among many individuals and within many small-scale organisations. Excessive support for larger activist groups will inevitably result in financial resources being wasted on unnecessary organisational structures.

Thou shalt "prosume"

It is customary that a project proposal must include a section on how it is going to reach its audience. In effect, the presenter of the idea is required to define what type of content will be produced through the project and how this content will find its way to the consumer. The requirement here is to discuss how the content will pass the electronic wall of filtering and how the safety and security of the consumer is guaranteed. This notion seems to have stuck in the forms and proposal templates of Web 1.0.

Web 2.0 is about 'prosumption'. The model of interaction on the web, in which one body would produce content and another body would consume it, is history. In the age of social networks, the line between production and consumption is fading out. Content is in fact produced and consumed at the same time and in one action. A major premise of an entity such as *Facebook* or *Google+* is that individuals produce and consume content collectively and therefore they act as a social entity, therefore a "social network".

During the Cold War, the liberal democracies of the West put their resources into providing politically charged content which they hoped would cause displeasure in the present system and eventually revolt when consumed by the inhabitants of the land behind the Iron Curtain. One may call this strategy the attempt to cause change through consumption. The similarity between this approach and the medicinal recommendation of substances may in fact be one source of the misunderstanding that change is caused externally. In the 21st century all-connected world, however, individuals produce a significant amount of content and also consume important doses of content produced by their peers. Not only can what they consume be charged with desire for change, but the act of production itself can lead to raising the level of change hormones in the individual and society.

The point of the matter is that any project which attempts solely to produce new content is inevitably suspected of being a Zombie-like effort. It may walk, it may attract attention, but it is quite probable that it is its own demise. Consumption per se is not the way to change the world anymore. It is through inviting individuals to produce new content that modern societies find their identity and move towards leading a healthier life. Any project that attempts to stimulate positive change in Iranian society must be able to provide a solid answer to the question of how it is going to encourage production of content by the target individuals and provide a means for the distribution of content among both participating individuals and society at large.

Internet is the means, not the end

Technology is seductive, especially for the younger generation, which is able to create an identity based on its distinction from the previous generation, which is not as comfortable and skilful in utilising modern gadgets and concepts. New technology assists in deconstructing what is present and what has been inherited from the past. Additionally, technology happens on slick devices with shiny surfaces and exotic curvatures. What took people hours of activity a hundred years ago is now complete in a blink of an eye. Want to have a conversation with an acquaintance? It is a matter of opening *Facebook* and shooting off a short message. If the person is not on *Facebook*,

well, most probably the person does not matter in the first place. Technology gives individuals the impression that they are doing things faster, while all they have done is paid a few hundred dollars for the device and a hundred dollars per month for the connection. The rest has been invented and manufactured by well-paid engineers and minimum-wage workers in California and Zhengzhou, respectively. Nevertheless, modern technology allows its users to exhibit their proficiency in utilising gadgets as if they have been born with a third eye or have been a key element in the creation of something new.

It is vital that when a statement about the possibility or necessity of carrying out an action on the internet is made, the presenter should follow with a description of the impact of the said action in the physical world. There exist many actions which are doable and "cool", when they are done on the internet, but have minimal or no outright impact in the physical world. The fact is that, at the end of the day, Iran, i.e. the geographic location which has over seventy million flesh-made inhabitants, is going to step towards democratisation and better standards of living. The internet can be an effective avenue for bringing about change only if the bridge between the physical world and the virtual world is kept functional at all times. The regime obviously knows about this important requirement and that is why the filtering regime is established and maintained, albeit at a high cost.

To destroy the virtual world, one does not necessarily need to hijack server farms or detonate explosives at the headquarters of *Google* and *Facebook*. The blood line of the internet is connected to its physical heart. In the event of one being able to sever this connection, as the filtering regime attempts to do, the internet will become an irrelevant bunch of pointless rants and ineffective ponderings. Therefore, while it is important that it is hazardous to publish a print magazine in Iran, and while it is crucial that the said publication can be established on the web, the third side of the triangle is that there has to be some thinking on how the potential audience of the content which was to be printed on paper are going to be encouraged to consume the same content on their monitors. In the absence of a careful assessment of this key component, the triangle will collapse.

Last word

The internet allows for a wide variety of activities, many of which are hard or impossible to carry out in the physical world in Iran at the present time. This dichotomy must not cause the illusion that investing in any web-based activity is necessarily fruitful. This contribution argues that small-scale projects which encourage Iranians to produce content are more likely to succeed. The argument is that any project should have a theory as to how its impact will extend to the physical world. We recommend avoiding the direct involvement of governmental agencies in work carried out on the ground.

Waging war against Iranians' rights and freedoms in cyberspace

Mohammad Hossein Nayyeri[140]

Since the introduction of the internet in Iran in the 1990s, the discussion of its alleged potential risk and threat to public morality and Islamic values has, more than any other aspect of the issue, dominated the Iranian government's perception of the online platform. The introduction of new online concepts, such as e-government and e-commerce, has raised concerns about online security and potential criminality. Concurrently, the rapid proliferation of blogs and users on social networks has been seen as a threat to the ideological foundations of the Islamic Republic and legitimacy of the government. All these factors have created a sort of "perfect storm" for Iran's leadership and left no doubt for those in power that the internet should be considered a serious threat.

And in the Iranian government's perception, just like any conventional war, this "soft war" required the efforts of a strong "army" to fight these ideological enemies in a new and uncharted battlefield. New supervisory bodies have been formed to meet this need and the intelligence forces and police, together with newly established specialised departments, have begun to explore this battlefield and defuse potential threats. **However, in this hunt, the rights and freedoms of citizens have increasingly been ignored and arbitrary practices have become the norm.** Furthermore, the legislation necessary for regulation and criminalisation has taken extensive periods of time to prepare and the result has not been promising.

In 2008, the patience of some Members of Parliament who had long been awaiting the adoption of a comprehensive cybercrimes law expired and they took matters into their own hands. These frustrated parliamentarians proposed a new Bill according to which "establishing any weblog and website that spreads moral corruption and pornography and blasphemy" was regarded as *Moharebeh* (waging war against God) and *efsad-e fel-arz* (spreading corruption on earth), punishable by the death penalty.[141] In furtherance of this extreme position, this Bill considered allegedly criminal online activities to be equivalent in harm and punishment to crimes such as armed robbery and rape. The Bill, although initially passed as an urgent matter, never made its way out of Parliament due to widespread criticisms of its provisions. However, in less than a year, the Computer Crimes Act (2009) was finally passed, allowing the possibility of the death penalty for the digital publication of pornographic contents (article14).

Incorporating some provisions from the Convention on Cybercrime (Budapest, 2001), the Computer Crimes Act prescribed punishment for crimes such as fraud and forgery in the digital sphere. However, it was clear from the beginning that this law was not meant to accord with international standards. The Act clearly failed to address many cybercrimes and, instead, referred the treatment of these crimes back to general criminal laws and the Penal Code. Moreover, it provided a limited number of procedural provisions exclusively for the crimes addressed in this Act, and referred other cybercrimes to the general Criminal Procedure Code (article 52). In other words, it failed to address the main reason for which it was adopted, and, with the exception of some selected crimes, the rest of the crimes were left to be dealt with under the

old general rules. In fact, for years before this law even came into existence, online activists had been summoned, arrested, prosecuted and convicted by Revolutionary Courts and under the national security provisions of the Penal Code.

Another major flaw of the law was that, instead of determining illegal content in the law, the law gave exclusive power to the "Committee Charged with Determining Offensive Content" to decide which websites or blogs should be blocked. So far, the Committee has provided a list of 78 topics of forbidden content, and almost all of them are subject to interpretation and can be arbitrarily applied. However, it should be noted that the Committee had originally been established in 2002 and had already blocked thousands of websites and blogs.

This Act, however, did not change these arbitrary and draconian practices, but, instead, provided a new legal guise for them. It gave the judges and supervisory committees a new tool to suppress and control. But in an overview of the holistic landscape of cyberspace in Iran, this Act is, in reality, only a small piece of a larger puzzle. Certainly, the picture that emerges upon completion of this puzzle seems extremely concerning. Arbitrary disruption of access to the internet and reduction to internet speed, arbitrary censorship of non-conforming content and sources of information, hacking into emails and violating people's right to privacy, the criminalisation and blocking of access to social networks, and finally the widespread prosecution of online activists can all be seen as systematic violations of Iranian citizens' rights to information, opinion, and expression. This is, indeed, a "war" waged by the IRI against its own citizens and their fundamental rights and freedoms.

#Filternet

Mehdi Saharkhiz[142]

That is what the people of Iran call the internet. Imagine the speed of dialup internet, then make it painfully slower, and block every site that you want to access. That is what an Iranian faces each time they connect to the World Wide Web. It seems like the Iranian government didn't get the message about the internet being worldwide...

Concerned citizens on the outside are asking: **what can we do to help? What is the solution? How can we help the activists?** Some believe we should petition the Iranian government and demand reform of the laws governing the internet. I think differently; demanding reform will be useless, as the country does not even follow its own laws! For example, *Twitter* and *Facebook* are filtered in Iran; according to the laws you are not forbidden to have an account on either of these sites, but you are not allowed to use tools to circumvent the filters and access blocked sites. Funnily enough, not only are millions of Iranians inside Iran accessing *Facebook* and *Twitter* – using "unlawful" tools – but even more hypocritical is the use of these unlawful tools by the regime officials, as evidenced by their massive online monitoring during the recent Presidential elections.

This illustrates the one-sided and hypocritical nature of Iran's existing laws; favouring the regime at the expense of society. The regime arbitrarily arrests people at will for posting on *Facebook* or other popular online forums. So, if petitioning won't

be effective, what alternatives exist? **I believe the only way to help Iran and the activists inside is from a commercial vantage point; providing them with the same World Wide Web that people use in most other parts of the world.** Providing more anti-filtering tools is palliative and unsustainable in the long term; if we want to see real change happen through leveraging the World Wide Web, we need a stronger commercial rationale that provides them with the **actual** World Wide Web.

You might ask: *Why would a company invest in making such a dream a reality? Would it even be cost-effective?* I believe part of the answer lies in the same logic that supports providing customers with free Wi-Fi access in different locations – from local shops to entire cities, such as in San Francisco – all over the world. I am especially looking at companies like *Google* to lead such an ambitious and creative opportunity.

Iran, a country of 75 million people, has a very ripe demographic that could support a search and click-based advertising business model. Most Iranians are below the age of 35, are very well educated, and very tech-savvy; providing them with a high quality internet at a price that matches their economic means (subsidised or free) will allow the company that facilitates this to have first right of access to this enormous demographic, providing countless opportunities for click-based earnings. It will also allow this company the first right of access to a rich tech-savvy talent pool – the likes of which are handpicked to attend MIT, Harvard and other reputable global universities – to help with product development and business model contextualisation.

I am neither an engineer nor a business guru; I can't begin to intelligently predict the costs, business model or risks associated with taking on such a massive project. But, with so many examples of large corporations having profited through giving away free Wi-Fi service, I am certain comparable business models and logics exist to help build a case for intervening in Iran. More than that, I am sure that these large technology companies have the creativity and business intelligence to conceive of a way to provide some kind of enhanced service that compares to global Western standards of accessing the internet – even through a cost-recovery model – to fundamentally expand access to the internet in Iran. Whoever takes on this challenge will not only access an untapped market, but will help strengthen the social reputation and brand of that organisation by giving people a doorway to access information and by enhancing human prosperity and freedom; a fundamental and universally recognised right of each human being.

"An individual has not started living until he can rise above the narrow confines of his individualistic concerns to the broader concerns of all humanity."

– Martin Luther King, Jr.

Testimonies of individual activists facing human rights violations

This section presents the most significant contextual substantiation; the information this report is based on concrete testimonies from Iranian activists who have been effectively silenced by the Iranian regime because of their digital activism and their attempts to exercise their basic human rights, notably the right to freedom of expression. Not only have the activists been harassed, prosecuted and silenced, but in the process people have been subjected to a whole range of violations of human rights, from torture to the denial of the basic right to a fair trial. These human rights violations include, among others:

- Torture and other ill-treatment, including beatings, sexual humiliation, threats and mock executions;
- Cruel, inhuman and degrading treatment of people under arrest and their relatives, including being held in prolonged solitary confinement;
- Denial of the right of access to a lawyer;
- Denial to the right of access to family members;
- Denial of adequate medical treatment and care while in custody;
- Admissibility in court of evidence obtained through torture and other ill-treatment.

ARTICLE 19 gives credence to these testimonies.

Testimonies include those of:

- Mr Foad Sojoodi Farimani[143]
- Ms Sara *(pseudonym)*
- Ms Maral *(pseudonym)*
- Mr Mehdi Saharkhiz, on behalf of his father, the prominent Iranian investigative journalist Isa Saharkhiz.

Foad Sojoodi Farimani[144]

Background

Foad Sojoodi Farimani completed his bachelor's degree in 2007, and started his master's program in Biomechanics at Amir Kabir University, which he completed in 2010. He managed to register two of his inventions in the field of robotic surgery. Later in 2010, just as he was about to start his PhD studies, he was arrested.

"I had a weblog during that time, but writing a blog was not my primary job. I was mostly active in *Google Reader* and also was writing in social media. I would create about 20 to 30 per cent of the material myself, and for the rest I would re-post material written by my friends and people I knew. The blog was mostly focused on two issues. One was fighting against religious superstition. The second goal was introducing new tools to internet users, so they could better utilise the Web. This included introducing proxy sites, social tools or other similar things."

"During these years, in addition to my online activities, I was mainly active in the university and was also involved in political and human rights issues. I never did anything secretive or illegal. While in university I always asked for official permission before doing anything. I never did anything underground or under an assumed name."

"In March 2010 I was in Mashhad. My stepfather was in hospital and I was visiting him. They called and told me I should go to the Ministry of Intelligence's investigation office which was behind Bazaar Reza in Tehran. This was the only time I was summoned and it was done over the phone and not by written request, even though my address was known. After my stepfather died that same month I stopped my political activities almost completely to look after my family."

Unlawful arrest

Foad Sojoodi Farimani was a research assistant at Amir Kabir University. On the evening of 4 September 2010, he was detained and taken into custody by members of the Revolutionary Guard. "They were all plainclothes agents. They were almost certainly Revolutionary Guard members because later they took me to Ward 2-Alef (2-A) of Evin Prison, which belongs to the Revolutionary Guard. They dragged me to the floor in such an aggressive manner that the injury to my right arm is visible to this day. They insulted me. Without showing me a warrant they put me in a dark green Peugeot, put my head between my legs and drove off. I didn't know where they were taking me. It was very scary. To this day, I still have nightmares about this incident."

"I guessed that they were taking me to Evin from the turns the car was making. This gave me some peace of mind, because I thought 'at least I'm not in the hands of some strange group'."

"When we got [to the prison], they took me out of the car [into the prison] and sat me down. […]. They took an inventory of my belongings [including my laptop] and sent me to be fingerprinted. Then they sent me to a room and disrobed me, which was a clear violation of my human rights. Throughout, every time I asked them where they were taking me they would just respond with offensive words."

Placement in prolonged solitary confinement in Evin

"After that, they transferred me to the solitary cell number 152. My number was 9050. Later I found out that I was in Ward 2-Alef, which is run by the intelligence division of the Revolutionary Guards. At the time I didn't know. I found this out later."

> "The cell was 1.5 metres by 2.5-3 metres. I could take about five steps in it. The ceiling was about 4 metres high. […]. There was a bathroom that had an aluminium lid. The cell had a window. […]. In the cell I had no contact with the outside world."

Foad continued to express his opinions even during his imprisonment. "There were some inscriptions on the wall. […]. The word "freedom" was carved on one part. I was able to get a piece of metal from the air conditioner and carve the word deeper. […]. I was able to open a screw and wrote the poem *Yar-e Dabestani-e Man* (My Grade-School Friend) on the rocks. Later, I was subjected to a lot of beatings because of the things I had written on the walls."

Torture and other ill-treatment

Like many young activists, Foad was aware what his rights were as a prisoner of conscience. Whether those rights were respected is a different matter altogether. "The day after I was arrested, early in the morning, they took me for interrogation. I told them I had a right to have an attorney. They laughed at me, called me names and hit me on the back of the neck. They sat me down and handcuffed me to a chair with folding arms. They put me in a corner of the room. They had printed out a lot of the stuff I had shared on *Google*. They thought they had conducted an excellent investigation. They told me, 'See how much evidence we have gathered against you! The minimum sentence you could get is execution'."

"I had four interrogators. The main one introduced himself as Saeid. His assistant was called Seyed. Another interrogator was called Haji. There was also a young interrogator who said his name was Pouriya Parseh. He couldn't have been older than 23-24-years-old. He brought tea for the other interrogators. He played the good cop. He told me that if I co-operated with the interrogators he could help me."

After breakfast and the morning walk outside, Foad Sojoodi Farimani was taken for interrogation. "Immediately after coming back to the cell, they would tell me to put on my blindfold and take me for interrogation. I was in interrogation until about noon, then I would go to my cell to have lunch which was usually rice or something with bread. We were served on plastic plates. After that, I would go for interrogation again. They would take me back to my cell after it was dark."

"During the 105 days [that I was imprisoned] I think I was questioned on about 60 days. On some days I was interrogated two or three times a day. They even questioned me on holidays and during the night. Later, I found out that they would work overtime to increase their salary."

Interrogators use a variety of tactics, including false accusations, to break your will. "During the interrogations [the interrogator] asked me every kind of question: 'You are a terrorist. You were planning on bombing somewhere. You are connected with the Mojahedin (MEK). You have insulted Islam', and so forth. They tried to scare me in[to] believing I would receive the worst punishment, so that I would agree to anything. I understood their strategy later on. But nevertheless, I was completely defeated."

"Some of their questions were verbal [and not written], so they could scare me, or, as they would put it, 'break me'. Sometimes they would give me written questions and would ask me to write down the answers. At the top of every page it read, *al-nejat fel-sedgh* (truth will set you free). If they didn't like my answers they would tear up the paper, beat me, send me to solitary confinement, prevent me from having phone conversations with my family or they would take away my privilege of going outside (in the prison yard). For example, once they told me, 'Confess to working with the Mojahedin'. I told them, 'I'm a liberal. My father was killed during the [Iran-Iraq] war.[145] Plus, I have a problem with religion and communism. I can't be guilty of what you are accusing me of.' I wouldn't say it exactly like this but in a more respectful manner."

"They tried really hard to make me confess that I was connected with the Mojahedin [-e Khalq]. My interrogator told me if I didn't confess they would hang my mother. I would ask them, 'What exactly do you want me to say? I don't know any Mojahedin members. Give me a name, so I can say I was in contact with that person.'"

"During this period, I was taken to the court inside Evin prison[146] on three different occasions. The first time was around five or six days after my arrest. They took me to court to tell me the charges against me. The case investigator was Mr Mohebi [the investigator at Shaheed Moghaddasi, Branch One Court in Evin]. He treated me quite rudely. I told him numerous times, 'Let me have a lawyer'. He would just look at me over his glasses. He wouldn't give a clear answer. When my charges were first read out, the only things the interrogator accused me of related to my political activities and not [anti-]religious activities. Later, however, they focused on what I had written or reposted on *Google Reader*. They were especially sensitive about the religious issues (I had commented on)."

"During early interrogations, I realised they took issue with my political activities and used confessions by others against me. Back then, they hadn't accused me of [anti-] religious activities. Until the fourth or fifth day that I was questioned, they didn't even mention any charges like insulting Islam or anything like that. Most of the charges against me were things like, 'acting against national security', "spreading falsehood', and 'creating public anxiety'. I had saved an aerial picture of Tehran from *Google Earth* on my hard drive. They would ask me, 'Tell us where you were planning to bomb?'"

"Unfortunately, I had acted naively and had not hidden any of my actions. I had my computer on me when they arrested me and I had saved my email password on it. Still, they hit me for two days until I gave them my password."

"Over time, the accusations against me changed from political charges to religious ones such as 'insulting divine principles'. After they had accessed my *Google Reader* posts they told me that I had insulted Islam. I told them that I had only reposted the material, but they wanted me to confess to writing it myself. I remember one specific post that I had only reposted, the article was even incorrect and I had asked others not to write such things but my interrogators still forced me to confess to writing it."

"For example, I had written emails to my friends and had answered some of their questions. In one of the emails I had said that those who have schizophrenia claim they are prophets. I was subjected to a lot of beating for that one sentence. I don't understand how I had 'insulted Islam' in a personal email to a friend."

"They would read my personal emails to find evidence against me. They would say the emails were insulting to Islam. The interrogators really didn't have any evidence against me and I would say about 80 per cent of what [they forced me to] confess to was related to what I had posted on *Google Reader*. The other 20 per cent was for taking part in protests."

Forced confessions taken from prisoners were a common trend right after the 2009 presidential election protests. "The events of Ashura [Shi'a religious day] on 16 December 2010 were especially important to them. It seemed like they had arrested a university student and he had said that I had set a bank on fire that night. They put a lot of pressure on me to make me confess. However, I wasn't even in Tehran on that day, I had run away to Mashhad. [Because I would not confess to starting the fire] they didn't allow me to get fresh air for two days. Psychologically it was really bad, I felt like all the walls were closing on me and I would get anxiety attacks. I would beg them to take me outside and told them I would confess to whatever they wanted. I said, 'Fine, I set a bank on fire but I don't know which bank. Just give me a bank and I will say I set it on fire.' Later, after I was out of prison, I showed my plane tickets to the judge and told him that on that day, I was not in Tehran. I was either in the airport or on the plane flying to Mashhad. I wanted to show the judge that my entire confession was made under pressure but he did not care."

"There are many forms of torture. Some torture is psychological and some is physical. […]. One of the worst psychological tortures was the intrusion into my personal life. Searching through my personal writings, pictures of my family that were on my computer and my personal email. They had separated all the text messages that I had sent to female recipients from other text messages."

Foad Sojoodi Farimani was subjected to sexual humiliation. "They would project their own sexual fantasies on me. […] They would ask me if I had done some act and would ask me, 'How was it?' They would say disgusting things. **I think this sexual humiliation is one of the worst things they do.** My stepfather's mother is like my grandmother. Her name is Masoumeh. They would tell me that this was my girlfriend's name. They wanted me to confess to having had a sexual relationship with her."

"I had around 15-16 female students working with me. The interrogators wanted me to confess to being involved with them. They would look at my pictures taken at a wedding or pictures of my mother or my sisters that were taken at home. I would ask them, 'Why are you looking at these pictures?' They would tell me that they had religious permission to check the pictures."

"During the interrogations my right eardrum was injured […] as a result of their beatings and also because I had put some chewed paper in my ears to [protect] my ears from their screams. The combination of the two resulted in an ear infection and I was taken to the doctor."

"During my incarceration, I would often attempt suicide, because I had lost hope. I attempted suicide in various ways. One time I collected some freezer bags for a couple of weeks. Then I twisted three of them and tied them all together to make a long rope. I hooked the rope up to the air duct and, while I stood on the blankets, tried to hang myself. It didn't work so I had to come down. On another occasion I snapped off a piece of zinc from the air duct and sharpened it. Then I tried to cut the veins in my left wrist several times, but since the zinc was too soft it didn't slice through. One time I lost a lot of blood, to the point that I almost fainted, but somehow I was still alive and could get up in the morning."

"One of my worst experiences in prison was mock execution." During one of the interrogations, "Haji asked me, 'What is the last book you read?' I asked, 'What is the last book you read?' He said, 'No! I don't need to read any books; I follow religious teachings.' I talked to him about physics and he said, 'So you don't believe in God.' I said, 'No.' Then, he gave me a piece of paper and said, 'Write your will.' So I did. Then he handcuffed me, put something around my neck and began pulling it from behind. Before this incident, I had attempted to kill myself in prison. So I really hoped that he would kill me, so it would finally be over. But after he saw that I wasn't making any noise or resisting, he changed his mind."

Interrogators also subjected relatives to cruel, inhuman and degrading treatment: "Another horrific thing was that my family was informed of my arrest very late. It was about five or six days after my arrest. My [...] mother was in a very bad psychological state when she heard about my arrest.[147] My interrogators […] sent my mother a will that I had written. My mother thought they were really going to execute me."

"Every week I could make a phone call for about three minutes. Every time I made a phone call, someone would stand next to me so they could hang up the phone if I began saying [anything they didn't like]. I was only allowed to say hello, and say that I'm doing well. If I said that I'm not well, they would hang up the phone. And I had to emphasise to them that they could not give any interviews to the media."

Release

"The second time they took me to Mr Mohebi, the investigator at Evin court, he told me he would not release me on bail because I was 'spreading corruption on earth', meaning that, according to him, my freedom was equal to 'corruption on earth'. I objected. The last time I saw him he said he wanted 500 million Tomans [approximately US $500,000 in 2010] to release me on bail. My family gave the deed to my uncle's house as bail and I was released on 19 December 2010."

"Sometime after my release my mental health deteriorated really badly. I was on the verge of committing suicide and had completely lost hope. To stop myself from doing it I went to the doctors and committed myself to the Mehregan psychiatric hospital in Tehran for ten days. During this time, the Ministry of Intelligence sent one of their agents to talk to me. The [agent] pretended he was one of my friends and I told him what had happened to me in prison. They were upset about the fact that I was talking about prison. Therefore, Saeid, one of my interrogators called me and threatened that he would 'take care of me'. After that, I changed my cell phone and went to Mashhad."

Unfair trial

Foad is one of many victims who faced an unfair trial. "My trial began on 4 May 2011 at Tehran's Revolutionary Court, Branch 26, with Judge Pir-Abbasi. […]. I don't know if what occurred could be called a trial. It wasn't like they presented charges against me and then I was able to defend myself. Most of the exchanges were about unrelated things. What was said wasn't a legal argument."

"Because we didn't have good internet access in Iran, before my arrest I had saved various articles so I could read them later when I had time. One of the articles was about the Mohammad cartoons. I had saved the cartoons with the article on my hard drive. The investigators had printed all of them in colour and presented them to Judge Pir-Abbasi. The judge could not comprehend that I wasn't the one who drew the cartoons and he wouldn't even allow me to talk. He just held the cartoons up and asked me, 'What are these?' I told him, 'I didn't draw them nor have I re-posted them anywhere. Is it a crime to have them on my computer?' I pleaded not guilty and he said, 'You should have thought about that before.' My lawyer, Ms Maryam Daraei, also begged the judge to consider my young age and declared me not guilty."

A court clerk, named Satarifar, made oral threats during the court proceedings. "In the court, he threatened that he would 'take care of me'. He said, 'Your father was a martyr and you are acting like this? We will make an example of you'. […]. Judge Pir-Abbasi had ordered my belongings to be returned to me. I went to Satarifar asking for my things back. He told me, 'Boy, just leave before I do something to you'. I left the room. I was crying so hard that I couldn't see well and fell down the court steps. The tendon in my left leg was severely injured."

"Another horrible thing was that although they returned my laptop and hard drive, they had destroyed all my research projects. Everything I had done for the past ten years and all the articles that I had written were destroyed. I was willing to go to prison for eight years [to] get back all the work that I, and others, had done in the past ten years. I was in charge of one specific group with 30 students in it. We had agreed that I would be the only person in possession of the material. Unfortunately all this information was destroyed."

"**I received an eight-year sentence, five years for 'insulting Islam', two years for 'acting against national security', and one year for insulting Khomeini and Khamenei. I also received 100 lashes for insulting Ahmadinejad and a 100,000 Toman [approximately US $100 in 2010] fine for insulting the Guardian Council.** One of the charges in my indictment, which was illustrated by the Yalasarat header and was set by the Revolutionary Guard was 'insulting the Prophet [Mohammad]' and [the prosecutor] had asked the court to execute me. However, Pir-Abbasi sentenced me to prison."

"I appealed against the eight-year sentence. But I was never informed of the appellate court's verdict. I don't know what they ruled. In 2011, two weeks after I had got married, they told me that I had to go back to court in 20 days. They also sent an order to my uncle, the one who had used the deed to his house for my bail, asking him to turn me in.[148] Then I heard something that made me realise they were building another case against me. I began thinking: on one side was the 500 million Tomans (approx. USD 200,000) that I had given for bail. On the other side was the eight-year sentence

against me. I concluded that the option of leaving Iran, losing the 500 million Tomans and working later to repay that money would be better than going to prison for eight years. Plus, I could continue this fight and my education as well. Thus, in November 2011 I left Iran and went to Turkey. After that, they sent many summonses for me in Iran."

Harassment of and attacks on relatives after the prisoner's release

"After prisoners are released in Iran, sometimes people visit their families saying they are buddies with the presiding judge and if you give them money, they can have your case dismissed. One of these guys got very close to us. He knew too much about us. After I left Iran, he began harassing my family in Mashhad to get some money out of them. He would go to our door, yell and scream, and break our windows. No matter how many times my family called the police, it was never investigated. It got to the point where he even broke our door, got into our house, broke my mother's leg, my sister's arm and took a knife to my ten-year-old brother's throat.

"My mother went to court and filed a complaint against him in Mashhad. The judge turned around and told my mother, 'Madam, bring your son back from the US instead'. After that, my mother went to Evin prison in Tehran and asked them to stop this man. They said they were not involved. I still don't know if this man was sent by [the] Evin people or by another group in Mashhad. When he attacked our house, he stole my mother's cell phone, jewellery, her chequebook and even my younger brother's Xbox [a game]. All of this happened in front of the police. I have never seen anything like this: for someone to do such things and be protected by the police and the judicial system."

"I left Iran in November 2011. Currently I'm a visiting researcher at a European University."

Sara (pseudonym)

Background

Sara is an exiled former blogger and teacher from Iran aged between 20 and 39. She worked with children with special needs (children with brain damage, Downs Syndrome, etc) before being sacked from her job in Iran because of being as activist.

"I began my activism while attending the University of Kashan. Because of the politically sensitive nature of the articles I wished to publish, I eventually became the editor of the student political newspaper at one Iranian University. In my capacity as editor, I wrote articles and supported the publishing of articles questioning the role of religion in society, and I was quickly labelled an atheist (for being anti-religion and a rational thinker) by conservative decision-makers in the University. I was expelled from the University shortly afterwards."

She continued her activism about similar issues and started a weblog on *blogspot*, which took off right before Ahmadinejad's first term as president in 2005 and carried on into his second term in office.

"I eventually found work as a teacher for children with special needs. After I was hired as a teacher, I would discuss issues of culture and education in the classroom. Politics is, of course, a part of this – a consequence or reality of how society is managed. On my *blogspot* account I used to write and share satirical poetry, which had some political connotations, critiquing policies and the running of the country. It's during this time that the harassment began, first via very abusive and distasteful comments in the comments feed made by conservative digital bloggers or the paid security services of the state, who would regularly monitor my blog. It was followed with abusive and intrusive emails, threatening me about my views."

"Once the *Blogger* platform closed down, I moved my online profile and content to *Gooder (Google reader)*. Now I use *Google+* and have somewhere between 5,000-6,000 followers. *Google+* is unfiltered, so I have more control over the posts I choose to share. My posts vary in frequency but I try to share two to three things per week. I still have a following in Iran, even though I live in Turkey."

"In terms of online activism, I share speeches, notes from other activists, insightful comments about civic rights and responsibilities. On *Twitter* I retweet important news about civic developments and other people's views about the state of politics and civil society in Iran. I am a reformist."

Recent activism

Her legal troubles with the state began after she was expelled from the University. "I received a couriered letter from the Ministry of Intelligence, stating that the University had made a complaint about my behaviour. The letter also included one line of vague accusations against me."

"My family is from a religious city in Northern Iran. On one occasion I was summoned into the local police station and held for one night. I was interrogated heavily about my

online activism but was released the following day. Since my town is a very religious city, they rarely keep women in custody for lengthy periods of time. I tried to distance myself from my online profile and gave in to their warnings and advice. I believe the whole experience was meant to intimidate me. During my detention I wasn't physically or emotionally abused, but I was pushed and spoken to rudely."

"My activism evolved, from critiquing issues around education and culture to the treatment of LGBT (Lesbian, Gay, Bi-Sexual and Transgender) communities. I began fighting for the cause of legalising their inclusion in society on my blog [fighting for their human rights]. From there I began working directly with homosexual activists and was eventually introduced to activists from the 2009 Green Movement."

"Things changed after the second or third year [2010 and 2011] of Ahmadinejad's term. I no longer received letters from the Ministry, but phone calls that could not be traced. I noticed a big shift in the legal ways [in which] the government would go about getting activists into the system. They adopted a more opaque and clandestine pattern of activity. They appeared less interested in courts and processes and more in intimidating [people through] telephone interviews that don't leave a trace."

2009 Green Movement

As was the case for many bloggers, the June 2009 post-election protests was the first, or one of the few, opportunities to step away from their computers and rally in the streets of the city with many other protesters. "I eventually joined a street protest one night during the Green Movement uprising. I believe the security forces took films of me while I was demonstrating on the streets. I also joined the Green Movement protests on the 2009 Day of Qods [19 September 2009] and think security forces took video footage of me there as well."

As the government witnessed the growing, perseverant opposition, it started to use more violence in its crackdown. "In Khordad 1389 (June 2010), things became very dangerous for the likes of bloggers and activists like me. I was working very closely with another activist, Mohammad Ali Najafi, a close friend of Green Movement Opposition Leader, Mir Hossein Moussavi. I feared that I would be arrested this time around for my involvement and proximity to the movement so I decided to go underground and leave Iran for a short period of time. I went to Turkey in 2010 legally. I told the border agents that I was exploring university options there and would return shortly. The [Iranian] security forces allowed me to leave."

Interrogation and detention

"Upon my return [to Iran] a few short weeks later, I was interrogated by plain clothes guards at Imam Khomeini airport [in Tehran] and taken into custody. They told me that they knew about my role in the protests, that they had film evidence on me, and about my activism online. I began crying […], again trying to distance myself from the movement, other figures and my activism. By this point, my online activism had

decreased significantly, since I was already fearful about the consequences prior to leaving. […]. My passport was taken away and I was strictly instructed to close down my blog and not stay in Tehran for more than seven days at a time. I could only travel through Tehran, and had to spend my time in my town with my family. […]. They eventually let me go."

"My family distanced themselves from me, as they were unsupportive of my activities and views. From 2010 onwards, I remained underground, abiding by the restrictions to ensure I would get my passport back. After one year of persisting, I eventually got my passport back and left Iran for good to live in Turkey in 2012."

Life as a refugee – Supporting activists inside Iran from Abroad

Sara is currently a refugee in Turkey. "I have not been back to Iran since [that time]. I have restarted my activism from here but focus more on supporting initiatives ... inside Iran - giving them support from the outside. One thing I was involved in was the *Salam* campaign, which tries to give hope to activists back home, by removing the gap between people there and [the] outside diaspora. I've also been involved in a number of anti-sanctions campaigns, trying to increase the trending potential of certain online posts from inside Iran on *Twitter*."

"I believe that since Sattar Beheshti's arrest and death in custody [November 2012], most activists are incredibly paranoid about being identified by [the] security forces. Most people are also very paranoid and confused about how to effectively bypass the filtering and blocking technologies used by the state; people don't know which VPNs are safe, and which aren't. The atmosphere is very tense and this has slowed down the pace of activism inside Iran. Most people are no longer using their real names and are moving to using pseudonyms which negatively impacts the credibility of posts and broad activism efforts."

"I believe the state is learning how to streamline repression tactics, which is causing many activists to go underground. **People are scared, and the online space, which was once a sanctuary, is turning into a hunting ground**."

Maral (pseudonym)

Background

Maral is aged between 20 and 39 and has been an activist since 2009 (1388). Like many others, she became involved in activism a few (in Maral's case, six) months after the fraudulent presidential elections. She began with a public *Twitter* account, sharing articles and viewpoints on freedom of speech and dissent against the regime. She mostly retweeted news on *Twitter* since she found *Facebook* overly private and *Google+* not very useful.

Recent activism

Maral's activism continued in this form until the Ashura protests in February 2010 (Bahman 1389). "Prior to this, I was on a family trip to Dubai and had taken several pictures of my family without wearing my headscarf (hijab). I had shared some of these photos on my *Twitter* account. Upon returning to Iran after this family trip, I had attended Ayatollah Montazeri's funeral and protest. Someone from a news agency took photos of me at the funeral. On the 9th of Dey, 1389 (30 December 2010), Raja News re-shared the photo of me without a headscarf (hijab) on my family trip to Dubai and put it next to the photo that had been taken of me at Ayatollah Montazeri's funeral and protest, essentially trying to show how disrespectful of cultural and moral norms I was. This was a carefully curated attempt at character assassination. Between seven and nine days after this was published, the photo was re-published by the ultraconservative newspaper, *Keyhan*. After this happened, I became extremely fearful about my future and severely reduced my activism [online and in person]."

Interrogation and abuse

"On the 29th of Bahman 1389 (18 February 2011) at 12 midnight, eight officers – a mix of plain clothes and uniformed officers – came to my parents' house to detain me. They woke up my parents and interrogated me in the house until 4.00 or 5.00 am. They took it in turns to interrogate me, asking me about that family trip we took to Dubai, my activism and contact with 'foreign powers'. Before they left, the security forces confiscated my laptop, mobile phone, identification – including [my] passport – flash drives, hard drives, physical photos and anything else they could get their hands on. They left after several hours of interrogation."

"The day after, I was summoned to the Ministry of Intelligence for further questioning. The questions pursued a similar line of reasoning/logic. On several occasions they accused me of insulting the state, being against the regime (*zede nezam*), and claimed that my online and physical activism was a threat to the stability of the state. When the first round of in-person interrogations ended, they returned everything they had confiscated except for the hard drives (including my photos) and my passport."

"Once I retrieved my things, I began applying for visas to other countries (Canada, US, Australia, etc) so I could leave Iran. I desperately wanted to leave, but when I saw the case they had built against me from the Ministry of Intelligence, I realised they had legally barred me from leaving the country. After this, my case was ... passed from the Ministry of Intelligence to the Islamic Revolutionary Court at the notorious Evin prison."

"In Evin I was interrogated and asked 'Why are you planning to leave the country? Why are you insulting the state, promoting subversive satirical poetry on your *Twitter* account?' They would not hear me out, and forwarded my case to the Islamic Revolutionary Court for a verdict. This happened in the month of Mordad (July 2011). I waited until Aban of that year (October 2011) but was it was never, never clear to me why I was barred from leaving the country. No one ever provided me with an [official] explanation."

"Eventually I was told by the Islamic Revolutionary Court that they had lost my file. I followed up in person and discovered that it had been sent back to Evin prison for further research. I think that either there was not enough evidence against me to try me in court or the verdict was negative […]. When I went to retrieve my file and find out if the ban had been removed, they wouldn't let me enter the court inside Evin prison."

"Several months later, security officials from the Ministry of Intelligence sent me an official arrest warrant (*hokme bazdasht*) for my activism. I contacted the Ministry and was advised not to continue my activism, and [to] reduce everything to zero. They told me that 'until we know for sure you won't do anything, we will hold on to your passport. We need to see that you won't pursue activism and won't encourage others to do similar things. We'll return the passport after six months of good behaviour'."

"This process has so far lasted over 22 months, and I still haven't got my passport back. I think they are tracking my movements, particularly my online accounts, to see if I've done well and kept my promises. Some of my friends were pulled in for interrogation to give a better sense of what my real movements were like (both public and underground)."

Another tactic commonly used by the officials is summoning activists back and forth for interrogation. "In total, over the past three years, I've been summoned to the Ministry of Intelligence on eight different occasions. Each interrogation/questioning session lasts anywhere between two and four hours. Every interrogation session includes two officers, one young and one older man. They are all held face-to-face. They begin by telling me that their duty is to monitor, control and neutralise any threats to the stability of the political environment."

"After the in-person interrogations stopped, they began following up on the phone. Initially, someone with a rude tone would call me and make threats, saying what they would do terrible things to me if I continued my activism. On that first occasion, the officer spoke very rudely to me and I responded in a similar tone."

Legal Case

"The legal reasons they used in order to build a case against me included:

- Protesting and dissenting against the state (*etteraaz*).
- Cyber-activism protesting against the elections (substantiated by using my online posts)
- *Parvadehye akhlaghi* - moral indignity and cultural/behavioural issues – substantiated by using my posts and photos, especially the one without a hijab in Dubai."

"I believe that my case was not escalated further because I showed incredible restraint when dealing with the security officials and did not upset them and speak rudely when they engaged with me (except for that one occasion on the phone); I was mostly compliant and obedient because I felt I had very little to hide. […]."

"It's totally random who you get and how they treat you. Since that very first phone call, all follow-up calls have not used threats and insults, but a very professional but stern tone. They have a lot of power and have been very systematic in their approach."

"I have over 7,000 *Twitter* followers in Iran, and a lot of friends outside of the country. I know I have influence. Maybe they thought my name would go viral if they did anything extreme to me? Maybe they didn't want things to blow out of proportion? Who knows? Time will tell if I ever get my passport back."

Mehdi Saharkhiz

In an interview with Mehdi Saharkhiz, Mehdi spoke on behalf of his father, Isa Saharkhiz[149], a prominent Iranian investigative journalist. Isa Saharkhiz was also the Head of the Press Department of the Ministry of Culture and Islamic Guidance during Mohammad Khatami's administration.

Background, Arrest and Denial of Medical Treatment, and Cruel, Inhuman and Degrading Treatment

"My father Isa was tracked down by state security forces in 2009, following the Green Movement uprisings, using triangulation technology provided by *Nokia-Siemens*. Apparently this technology was sold to Iran with the intention of helping them meet their security needs."

"My father Isa was arrested with a general warrant, instead of a specific warrant with a series of well-defined allegations. Since his incarceration, he has spent countless days in solitary confinement and has been transferred to and from two different prison facilities, Tehran and Karaj. **During his incarceration, his physical condition has deteriorated significantly.** He has visited the prison hospital on many occasions. On one occasion, after his conditioned worsened, he was taken to a hospital outside of the prison to be examined by third party doctors. **Doctors there strongly recommended that Isa should not return to prison.** They provided official testimony to the authorities to support these medical claims. They recommended he should be released [because of] his health. However, officials in charge of Isa's case told his lawyers that such testimony had apparently been 'lost' and that Isa must return to prison. During the last few months, Isa has continued to stay in hospital with three guards always by his side."

"His physical deterioration stems from a series of compounding medical issues. First, he suffers from high levels of stress. Second, his stress has led to kidney failure (he has only 30% use of his kidneys). Third, he has unstable blood pressure and chronic heart disease, which is heavily stress-related. He is currently in a critical condition. Doctors recommended he follow a special diet to help mitigate the health risks of these compounding medical problems but the guards and officials there provide nothing of the sort to my father."

ARTICLE 19 believes that this denial of adequate medical treatment and care and Isa's current conditions of detention amount to cruel, inhuman and degrading treatment.

Unfair trial

"In terms of legal allegations, two cases were brought... against him during his incarceration, […] including disrespecting the government and the Supreme Leader, and planning to overthrow the Islamic Republic. For these two charges, he received a joint sentence of four years in jail. The authorities substantiated these claims by using his writings and journalism as evidence against him. He has been unable to defend himself against these claims and even sat through the mock trials of 2011, forced

to confess under duress to these allegations. In my father's own words, 'you have freedom of speech in Iran but you don't have freedom after your speech'."

Nokia-Seimens' involvement

"My father and I brought a legal case against *Nokia-Siemens* in the United States for their involvement in my father's arrest." Moawad & Herischi, a Maryland law firm, submitted an official complaint to a federal court in the US state of Virginia, alleging that Saharkhiz was tortured and mistreated because of the government's monitoring of his conversations. The *Nokia-Seimens* Network had confirmed to The Guardian that it sold the Iranian regime a monitoring system called Lawful Interception Management System (LIMS) in 2008.[150]

"Subsequent to this, the issue gained international attention. It was the first legal action against the company for its detrimental involvement in helping quash the democratic uprising in Iran. The case was eventually dismissed [for the] reasons that my father needed to be present to testify and provide additional details. However, once enough pressure built about the company's role in providing technology that had enabled the Iranian government to crack down on popular dissent and on its own people, the company pulled out of Iran and ended their commercial relationship with the regime."

Section III - Analysis and Recommendations

Analysis and conclusions

Until now, past policies and positions indicate that Iranian leaders choose political control over the benefits of a more open society supported by open access to the internet.

Based on our research, ARTICLE 19 believes that citizens, journalists and activists may continue to be identified and targeted on the pretext that they have committed cybercrimes. Insights from our research reveal that digital activists who exhibit some of the following characteristics are extremely vulnerable to state-orchestrated harassment, including unlawful arrest, torture and other ill-treatment and unfair trials:

- A high level of online activity, including a large number of posts or re-shares of opinions, in multiple online fora;
- A strong online following: either popularity or authority/legitimacy on a particular subject (or both);
- Multiplier potential, determined by the number of 'followers' garnered and by how the activist's endorsement of ideas or issues might help spread dissenting views further to other like-minded online communities and, potentially, offline to the public at large.

Our research also reveals that given the overly broad and ambiguous nature of the Computer Crimes Law and of the term "cybercrimes", broadly defined in the Iranian legal framework, victims of state-orchestrated harassment or arrest did not always have a clear idea of what they were being charged or threatened with legally and what laws they had broken. ARTICLE 19's research shows that there has not been a noticeable shift away from using the existing Iranian Penal Code and towards using the Computer Crimes Law to suppress digital activism.

ARTICLE 19 believes that the Iranian government does not need the Computer Crimes Law to repress activists and could choose to continue to rely on the traditional existing legal apparatus, particularly the Penal Code, to intimidate and punish digital activists for expressing their views publicly.

ARTICLE 19 also believes that the Computer Crimes Law is a critical legal tool contributing to a larger orchestrated campaign aimed at diminishing and effectively minimising or even eliminating the freedoms provided in online fora to discuss and challenge critically the Iranian government on its control of society and politics.

Recommendations

Recommendations to the Islamic Republic of Iran

The Computer Crimes Law and the Iranian regime's overall approach to censoring freedom of expression over the internet are contrary to international norms, human rights laws and interpretive standards in multiple ways. ARTICLE 19 believes that restoring the right to freedom of expression in Iran requires wholesale reform to redress the conceptual failure signified by the Computer Crimes Law and other legislation. The protection and promotion of freedom of expression must be reasserted as the norm and limitations on free expression as the exception.

ARTICLE 19 hopes that the most recent steps taken by President Rouhani will pave the way for more progressive policies enshrining, not demonising, freedom of expression and human rights, and will lead to more constructive relationships with all stakeholders interested in advancing human rights globally.

Therefore, ARTICLE 19 recommends the following to the executive body of the Islamic Republic of Iran:

- The protection and promotion of freedom of expression must be reasserted as the norm, and limitations on free expression as the exception.
- The practice of arbitrary arrests and the intimidation of civil society actors should be stopped immediately.
- All individuals who have been deprived of their liberty and imprisoned or detained for peacefully exercising their rights to free expression, association, and assembly - in particular bloggers, software developers and others arrested on the pretext of cybercrimes - should be immediately released.
- State-sponsored censorship activities, including systematic filtering of internet content, should be immediately abolished.
- Investment in information technology infrastructure, including increasing the speed and connectivity of the internet, should take place to help Iran catch up with the rest of the developed world and help Iranians engage in commercial development activities for the benefit of the country (trade, exchange of services and international commerce).
- ARTICLE 19 recommends the following to the legislative and the judiciary bodies of the Islamic Republic of Iran:
  - The repeal of the Computer Crimes Law in its entirety, and comprehensive legal reform to amend any legislation that restricts the legitimate exercise of freedom of expression.
  - The immediate repeal of any law imposing liability on internet Service Providers for the content of expression that passes through their systems.

Recommendations to Concerned Governments, Including EU Member States, Canada, and Australia

ARTICLE 19 encourages concerned governments, including EU Member states, to exert pressure on Western companies, such as *Gamma International* and *Trovicor*, which make software available to repressive regimes. This includes software that allows users to infect computer and phone devices and intercept e-mails, social media messages and *Skype* calls. These companies should be pressed to stop pursuing questionable business practices that may be in breach of the Organisation for Economic Co-Operation and Development (OECD) guidelines for "responsible business conduct". We also urge these governments to install national export controls that place restrictions on equipment being used to quash dissent.[151]

ARTICLE 19 believes that EU Member States, Canada and Australia should tighten their export legislation for highly sensitive equipment that can be adapted for dual use, that is, both civilian and military purposes.[152] EU Member States, Canada, and Australia – as well as companies in these countries - are discrediting their own values by developing lawful interception technology and exporting it to governments with poor human rights records and questionable intentions, including the Islamic Republic of Iran.[153] Tighter export controls would help reconcile this inconsistency between values and practices.

Finally, ARTICLE 19 encourages concerned governments, including EU Member states, Canada and Australia, to consider admitting more Iranian asylum-seekers outside the UNHCR refugee process, especially those who have left Iran because of persecution in response to their civil society or political activities.

Recommendations to the United States of America

ARTICLE 19 expresses cautious optimism about Iran's more moderate tone under President Rouhani. ARTICLE 19 applauds the difficult but important attempts made by President Obama and President Rouhani to engage in dialogue without intermediaries for the first time in over three decades. We also congratulate US Secretary of State John Kerry and Iranian Foreign Minister Mohammad Javad Zarif on their first private meeting without deputies or note-takers, and applaud Iran's gesture of goodwill as represented by the release of more than 80 prisoners, including a dozen political prisoners (particularly the prominent human rights lawyer, Nasrin Sotoudeh) ahead of their visit to the United Nations General Assembly. These are big steps forward for both countries.

ARTICLE 19 encourages the Iranian leadership to continue demonstrating a greater degree of flexibility, reflected not only in a shift in the country's diplomatic policy, but also in its domestic approach towards civil society actors and human rights defenders. The possibility of improved relations between the United States and Iran, including a resolution of the nuclear impasse in exchange for a new international and regional standing, should not come at the expense of human rights or freedom of expression and information, nor should it give Iran a renewed mandate to suppress civil society actors at home.

ARTICLE 19 strongly encourages both sides not to pursue a "lowest common denominator" policy that neglects and sidelines the protection and promotion of human rights. A strong civil society is the cornerstone that ensures long-term accountability and democratic progress in Iran. The nuclear issue is a crucial impediment to improved relations between both countries, but resolving it should only be regarded as a first step towards better relations; the promotion and protection of human rights must be at the core of the agenda of "deeper relations".

Recommendations to Governments with Constructive Diplomatic Relations with the Islamic Republic of Iran (particularly Brazil, Russia, India, China and South Africa)

ARTICLE 19 strongly encourages governments with constructive diplomatic relations with the Islamic Republic of Iran to leverage their political, social and diplomatic capital and advise Iranian leaders to show restraint and a more enlightened approach in the way in which they balance the promotion of civil society, human rights and freedom of expression against "national security". The current prioritisation of political control over the benefits of a more open society is a self-defeating position. A more open posture and more progressive policies toward the internet, and by extension toward human rights and freedom of expression and information, will greatly benefit the country, and have positive consequences, ameliorating Iran's international reputation and regional standing.

A strong civil society, supported by laws enshrining human rights and freedom of expression, will help, not hinder, Iran's ability to deal with the challenges of modernisation and development. Governments concerned about Iran's national interests would do well to reiterate these insights and values to the leadership in Iran.

Acknowledgements and partners

ARTICLE 19 wishes to thank the interviewees and expert contributors who assisted in the preparation of this report. In particular, ARTICLE 19 would like to acknowledge the courage of the activists who provided witness testimonies, and the risks they bore in order that their accounts would bring this report to life. We are deeply indebted to them as well as to the expert contributors who provided valuable time and resources to this project.

The views and opinions set out in this report, including those of the expert contributors, are endorsed by ARTICLE 19. They do not, however, reflect the views and opinions of any organisations associated with the expert contributors.

About ARTICLE 19

ARTICLE 19 was founded in 1987. It envisages a world where people are free to speak their opinions, participate in decision-making and make informed choices about their lives. ARTICLE 19 campaigns with people around the world for the right to exercise these aspirations and rights. It believes freedom of expression and freedom of information are fundamental human rights that are central to freedom and democracy. People everywhere must be able to exercise their right to freedom of expression and their right to information. Without these rights, democracy, good governance and development cannot happen. With offices in Bangladesh, Brazil, Kenya, Mexico, Tunisia, Senegal and the UK, and in collaboration with 90 partners worldwide, we:

- Work on behalf of freedom of expression wherever it is threatened. This work includes monitoring, research, publishing, advocacy, campaigning, standards setting and litigation.
- Advise on the development of legislation to protect freedom of expression and freedom of information in countries emerging from conflict, war and genocide.
- Campaign to safeguard pluralism, independence and diversity of views in the media.
- Champion freedom of expression, including freedom of information, as a fundamental human right that is essential for the protection of other rights.
- Advocate for freedom of information legislation to ensure transparency and to strengthen citizens' participation.

About ARTICLE 19's Iran Programme

In 2008, ARTICLE 19 designed and implemented a limited programme aimed at combating censorship in Iran. The June 2009 elections brought about big changes in the field of freedom of expression and information in Iran, and the original ARTICLE 19 project grew organically into a two-year initiative focused on publicising daily violations of people's rights to free speech and information. This project maintained a valuable flow of information to and from Iran, and it became evident that it was a vital end in itself at a time when little else could be done to combat censorship in Iran.

The momentum generated by the recent movements for democracy in the Middle East and in North Africa provide a small window of opportunity to draw on these experiences in order to influence the Iranian regime. Naturally, there are significant obstacles to improving freedom of expression and access to information in Iran, and ARTICLE 19 takes a long-term approach to sustaining civil society and human rights defenders to ensure that their aspirations for full enjoyment of human rights are not suppressed.

ARTICLE 19 hopes that the most recent steps taken by President Rouhani will pave the way for more progressive policies, policies that enshrine freedom of speech and human rights rather than demonising them, and that this will lead to a more constructive relationship with all of the stakeholders interested in advancing human rights globally.

Appendix A – List of people Imprisoned in Iran under the Computer Crimes Law

1. Saeed Malekpour – Saeed Malekpour is an Iranian-Canadian sentenced to death in Iran for allegedly designing and moderating pornographic websites. Malekpour developed an internet photo-sharing tool that his supporters assert was used without his knowledge for pornographic purposes. Prior to his arrest in Iran in 2008, Malekpour had been living and working in Canada as a permanent resident. The Canadian government and *Amnesty International* have called for his immediate release. In December 2012, Malekpour's lawyer announced that the death sentence had been suspended because Malekpour had expressed remorse for his behaviour.[154]

2. Hossein Ronaghi Maleki – Hossein Ronaghi-Maleki is an Iranian blogger and political dissident who was imprisoned in 2009 for his role in the post-June 2009 election protests in Iran. He also wrote under the pen name 'Babak Khorramdin'.[155]

3. Vahid Asghari – Vahid Asghari is an Iranian blogger and information technology student who was sentenced to death by the Islamic Republic's government in 2012. While studying in India, Asghari was arrested in 2008 at Tehran's Imam Khomeini International Airport and has been held in custody ever since. He was sentenced by Abdolqassem Salavati, president of the 15th Chamber of the Revolutionary Court for allegedly hosting a pornography network.[156]

4. Kaveh Taheri – Kaveh Taheri, a blogger from Shiraz, has been detained without trial on charges relating to writing a blog since Sept 23, 2012.[157]

5. Poorya Farazmand – Poorya Farazmand writes the blog *Azadi Baraye Hamegan* (freedom for all) and served on the editorial board of *Mosht* (fist), a banned student newspaper. Student witnesses said Farazmand never wrote anything pointing to foreign associations and that he only wrote about internal politics in Iran.[158]

6. Ahmadreza Najdad – Dissident writer and blogger Ahmadreza Najdad was arrested while leaving Iran.[159]

7. Arash Honarvar Shojai – Arash Honarvar Shojai, a dissident blogger and cleric.[160]

8. Mojtaba Danesh Talab – Mojtaba Danesh Talab, a conservative blogger and cleric who was tough on demonstrators in 2009, went to prison because of a single criticism of a message from the Supreme Leader.[161]

9. Sakhi Rigi – Sakhi Rigi, a blogger and a member of Mir Hossein Mousavi's campaign staff, has been sentenced to twenty years in prison by the Revolutionary Court in Zahedan [Sistan and Baluchistan Province].[162]

10. Badri Safyari – Badri Safyari is a student at Kavar Fars University, and a writer and blogger for the blog called *Sufi*.[163]

11. Mohammadreza Pourshajari – Pourshajari (Siamak Mehr) is an imprisoned blogger and political activist.[164]

12. Fereydon Seyedi Rad – According to the Committee to Protect Journalists, Seyedi Rad was arrested in March 2011 and later sentenced to one year in prison for "propaganda against the regime". According to a different source, Seyedi Rad received a three-year sentence.[165]

13. Mohammad Davari – Mohammad Davari (born c. 1974) is an Iranian journalist. After he documented abuses of prisoners at Kahrizak Detention Centre he was sentenced to five years in prison by the Iranian government, attracting international protests. As a student, Davari volunteered to fight in the Iran-Iraq War, in which he was wounded in the eye and leg. He went on to become a journalist, acting as editor-in-chief for *Sahamnews*, the news website of opposition presidential candidate, Mehdi Karroubi.[166]

14. Khosrow Kordpour – Intelligence forces have arrested Khosrow Kordpour, editor-in-chief of *Mukrian* News Agency, an outlet that covers the arrests and prosecutions of Kurdish activists and documents human rights violations. The US government-funded *Radio Farda* reported that the authorities had a warrant out for his arrest and that they had searched his home, but did not offer further details.[167]

15. Massoud Kordpour – Khosrow Kordpour's brother, freelance journalist Massoud Kordpour, was arrested at the Boukan Intelligence Office the day following his brother's arrest (see above), when he went to enquire about the imprisonment of his brother. Authorities later searched his home and confiscated personal items. Massoud Kordpour had frequently covered human rights in Kurdistan province, and his work has been published by *RFI Persian*, *Deutsche Welle Persian*, *Voice of America Persian*, and on local and Kurdish-language websites.[168]

16. Shahram Golshani – The webmaster of *Mesghal*. This website is regarded as one of the most reliable and significant points of reference for exchange rates in Iran.[169]

17. Mehdi Dowlati Darabad – Software engineer and web developer.[170]

18. Hamed Ataei – Hamed Ataei, the editor-in-chief of *Ayna-news*.[171]

19. Mohammad Seddigh Kabodvand – Mohammad Sadiq Kaboudvand is an Iranian Kurdish activist and journalist. He was the editor of *Payam-e Mardom*. He is also the founder of the *Kurdistan Human Rights Organisation* (*Rêxistina Mafê Mirovan li Kurdistanê* in Kurdish). Founded in 2005, the organisation is a politically and religiously independent body. It has offices in Tehran and in Kurdistan province.[172]

20. Payman Samadi – Arrested and sent to Ward 209 at Evin Prison. Released on bail. Sentenced to four years, reduced by the Appeals Court to a one-year sentence plus a three-year suspended sentence. He began serving his sentence in March 2013.[173]

21. Nasour Naghipour – Thirty-year-old Nasour Naghipour, a university student majoring in Information Technology and a researcher in philosophy and political ideologies, was managing a website archiving articles written in Persian in the field of Humanities.[174]

22. Mohammad Nasiri – Mohammad (Kourosh) Nasiri, an internet activist who was detained for being a member of the Imam Naghi *Facebook* page, has been handed a 10.5-year prison sentence. Mohammad Nasiri was detained at his home on 23 May 2012 and transferred to Ward 209 of Evin prison, which is under the jurisdiction of the IRGC Intelligence unit. He spent 30 days in solitary confinement in wards 209 and 240 of Evin prison.[175]

23. Mehdi Alizadeh Fakhrabad – 31-year-old Mehdi Alizadeh Fakhrabad is from the city of Mashhad and is married. He was first arrested in the summer of 2008 in a case known as the "Deceptive Project" (obscenity-related). Alizadeh was incarcerated in Ward 2-A of Evin prison for nine months before being released on a bail of 100,000,000 Tomans (approximately $41,000). He was re-arrested in March of 2011 and is currently in Ward 350 of Evin prison.[176]

24. Shaygan Esfandiari (Pseudonym*) – 'Shaygan Esfandiari' is an Iranian Blogger. He lives in Bandar Abbas and was arrested there. His current status is unclear – we cannot find any sites corroborating his arrest other than the above.[177]

25. Behnam Ebrahimzadeh – Behnam Ebrahimzadeh (Asad), a workers' and children's rights activist, is in Evin prison. His twelve-year-old son, Nima Ebrahimzadeh, was diagnosed with cancer and is in hospital. Behnam was arrested for participating in May Day in 2009 and was later released. Thirteen months later in June 2010, he was arrested in Laleh Park in Tehran and severely beaten. Several of his ribs were broken and he was taken to the notorious Ward 209 of Evin prison. He suffered physical and psychological torture for four months.[178]

26. Omid Dehdarzadeh – Omid Dehdarzadeh, a political activist, was arrested by the Iranian regime's Cyber Police. He is a member of a Pan-Iranian group.[179]

27. Hasan Sisakhti – Hasan Sisakhti, a 22-year-old from Shiraz, is a programmer and cyber-activist. In 2009, he was arrested in Shiraz under the Mozellin plan. He was tortured and placed in the solitary confinement of the IRGC for a year. He was sentenced to death on 23 July 2011 by the 15th Branch of the Revolutionary Court but his sentence was later reduced to life imprisonment.[180]

End notes

1 http://www.article19.org/data/files/medialibrary/2921/12-01-30-FINAL-iran-WEB[4].pdf

2 http://www.bbc.co.uk/news/world-middle-east-14542234

3 Ibid.

4 Ibid.

5 http://iranprimer.usip.org/resource/new-political-tools

6 http://www.bbc.co.uk/news/world-middle-east-14542234

7 http://www.222ministries.org/iran/iran-today/internet-in-iran/

8 http://www.humanrightsfirst.org/our-work/business-and-human-rights/internet-freedom-and-privacy/

9 http://www.222ministries.org/iran/iran-today/internet-in-iran/

10 http://iranprimer.usip.org/resource/new-political-tools

11 Ibid.

12 http://www.freedomhouse.org/report/freedom-net/2012/iran

13 Ibid.

14 Ibid.

15 *Arseh Sevom*, "Attack on Civil Society in Iran", 2010, http://www.scribd.com/doc/38063573/Attack-on-Civil-Society-in-Iran

16 Ibid.

17 Ibid.

18 Ibid.

19 Ibid.

20 *Arseh Sevom*, "Attack on Civil Society in Iran", 2010, http://www.scribd.com/doc/38063573/Attack-on-Civil-Society-in-Iran

21 Ibid.

22 Ibid.

23 Ibid.

24 Ibid.

25 Ibid.

26 Ibid.

27 Ibid.

28 *Reporters without Borders*, Enemies of the Internet, Iran – http://en.rsf.org/internet-enemie-iran,39777.html & http://surveillance.rsf.org/en/iran/

29 Ibid.

30 *Arseh Sevom*, "Attack on Civil Society in Iran", 2010, http://www.scribd.com/doc/38063573/Attack-on-Civil-Society-in-Iran

31 Iranian Internet Infrastructure and Policy Report, Jan - Feb 2013 – http://smallmedia.org.uk/sites/default/files/reports/IIIP02.pdf

32 http://www.222ministries.org/iran/iran-today/Internet-in-iran/

33 Information Policy Blog & International Business Law Services, Kelly O'Connell, IBLS Editorial Department I http://www.i-policy.org/2009/12/iranian-Internet-law.html & http://www.ibls.com/internet_law_news_portal_view.aspx?s=articles&id=EB50E2B3-69E9-47DB-8CE7-FFD9A259595D

34 http://www.222ministries.org/iran/iran-today/internet-in-iran/

35 *Reporters without Borders*, Enemies of the Internet, Iran – http://en.rsf.org/internet-enemie-iran,39777.html & http://surveillance.rsf.org/en/iran/

36 Ibid.

37 *Reporters without Borders*, Enemies of the Internet, Iran – http://en.rsf.org/internet-enemie-iran,39777.html & http://surveillance.rsf.org/en/iran/ and: Information Policy Blog & International Business Law Services, Kelly O'Connell, IBLS Editorial Department I http://www.i-policy.org/2009/12/iranian-internet-law.html & http://www.ibls.com/internet_law_news_portal_view.aspx?s=articles&id=EB50E2B3-69E9-47DB-8CE7-FFD9A259595D

38 http://iranprimer.usip.org/resource/new-political-tools

39 Information Policy Blog & International Business Law Services, Kelly O'Connell, IBLS Editorial Department I http://www.i-policy.org/2009/12/iranian-internet-law.html & http://www.ibls.com/internet_law_news_portal_view.aspx?s=articles&id=EB50E2B3-69E9-47DB-8CE7-FFD9A259595D

40 Ibid.

41 Ibid.

42 Ibid.

43 http://iranprimer.usip.org/resource/new-political-tools

[44] http://isna.ir/fa/news/91112213010/-تع-رس-ی-دن-ک-دراد-ن-ی-طبر-دن-اب-ی-ان-هپ-هب-تن-رت-ن-ی-ا

[45] Iranian Internet Infrastructure and Policy Report, Jan - Feb 2013 – http://smallmedia.org.uk/sites/default/files/reports/IIIP02.pdf

[46] Ibid.

[47] "The Internet manager of Ministry of Culture: Iranian users should use Iranian social networks", Gerdab, July 27, 2011, http://tinyurl.com/qjsooqh

[48] "Is being a member of social networks a crime?" Jahan News, November 17, 2011, http://www.jahannews.com/vdcdkk0fxyt0no6.2a2y.html.

[49] Amrutha Gayathri, "Muslim Cleric Says Facebook is Un-Islamic, Membership Sin", International Business Times, January 11, 2012, http://www.ibtimes.com/articles/280026/20120111/muslim-cleric-facebook-un-islamic-membership-sin.htm.

[50] Iranian Internet Infrastructure and Policy Report, Jan - Feb 2013 – http://smallmedia.org.uk/sites/default/files/reports/IIIP02.pdf & http://storify.com/smallmedia/is-iran-capable-of-developing-the-software-it-woul

[51] Iranian Internet Infrastructure and Policy Report, Jan - Feb 2013 – http://smallmedia.org.uk/sites/default/files/reports/IIIP02.pdf

[52] Ibid.

[53] Ibid.

[54] Ibid.

[55] Ibid.

[56] http://iranprimer.usip.org/resource/new-political-tools

[57] Ibid.

[58] http://www.freedomhouse.org/report/freedom-world/2013/iran

[59] http://www.bbc.co.uk/news/world-middle-east-14542234

[60] http://www.freedomhouse.org/report/freedom-net/2012/iran & http://iranprimer.usip.org/resource/new-political-tools

[61] http://www.freedomhouse.org/report/freedom-net/2012/iran

[62] Ibid.

[63] http://www.freedomhouse.org/report/freedom-net/2012/iran

[64] Saeed Malekpour, interviewed by Olivia Ward, "Saeed Malekpour: A Canadian on Iran's death row", The Star, 18 February 2012, http://www.thestar.com/news/world/article/1132483--a-canadian-on-iran-s-death-row; *Amnesty International*, "Iran must halt execution of web programmer", 19 January 2012, http://www.amnesty.org/en/news/iran-must-halt-execution-web-programmer-2012-01-19.

[65] Danny O'Brien, "Online publishers, developers sentenced to death in Iran", *Committee to Protect Journalists*, 20 January 2012, http://cpj.org/internet/2012/01/online-publishers-and-developers-sentenced-to-deat.php.

[66] "Iranian blogger on hunger strike close to death, warn fellow prisoners", *The Guardian*, 6 June 2012, http://www.guardian.co.uk/world/iran-blog/2012/jun/06/iran-blogger-hossein-ronaghi-maleki-hunger-strike.

[67] "Iranian blogger loses appeal against 19-year sentence", *The Guardian*, 9 June 2011, http://www.guardian.co.uk/world/2011/jun/09/jailed-iran-blogger-loses-ap....

[68] "8 people imprisoned in Iran for holding discussion on Islam in Internet", *APA*, 21 January 2012, http://en.apa.az/news.php?id=164113.; "Iran sentences 8 people to prison for expressing religious beliefs in Internet social network", *HARDIP*, 20 January 2012, http://hrdip.com/iran-sentences-8-people-to-prison-for-expressing-religious-beliefs-in-Internet-social-network/.

[69] Rick Gladstone and Artin Afkhami, "Pattern of Intimidation Is Seen in Arrests of Iranian Journalists and Bloggers", *The New York Times*, 25 January 2012, http://www.nytimes.com/2012/01/26/world/middleeast/iran-steps-up-arrests-of-journalists-and-bloggers.html?_r=1&scp=1&sq=afkhami&st=cse.

[70] http://www.freedomhouse.org/report/freedom-world/2013/iran

[71] *Arseh Sevom*, "Attack on Civil Society in Iran", 2010, http://www.arsehsevom.net/site/wpcontent/uploads/2010/06/Arseh-Sevom_Attacks-on Civil-Society.pdf

[72] Information Policy Blog & International Business Law Services, Kelly O'Connell, IBLS Editorial Department | http://www.i-policy.org/2009/12/iranian-internet-law.html & http://www.ibls.com/internet_law_news_portal_view.aspx?s=articles&id=EB50E2B3-69E9-47DB-8CE7-FFD9A259595D

[73] http://www.globalsecurity.org/military/world/iran/scrc.htm

[74] Information Policy Blog & International Business Law Services, Kelly O'Connell, IBLS Editorial Department | http://www.i-policy.org/2009/12/iranian-internet-law.html & http://www.ibls.com/Internet_law_news_portal_view.aspx?s=articles&id=EB50E2B3-69E9-47DB-8CE7-FFD9A259595D

[75] Ibid.

[76] http://www.freedomhouse.org/report/freedom-net/2012/iran

[77] "12 members of Committee in Charge of Determining Unauthorized Sites", *Weblognews*, 16 December 2009, http://weblognews.ir/1388/09/mediablog/5740/.

[78] http://www.freedomhouse.org/report/freedom-net/2012/iran

[79] Fanavaran, Alireza Shirazi, interviewed by Shabnam Kohanchi, "Filtering killed the indicators of blogosphere", 17 December 2011, http://www.itmen.ir/index.aspx?pid=10324&articleid=3954.

[80] Ibid.

[81] http://www.zawya.com/printstory. cfm?storyid =EIU20081001211715204&l=000000080818

[82] http://www.222ministries.org/iran/iran-today/internet-in-iran/

[83] Ibíd.

[84] http://www.genderit.org/sites/default/upload/A_Report_on_internet_Access_in_Iran_2_.pdf

[85] http://www.theguardian.com/technology/2006/dec/04/news.iran

[86] http://latimesblogs.latimes.com/babylonbeyond/2009/05/iran-ahmadinejad-islam-facebook-social-networking-mousavi-tehran.html

[87] http://www.telegraph.co.uk/news/worldnews/middleeast/iran/5523414/Iran-elections-rival-Mir-Hossein-Mousavi-wont-accept-Mahmoud-Ahmadinejad-victory.html

[88] http://www.scmagazine.com/iran-election-protesters-use-twitter-to-recruit-hackers/article/138545/#

[89] http://www.counterpunch.org/2009/07/02/iran-networked-dissent/

[90] http://www.nytimes.com/2009/06/16/world/middleeast/16media.html?_r=0

[91] http://www.boston.com/business/technology/articles/2009/06/19/activists_utilizing_twitter_web_proxies_to_sidestep_iranian_censorship/

[92] http://www.aljazeera.com/news/middleeast/2009/06/200961317213030395 5.html.

[93] http://www.reuters.com/article/rbssTechMediaTelecomNews/idUSWBT01137420090616

[94] https://blog.twitter.com/2009/and-away

[95] http://www.theguardian.com/politics/2009/jun/19/gordon-brown-internet-foreign-policy

[96] http://vorige.nrc.nl/international/article2280315.ece/Iconic_Iran_video_was_posted_in_the_Netherlands

[97] https://whyweprotest.net/community/threads/msn-news-internet-underground-takes-on-iran.41861/

[98] http://blog.austinheap.com/building-the-stack/

[99] http://www.slate.com/articles/technology/technology/2010/09/the_great_internet_freedom_fraud.html

[100] http://www.economist.com/node/17043440

[101] http://www.bbc.co.uk/news/technology-11298022

[102] http://www.i-policy.org/2009/11/article-19-iran-government-launches-web-crime-unit-.html

[103] http://www.dailymail.co.uk/news/article-1236873/Iranian-Cyber-Army-hackers-Twitter-early-morning-attack.html#ixzz2cEOtYqEq

[104] p.6 http://www.article19.org/data/files/medialibrary/2921/12-01-30-FINAL-iran-WEB[4].pdf

[105] http://www.freedomhouse.org/report/freedom-net/2012/iran#_ftn1

[106] Ibíd.

[107] http://www.presstv.ir/detail/161659.html

[108] http://www.freedomhouse.org/report/freedom-net/2012/iran#_ftn25

[109] http://iranbriefing.net/?p=4411

[110] http://nymag.com/daily/intelligencer/2011/02/iran_tries_internet_censorship.html

[111] http://technet.microsoft.com/en-us/security/advisory/2524375

[112] http://blog.mozilla.org/security/2011/03/22/firefox-blocking-fraudulent-certificates/

[113] http://blogs.comodo.com/it-security/data-security/the-recent-ra-compromise/

[114] http://www.rferl.org/content/iran_announces_new_Internet_restrictions/24442396.html

[115] http://www.theguardian.com/world/2012/jan/05/iran-clamps-down-Internet-use

[116] http://www.washingtonpost.com/blogs/blogpost/post/iran-gets-back-e-mail-access-but-other-sites-remain-blacked-out-ahead-of-protest/2012/02/13/gIQAgxz5AR_blog.html

[117] Ibid

[118] Ibid

[119] http://www.bbc.co.uk/news/world-middle-east-17288785

[120] http://www.google.com/hostednews/afp/article/ALeqM5hQlydlnb790FFK2N0dlsbGLUrhMQ?docId=CNG.d1c3331ce6b077cb9584c9a4521f1f20.a11

[121] http://www.reuters.com/article/2013/03/10/us-iran-Internet-idUSBRE9290CV20130310

[122] http://storify.com/smallmedia/has-iran-finally-launched-the-halal-net

[123] http://www.theguardian.com/world/2013/jul/02/iran-president-hassan-rouhani-progressive-views?guni=Article:in%20body%20link

[124] Dr Ahmed Shaheed was appointed as the Special Rapporteur on the situation of human rights in the Islamic Republic of Iran in July 2011 by the United Nations Human Rights Council. Dr Shaheed is currently a visiting professor at Essex University in Colchester, England, as well as a visiting professor at the City University of New York in the United States. He has twice held the Office of Minister of Foreign Affairs for the Republic of Maldives, from 2005-2007 and from 2008-2010. He led the country's efforts to sign and ratify seven international human rights conventions and to implement them in law and practice.

[125] A/HRC/17/27; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue; 2011 http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

[126] A/67/369; Situation of human rights in the Islamic Republic of Iran, 2012; paragraphs 14-15

[127] Ibid.

[128] Collin Anderson is a Washington DC-based researcher documenting electronic surveillance and internet censorship. He has also been involved in identifying the international flow of surveillance equipment and exploring alternative means of communications that bypass normal channels of state control. His involvement in issues of freedom of expression has included advocating for the availability and legality of online communications services to people living under sanctions restrictions, as well as exploring the ramifications of export regulations to democratisation movements.

[129] http://english2.farsnews.com/newstext.php?nn=9203183278

[130] http://tinyurl.com/qbqzosv

[131] http://investigations.nbcnews.com/_news/2012/12/05/15701843-foreign-tech-companies-pitched-real-time-surveillance-gear-to-iran?lite

[132] http://m.npr.org/news/Technology/204535262?start=5

[133] http://www.presstv.com/detail/2012/11/13/272003/iranian-blogger-died-of-cardiac-arrest/ http://articles.washingtonpost.com/2013-01-30/world/36631347_1_journalists-mehr-news-agency-news-media

[134] http://storify.com/smallmedia/a-new-era-for-iran-s-conservative-bloggers-filteri

[135] http://www.edri.org/book/export/html/3165

[136] The moral police

[137] Executive Director of the Iran Human Rights Documentation Centre.

[138] Director at *Arseh Sevom* (@ETori).

[139] Arash Abadpour (http://abadpour.com/) has been a blogger since October 2004, under the pen name 'Arash Kamangir'. His Persian blog *Kamangir* (http://persian.kamangir.net/) is among the twenty most-read blogs in the Persian blogosphere according to various statistics. Arash Abadpour is regularly consulted and interviewed on matters relating to the internet in Iran. He provides commentary regarding the Persian blogosphere and has been involved in a number of research projects about the relationship between Iranian users and the internet.

[140] Iranian Attorney at Law and Human Rights Lawyer, Legal Adviser of the Iran Human Rights Documentation Centre.

[141] Bill of "Intensifying the Punishment of Agitators of Mental Security of the Society".

[142] Mehdi Saharkhiz is an activist and art director living in the United States. He has a large following on the internet and has been a proponent for human rights and freedom of expression in Iran. Most recently, he has been advocating for the release of his father, Isa Saharkhiz, a prominent Iranian investigative journalist.

[143] Interview transcript generously provided by the Iran Human Rights Documentation Centre (IHRDC), which originally carried out the interview on 15 March 2013. The original transcript can be found here – http://www.iranhrdc.org/english/publications/witness-testimony/1000000357-witness-statement-of-foad-sojoodi-farimani.html#.UmkohhAvuRQ

[144] Interview transcript generously provided by the Iran Human Rights Documentation Centre (IHRDC), which originally carried out the interview on 15 March 2013. The views and opinions of the witness expressed herein do not necessarily reflect those of the Iran Human Rights Documentation Centre.

[145] From the witness: "My father was a physician in the Revolutionary Guard and was kidnapped from in front of the door to our home in Orumieh in 1984. His tortured, dead body was later found in a desert. In that time my father's suspicious death was imputed to the Mojadedin-e Khalq organisation or the Komala party by the Iranian authorities."

[146] The Shaheed Moghaddasi court located in Evin prison was established in the winter of 2009 following a mass arrest of those individuals connected to the post-June 2009 presidential election protests. See: http://www.kaleme.com/1388/12/04/klm-12165/

[147] "45 days that Foad Sojoodi Farimani, imprisoned student in the Revolutionary Guard ward, is incommunicado" *JARAS*, 2 December 2010, available at: http://www.rahesabz.net/story/26542/

[148] "Summons for Foad Sojoodi Farimani, son of a martyr and a PhD candidate, who was barred from study for his eight year prison sentence", *KALEME*, 16 November 2011, available at: http://www.kaleme.com1390/08/25/klm-80368/

[149] See case sheet provided by Amnesty International: http://www.amnestyusa.org/pdfs/Iran11.pdf

[150] http://www.theguardian.com/world/2010/aug/24/iranian-sues-nokia-siemens-networks

[151] 19 February 2013 - Financial Times article "An attempt to take tools from tyrants"

[152] 19 February 2013 - Financial Times article "An attempt to take tools from tyrants"

[153] "An attempt to take tools from tyrants", http://www.nytimes.com/2013/02/19/world/europe/19iht-letter19.html?_r=0

[154] http://en.wikipedia.org/wiki/Saeed_Malekpour

[155] http://en.wikipedia.org/wiki/Hossein_Ronaghi

[156] http://en.wikipedia.org/wiki/Vahid_Asghari

[157] http://www.iranhrdc.org/persian/permalink/1000000302.html#.UkBci4ZwpuI & http://www.iranhrdc.org/english/news/inside-iran/1000000298-a-message-from-laleh-taheri-about-her-brother-kaveh-taheri-an-imprisoned-blogger-in-iran.html#.Ukyu59LBPAs

[158] http://chrr.biz/spip.php?article20618

[159] http://chrr.biz/spip.php?article21608

[160] http://honarvar.net/ & http://hra-news.org/1389-01-27-05-27-21/15774-1.html

[161] http://theiranproject.com/blog/tag/mojtaba-daneshtalab/ & http://daneshtalab.ir/

[162] http://advocacy.globalvoicesonline.org/2011/06/10/iran-record-breaking-20-year-jail-sentence-for-blogger/

[163] http://www.hra-news.org/00/15137-1.html

[164] http://iranian.com/posts/view/post/18847 & https://hra-news.org/en/tag/mohammad-reza-pour-shajari

[165] http://cpj.org/reports/2013/05/as-election-nears-irans-journalists-are-in-chains.php & https://www.tribunezamaneh.com/archives/12040

[166] http://en.wikipedia.org/wiki/Mohammad_Davari

[167] http://cpj.org/tags/khosrow-kordpour

[168] http://archive.radiozamaneh.com/english/category/write-ups/khosro-and-massoud-kordpour

[169] http://sahamnews.org/1390/11/165722/ & http://iranmediaresearch.org/sites/default/files/research/pdf/1342550221/884/iran_media_program_and_asl19_monthly_media_analysis.pdf

[170] http://hra-news.org/00/16590-1.html

[171] http://news.kodoom.com/en/iran-politics/editor-in-chief-of-aina-news-sentenced/story/1484921/

[172] http://en.wikipedia.org/wiki/Mohammad_Seddigh_Kaboudvand

[173] http://www.kaleme.org/1392/04/29/klm-152271/

[174] http://persianbanoo.wordpress.com/2012/07/11/journalist-and-human-rights-activist-nasour-naghipour-arrested-to-start-serving-a-seven-years-sentence/ & http://www.rahesabz.net/story/30506

[175] http://chrr.biz/spip.php?article21447

[176] http://www.youtube.com/watch?v=ZiT5ymw1cfE & http://alborznews.net/fa/pages/?cid=7397 & http://persianbanoo.wordpress.com/2012/01/28/web-developer-and-humorist-mehdi-alizadeh-has-been-sentenced-to-death/

[177] http://gameron.wordpress.com/

[178] http://ireport.cnn.com/docs/DOC-1010689 & http://hra-news.org/1389-01-27-05-27-21/15941-1.html

[179] http://sahamnews.org/1391/05/234211/ & http://www.kaleme.com/1391/09/06/klm-121712/

[180] http://www.hra-news.org/685/1389-01-27-05-27-21/14828-1.html

DEFENDING FREEDOM
OF EXPRESSION AND INFORMATION

ARTICLE 19 Free Word Centre 60 Farringdon Road London EC1R 3GA
T +44 20 7324 2500 F +44 20 7490 0566
E info@article19.org W www.article19.org Tw @article19org facebook.com/article19org

© ARTICLE 19