Center for Media and Cultural Freedom

Digital Rights, Online Media and Electoral Campaigns

March 2016

A report by:

THE SAMIR KASSIR FOUNDATION

About the project:

This report represents the Samir Kassir Foundation's contribution to the project entitled "Civil Advocacy and Mobilization for Electoral Reform" funded by the European Union under contract No. ENPI/2013/313-615.

The project is implemented by a consortium under the leadership of the Lebanese Association for Democratic Elections and including the Democratic Gathering of Lebanese Women, the Lebanese Physical Handicapped Union, the Lebanese Transparency Association, Maharat Foundation, and the Samir Kassir Foundation.

The contents of this report are the sole responsibility of the Samir Kassir Foundation and can in no way be taken to reflect the views of the European Union.

Table of Contents

Introduction

The success of US President Barack Obama's election campaigns in 2008 and 2012 brought the political power of social media to worldwide attention. Both campaigns made extensive use of social media such as Facebook, Twitter and YouTube to mobilize voters and raise funds.[1] The highly personal nature of social networking sites provided campaign managers with an unprecedented level of access to individual supporters enabling them to send out millions of custom-tailored messages and directly respond to attacks from their competitors. Obama's ultimate success has been considered a watershed moment for big data campaigning that fundamentally changed the way politicians and parties engage with their electorate.[2]

Data mining technologies allow media campaigners to gather and compile vast amounts of information into complex voter profiles and to assess the changing mood and composition of electoral districts in real time. Social media provide just one of many data sources in this emergent culture of 'smart' campaigning. Yet, they are widely regarded as one of the most effective tools for micro-targeted campaigns.

Lebanon is a far cry away from such pervasive infrastructures of voter surveillance. This does not mean social media are marginal or irrelevant. 99 percent of Lebanese citizens are currently communicating on Whatsapp; 95 percent have Facebook accounts; 75 percent watch videos on YouTube; and 39 percent have Twitter accounts.[3] The fact that politicians in Lebanon have not yet fully exploited the potential of social media to communicate with their supporters may therefore be more strongly related to the closed architecture of the political system than a lack of opportunity.

The political stalemate over the election of a new head of state since May 2014 and the postponement of parliamentary elections in June 2013 then November 2014 have taken the power to vote out of the hands of Lebanese citizens. Further contributing to the current political crisis is the lack of consensus over a new electoral law and the redrawing of voting districts. What is at stake in the reform are old inherited structures of influence and power. Any change in the electoral map may have repercussions on the ability to form coalitions and to win the majority of available seats.

The highly personalized nature of political relations in Lebanon has also made parliamentarians less dependent on sophisticated data mining. Information about voters is to a large extent collected through old established, real-life social networks that have long defined the exchange between

1. Marwick, A. (January 9, 2014). *How Your Data is Being Deeply Mined.* New York Review of Books. Available at http://www.nybooks.com/articles/archives/2014/jan/09/how-your-data-are-being-deeply-mined/?pagination=false&printpage=true; Bennett, C. (2013). *The politics of privacy and the privacy of politics: Parties, elections and voter surveillance in Western Democracies.* First Monday. Available at http://firstmonday.org/ojs/index.php/fm/article/view/4789/3730#p4; and Smith, A. (2013). *Digital Politics: PEW Research Findings on Technology and the Campaign 2012.* Pew Research Center. Available at http://www.pewInternet.org/~/media//Files/Presentations/2012/Feb/Social%20Media%20Week%20Feb%202013_v2_PDF.pdf

2. NESTA (May 23, 2014). *Big data and the 2015 UK General Election: digital democracy or digitally divisive?* Available at http://www.nesta.org.uk/blog/big-data-and-2015-uk-general-election-digital-democracy-or-digitally-divisive#sthash.ZvAUvVwb.dpuf

3. TNS (2015). *Arab Social Media Report* presented to the Arab Social Media Influencers Summit. Available at http://www.wpp.com/govtpractice/~/media/wppgov/files/arabsocialmediareport-2015.pdf

politicians and their followers in Lebanon. The lack of institutional support has left citizens largely reliant on individual figures to articulate their demands and grievances. This has incentivized the trading of gifts in exchange for votes and popular appraisal, and invested the relationship between politicians and voters with a degree of dependency that made personal networks and sectarian affiliation the core backbone of political communication on domestic affairs.[4]

The entrenched structure of cronyism and corruption in Lebanon lays out a markedly different trajectory for the use of social media in electoral campaigning. Yet the disquieting parallelism between the manipulative power of favoritism and the more nuanced, deceptive qualities of micro-targeted campaigns can hardly be overlooked. Both fundamentally undermine the capacity of independent and informed decision-making and violate one of the core principles of free and fair democratic vote.

Social media and networking sites introduced a variety of new ways for civil society groups, citizen journalists and bloggers to expand critical oversight and democratic participation in the country. Yet their attempts have so far been hampered by outdated media and electoral laws. As our monitoring of legal cases against social media users in Lebanon shows, voicing critique and exposing wrongdoing or the abuse of power is routinely sanctioned with defamation charges that criminalize innocent tweets or Facebook posts and lead to criminal investigation and even prison sentences. No legal code has so far even remotely addressed the changing nature of journalism and public communication introduced by social media. Long standing ills built into laws against defamation, libel and slander have rather been extended to social media without further consideration of their distinctive function and role within the highly politicized media landscape in Lebanon. Silencing critics through expensive lawsuits for damages to status and reputation has been a long-standing practice among Lebanese politicians.[5] The informal and unfiltered mode of communication on social networking sites is likely to exacerbate this culture of indirect censorship which can severely backfire in future elections to come.

Recognizing the rising number of criminal charges against social media users the Samir Kassir Foundation's SKeyes Center for Media and Cultural Freedom has endeavored to put together a set of recommendations for Lebanese government officials and lawmakers to implement long overdue amendments in the existing media and electoral law and practices. This research is conducted within the framework of the European Union-funded project entitled "Civil Advocacy and Mobilization for Electoral Reform" led by the Lebanese Association for Democratic Elections (LADE).

4. Makdisi S., Kiwan, F. and Marktanner, M. (2010). *Lebanon: The Constrained Democracy and its National Impact* in: Elbadawi I. and Makdisi , S. (Eds.), Democracy in the Arab World, Explaining the Deficit. Available at: http://www.idrc.ca/EN/Resources/Publications/openebooks/491-8/index.html

5. Frangieh, G. (2014, February 27). *Lebanon's Cybercrime Bureau: A License to Censor?* Legal Agenda. Available at http://english.legal-agenda.com/article.php?id=590&lang=en#.Uzh3O_mSwbP; Zayadin, H. (2014). *Lebanese government moves to control expression in the online realm.* IFEX. Available at http://www.ifex.org/lebanon/2014/03/28/bloggers_facing_threats/; and Open Net Initiative (2009). *Country Profile Lebanon.* Open Net Initiative. Available at https://opennet.net/research/profiles/lebanon

The main aim of this initiative is to equip legislators and decision-makers with conceptual and regulatory tools to constructively engage with the open and inclusive nature of social media, and to strengthen their potential for enforcing fundamental democratic principles and liberties. In line with this overall goal this report provides a set of recommendations to safeguard against the abuse of the new communication platforms and to prevent violations of voter privacy through unchecked data trading and harvesting. These recommendations are based on a systematic review of social media policies in Europe, North America and elsewhere and draw out key trends and lessons learned about the key risks and potentials of personalized public communication in political campaigns.

Background

New Media, New Challenges

Electoral laws are designed to ensure free and fair elections. They provide one of the fundamental guarantees of equal access and opportunity to vote. The media have traditionally been subjected to special scrutiny by national legislators for they play the role of key interface and mediator between political candidates and the public. This role assigns them special responsibilities in facilitating a balanced and impartial education of the electorate. The Lebanese electoral law requires media to clearly label and separate political advertisements from journalistic facts and information, and to make room for campaign messages that represent the entire spectrum of voices and candidates. These regulations were designed to minimize the risk of influencing voting decisions and to contain the power of print and broadcast media to simultaneously broadcast campaign messages into millions of homes.

Social media have fundamentally transformed the way in which media operate and become effective. Social media replaced the paternalistic one-to-many broadcasting model that has characterized the television era with new participatory media platforms. The information-driven public of today is far less reliant on journalists and editorial decision-makers to filter and access information. Instead, individuals' search and browsing behavior has become a key source of news-making and reporting in and of itself. Legacy media increasingly draw up on the trend barometer of social networking sites to identify upcoming topics and conversations thereby transforming what was once a highly centralized and one-directional process of news-making into a collaborative, many-to-many journalistic enterprise. BBC World's "Outside Source" or Al-Jazeera English's "Listening Post" are just examples of this new form of 'open' journalism in which the people, "formerly known as audiences,"[6] actively contribute to and participate in their information environment.

The inclusive and participatory nature of social media confronts lawmakers with a unique set of challenges. Messages circulated through social networking sites rarely have a singular source or origin but rather feed off of each other in ways that escape the framework of national laws. Social plug-ins such as Facebook's 'Like' button or 'Share' function allow for instant and spontaneous modes of expression that bring long established distinctions between institutionalized speech and informal comment, fact and opinion to blur. The recent resignation of CNN news anchor Jim Clancy shortly after a controversial tweet on the Charlie Hebdo attack in Paris[7] or the persistence of legal charges against humorous or satirical posts about Lebanese politicians on Facebook or blogs are powerful cases in point.

Lawmakers in Europe, North America, Asia and Australia have responded in markedly different ways to the new user-driven environment of social media and smart applications. Yet, the fundamental challenge of how to define lobbying activity and political campaigning in the age of 'likes,' 'shares' and tweets remains unresolved. Now that everyone has become a potential media-maker the task of determining new rules and guidelines has become paramount.

6. Rosen, J. (2012). *The People formerly known as audience* in Mandiberg, M. The Social Media Reader. New York Univeristy Press.

7. Selby, J. (January 21, 2015). *Jim Clancy resigns: CNN International correspondent quits for 'suggesting Israeli propaganda had hand in Charlie Hebdo attacks'.* Independent. Available at http://www.independent.co.uk/news/people/jim-clancy-resigns-cnn-international-correspondent-quits-for-suggesting-israeli-propaganda-had-hand-9992030.html

Should bloggers and social media users be held to the same ethical and legal standards as professional journalists and news-makers? And if not, how can we meaningfully distinguish between media professionals, bloggers and digital citizens? In the specific context of electoral laws the challenge extends even further. How can fair and balanced voter education be accomplished in the messy media environment of center-less networks over which no one is fully in charge?

The ubiquitous nature of social networking sites and mobile computing requires a radical re-conception of electoral laws and media regulations. Instant messages on Facebook or Twitter are not reducible to fixed temporal schedules and geographic locations. The ability to transmit and access information anytime from anywhere fundamentally undermines normative principles built around fixed spatial or temporal registers inherited from terrestrial media. The new media ecology of roaming frequencies and infinitely replicable data signals renders the core assumptions of media regulators ineffective. Simply applying the existing regulatory framework to social networking sites and smart applications is not sufficient for addressing their key characteristics and challenges. For legal reform to become effective it needs to take social media's distinct qualities into account.

Rethinking Media in Post-Broadcasting Democracies

Social media produced a whole new genre of speech that is not reducible to the literal meaning of verbal expressions. Functional features such as links, tweets, 'following' and 'befriending' obtain their meaning through the purposes they serve. How to classify this new category of speech and behavioral expressions through media law and regulations poses a fundamental problem for lawmakers around the world.

Can links inflame? And if so, who is to be held accountable for references to inciting or incriminating content? At what point in fact do social media messages turn into hate speech or a criminal offense? The conviction of American journalist Barrett Brown[8] comes as chilling reminder of the arbitrariness with which links can be criminalized into federal offences. Brown linked to leaked material issued by the hacker activist groups *Anonymous* and was sentenced to 63 months in prison for proximity to sources in the hackers' underground.

Relayed back to the issue of electoral campaigning the question becomes: at what point do links, 'likes' and followers count as political affiliation or as campaigning? And how may they undermine the principle of fair competition and voter education during electoral campaigns?

The past two years have seen arrests for online communications pertinent to politics and social issues in 38 of the 65 countries monitored in the latest Freedom House report.[9] Criminal charges against digital speech are most prevalent in Africa and the Middle East. But Freedom House also observed a rising number of arrests in high tech nations such as South Korea. There, the former head of national intelligence was indicted on the charge of orchestrating more than one million tweets and online comments in support of acting President Park Geun-hye before her election in December 2012. As

8. The Sparrow Project (January 22, 2015). *Barrett Brown sentenced to 5 years issues official-statement*. Available at http://www.sparrowmedia.net/2015/01/barrett-brown-sentenced-to-5-years-issues-official-statement/

9. Freedom House (2015). *Freedom on the Net.* Available at https://freedomhouse.org/report/freedom-net/freedom-net-2015

more and more countries are starting to amend their election laws and allow online campaigning such cases of political manipulation are highly likely to increase.

The fact that social media have become a target for criminal investigation testifies to their tremendous effectiveness in political mobilization. One does not have to reiterate the optimistic accounts on the role of Facebook and Twitter during the early days of the Arab uprisings to acknowledge that social networking sites have become an essential part of the infrastructure through which political conflicts and struggles unfold. Yet the response of lawmakers has so far primarily addressed the disruptive power of social media; their ability to circumvent state control undermines existing structures of order. Also, authorities have been hesitant in strengthening social media's capacity to empower citizens and enhance their participation in the democratic process.[10] Up to this point only Italy, Brazil and Iceland have openly acknowledged the informational sphere as critical domain for citizen autonomy and self-determination, while most other countries in Europe, North America or Asia continue to regulate online media as separate from the social and political domain. Yet constitutional commitments to free speech and data protection acts are no sufficient to protect fundamental democratic rights such as access to and control of information and independence of decision-making. They require an acknowledgement of the vital links between data, ownership and self-determination that are waiting to be addressed.

Different approaches to free speech and privacy protection in the USA, Europe and Asia have hampered attempts to enforce digital citizenship rights across the globe in a unified manner. As Colin Bennett argued,[11] privacy practices are dependent on corporate policies and technical standards of social media provider whose approaches are varied and fluctuating. They are designed to encourage the unrestricted disclosure of personal information rather than acknowledging data as integral part of a person's identities and social existence in a media-driven world.

The Expressive Qualities of Social Media Data

Not only do social media allow for new modes of voter mobilization and campaigning, they also generate new types of information that overwrite the golden rule that "content is king."

What is said on social media is as important as what can be read off from social media behavior, including but not limited to search queries, sharing images and content or building up networks of followers and friends. Track records of people's day-to-day activities on networking sites and smart applications have become one of the most valued currencies of the 21st century. Social media data is particularly precious to election campaigners who need to know about voters' tendencies and their potential to swing them into the desired political camp.[12] Polling suggests that young voters do not trust parties or media organizations but are more likely to be influenced by the behavior of their friends.

10. The massive expansion of national and global surveillance in the fight against militant movements such as the Islamic State and other groups labeled as terrorists is just one example here. The UK secret service only just recently announced plans to establish an entire new division of psychological warfare that will operate primarily in the social media sphere. MacAskill, E. (January 31, 2015). *British army creates team of Facebook warriors.* The Guardian. Available at http://www.theguardian.com/uk-news/2015/jan/31/british-army-facebook-warriors-77th-brigade

11. Bennett, C. (2013). *The politics of privacy and the privacy of politics: Parties, elections and voter surveillance in Western Democracies.*

12. NESTA (May 23, 2014). *Big data and the 2015 UK General Election: digital democracy or digitally divisive?*

The Obama campaign in 2012 has made particularly effective use of this trend.[13] In the final weeks of the campaign, as described by Bennett, over 600,000 Facebook friends of the Obama campaign signed up for an "Obama for America" application that allowed the sharing of specific content about the campaign with their friends. In an instant, the campaign had access to more than five million new contacts who potentially saw each other registering to vote, giving money, sharing videos and voting on Election Day. Scientific studies indicate that this kind of 'targeted sharing' through Facebook can have small but significant impact on voting behavior, especially among the youth.[14]

Social media profiles and timelines provide campaigners with an unprecedented level of detail about individual mindsets and dispositions. Geo-tagging messages and measuring sentiments in Facebook, Twitter or Instagram postings add critical insights into the social life of voters that governmental data or consumer statistics do not provide. Lining this highly personalized information to commercial marketing databases and publicly available information has become an essential strategy in political campaigning. As the British NGO NESTA estimates, a substantial part of the GBP 31 million spent by UK parties in 2010 were spent on buying social media data and using it to spread custom-tailored messages to the electorate.[15] The same holds true for the USD 6 billion spent on the Obama and Romney 2012 campaigns.[16] The last Indian elections saw a similar surge in businesses offering big data analytics and digital tools to identify, profile and reach voters. As NESTA concludes, there has been an explosion of political start-ups trying to give politicians that vital edge in the political data war.

The fusion of social media, government and marketing data constitutes a new regime of power and surveillance. It not only widens the asymmetry of knowledge between politicians and voters but also undermines fundamental principles of autonomy and independent decision-making that are essential for free and democratic vote.

The fact that critical infrastructures for public debate are now operated by private corporations brings critical distinctions between state and market, citizens and consumers to blur. Voter profiling software operate with big data sets accumulated from a variety of sources to map individual attitudes, character traits as well as ethnic, religious or political affiliations. But they also allow calculating complex simulations to monitor the state of ongoing elections and to predict the voting behavior of targeted individuals and geographic areas.[17]

These new forms of voter surveillance subject fundamental social and political rights to a bundle of vested interests that undermine basic democratic principles such as freedom of conscious and decision-making. Their impact calls for new concepts and approaches to legislative oversight. Yet,

13. Sherer, M. (November 20, 2012). *Friended: How the Obama campaign connected with young voters*. Time Magazine. Available at http://swampland.time.com/2012/11/20/friended-how-the-obama-campaign-connected-with-young-voters/

14. Bond, R. M., Fariss, C. J., Jones, J. J., Kramer, A. D., Cameron, M., Settle, J. E., & Folwer, J. H. (September 13, 2012).
A 61–million–person experiment in social influence and political mobilization in Nature. Available at http://www.nature.com/nature/journal/v489/n7415/full/nature11421.html

15. NESTA (May 23, 2014). *Big data and the 2015 UK General Election: digital democracy or digitally divisive?*

16. *ibid*

17. Marwick, A. (January 9, 2014). *How Your Data is Being Deeply Mined*; and Bennett, C. (2013). *The politics of privacy and the privacy of politics: Parties, elections and voter surveillance in Western Democracies.*

as we will show in the pages that follow, legal reform cannot limit itself to amendments to data and privacy protection in existing media and electoral laws and regulations. It needs to address the widening asymmetry in power and knowledge between politicians and voters in ways that take the ontological dimension of information into account.

As Florian Floridi argues,[18] information technologies have changed the very nature of privacy as well as our appreciation of it. Privacy, he suggests, has moved far beyond questions of access and control over a person's life and information to include far bigger concerns about what can be done with personal data and how that impacts our sense of self and the idea of independence of consciousness and minds. The key challenge at hand for lawmakers today is therefore to develop new instruments and mechanisms that protect essentially informational nature of human beings and their operations as informational agents in the social sphere. This report, for the first time, lays out some key parameters and recommendations for how such a re-conception could be envisioned and provides policy directions towards their implementation within the framework of Lebanese media, telecommunication and electoral law. The report's overall goals are to raise awareness about the critical link between information, autonomy and self-determination and to redirect the power and impact of social media on the democratic process to the benefit of (digital) citizens in Lebanon.

18. Floridi, F. (2005). *The ontological interpretation of informational privacy*. Ethics and Information Technology, Available at https://www.researchgate.net/publication/30384197_Informational_privacy_and_its_ontological_interpretation

Digital Innovations and Archaic Legislations

The distinct characteristics of social media challenge the social, spatial and temporal parameters within which many laws regulate media in electoral campaign. The global decentralized architecture of social networking platforms confronts lawmakers with a unique set of challenges. They are not reducible to predictable temporal patterns and schedules as radio, television and even print media once were. The ubiquitous and instantaneous nature of user-driven media undermines normative principles that confine political speech to clearly delineated temporal or geographic locations and thus call for a meaningful reconsideration of the actors, platforms and channels targeted by media and electoral laws. The profound transformation of the media sphere over the last decade demand for a radical re-conception of the idea of media in national law and media regulations. Electoral silence and equal-time rules are two clear examples of archaic legislations not fitting current time.

Electoral Silence

Electoral silence is a ban on political campaigning prior to an election session. Different in length from country to country, it is a specific legal time in which media are not allowed to publish any political propaganda message or public opinion poll. It is used to ensure a free voting environment and aimed to allow voters to peacefully reflect before casting their preferences. Roughly, electoral silence is also an important practice to cool off the campaign period and reduce tensions and potential for conflicts on Election Day. It can be established by law like in Lebanon, France, Italy, Spain and Russia, or it is enforced by a so-called 'gentlemen's agreement' between the main political forces as is the case in Sweden and in the Netherlands. From other perspectives, electoral silence is a completely unknown phenomenon: for instance, in the United Kingdom or the United States it is regarded as an explicit violation of freedom of expression.

The challenging of electoral silence principle is among the many consequences of the communication renewal process and, in particular, the use of online social platforms for political scopes is increasingly nurturing a glowing debate on the actual value of the aforementioned principle in the countries where it is applied. Indeed, despite the ban, during the electoral silence period, many Internet users campaign for politicians or political parties on both their public and private accounts and, claiming the right of free speech in the digital space, they publish messages and propaganda also on Election Day.

Worldwide laws enforcing electoral silence are mostly anachronistic; no single word on the use of social media is reported. Surely, they did not aim to forbid politically engaged people to speak with friends or sympathizers but, nowadays, as online social platforms do not sparkly separate private and public communications, uncertainties rule this endeavor. For instance, the law-expected fines for those who digitally break electoral silence on social media have never been and cannot possibly be applied.

In this framework, in September 2014, the Italian Court of Cassation defined Facebook as an "open social community which user-profiles are accessible to everyone" and a "virtual, immaterial public agora." The specific case bearing this sentence was a digital harassment of a journalist, insulted by a colleague on his public wall. Basing on this case, and arguing for extension, most Italian jurists have stated that the law regulating electoral silence (enacted in 1956) is applicable in all its parts also in the digital space.

This Italian review is receiving worldwide approval by restrictive governments, however, a strong civil opposition and disobedience is increasingly questioning the insight. Activists argue that, by imposing electoral silence to social media, freedom of expression constructed and acquired through the use of the online social platforms is considerably violated and, moreover, the attempt to hush the "virtual agora" bears many practical and substantial difficulties.

First and foremost, what regulation should respect pages located on foreign servers? Does a Lebanese political blog using a US server respect Lebanese electoral silence laws or the ultra-liberal American vision? Furthermore, information and expression are transmitted and exchanged in the global net regardless of time differences. What timing should respect an Italian voter based in Japan? Then, how to distinguish direct messages from normal tweets and posts? And once the previous questions are answered, who will be in charge to judge? How can the immense amount of digital material be scanned and checked? It seems to be such an impossible mission requiring incredible efforts. Last but not least, what if an Indonesian blogger supports and campaigns for a certain political party in the French elections? Who can sue him?

Par Condicio? The Equal-Time Rule in the Digital Era

On the same note as the electoral silence, the equal-time rule seems to be another anachronistic practice strongly challenged in the social media universe. It specifies that every media channel must provide equivalent time, space and opportunity to all political candidates. Roughly, it states that positive coverage provided to a candidate must be balanced by similar coverage to other candidates for a similar duration at a similar time-slot.

In countries like France, Denmark, Norway, Italy, Netherlands, Japan, and the United States, the equal-time rule is applied with various criteria. The main motive for this doctrine is to ensure that viewers are exposed to a diversity of viewpoints. The rule was established by the US Federal Communications Commission in order to avoid media manipulation of election outcomes by presenting just one point of view and excluding other candidates.[19]

How can this principle of fairness be applied to the Internet? Providing interactive tools of communications, social media once again become extra-legal and laws establishing the equal-time rule appear mostly overpassed or not suitable to the online scene.This practice faces the same challenges affecting the electoral silence rule and, most importantly, web-users are active participants in the news research and production processes while the equal-time rule was designed for a passive audience.

19. Equal Time Rule, Encyclopedia of Television. Available at http://www.museum.tv/eotv/equaltimeru.htm

Big Data: Privacy and Voter Profiling

Article 17 of the UN International Covenant on Civil and Political Rights (1966) states: "No one shall be subjected to arbitrary or unlawful interference with his privacy." Even though consistent and direct in its meaning, and having been the pillar around which privacy policies have developed throughout decades, this statement fails to strictly define what "arbitrary" means. Nowadays, fifty years after the adoption of the Covenant, the time is ripe to discuss how governments and private firms have been arbitrarily collecting enormous material to be analyzed by technological innovations.

Governments and corporations' data-memory capacity provides for nearly indefinite storage. Digital data now can be accumulated without time constraints and, whether intentionally or inadvertently, people supply any kind of information through the web, social media, smartphone applications, state and regional records, commercial investigations, geospatial observations, surveys, and plenty of analogue-converted materials from physical devices such as sensors, cameras and microphones. The very innovative analysis processes make this storage more than about huge data numbers; big data implies the ability of scanning and aggregating the gathered information at irrepressible time.

The great variety of processes through which data are stored and analyzed raises concerns that our legal, ethical and social norms are unfit to protect the rights of both individuals and communities. Throughout history, collecting information about citizens has been a common and dominant methodological preference of governments and it is then hardly surprising that, compared to the past, technological progress has increased the capacity and skills of both governments and corporations to acquire data. What is gathered about us? What is possible to do with data analysis? Who stores the data and who defends individual privacy? And who controls the controllers? Data collection in political campaigns is a boosting segment and it is becoming a phenomenon that pay lip service to civil freedoms while accumulating private information about each and every Internet user.

A Global Overview

Big data provides politicians with unprecedented insights into voters' beliefs, values and aspirations. Political parties and well-prepared candidates can use databases and Internet technologies to raise money, organize volunteers, gather intelligence on voters, and conduct opposition research. They want to know what motivates voters, what they value and how they feel about key issues.[20]

A briefing document entitled "Social Media in Election Campaigning" by the European Parliamentary Research Service (EPRS)[21] explains this process based on the US 2012 presidential campaign: "The 2012 Obama campaign developed a central unified database with information on millions of voters. One source for this information came from inviting volunteers to sign into the campaign website with their Facebook credentials, automatically uploading information on themselves but also data about their network of friends. Data mining techniques were then applied

20. NESTA (May 23, 2014). *Big data and the 2015 UK General Election: digital democracy or digitally divisive?*

21. European Parliamentary Research Service (March 21, 2014). *Social media and election campaigning*. Available at http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140709/LDM_BRI(2014)140709_REV1_EN.pdf

to this central data store to classify voters based on characteristics such as socio-economic class, personal interests and residence."

US journalist John Nichols even wrote: "Obama's Chicago-based campaign offices were dominated by his secretive analytics department, where hundreds of specialists crunched numbers," adding: "Data mining drives the money-and-media election complex that is rapidly turning American democracy into an American Dollarocracy, where election campaigns are long on technical savvy but short, very short, on vision."[22]

"The 2012 election will be remembered as the first election where big data and analytics played a crucial role and had a tremendous impact on the outcome of the presidential election,"[23] concludes George Shen, an information management specialist with Deloitte Consulting. Nowadays political candidates, political parties and lobby groups are among the most ambitious data gatherers and miners around.

The 2014 Brazilian presidential election is another good example of the increasing importance of online campaigning and data collection for political ends. In an article published in The Economist, we learn that "Just before Dilma Rousseff was elected president in 2010, 6 million Brazilians used Facebook at least once a month. As they gear up for a presidential poll in October, 83 millions do. Only the United States and India have bigger Facebook populations."[24] The article adds: "During the campaign free television time is divvied up using a complex formula which takes into account the size of electoral alliances – and tends to favour the incumbent (…) That would leave the president with around half of the (…) television slots; the other candidates would split the rest." As a result, the rival candidates placed their focus on Facebook. Extracting data from all social platforms, Brazilian politicians canvassed the community, pre-determining angles of attack and devising targeted approach to obtain votes. The 2014 Indian election followed the same trend: it collected data from half a billion voters, thus reaching the most extensive use of data-collection process yet undertaken.

Key Issues of Privacy Violation

Data gathering techniques raise increasing concerns for voter privacy for several motivations. First and foremost, as highlighted by electoral campaigns since the beginning of this decade, nowadays politicians do not direct their electoral messages to a certain group of people, but specific campaigns are designed to affect differently each and every individual. Using data mining techniques (that means scanning personal profiles, likes, shares, friends, events, private messages, and crossing it with friends or similar personal profiles) an analyst can tell a politician what moves an individual, and how to get a vote from that person. This leads to a scenario where politicians no more need to devise true electoral strategies: by monitoring web-user behaviors politicians can forgo an electoral program; they can outright shape efficient messaging based on data analysis.

22. Nichols, J. (June 12, 2013). *Not Just the NSA: Politicians Are Data Mining the American Electorate*. The Nation. Available at http://www.thenation.com/article/not-just-nsa-politicians-are-data-mining-american-electorate/

23. Shen, G. (2013). *Big data, analytics and elections*. Available at http://www.analytics-magazine.org/january-february-2013/731-big-data-analytics-and-elections

24. The Economist (March 15, 2014). *Winning hearts and likes*. Available at http://www.economist.com/news/americas/21598975-social-media-will-play-big-part-years-campaign-winning-hearts-and-likes

Cookies are another instrument to reduce users' privacy. Today, an increasing number of websites require users to release personal information in order to access contents. This data can be sold or exchanged and, in this way, user information's trade has become a growing segment of the market. Data are the new gold, especially in political campaigns.

Political Communication, Social Media and the Law in Lebanon

The Telecommunications Law of 2002

Lebanon's telecommunications sector was destroyed during the 1975-1990 civil war. In the early 1990s, the Lebanese authorities decided to provide mobile phone (GSM) contracts to local subsidiaries of major European operators to build, operate and transfer networks back to the government at the end of the stipulated time, initially set in 2001.

Then, a Telecommunications Law was passed in 2002, with the intention of restructuring Lebanon's telecommunications field away from state monopoly, and was based on four pillars: The first is the liberalization of the sector and the introduction of competition; the second is the establishment of the Telecommunications Regulatory Authority (TRA), designed to promote and oversee efficiency and competition in the field; the third is to offer opportunities for private participation through the privatization of the national telecommunications operator; and the fourth is to engage in social and public policy objectives "such as ensuring access to telecommunications services in all Lebanese territories [and] safeguarding consumer interest."[25]

The Telecommunications Law was enacted seven years after Lebanon first accessed the Internet, but is significant in its glaring oversight concerning web regulations. When the Internet is discussed, it is in terms of how to technically procure a permit for service provision. The law sets out criteria for class licenses, which are "authorizations granted on a general basis to a class of providers offering the same type of service... for example, to Internet and data service providers."[26] It does not however attempt to classify content on the Internet and its possible usages.

The TRA was created by the 2002 Law with the purpose of ensuring market transparency, regulating disputes and implementing the various articles of the law, among other things. The TRA was supposed to be a neutral, independent, powerful authority that would help improve the telecommunications sector and resolve disputes, push for transparency and draft laws to keep up with the rapidly changing face of telecommunications. Instead, it has become a tool in the Lebanese political arena. The TRA was created to undo the state monopoly on the sector and relegate the Ministry of Telecommunications to setting general policy and recommendations, but life on the ground does not always follow the letter of the law. Ministers of Telecommunications have often attempted to circumvent the role of the TRA to retain the power of their office.

The TRA was to have the power to settle disputes between providers of telecommunications services and between the providers and their clients. It was to have independence and promote transparency and an open market; all characteristics of modern democracies. Instead, it has been relegated to a role that is almost ceremonial, with its relevance and status under question.

25. El Assir, O. and Alem, M. (2009). Alem & Associates, Barristers & Solicitors. Lebanon Chapter *in* International Telecommunications Law. Yorkhill Law Publishing. Available at http://www.alemlaw.com/~alemlaw/images/knowledge/publications/International_Telecommunications_Law-Lebanon_Chapter.pdf

26. *ibid*

Article 47 of the Telecommunications Law states that in the case of events concerning national security, the first priority for telecommunication providers is to cooperate with police, security and law enforcement authorities.

Article 1 of Law No. 140, adopted in October 1999, "provides for the principle according to which the right to make confidential internal or external calls by using any telecommunications means (such as fixed telephones, mobile devices of any type whatsoever including cellular phones, fax and email) is protected by the law and is not subject to any form of wiretapping, monitoring, interception, or disclosure." Still, the law does have some exceptions. Interceptions can by authorized by court order in "cases of extreme emergency,"[27] and should the individuals in question be suspected of a crime, they can be detained and face prison sentences. For this sort of surveillance to take place, the court order must specify the means of communication, the subject matter behind the interception, the crime subject matter, and the duration of the surveillance.

Interceptions can also be taken by the administrative decisions of the Minister of National Defense or the Minister of the Interior, with the aim of gathering information on terrorism, matters that threaten national security, and organized crime. To take effect, these decisions must be in writing, with an appropriate justification, and approved by the Prime Minister. Just as in the case of a court order, the form of communication to be monitored, relevant subject matter and surveillance time – which must be under two months – must be specified. The President of the Republic, Speaker of Parliament, Prime Minister, Members of Parliament and ministers are exempt from surveillance and monitoring.

As Omar El Assir and Mohamed Alem explain,[28] in order to prevent abuse by the system, monitoring requests that are made by administrative order are verified by an independent commission, made of the first president of the Court of Cassation, the president of the State Council and the president of the Court of Audit.

What does this mean for democratic debate on social networking sites? A strong TRA would have reduced the state monopoly and therefore have induced more freedom, and may even have contributed to the production of further laws that deal exclusively with the role of the Internet in the telecommunications sector. As it stands, the current law that is supposed to discuss this industry all but skips over the role of the most vital cog of all – the Internet. The Telecommunications Law is not helpful for establishing democratic debate on social networking sites, but rather the opposite; it provides a way to access and monitor the personal information of private citizens, all in the name of national security. While this may have been done for the right reasons, several instances have shown that these measures have served to combat free speech on the web, with bloggers and private citizens paying the price. The industry remains dominated by the state, but with the farce of an independent TRA.

To adhere to democratic principles, the current state of the telecommunications sector must be fundamentally altered. The role of the state in administering all areas of the field must be re-arranged so that the 2002 Law is truly implemented and the TRA as an independent authority takes the reins, with the Ministry of Telecommunication taking a back seat.

27. *ibid*

28. *ibid*

Further laws concerning the Internet and classification of speech types, political and otherwise, should also be discussed, along with the rights and obligations that naturally follow along. Delays in such a process leave political elites free to do as they wish with data exploitation and surveillance open to abuse.

The Electoral Law of 2008

The Lebanese parliamentary election law[29] lacks any explicit provision on the use of social media and online campaigning. However, it does address and regulate broadcast media. Article 68 – Paragraph 4 lists the practices that are forbidden or considered unlawful.

During the electoral campaign, the audiovisual media, lists and candidates shall abide by the following obligations:

- Refrain from any act of libel, slander and defamation towards any list or candidate.
- Refrain from broadcasting anything that might trigger religious/confessional/ethnic sensitivities or acts of violence or riots, or support for terrorism, crimes, or sabotage.
- Refrain from broadcasting anything that might be a means of pressure, intimidation, mistrust, allusion to or promise of material or in-kind benefits.
- Refrain from distorting, screening, falsifying, omitting, or misrepresenting information.

Yet, none of the abovementioned terms is clearly defined. Their scope remains elastic and is matter to interpretation.

The wording of Chapter Six of the election law – Electoral Media and Advertising – opens the door to including online campaigning in its scope, starting with Article 63, which defines electoral promotion as "any material related to the candidates' programs, electoral campaigns and political and electoral positions, recorded/filmed inside or outside the media company studios, and through which the candidate wishes to address the voters by broadcasting it, at their own expense, in the company's programs dedicated for this purpose, against a specific price." If a news website with video capacity is defined as a "media company" then such an article can apply to online campaigning. But, this would not cover campaign-generated videos posted on YouTube, Facebook and other social networks, or even the candidate's personal website.

When it defines electoral advertising as "any material promoting the election of a certain candidate broadcasted against specific prices, during the commercial breaks of the media company," the electoral law clearly shows how unsuitable it is for the Internet as the concept of "commercial breaks" is irrelevant online.

Conversely, Article 65, which states: "During the electoral campaign period determined in this law, the electoral material used in the audio visual and printed media starting the date of application for candidacy until the closing of ballot boxes, shall be governed by the provisions of the present chapter,"

29. Parliamentary Election Law - No. 25, issued by the President of the Republic on October 8, 2008 and published in the Official Gazette No. 41 of October 9, 2008. Available at http://www.elections.gov.lb/Legal-Framework/Law-no--171-Issued-on-6-January-2000/Election-Law.aspx

can be interpreted in a way to completely exclude Internet-based media and campaigning from the scope of the electoral law, as it cites explicitly and exclusively "audio visual and printed media." The same applies to Article 66.

As for settling disputes, it is provided in Article 75 that the Supervisory Commission on Election Campaigns (SCEC) "shall immediately consider any complaint filed by a wronged list or candidate. Decisions as to filing such complaint in the competent Court of Publications shall be taken within twenty four hours of receipt."

In case of violation of the provisions of this chapter on electoral media and advertising by a media outlet, the SCEC can, according to Article 76, "refer the defaulting media to the competent Court of Publications who shall take one of the measures hereunder:

- Impose a financial fine on the defaulting media ranging between 50 and 100 million Lebanese pounds.
- Partially suspend the work of the defaulting media for a maximum of three days. This measure shall include suspending all political and news programs, bulletins, interviews and fora.
- If the violation recurs, totally suspend the work of the defaulting media and totally suspend all of its programs for a maximum of three days."

These provisions cannot directly be applied to online media unless the Ministry of Telecommunications conveys to Internet Service Providers (ISPs) the order to block access to the incriminated websites. But, an outright suspension of programs remains technically impossible.

Also in case of violations, "the Public Prosecution shall sue the defaulting media before the Court of Publications directly or upon a request filed by the wronged party. The defaulting media shall submit a brief to the court within 24 hours of notification.

The Court of Publications shall render its judgment within a maximum of 24 hours. The Public Prosecution and the accused party may appeal the decision before the Court of Appeal within 24 hours starting from the judgment declaration date for the Public Prosecution, and from the notification date for the defaulting media."

While issuing a judgment "within a maximum of 24 hours" could be possible when the number of media outlets is finite, i.e. printed and audio visual media only, this provision cannot be respected if hundreds of complaints are filed based on tens of thousands of posts, tweets, user- or party-generated videos, blog posts and articles on online platforms.

Therefore, we conclude that Chapter Six of the election law cannot be practically applied to online media – let alone social media. The equal time and electoral silence rules would not work, the definition of promotion and advertising are unsuitable to the Internet, and the time constraints placed on the Court of Publications to issue its rulings are virtually impossible to meet and would clog the dispute settlement mechanisms during the campaign period.

The situation would become even more complicated in case the Anti-Cybercrime and Intellectual Property Bureau [herein: Cybercrime Bureau] at the Internal Security Forces (ISF) gets involved.

"While the Cybercrime Bureau is designed to address online crimes such as identity theft, money laundering and child pornography, by merit of being the only unit within the ISF specialized to Internet-related crimes, it also handles online defamation, libel and slander complaints. This means that it has given itself the authority to summon, detain and interrogate online journalists, bloggers and Internet users accused of defamatory online speech, and, by nature of the Bureau, treat them as suspected cybercriminals," writes Anna Lekas Miller in a Samir Kassir Foundation's report.[30]

Also, "the majority of the information pertaining to the Cybercrime Bureau has been attained through leaks and hacks, such as the July 2015 Hacking Team data hacks,[31] and is not readily transparent, nor otherwise available to the public," adds the report.

Any involvement of the Cybercrime Bureau in election-related investigations would add to the problems and raise serious concerns related to the interference of a police unit in elections, protection of election data and campaign strategies.

30. Lekas Miller, A. (2016). *Digital Rights and Online Expression in Lebanon*. Samir Kassir Foundation. Available at http://www.skeyesmedia.org/extensions/pdf/Digital_Rights_in_Lebanon.pdf

31. York, J. (August 3, 2015). *Hacking Team Leaks Confirm What Arab Privacy Advocates Already Knew.* Electronic Frontier Foundation. Available at https://www.eff.org/deeplinks/2015/08/hacking-team-leaks-confirm-what-arab-privacy-advocates-already-knew

Recent Attempts at Regulating Online Campaigns

The UK Guidance on Political Campaigning

In the UK, the use of big data for political ends is an increasing civil concern. In a country where privacy is a fundamental value, the reluctance of its political parties in the 2010 general election to follow the US example in micro-targeting voters was due to concerns about legal challenges based on data protection legislation. To this end, and to prevent privacy breaching, in 2014, the UK Information Commissioner's Office (ICO) issued the "Guidance on Political Campaigning."[32]

The document, addressed to parties, MPs and councilors, acknowledges the right of candidates in "healthy democracies" to promote themselves through several campaigning methods. It considers political campaigning a form of direct marketing, and thus it implies several principles to guarantee fairness and the respect of fundamental liberties. These principles are said to ensure maximum privacy for individuals and to respect their right to exercise objection to any form of direct marketing. Organizations must comply with these rules, under the Privacy and Electronic Communication Regulations (EC Directive) 2003 (PECR)[33] and the Data Protection Act 1998 (DPA),[34] enforced by the Information Commissioner in the UK. Failure to comply with these rules is considered a breaking of law and therefore a criminal offense.

What is direct marketing?
The guide defines direct marketing as "the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals." This would entail any form of promoting ideas or aims that might push receivers to act accordingly, including the appeal of political campaigns for individuals to vote, support campaigns or collect funds. Note that mailings that are not addressed are not considered direct marketing, since direct marketing only includes what is "directed to particular individuals," according to the guide.

It is important to highlight that political profiling is caught up in the definition of direct marketing, where campaigners tend to collect records of individuals to follow up on it in the future and contact these individuals.

The guide lists a number of traditional and online communication methods, without covering though the social networking platforms such as Facebook or Twitter. These methods are: post addressed to particular individuals, fax, telephone, email, SMS, MMS, voicemail left on answering machines, and "tell a friend" campaigns.

32. Guidance on Political Campaigning (2014), Information Commissioner's Office. Available at https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf

33. The Privacy and Electronic Communications (EC Directive) Regulations 2003, The National Archives, United Kingdom. Available at http://www.legislation.gov.uk/uksi/2003/2426/contents/made

34. Data Protection Act 1998, The National Archives, United Kingdom. Available at http://www.legislation.gov.uk/ukpga/1998/29/contents

An organization has received an objection to direct marketing from an individual; what does it need to do?

Each individual has the right to object to direct marketing. Organizations must respect the individual's will and preferences, or any request received to not to promote materials. Election freepost mailings is excluded.

When contacting individuals by post, campaigners have the right to unlimited access to the full electoral register and to legitimately use it during elections and referenda. Individuals on the list may be contacted by post. Moreover, campaigners are allowed to send one unaddressed postal communication to each address. When directly collecting information from individuals, organizations must explain that these information would be used for direct marketing. The same rule applies to email, text message, video message and voicemail.

When using viral marketing or "tell a friend" campaigns to send email, text message (SMS) or video message (MMS), an "organization is not responsible for the malicious activities of an individual using the service it provides, [but] it should bear in mind that the recipient may associate it with that unpleasant experience," as stated in the guidance.

When collecting individuals' information for direct marketing purposes, organizations must comply with the principle of "good information." This means that it must be transparent about the usage of information, ensure that information is secure, does not keep it longer than necessary, and destroys it after it had served its purposes. Organizations may only send information outside the European Economic Area if they guaranteed that it is protected. And in each case, organizations must respect individuals' preferences, their consent, their right to access their own information, and their right to object to usage of their information.

In every case, an organization must identify itself when contacting individuals and provide details to allow them to contact it in case of objection to direct marketing. Also it must have the consent of contacted individuals when using all of the aforementioned communication methods, excluding telephones and post, and should respect requests to not receive promotional material.

International Conference of Data Protection and Privacy Resolution

The 27th International Conference of Data Protection and Privacy Commissioners issued a resolution on the use of personal data for political communication in September 2005.[35] The resolution upholds the rights of citizens/data subjects to be informed of the political communication activity, and to be protected from unjustified intrusions, damages and costs. Additionally, the resolution emphasizes the responsibility of entities to carry out political communication activities in a legal manner, and to respect data protection laws and principles.

According to the resolution, "any political communication activity, including those not related to electoral campaigns, which entails a processing of personal data, should respect fundamental rights

35. Resolution on the Use of Personal Data for Political Communication (2005), 27th International Conference of Data Protection and Privacy Commissioners. Available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/05-09-16_resolution_political_communication_EN.pdf

and freedoms of interested persons, including the right to the protection of personal data, and should comply with data protection principles affirmed."

The resolution lists the following principles:

1. Data minimization principle: Processing personal data should only happen when it is needed to meet the purpose for which it was gathered.
2. A lawful and fair collection: Personal data should only be gathered from reliable, just sources and should be presented in a fair manner.
3. Quality of data: Data should not be overused and ensure that it is recent and relevant to purposes.
4. Finality principle: Personal data used is fair game for political debate when they are applicable and align with the reason they were collected.
5. Proportionality: Personal data that is collected should be approached and carried out with the appropriate and admissible procedure pertaining to the purpose of the data.
6. Information to Data Subjects: Notice should be given to the person that the data is being collected from before the collection is made.
7. Consent: The approval of collection of personal data from the subject is imperative.
8. Storage of data and security measures: The controller must protect all of the data that is collected.
9. Rights of Data Subjects: Subjects that the data came from must be able to control the information collected from them. They must also be given the ability to object communication they do not agree with or wish to receive.

Regulating Big Data

A proposed EU General Data Protection Regulation contains a number of provisions concerning the use of personal data in big data analytics. In particular: the principle of data minimization and the need for organizations to justify their processing of personal data. The proposed Regulation does not deal directly with election campaigns but if adopted, data collected during campaigns will be covered by its provisions.

The collection of personal data must be "limited to the minimum necessary in relation to the purposes for which they are processed" and shall only be processed "if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data" (Article 5).[36] Personal data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed." Furthermore, the 'right to be forgotten' under Article 17 means that data subjects can obtain the erasure of personal data if it is no longer necessary for the purposes for which they were collected or processed.

36. European Parliament legislative resolution of March 12, 2014 on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. Available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0219+0+DOC+XML+V0//EN

The Regulation proposes many practical measures to protect privacy rights. Among them, it includes a specific requirement to build in "data protection by design and default" (Article 23). Data controllers have to implement mechanisms to ensure that only the minimum amount of personal data is used and is kept no longer than needed for the processing.

The Regulation suggests a desire to shift the balance of power in favor of the individual by giving them more explicit rights over the processing of their personal data. The individual would have a right to object to processing carried out for certain purposes (article 19) and the right not to be subject to automated profiling which has "legal effects" on them or "significantly affects" them (Article 20). What constitutes a significant effect is open to question, but these provisions are potentially relevant to the processing of personal data in big data analytics.

Finally, the Regulation would also extend the scope of data protection to apply to data controllers outside the EU that are processing the personal data of people in the EU, if the processing relates to offering them goods or services or monitoring their behavior (Article 3).

Recommendations and Areas for Development

The purpose of this report is to shed the light on an issue that has not yet been tackled by groups, parties and individuals who are working on electoral reform in Lebanon. This research has been conducted by the Samir Kassir Foundation's SKeyes Center for Media and Cultural Freedom over a course of one year. It is meant to trigger research about the topic of digital rights during electoral campaigns not only in Lebanon but also on the international level.

This report includes many examples of the usage of social media for electoral campaigns from other countries, but the issue remains nevertheless a worldwide grey area that needs more in-depth research for a better understanding of these rights by decision-makers, candidates and citizens, and is necessarily intertwined with the international debate and research on digital rights, privacy and Internet governance.

Recommendations for Parties and Candidates

- Use Twitter and Facebook certification processes to identify official accounts of parties and candidates.
- Use Twitter's "purple badge" option. Twitter provides a purple badge for political campaign ads paid for by candidates and political parties. This would allow transparency and the consistent monitoring of and filtering of people campaigning outside the official campaign's budget.
- Clearly mention in the presentation of the Twitter, Facebook, YouTube, LinkedIn, Snapchat, Instagram (and other social networking site) account whether it is the party or the candidate's official one.
- During electoral periods, candidates that use official social media pages such as Facebook and Twitter to campaign should follow ethical and legal guidelines not only for their own posts but also to moderate users' comments on their online profile.
- Candidates must declare to the SCEC official websites and social media pages and handles used for the electoral campaign.
- Candidates must declare to the SCEC the amount of money spent on social media advertisement as part of the total sum used for the electoral campaign.

Recommendations for the Supervisory Commission on Electoral Campaign

- Apply campaign silence period to the official online and social media accounts of parties and candidates only.
- Provide clear and unambiguous definition of words that can have different interpretations, such as libel, slander, defamation, intimidation, blasphemy, and religious/confessional/ethnic sensitivities, which are included in Article 68 of the electoral law No 25/2008, in case it is not amended by the Parliament ahead of the 2017 election.

- Set up a complaints unit within the SCEC dedicated to online and social media.
- Include expenses for community managers, Facebook, Twitter and Google ads in the campaign expenditures that are monitored by the SCEC, after establishing contacts with the social networking sites to release data on payments made by parties and candidates during the of electoral campaign period.

The abovementioned measures should be implemented taking into account that no one should be liable for content on the Internet of which they are not the author, unless they have either adopted that content as their own or refused to obey a court order to remove that content.

When a text posted on online or social media contains hyperlinks, the owner of the page or the account should not be considered liable or responsible for the illegal content of the hyperlinked pages, unless they have control of the webpage linked to or have publicly endorsed the webpage content.

Guidelines for what is considered as campaigning on social media have to be made known to regular citizens by the SCEC ahead of the election campaign period.

Recommendations for the Lebanese Government and Parliament

The Lebanese government should issue a decree clearly defining the scope of work and jurisdiction of the Anti-Cyber Crime and Intellectual Property Bureau at the Internal Security Forces, which would exclude cases linked to online expression.

The Lebanese Parliament should:

- Update the current Press Law to protect freedom of expression for online journalists and bloggers, giving online media-makers the protection to create critical, sarcastic or controversial content without fear of criminal consequence.
- Remove "libel, slander and defamation" from the Penal Code, making it a civil, rather than a criminal offense, thus removing it from the jurisdiction of the Anti-Cybercrime and Intellectual Property Rights Bureau once and for all.
- Adopt and enforce a law pertaining to retention of users' data by third parties, including but not limited to private companies, political parties and campaigns.
- Explicitly mention online media and social media in the electoral law's media regulations with guidelines that are practically applicable to online content and in line with a liberal interpretation of Article 19 of the Universal Declaration of Human Rights: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."
- Exclude online offenses from the scope of work of the Court of Publications during the election campaign. In case a losing candidate disputes election results before the Constitutional Council and considers that the winning candidate's campaign acted in an unlawful way online, social media posts and online media content would be reviewed as part of the investigation.

In addition to decriminalizing online defamation to allow for freedom of expression, it is essential that Lebanon's surveillance of citizens is necessary and proportionate. Data collected by telecommunications companies and Internet service providers should be kept private, only accessible through a warranted search.

Project coordinator: Firas Talhouk
Introduction and Background: Dr. Monika Halkort, LAU School of Arts and Sciences, Department of Communication Arts, Lead Academic Supervisor and Senior Researcher
With the contribution of: Maria Abou Atmi, Safa Hamzeh, Khalil Kadri and Ziad Kiblawi, Students, LAU School of Arts and Sciences, Department of Communication, and Luca Paolo Cirillo

Editing and reviewing: Ayman Mhanna
Graphic design: Jamal Awada

NECG-Dib Building, 3rd floor, Sioufi Garden Street, Ashrafieh, Beirut – Lebanon
Tel/Fax: (961)-1-397331
Email: info@skeyesmedia.org
http://www.skeyesmedia.org

This project is funded by the EUROPEAN UNION

The contents of this report are the sole responsibility of the Samir Kassir Foundation and can in no way be taken to reflect the views of the European Union.