Freedom of Expression and Information (FEI) and the Security Dilemma in the Moroccan Cyberspace[1]

This paper proposes to focus on the Security Dilemma which has become more and more complex due to a number of factors. On the one hand, there is the unprecedented proliferation of a staggering cybertechnology that mates with the demands of the Information Society in the field of Human Rights (HR), particularly the right to Freedom of Expression and Information (FEI) facilitated by a growth of Cyber Social Media (CSM). On the other hand, there is the will of States to ensure Public Order (PO) and ward off Internal and/or external threats. The argument behind this work is that biopolitical theories of governmentality have shortened the distance between Internal and External threats exacerbating the issue of security because abuses may come from ignorance of the law or its misinterpretation/ overinterpretation, which can easily emanate from CSM users as well as law/enforcement agencies. The use of a survey conducted on such issues coupled with a comparison of documents taken from WhatsApp may serve to illustrate the opacity of laws in Morocco just as elsewhere (USA and Canada for instance) leading to conflicts of laws, but occasionally to abuses on both sides.

Keywords: *Security Dilemma – Human Rights (HR) - Freedom of Expression and Information (FEI) – Public Order (PO) – Cyber Social Media (CSM) – Biopolitics of Governmentality.*

Issues of security dimension —such as Public Order (PO) securitizing, intellectual and private property and identity safeguarding— have become challenging problems for States-legislatures, security agencies and Service Providers (SP) around the world. The paper purports to shed some light on such a *Security Dilemma* and its ramifications first by looking at the issue of security —particularly as it is central to PO— and how current epistemological systems shape internal and/or external political discourses; second by shedding light on how the concept of FEI quite often clashes with other legal texts sometimes resulting in abuses by the enforcing agencies or by the Civil Society (CS) as the case may be. Abuses come either as measures to safeguard PO — itself subject to discrepant interpretations— or as failures to abide by the public responsibility on the part of the CS.

This dilemma is specifically looked at as a result of the proliferation of Cyber Social Media (CSM), a use exacerbated by the technology which is becoming more and more sophisticated more often allowing to escape any rigorous and legal control be it by the State or by the SP. Focus on such an issue should normally be looked at as a global concern, a transnational one, but

[1] It is indeed much of an oxymoron to speak of geographical limitations of cyberspace which is by definition extraterritorial.

for practical reasons, as a territorial one. However, the limited territoriality proposed in this paper—albeit an oxymoron in cyberspace— should be upheld for practical reasons as concern will be limited to certain scattered examples mostly from Morocco.

It is imperative though to underline the fact that bringing forth the idea of the preservation of a PO alongside the discourse and claims made by Advocacy Groups (AG) in keeping with HR paradigms cannot be conceived outside the framework of a security discourse. This brings into play the opposition and potential conflict between rights —which need to be secured, basically by the State institutional apparatuses— and the responsibilities which also need to be safeguarded by the same State institutions. This form of security concern has only been recently advanced as one that the State should provide for. Given this novelty, there is need to define first of all (i) what it consists of and (ii) what different schools and academics in the domain acknowledge as "security". Such a step seems necessary as it would help understand how the concept of PO and security collide, as well as the way they have evolved over the years and may continue to evolve as the cultural context worldwide continues to change.

To bring more light into such issues, this paper attempts, in its first part, to lay bare the theoretical underpinnings of such an endeavour by defining the various and relative approaches to the issue of security and how it ramifies and relates to both the preservation of the rights of the individuals and the responsibility the authorities and the CS have to abide by to uphold PO, particularly at a time where paradigm shifts seem to have stronger effects on governmental biopolitics.[2] The second part will be more practical as it brings to light the conflict(s) rising from such interpretations of the law and the HR provisions more specifically as they relate to the uses and abuses perpetrated against and by CSM users. Illustrations of such practices will be brought through a cursory study of a corpus of documents exchanged via one of the commonly used CSM (WhatsApp) which offers easier access and use of cyber-texts and videos.

On the Concept of Security

Speaking of security in a digital age should not be done without looking at the cyber-culture, its technology which is developing at a rapid pace and the impact it has on concerns vested by the CS and governments alike. The latter are more focused, now more than ever, on the uses of CSM, which are becoming more pertinent and complex as they keep evolving, and as the conceptions of 'security' become more oriented towards preserving public welfare through respect of HR, particularly FEI wherein lies the concern of this paper.

[2] For more details on the concept, see Jacob Nilsson and Sven Olov Wallenstein, *Foucault, Biopolitics and Governmentality*, Solderton Philosophical Studies, Solderton University, The Library 2013.

The Webster online dictionary[3] offers a variety of meanings and connotations associated with the term “security”; but it mostly associates it with the concept of “threat”. Political philosophy and discourse, in general, fuse the two making them into one non-separable concept. This has been the case at least in the report produced by the International and Strategic Relations Institute[4] (ISRI) in which the authors combine both the term “threat” and “security” in the sense that a threat is an act that disturbs a state of ‘quietude’ producing thus a state of insecurity. The same report goes further as to fuse both external threats and security with international peace and stability:

> all States put an emphasis on the fact that there is a progressive disappearance of the demarcation between external security and internal security. External security threats are becoming internal security threats, and nowadays, they are starting to overshadow ‘traditional’ threats of delinquency and criminality.[5]

The report also emphasises the different conceptions between countries on what the scalable concern of their security priorities should be; a fact which relativizes the concept.[6]

On the same issue, one may focus on the differences and/or the similarities of the conception of security/threat paradigm between the various schools of political thought, notably the Realist School, the Liberal and the Constructivist. The first offers what one may call a doctrinal conception of security (Wohlforth 2010:10) as being generated by a state of anarchy and eventually leading to war. It should, therefore, be kept under check either locally or regionally and/or at the international level by forming alliances (groupisms) to keep a certain balance of power even through a Zero-sum-game (Hens

[3] The Following definitions are taken from Merriam Webster Online Dictionary. security means: 1. the quality or state of being secure: as a) freedom from danger; safety: (b) freedom from fear or anxiety; (c) freedom from the prospect of being laid off (job security); 2. (a) something given, deposited, or pledged to make certain the fulfilment of an obligation; (b) surety; 3. An instrument of investment in the form of a document (as a stock certificate or bond) providing evidence of ownership; 4. (a) something that secures: protection; (b) (i) measures taken to guard against espionage or sabotage, crime, attack, or escape (ii): an organization or department whose task is security. web: http://www.merriam-webster.com/ dictionary/security accessed 23rd September, 2016.

[4] Jean-Pierre Maulny and Sabine Sarraf, “Assessment and Prospects of Security Threats: Synthesis Report for the International Forum TAC (Technology Against Crime) 2016. IRIS, April 2016. Web. See IRIS: *Institut des Relations Internationales et Stratégiques* —

[5] Ibid. p.3

[6] “The definition of what can constitute asecurity/threat is subjective and scalable. It depends on the point of view from which it is determined. It is noticeable that different countries do not tackle security in the same way. Whereas France and the Netherlands favour an approach based on the intended security objective, such as territorial protection, economic stability or health security; other contributing countries take an interest in security on the basis of identified threats. Consequently, the Dutch and the French consider that security covers a broader range of hypotheses, taking into account unintentional threats such as major natural disasters or technical failures. It is an exhaustive definition that does not exclude a prioritisation of the threats, even though this exercise is not necessarily codified in a text. However, a majority of countries understands the notion of security as meaning safety, that is to say the fight against a malevolent intention or action” Ibid. p. 3

Morgenthau 1979). The overarching paradigm of such an approach is that violence is State-centred. The later should provide for, albeit, a semblant of security referred to as “hegemonic security” (Wohlforth 15). The second (the Liberal School) levels criticism at such a concept on the grounds that it never considers internal affairs as part of the security States should provide for. In the aftermath of WWII, this becomes the rallying cry of AG armed in their legal struggle by the Covenants and Treaties (the Charter, the UDHR and the various protocols) drafted by the UN. The concept of alliances and groupisms also came under fire by the succeeding school, namely the Constructivist (Mutiner 2010), through the alternative offered by focusing on strengthening democracy, friendly relations and building up economic interdependencies and credible international institutions (Rousseau and Walker 2010). This approach which has brought necessary attention to internal security (economic and social) is basically a philosophical and sociological perspective on things inspired by Post-Structuralist and Post-Modernist thought (Critchley 1998).

Such drives have, as a result, produced a grab-bag of security issues related to societal problems, environmental issues, economic ones and in later years human mobility crises (Ardau and Munster 73). This has opened up the theory on security as to include a biopolitical dimension —to quote Michel Foucault’s work on *governmentability*[7]. These new dimensions point out to the necessity of changing our conception from one concerned with State sovereignty —à la Carl Schmitt[8]— to one where “the biopolitical manages the well-being and life changes of the populations (Ardau and Munster 75). This has, indeed, paved the way for a focus on non-standard security issues as identity issues, threatened by the globalizing drive, health issues and the pandemics that have become common over the last few decades, transnational crime in the form of drug and human trafficking, economic and poverty issues and their role in human trafficking, forced and voluntary mobility of humans across the continents, religious and nationalist issues, environmental issues closely related to migration and the ethnic imbalance they lead to worldwide (Thiery Balzacq 2010).

As a notion that has brought additional value to the meaning economy of the discourse on political decision making, the concept of *governmentability* and biopolitics is central to the present work in that it enables to find a level ground between HR —basically FEI — and the preservation of PO at an age where cyber-technology is making such a balance difficult if not impossible to keep. Such a task, in fact, is problematic because nation-states’ politics is still trapped within the bounds of a solidified territoriality conception that is becoming more and more obsolete and irrelevant. Yet, it would be a state of denial to say that as we progress into the 3rd decade of the 21st century, the

[7] For further information see Inda, Jonathan Xavier (ed.) *Anthropologies of Modernity: Foucault, Governmentality, and Life Politics*, USA. Blackwell Publishing, 2005

[8] Carl Schmitt conceives of security as an issue of survival for the State and therefore treats the idea as one friendly enemy binarism.

strategic discourse of the state of exception[9] is a thing of the past. In the recent past, events show State concern for safeguarding PO and political stability, the two being a major priority even if that meant abusing HR provisions. Indeed, one still sees a survival of conventional measures such as the state of exception which has been enacted by States in the form of a "*kill-switch"* cutting off the links of the Net and preventing users from accessing a certain number of programs and information deemed threatening. Obama threatened to do so[10]; Egypt did so during the Arab Spring (2011); the California BART actually shut down phone connections in 2011,[11] preventing commuters from accessing programs for fear of fomenting trouble; David Cameron also threatened to do so during the London riots (2014); and in the last few weeks of November 2019 the Iranian enacted their *Kill-switch* to prevent the spread of riots[12]. The overriding principle that filters out from such acts is that security agencies have been forced to incorporate cybersecurity norms and practices when two or three decades ago that has never been envisaged as a part of any political program. Now more than ever, it is a mobilizing principle which captures more attention and requires more capabilities than some States can offer. It is not clear though if the Moroccan *Diréction Générale de la Sécurité des Systèmes d'Information* (DGSSI) nor if *La Commission Nationale de la Protection des Données* (CNPD) have ever intervened by using the *Kill-switch* even at times of serious crises. Privacy International has indeed reported that Moroccan security agencies have purchased surveillance technologies, but it is not clear if they have ever been used albeit permissibly[13].

It is also significant, for the purpose sought in this paper, to underline that such draconian measures have shown their limit since users of these CSM have found ways to circumvent them and access the information they want through VPN capabilities. States have also realized that such practice may cause more damage to their own economies and make sure they consider all odds before

[9] Carl Schmitt's premise of "state of exception whereby exception produces not only sovereignty and homogenous political communities, but also minor images of bare life; i.e life that can be killed with impunity" (Ardau and Munster 75).

[10] Protecting Cyberspace as a National Asset: Comprehensive Legislation for the 21st Century: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs, 111th Cong. (2010), available at http://www.hsgac.senate.gov/download/2010-06-15-reitinger-testimony (statement of Philip Reitinger, Deputy Under Secretary, National Protection & Programs Directorate, Department of Homeland Security) ("Section 706 of the Communications Act and other laws already address Presidential emergency authorities and Congress and the Administration should work together to identify any needed adjustments to the Act, as opposed to developing overlapping legislation.").

[11] See Jennifer Spencer "No Service: Free Speech, the Communications Act, and BART's Cell Phone Network Shutdown" *in Berkeley Technology Law Journal* Volume 27 Issue 4 Annual Review 2012 Article 20 6-1-2012. See also Mirae Yang "The Collision of Social Media and Social Unrest: Why Shutting Down Social Media is the Wrong Response" in *Northwestern Journal of Technology and Intellectual Property* Volume 11 | Issue 7 Article 7 Fall 2013.

[12] It is not clear how much of these similar measures have been undertaken in the proliferating hot places round the world in this year alone.

[13] Cf. Privacy International, « State of Privacy in Morocco: Surveillance capabilities" privacyinternational.org, pp.5-6, January 2019. Web: https://privacyinternational.org/state-privacy/1007/state-privacy-morocco
Retrieved on 31st January 2020.

they activate it. Egypt for instance, woke up, in the aftermath of its Spring (2011), to realize that it has shot itself in the foot by using the *Kill-switch*. Estimates available show that within the 5 days that the Net has been shut down, the country has lost closer to $90 million dollars; and although no figures have been given, estimates speak of more loses than advanced in the days that followed[14].

Given this state of affairs, the issue at stake here is how nation-States — Morocco in particular— can ensure albeit a semblant of reasonable balance between the PO they are entrusted with in a cyberspace that slips away from their control at a very high speed; and respect the HR provisions they have signed for. For some, such a situation premises the demise of nation-State sovereignty as this became superseded by independent actors (non-State) who may have cyber technology capabilities and expertise they can use to their advantage.

This dilemma —one has to confess— is more challenging for developing and under-developed countries, Notably Morocco. In fact, if developed countries — with more advanced cyber capabilities— are struggling to set up a balance between the necessity to keep their cyber-space free and democratic and the safe-guarding of PO, the challenge for developing and/or underdeveloped countries with less cyber capabilities is incommensurable. They lack the technology and the expertise that goes with it. It would be fair, however, to say that Morocco has been struggling in the last part of the 1990s and more specifically in the last two decades to jump on the bandwagon of cybertechnology by trying to facilitate Internet penetration and use. The country is also making giant strides in its attempt to build up institutions likely to help improve the securitizing aspects of the users and the data being processed.[15]

What is more disheartening is that there is a paradox resulting from such a situation in a flagrant manner; one brings to mind the foundational principles of the objectives set up by the Information Society in their drive to democratise information and knowledge.[16] Indeed, far from providing these countries with

[14] Ibid.

[15] This assertion is based on a recent publication "The State of Privacy in Morocco" by Privacy international.org in January 2019. According to the report, penetration has reached 22.54 million users by the end of 2017 bringing the rate of Internet penetration to about 64% one the highest in the region. Web: https://privacyinternational.org/state-privacy/1007/state-privacy-morocco Retrieved on 31st January 2020.

[16] The principles, in question, have been a subject of debate during the summit held in Geneva on 12th December 2003 and summed up as a Declaration of Principles which is given in the following pledge: "We are resolute in our quest to ensure that everyone can benefit from the opportunities that ICTs can offer. We agree that to meet these challenges, all stakeholders should work together to: improve access to information and communication infrastructure and technologies as well as to information and knowledge; build capacity; increase confidence and security in the use of ICTs; create an enabling environment at all levels; develop and widen ICT applications; foster and respect cultural diversity; recognize the role of the media; address the ethical dimensions of the Information Society; and encourage international and regional cooperation. We agree that these are the key principles for building an inclusive Information Society." See World Summit on the Information Society, "The Geneva Declaration of Principles and Plan of Action", Geneva: December 2003. Web. http://www.itu.int/net/wsis/docs/geneva/official/dop.html, accessed on 12th October, 2016.

the golden fleece promised, these States realize that they need safe-guards against abuses that such technologies offer to pernicious users who seem to relish this anarchical situation wherein States and civilians have become sitting ducks of cyber-nerds of all kinds, threatening their identity, their property and even their well-being. A review of the discursive practices, laid out above, shows that new economies of meaning that have evolved to express growing concern with issues of security are very porous. Subsequently, the section below will attempt to shed some light on such types of discourse by clarifying the evolving epistemologies surrounding PO.

PO, FEI and the use of CSM on the Balance

So far, PO has been treated with much latitude as it has been taken for granted that it be equated with the insecurity coming from outsiders as well as insiders. While this can be true even in the scope of the present work, it remains a notion that needs circumscribing to be accounted for in a way that narrows the scope of confusion. One of the definitions provided by Bernard Stirn (2015) describes it as a fundamental notion that is very polysemic because very difficult to circumscribe even by certain judges who, sometimes, need jurisprudential updating to remind them of what it is.[17] He also speaks of a material PO that is made clear through the Presidential directives or Royal decrees (Dahirs) that municipalities, counties and provinces have a duty of preserving. For instance, the French municipal law of 4th April 1884, article I, 2212-2 of the *General Code of the Territorial Collectivities* stipulates that "the municipal police is tasked with ensuring good order, surety, security and public wholesomeness".[18] In a way, this covers a large number of essential values that benefit from the consensus of the community. Yet, this also makes it a very porous notion and underlines its relativity through time and space. As for space, countries, each in its own way, determine what for their community can garner consensus and constitute a PO that suits them. Some countries, for instance, may tolerate gay-mating; others would create laws to reprimand it[19]. It follows then that the territorial dimension may be a factor in the determination of the PO worldwide even in a cyberspace. The temporal factor can also be determinant as laws/regulations change over time even on the local level; what is acceptable today may not have been a few years back and may not be in years to come.

Notwithstanding all these peculiarities, with cybertechnology —our focus in this paper— the territorial dimension evaporates opening up the notion to

[17] The actual definition provided is the following : President Odent explains that PO is "un moyen relatif à une question d'importance telle que le juge méconnaitrait lui-même la règle de droit qu'il a mission de faire respecter si la décision juridictionnelle rendue n'en tenait pas compte » (2015 :1).

[18] For the pertinence of it we provide the original article of the law : "la police a pour objet d'assurer le bon ordre, la sûreté, la sécurité et la salubrité publiques" (2015 :1).

[19] For further information on the relativity of HR norms see Marie-Louisa Frick, *Human Rights Relative Universalism*, USA: Library of Congress, 2019.

more and faster changes even if certain countries are not yet ready for the changes proposed. This creates more challenges for the policing and may probably lead to unrest. Recent literature on this treats the issue as one pertaining to an International Public Order (IPO) (Winston Nagan and Craig Hammer 2007); one that is extraterritorial, supra-national creating thus more challenges to PO safe-guarding because the world has not yet created such an encompassing legislation likely to help determine what an IPO would look like.

In the official or quasi-official political discourse, as shown above, PO is turned into a text open to various interpretations; but it is a fact that the official political discourse on security has always been conceived within a framework bound by economic and security interests of the parties at stake; to see it otherwise would be a blindness à la Paul de Man (1971). Discourse on PO has to be conceived as a strategic representation of interests since it should determine the geopolitical interests of the State. Having been described in the literature as a possessor of the monopoly of violence, the State is also endowed with the monopoly of truth, since no discourse (Media, official or otherwise) has salience unless the State determines what, how, why, when, and where its importance should be (Shapiro 1990). But history also shows that discourse on HR has always been subject to a practice that takes into consideration political and economic interests of the stakeholders. The literature on HR, ever since its inception in the UDHR (1947), is replete with examples of discourses and counter-discourses —sometimes held by the same actors— whereby one position, fervently defended, has been countered by another position quite antithetical to it by the same actors when their stakes changed. France and Great Britain, so much opposed to the application of HR in their respective colonies, have jumped on the bandwagon to defend the same rights when the heat generated by the Cold War required that they defend such a position[20].

One would find a porous ground in the same discursive economies upheld by actors in the international scene in this cyber-age. The position of countries like the US and the UK when it comes to HR discourse with regard to freedom of the Internet and the respect of privacy for instance —a discourse they saddle when it comes to practices by States they consider authoritarian— is a very edifying illustration. Notwithstanding their cosmopolitan ethical discourse they hold, the most flagrant abuses of HR in the present age, however, have resulted from States with more cyber-capabilities (so-called 1st tiered) (here the UK and USA among others); not only against 2nd, 3rd and non-tiered States, but also against their own citizenry[21]. Even the legislation they have come up with is not capable of preventing such abuses from happening because it is produced under a political discourse that is so confusing that it gets mired in conflicts of laws. In the section below an extensive approach to such contradictory discursive practices will be attempted. Focus will mostly be on CSM and the possible threats they face and/or may constitute. This will be done through a study of a corpus of CSM documents as suggested previously, followed by a

[20] See Dellal 2017.

[21] Ibid.

qualitative assessment of the results of a survey recently conducted on a student population on the same issue.[22]

Determining the Norms

The following questions underpin most of the endeavour to be conducted in the study and debate that follow in the sections to come.

1. How are the notions of "security" vs "insecurity" —as they relate to discourse on HR— produced by discursive practice via the CSM?
2. Does not this mean that one has to argue for the textual productions on CSM (documents and videos) as narratives involving a certain rhetoric hinged on binarisms between hostile vs friendly; violent vs soft; true vs false, etc.?
3. Being narratives, should not their value rest on the interpretative moves of the receivers? Or could it not also rest on the way they are articulated?
4. Because we are concerned with HR discourse production by two different and sometimes opposing forces (the State and the CS) should not the value of truth and untruth be measured against pre-existing or potential provisions of such HR discourse by official agencies and/or legal documents?
5. But more importantly, since the purpose is to speak about a match between discourses on HR, CSM and PO, should one not look at the competing claims for truth each text produced creates?
6. Does the claim for truth give authority to some discourse over the other? Or does the resulted-act constitute a violation of rights of other discourses which also claim a truth status?
7. What would be the criterion to use to draw a line between right (then allowed because it supports PO) and wrong (because it disturbs it)?
8. Can an official interpretation of HR trump the other interpretations simply because it is official? If so, then the difference between official and unofficial would be simply a question of discourse generated by a specific economic, political and social context. For example, a discourse produced by Right winged governments can be trumped by a context where a Left winged ideology is dominant, and the opposite can be true. It should be clear, then, that this is not a claim for a third discursive type, but one that draws attention on discourses that are context-bound; a fact which makes them very volatile and relative.
9. But more urgent is the question of whether CSM have any influence on the discursive economy of the official discourse and decision making worldwide and locally (Morocco).

[22] See Dellal's Doctoral Dissertation on *L'Ordre Public, le Droit d'Expression et à L'information dans le Cyberespace MENA : le Cas du Maroc* Faculty of Law, Mohamed I University, Oujda, Morocco, Forthcoming.

10. Do CSM users have any knowledge of HR provisions by local juridical texts, or not? Do they acknowledge their responsibilities as well as their rights? Or do they privilege their own readings of the provisions?
11. Do NGOs —as defenders of Net-users— use pressure to implement and/or introduce new provisions where they are missing? Or do they content themselves with the existing ones?
12. Does the nature of the narrative produced by CSM respond to some criteria of Truth? Quality of information? Or is it fabricated? Or amateurish needing in quality?

All these questions are premised on the basis of the following hypotheses:

1. CSM can enhance HR respect by States that come under their pressure if Internet access is kept free;
2. CSM may be used to disturb PO by agitators and/or users who have no knowledge and/or respect for HR.

The verification of such hypotheses may be done through: (i) a comparison of three (3) corpuses of documents from WhatsApp selected over three different periods; 2 documents, for illustration, will be analysed to show the vulnerabilities and/or strengths that the CSM use can lead to with regard to the preservation of HR and PO; (ii) the use of a survey conducted on a locally varied student population[23] within Moroccan High schools (Larroui) and different schools within 4 universities scattered in the North, East and South of the country[24]. This reading will help substantiate some of the arguments advanced to show the vulnerabilities, the contradictions and conflict laws that undermine the balance between the PO and the use of CSM in Morocco.

Case-Analysis: Crowdsourcing and/or Propaganda

The cases taken for this analysis through a cross-sectional selection are part of a corpus borrowed from WhatsApp given the facility it offers to record and exploit the documents. In fact, these have been collected over three different periods of time to see the change, if any, and the evolution they would take. Most of the selections are made up of chats to which I have been party since the last six or so months of 2016 and extending to the last months and weeks of 2019. The first selection is made up of documents of 2016, the second

[23] Actually 600 students have been touched by the survey, but on 581 have responded by filling the questionnaire handed to them. The results are included in a table appended in the end of this document.

[24] The University Schools surveyed are: Faculties of Letters and Humanities in Mohamed I University, Oujda and Nador; University of Abdelmalek Essaadi, Tetouan; University of Ibn Zohr, Agadir; The School of Business and Management, Oujda; the School of Applied Sciences, Laayoun.

includes chats from 2017 extending to the first part of 2018, while the third includes documents of the 2nd part of 2018 and the whole year of 2019.

These chats have been segmented based on the fabric or technical features used in their making; but they have also been segmented in terms of the content they convey. Subsequently, the segmentation has resulted in two major categories: (i) Written/Text Documents (TD) and (ii) pictorial and Videographed Documents: videos and photos or pictures (VD). In terms of the content, we have three major categories of documents: (i) those which are politically motivated which also could include both TDs and VDs (these chats would cover anything that has to do with politics and official policies); (ii) chats with pornographic content, also including both TDs and VDs; (iii) fun-oriented chats which could include funny story and jokes also in both forms.

While this last category, generally, does not seem to breach any rules be they of compliance with the laws in vigor or any form of ethical behavior, the other two previous categories namely the porn and the political do produce much more cause for concern as some of them seem to bathe in propaganda, information that cannot be verified or even pure disinformation as some of the documents brought for the purpose can duly demonstrate. Indeed, two of the documents on the exchangeability of the Dirhams[25] (one a TD and the other a VD) show discrepant quality as to the way and the validity of the information they want imparted. For the purposes of illustration, two documents will be closely looked into: one in the form of a Video (a Power Point Presentation) with audio visual components to help improve communication, while the second is a TD on the same issue. The purpose is to show how discourse and counter-discourses are built to voice points of view on some social and political issues. Both, indeed, deal with the same topic, namely the exchange-rate flexibility of the local currency (the dirham). It is my understanding that the video voices an official or quasi-official point of view concerning the decision of the flexibility, while the second illustrates a counter-discourse to the official one on the same topic. Their political pertinence is the main focus of the present endeavour. This will be determined through a close look at the information purported; its truth-value, the rhetorical style at the illocutionary level and the perlocutionary function both documents may have.

In the VD —signed by Attijari-Wafabank, at least according to its logo— the presenters have opted for a simplification of the style of rhetoric applied as they illustrate each and every piece of information advanced. Statistical data are provided and simplified so as to make it accessible to the profane users to the domain of finance and banking. The content is presented in two major parts with the first explaining the situation of the currency under State control. This part also brings forth the advantages and drawbacks of the current system. The second part presents the flexible currency, its difficulties, but mostly its advantages. This is believed to be the official and/or quasi-official position. The function being one of imparting information for fear some ill-intentioned contender may take the opportunity to call for civil disobedience in anticipation

[25] This being the local currency of the country. 10 MAD is about 1 US $.

of the worsening conditions for the population. Over and above, this also shows how the State is resorting to crowdsourcing on CSM to counter the anti-state propaganda.[26]

The TD, however, uses Moroccan Arabic, written exactly in the same alphabet as that used for Classical Arabic. This being an issue on its own because it is believed that those who can read the message may just as well read it in the formal language (Classical Arabic). But resorting to such a form of language (Moroccan Arabic) has a strategic, populist appeal to the people much in keeping with the left-wing propaganda of the 70s[27]. The text also provides statistical data to illustrate the gravity of the situation. For instance, the current value of the dirham compared to the dollar (not the Euro, the choice here being ideological more than anything else) is 0,12 (or 0,1) predicted to go down to 0,00000000001 to show its falling purchasing value. An actual comparison is made between the price of a washing machine purchased in Spain for 4000.00 MAD before the flexibility system which would end up at 10000.00 MAD after the flexibility becomes effective. The information is also compounded with reasons that this, like so many other measures, is imposed by the Britton Woods Institutions, and that the country does not have any choice; a remark reminiscent of a discourse of the Cold War period, but mostly of the hostility shown towards market economy discourse. What is more, the text is not signed and appears to be relayed from some other unknown source. The sarcastic style, in addition to satirical language used, show that the text is an anti-government propaganda. The deficiencies are, however, stark and staggering as the text needs depth, and has no compelling analysis likely to show the reasons why these fluctuations should actually take place. This shallowness shows that the author is more concerned with the political impact of the message rather than the truth-value of the information imparted. The likelihood, subsequently, is that viewers of the two messages would be more impressed by the depth of the VD through the pedagogical and professional approach used to convey the information rather than the sarcasm of the TD. But it is true that partisanship would determine which document would appeal to the readers most[28]. While no such documents can be selected from the other two latest selections, it is not clear whether this is a result of censorship laws being enforced or if it is the *chilling effect*[29] that led to some sort of self-censorship. This may also result from the CSM platform owners enforcing their new conditions of use, very restrictive in the view of some AG. One needs not

[26] See Dursun Peksen et al, "Media-driven Humanitarianism? News Media Coverage of Human Rights Abuses and the use of Economic Sanctions", in *The International Studies Quarterly* V.58, 2014 pp. 855-866. These authors explain that the State has to learn to use a counter discourse to dispel the doubts and suspicions of the public as to some of the news reports relating to public policies.

[27] One may easily recall the controversial daily humorist paper *Akhbar Essouk*, which was very popular among educated elites in the 1970s.

[28] Cf. Dellal "Information Society; Human Rights and the Security Dilemma", 2016.

[29] Cf. definition on the online dictionary which is "a discouraging or deterring effect, esp. one resulting from a restrictive law or regulation", web: https://www.collinsdictionary.com/dictionary/english/chilling-effect, retrieved on 2nd March 2020.

write off the possibilities of abusive uses be it on the part of the users or on that of the enforcing agencies. The staggering diminution and disappearance of such documents, though, is a matter that requires further probe that this work does not have space for at present.

The same can be said of porn-oriented documents which are very problematic specifically when they are used for revenge or to ransom some people or when they are about and addressed to teenagers. One example of revenge and ransom porn can easily be invoked in the case of the Berkane Blackmailer.[30] The guy video-taped women in very compromising positions because he had tricked into believing he had healing powers. His attempts to blackmail some of them ended up in disaster apparently leading to his being molested by vigilantes and eventually his arrest. Another similar story (known as *Hamza Mon BB*[31]) has been going viral on social media over the last few months. It is also alleged to be a case of blackmail and revenge-porn. But as with political-oriented documents, the last 2 sections do not include any revenge or juvenile porn; yet most of the porn is adult oriented.

Challenges and Perspectives

What the two examples show is that there is a propensity to use CSM (here WhatsApp) as platforms for political activism because they allow to touch a larger public given the fact that mobile-use penetration (64 % according to Privacyinternational.org) is one of the largest as the statistics would show.[32] The statistical data collected as a result of the survey conducted on the student population (581)[33] show that 90.9% of the respondents possess either a PC, a smart phone or a tablet or all the three at the same time.[34] But it is fair to say that there is a least one mobile (smart) phone in every household and computer penetration is growing in leaps and bounds too. Preference for smart phones, therefore, is motivated by such a wide-spreading of the 3G and 4G internet connectivity even in the remote areas of the country.[35] But this is an area that deserves closer researching, something the present work does not have space for. What is certain, though, is that users now do employ their smart phones to record and relay any information (TDs and VDs) on CSM that they see endowed with political and social potential to make a change. The following chart shows the fast growth of the chatting communities among the respondents.

[30] See Dellal, 2016. op.cit.

[31] See Safaa Kasraoui "Morocco Sentences 3 Suspects in 'Hamza Mon BB' Backmail Case" Web: https://www.moroccoworldnews.com/2020/02/293503/morocco-sentences-3-suspects-in-hamza-mon-bb-blackmail-case/ retrieved on February 13th 2020.

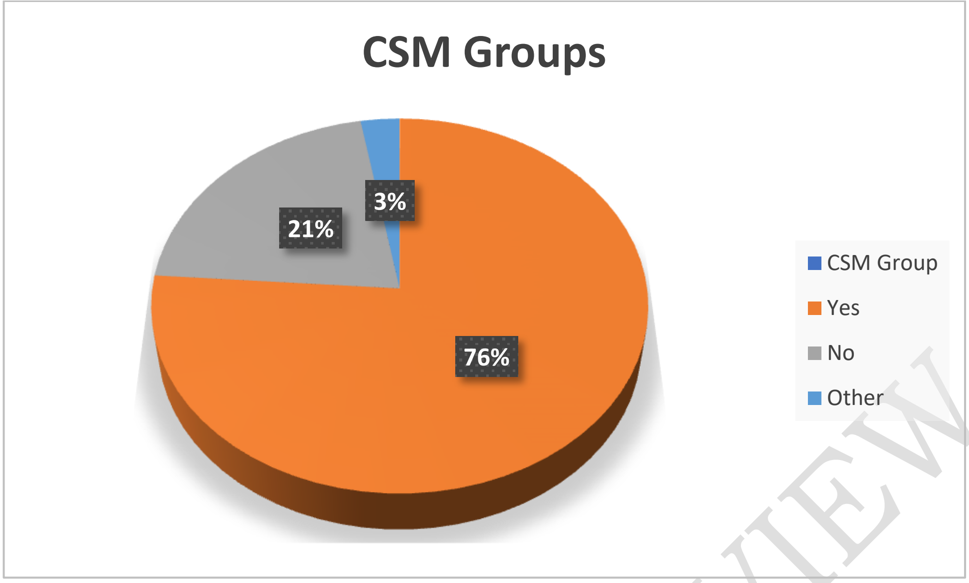
[32] See privacyinternational.org. op. cit (January 2019)

[33] See Table appended in the end of the document.

[34] See appendix 1

[35] Based on estimations of list of countries by smartphone penetration measured by the Pew Research Centersurvey conducted in 40 nations among 45,435 respondents from March 25 to May 27, 2016.

Chart 1. *Chatting Communities*



What is obvious, however, is that these communities spend more time —at least one hour a day—[36] relaying information with a rapidity that has never been seen or imagined before. An event that took place in a remote vocational and professional training school in Ouarzazate, showing a teacher being molested by his own student, has consternated people in Dahkla (in the extreme south), Oujda (the extreme north east), Tangier (in the north) and possibly every corner of the country in a record time. There is a possibility that the video may have been relayed to viewers outside the country. A copy of the same video has been posted back to viewers (including myself) in the country by Moroccan residents in the United States. A few days later, the government felt concerned and decided to issue a communiqué addressing the problem and bringing directives to condemn violence at school and requesting some tough measures to remedy the situation. The same reaction has been seen with regard to the incident involving the tragic death of a fisherman in Al Hoceima.[37]

It is therefore important to underline that the State would have to struggle hard to gag the people given the possibilities offered to them by these CSM. They now have voices stronger than the ones the public of Socrates in Athens had; they can voice their grievances as vehemently as they can. What is at stake though, here, is not much the FEI, but the fact that such a freedom can be abused either by the State which sees itself threatened or by the users who may trespass their responsibilities and threaten to disturb the PO as shown in the examples quoted above. Aware of this threat, States decide to react by using

[36] Reference is made to the same survey which shows that if we add up the 48% who are connected for 3-to 4 hours to 47 who are connected for 1 hour we end up having 95% of the respondents who are connected for at least 1 hour a day which is a significant amount.

[37] See Safaa Amrani, "Morocco protests after fisherman crushed to death in a garbage truck", the Guardian, web: https://www.theguardian.com/world/2016/oct/31/morocco-protests-after-fisherman-crushed-to-death-in-a-garbage-truck. Retrieved February 13th, 2020.

the same kind of tools either through cyber-militia or through outsourced agencies (crowdsourcing) to cut the grass from under the feet of malevolent authors. The example of the video by Attijari-Wafabank is an illustration of how States react to the use of CSM. This brings us back into questioning the boundaries of the rights and responsibilities of the users.

For a better illustration of such conflict, it is compelling to focus on what the law provides to combat abuses. To that end, a look at some cases —the ones stated above— can be helpful. But these cases, it has to be underlined, show that the Moroccan cases are not isolated ones should they be put in an international context as the cases of Chelsea Manning[38] and Edward Snowden[39] would show.

Public Order, CSM and the Moroccan Law

As suggested above, PO is normally guaranteed by law, although the type of PO facing extraterritoriality may not be clearly determined as such. In the *Moroccan Penal Code* —revised and issued on 15th December 2015, in other words, the most updated law so far— PO may be circumscribed along very diffuse provisions scattered around the chapters of Livre III[40]; basically, all of 'Titre Premier' which deals with crimes and infringements against the law. The crimes determined in this section (from article 163 to 607) determine the range of practices in keeping with PO and those likely to be considered as transgressive. In sum, these vary from threats to the royal family, to the regime in general, to espionage and illegal dealing in intelligence, to terrorist activities, illegal and abusive activities on the part of the citizens to those committed against these citizens by the law enforcing agencies. But it has to be underlined that the boundaries are still hazy and sometimes incomplete as the loopholes left by the legislation are plenty as can be seen in the gaps left by articles as the following one can show. Indeed, article 194 stipulates that:

> Is guilty of infringement against the external security of the State and is punished with imprisonment of one to 5 years and a fine ranging from 1.000 to 10.000 dirhams, any Moroccan or alien, who in the state of war, conducts an act as to cause nuisance to the national defence other than those enumerated in the previous articles (my translation).[41]

[38] Simran Hans, "XY Chelsea review – in search of the real Chelsea Manning: A documentary about the trans activist and ex-army intelligence officer is intriguing but lacks wider context", the Guardian, May 26th, 2019. Web: https://www.theguardian.com/film/2019/may/26/xy-chelsea-manning-documentary-film-review. Retrieved February 13th, 2020.

[39] Dave Davies, "Edward Snowden Speaks Out: 'I Haven't And I Won't' Cooperate With Russia" npr. September 19th 2019, web: https://www.npr.org/2019/09/19/761918152/exiled-nsa-contractor-edward-snowden-i-haven-t-and-i-won-t-cooperate-with-russia?t=1581591876947, retrieved on February 13th, 2020.

[40] The version referred to has been downloaded from the Net on 02/02/2018. It is available on the following: http://adala.justice.gov.ma/production/legislation/fr/Nouveautes/code%20penal.pdf

[41] The original article stipulates : Article 194 :

This undecidedness apparent in the use of language (an act as to cause nuisance) on the part of the legislator creates a deliberate ‘empty category’ likely to be filled by any type of crime that the legislation does not know of and which may appear in the future; Cybercrime being one, on condition that the State provides proof that it would harm it in a way the legislation would determine later. This empty category may be considered a shrewd way to frame potential crimes by CSM users and cyber-delinquents, in particular. It also betrays an incapacity to predict, with exactitude, what the law is trying to sanction. Defence lawyers would inevitable invoke the famous adage ‘*nullum crimen sine lege*”, which means that a crime would have to be determined ahead of time before it is treated as one. These are the same incapacities that cyber legislation is facing because cyberculture is in the making; and consequently, many things can either remain unsanctioned or wrongly sanctioned as long as a crystal clear law is not brought up.

Similarly, although a little more determinedly, article 196 (paragraphs 2,3,4) can be of some pertinence in determining behaviour on CSM as they deal with correspondence, reselling of documents to foreign agencies or individuals. This indeed might be an article that sanctions any crime that CSM users could indulge in.[42] Article 218-1 (7) is specifically and clearly data related and applies the same sanctions to any wrong doer. However, article 218-5 clearly incriminates any attempt to “incite, persuade, or provoke any of the infringements stipulated in articles 218-1 through 218-5”. These also open up a wider bracket as jurists would have to conduct a very controversial search to determine what semantics to privilege to determine the content of the terms like: ‘incitement’, ‘persuasion’ and/or ‘provocation’. This again looks like another empty category, a grab-bag that would include any act that the law cannot determine in a clear-cut way. This brings us back to the same stalemate situation as with article 194 invoked above.

Notwithstanding all these ramifications, the problem of attribution would remain the stumbling block despite the headways and breakthroughs achieved by security experts and emergency task forces.[43] In fact, ascribing a crime to an

« Est coupable d'atteinte à la sûreté extérieure de l'Etat et puni de l'emprisonnement d'un à cinq ans et d'une amende de 1.000 à 10.000 dirhams tout Marocain ou étranger qui, en temps de guerre, a accompli sciemment un acte de nature à nuire à la défense nationale, autre que ceux énumérés dans les articles précédents ».

[42] Article 196

2°Tout Marocain ou étranger qui porte sciemment la correspondance des auteurs d'un crime ou d'un délit contre la sûreté extérieure de l'Etat ou leur facilite sciemment de quelque manière que ce soit la recherche, le recel, le transport ou la transmission de l'objet du crime ou du délit;

3°Tout Marocain ou étranger qui recèle sciemment les objets ou instruments ayant servi ou devant servir à commettre lesdits crimes ou délits ou les objets, matériels ou documents obtenus par ces crimes ou délits;

4°Tout Marocain ou étranger qui sciemment détruit, soustrait, recèle, dissimule ou altère un document public ou privé qui était de nature à faciliter la recherche du crime ou du délit prévu aux paragraphes précédents, la découverte des preuves, ou le châtiment de ses auteurs.

[43] Morocco has also created a task force to remedy cyber emergency crises: Diréction Générale de la Sécurité des Systèmes d’Information (DGSSI), the Moroccan authority responsible for computer

IP address may seem simple, but it would require more evidence to show who actually has been operating the computer, the phone or the tablet or whatever gadget has been used to commit the felony. *Botnet-herders*[44] can operate whatever machine they want from any distance making attribution a bone of contention among jurists. This lack of clarity and completeness of the law are issues that have an international dimension as the cases of Manning and Snowden have shown and a few more courts around the world.[45]

In line with the same policies, constitutions around the world have also set up restrictions on the condition for the exercise of FEI, bringing laws into conflict. Although the 1st Amendment in the US Constitution sacralises freedom of speech, there have been attempts by the US Administration to curtail it. Examples of such tug-of-war between the conflicting legislations proposed worldwide by States and the CS are plenty but short of time we may restrict our attention to only one example. The Moroccan constitution (2011), like many other constitutions around the world provides the same guarantees as those provided by the UDHR for its citizens to exercise freedom of speech (expression) and opinion.[46] Likewise it also provides for freedom of the press; an activity that bloggers and chatters on CSM indulge in, presumably most of the time with no knowledge of such a law. As a matter of fact, the survey invoked above shows that 33% of the respondents are not aware of the existence of any legislation regulating the imparting of information on CSM. If one adds up the number of non-opiniated respondents (13% to 33%) who did not know of any laws, one ends up with 46% which is a massive number of people easy to crowdsource and manipulate. If one looks at the 58% percent who say they know but who are not clear about which type of speech to protect and to prohibit, one does not feel comfortable about the wide crowd out there to be exploited by malevolent agents. Indeed, when we compare the numbers of the discrepant responses they bring in relation to the types of speech they either want or not protected the gap of the 46% could easily swell up to swallow a big chunk of the knows making the vulnerability a serious problem to contend with.

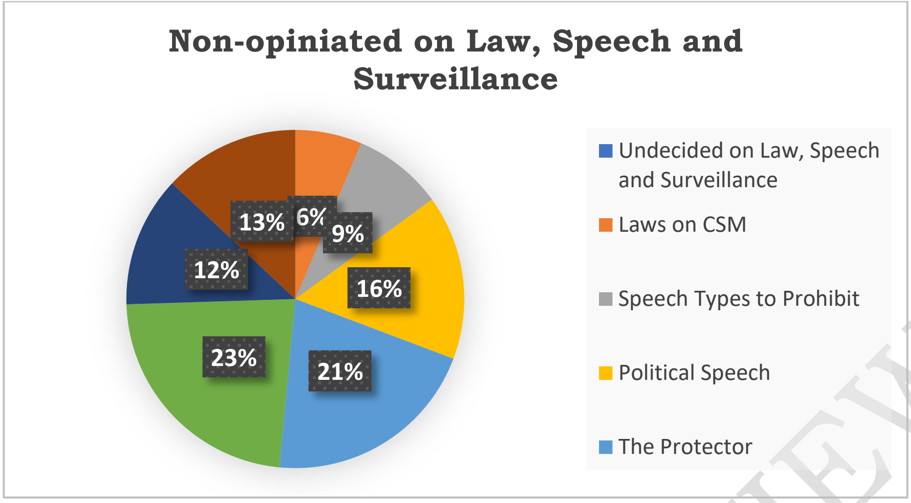
systems security and that supervises the work of the Moroccan Computer Emergency Team known as ma-CERT. Privacyinternational.org. op.cit. p.5

[44] Bot herders are hackers who use automated techniques to scan specific network ranges and find vulnerable systems, such as machines without current security patches, on which to install their bot program. Web. https://www.google.com/search?client=firefox-b-d&q=bot+herder+definition, retrieved on 28th November 2019.

[45] See the cases of case-laws debated by the ECJ. Indeed, the discrepant rulings of the court are many and may help enlighten the point I am trying to put forward.

[46] Article 25: Reference to art; Freedom of expression; Freedom of opinion/thought/conscience: The freedoms of thought, of opinion and of expression under all their forms[,] are guaranteed. The freedoms of creation, of publication and of presentation [exposition] in literary and artistic maters and of scientific and technical research [,] are guaranteed.

Chart 2. *On Laws and Speech-Protection (see appendix 2 for cross-referenced data)*



This ignorance of the law coupled with the paradoxical opinions advanced as to who to seek protection from (the State or the SP), the contradicting opinions as well as the confusing of Surveillance with Protection are additional sources of concern. They are, indeed, vulnerabilities that need mending through sensitizing campaigns mostly by AG who are tasked with making the Internet a space free from abuse.

When one adds up the confusions apparent in the phrasing of the laws, the legislation regulating cyberspace becomes very porous and a serious source of conflict. In line with this and in addition to confusions dealt with previously another confusion can be traced in the framing of Article 28, which says that:

> The freedom of the press is guaranteed and may not be limited by any form of prior censure. All have the right to express and to disseminate freely and within the sole limits expressly provided by the law, information, ideas and opinions. The public powers encourage the organization of the sector of the press in an independent manner and on democratic bases, as well as the determination of the juridical and ethical rules concerning it. The law establishes the rules of organization and of control of the means of public communication. It guarantees access to these means respecting the linguistic, cultural and political pluralism of the Moroccan society. In accordance with the provisions of Article 165 of this Constitution, the High Authority of Broadcasting [Haute autorité de la communication audio-visuelle] sees to the respect for this pluralism.

Although one may note the obsoleteness of such a notion that the law may “control the means of public communication” given the fact that this is not entirely true with the CSM, one has to underline that like the other laws, restrictions are brought to make sure that such provisions are not abused by the practitioners and the citizens, in general. In fact, article 165 says that these rights should be exercised “within respect for the fundamental values of civilization and for the laws of the Kingdom.” But pursuant to Article 2 (par 3) the use of information has been subject to specifications at the risk of criminalisation.[47] Other provisions such as the anti-terrorist law 03-03 specifically in article 1 (7) —where it refers to the processing of data which is exactly what chatting and blogging consist of[48]— have also tried to restrict the scope of such freedom so as to make it amenable to respect the liberties of others offering thus the NGOs a reason to protest this latitude given the court justices which they can exploit to restrict the FEI at their discretion.[49]

Conclusion

Aware of these shortcomings, and due to the pressure from the CS (through local and international NGOs), as well as international stake-holders (EU and the UN institutions), Morocco —according to Privacyinternational.org — is making giant efforts to close the gaps as much as possible. Indeed, it should also be made clear that efforts have been and are being made to update the laws governing a number of domains relating to the processing and use of information on the Web and the Internet.[50] In fact, a legislative arsenal, has and is being hammered on a continuous basis. In this connection we may state:

- the law on the *Exchange of Juridical and Electronic Data* (53-05) in November 2007;
- the law on Data Protection (09-08) promulgated on the 18th February 2009;

[47] Article 2 : (par 3) Une publicité interdite: a) la publicité contenant des éléments de discrimination en raison de la race, du sexe, de la nationalité ou de la religion, des scènes dégradantes pour la dignité de la personne humaine ou qui portent atteinte à ses droits, ou des scènes de violence, des incitations à des comportements préjudiciables à la santé, à la sécurité des personnes et des biens ou à la protection de l'environnement; b) la publicité de nature politique ; c) celle comportant des allégations, indications ou présentations fausses ou de nature à induire en erreur les consommateurs ; d) celle de nature à porter préjudice moral ou physique aux mineurs et ayant, notamment, pour objet: - d'inciter directement les mineurs à l'achat d'un produit ou d'un service en exploitant leur inexpérience ou leur crédulité ou d'inciter directement les mineurs à persuader leurs parents ou des tiers d'acheter les produits ou les services concernés ; - d'exploiter ou altérer la confiance particulière des mineurs à l'égard de leurs parents, enseignants et des personnes ayant une autorité légitime sur eux ; - présenter, sans motif légitime, des mineurs en situation dangereuse. e) celle comportant, sous quelque forme que ce soit, des indications de nature à induire les citoyens en erreur ou à violer leur droit à la confidentialité des informations relatives à l'état de leur santé, ou comportant des indications mensongères sur la santé ou incitant à la pratique illégale de médecine ou de charlatanisme; f) celle comportant le dénigrement d'une entreprise, d'une organisation, d'une activité industrielle, commerciale, agricole ou de services ou d'un produit ou d'un service, que ce soit en tentant de lui attirer le mépris ou le ridicule public ou par tout autre moyen.

[48] Law No 09-08 dated on 18 February 2009 relating to the protection of individuals with regard to the processing of personal data and its implementation Decree n° 2-09-165 of 21 May 2009 ("Law").

[49] See privacyinternational.org. op. cit. p,10 "In December 2015, a national coalition of NGOs strongly criticized the persistent legal vacuum surrounding security and intelligence agencies. In a report submitted to the UN Committee of Human Rights, 14 NGOs including the Moroccan Digital Rights Association called on the government to comply with the requirements of international law, in particular the International Covenant on Civil and Political Rights regarding the protection of privacy".

[50] See Privacyinternational.org. 2019, pp. 13-28.

- the creation of an oversight Authority (la *Commission Nationale de la Protection des Données à Caractère Personnel* CNDP) in May 2009[51];
- the improvement of the Press Code (88-13) promulgated in 2016;
- the law relative to the right to access information (31-13) promulgated in February 2018.

Based on this information, one can say that Morocco —on the face of things— is heading towards effective protection against CSM infringements and excesses. What we have seen, however, with the corpus and the analysed documents is that propaganda (incitement, persuasion and provocation), blackmail, and other infringements are abundant despite the laws incriminating them. What one also acknowledges is that the body of laws promulgated, which defend the individual (freedoms and all) run counter to the avowed FEI which are basic to the ideals the CS is battling for through the various NGOs, namely the Information Society mentioned above. Over and above, this situation, we have to admit, is also resulting from the confusion people have about the FEI, which some would still describe as part of an international law that US Supreme Court Justice Antonin Scalia describes as "nonsense upon stilts".[52] Yet, one needs to underline, in line with Confucianism that "discord" should be seen "as a serious ill, pointing either to the incapacity of the government or to the shortcomings in terms of individuals overstepping their boundaries and lacking self-restraint" (Shaoping, 2013).

Works Cited

A. Legal Texts

Dahir n° 1-03-140 du 26 rabii I 1424 (28 mai 2003) portant promulgation de la loi n° 03-03 relative à la lutte contre le terrorisme. Bulletin Officiel n° 5114 du Jeudi 5 Juin 2003, http://adala.justice.gov.ma/production/legislation/fr/penal/luttecontreterrorisme.htm, accessed on 06/02/2018.

Dahir n° 1-04-257 du 25 kaada 1425 (7 janvier 2005) portant promulgation de la loi n° 77-03 relative *à la communication audiovisuelle.* BULLETIN OFFICIEL N° 6526 -15 rabii I 1438 (15-12-2016) http://www.wipo.int/edocs/lexdocs/laws/fr/ma/ma048fr.pdf, accessed on 06/02/2018.

Dahir n° 1-07-129 du 19 Kaada 1428 (30 Novembre 2007) portant promulgation de la loi n° 53-05 *relative à l'échange des données juridiques.*

Dahir n° 1-09-15 du 22 safar 1430 (18 février 2009) portant promulgation de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, BULLETIN OFFICIEL N° 5714 - 7 rabii I 1430 (5-3-2009), http://www.cndp.ma/images/lois/Loi-09-08-Fr.pdf, accessed on 06/02/2018.

[51] Ibid.p.3

[52] Qtd in Winston P.Nagan and Craig Hammer, "Communication Theory and World Public Order: the Anthropomorphic, Jurisprudential Foundations of International Human Rights", *Virginia Journal of International Law*, Vol. 47:3, 2007.

Dahir n° 1-16-122 du Kaada 1437 (10 août 2016) portant promulgation de la *Loi n°88-13 relative à la Presse et à l’Edition.*

Dahir n°1-18-15 du Joumada II, (22 fevrier 2018) Portant promulgation de la *Loi 31-13 Relative au Droit à l’Accès à l’Information.*

Le Code Pénal, Ministère de la Justice et des Libertés, Direction de la Législation, Royaume du Maroc, Version consolidée 15 Décembre 2016. https://www.ilo.org/dyn/natlex/docs/SERIAL/69975/69182/F1186528577/MAR-69975.pdf, accessed on 06/02/2018.

Loi Française, *Le Code Géneral des Collectivités Territoriales,* Article I 2212-2 promulgué le 4 Avril 1884.

Public Servants Disclosure Protection Act, “Loi sur la protection des fonctionnaires divulgateurs d’actes répréhensibles », Amendé le 6 mars 2018. S.C. 2005, c. 46. Ministère de la Justice, Canada.

The International Covenants of Civil and Political Rights, https://treaties.un.org/docpublication/unts/volume%20999/volume-999-i-14668-english.pdf, accessed on 06/02/2018.

The United Nations Charter, http://www.refworld.org/pdfid/3ae6b3930.pdf, accessed on 06/02/2018.

The United Nations Millennium Declaration, http://www.un.org/millennium/declaration/ares552e.pdf, accessed on 06/02/2018.

The Universal Declaration of Human Rights, http://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf, accessed on 06/02/2018.

*World Summit on the Information Society, “*The Geneva Declaration of Principles and Plan of Action*”*, Geneva: December 2003. Web. http://www.itu.int/net/wsis/docs/geneva/official/dop.html, accessed on 12th October, 2016.

B. Secondary Sources

Amrani, Safaa, “Morocco protests after fisherman crushed to death in a garbage truck”, the Guardian, web: https://www.theguardian.com/worl:d/2016/oct/31/morocco-protests-after-fisherman-crushed-to-death-in-a-garbage-truck. Retrieved February 13th, 2020.

Ardau, C. and Rens van Munster, “Post-structuralism, Continental Philosophy and the Remaking of Security Studies”, in *The Routledge Handbook of Security Studies*, London and New York: Routledge.2010, pp: 74-83.

Balzacq, Thierry, “Constructivism and Securitizing Studies”, in *The Routledge Handbook of Security Studies*, London and New York: Routledge. 2010, pp: 56-72.

Cavelty, M. Dunn and Victor Mauer (eds) *The Routledge Handbook of Security Studies*, London and New York: Routledge.2010.

Christopher Wylie, « Christopher Wylie: Why I broke the Facebook data story and what Should Happen Now”, *The Guardian, International Edition*, web. https://www.theguardian.com/uk-news/2018/apr/07/christopher-wylie-why-i-broke-the-facebook-data-story-and-what-should-happen-now, retrieved May 14th, 2018.

Critchley, Simon, “The Other’s Decision in Me (What are the Politics of Friendship?)”, in *European Journal of Social Theory,* Vol 1, Issue 2, November 1st, 1998.

Dam, Jeff Van “The Kill Switch: The New Battle Over Presidential Recess Appointments” *in Northwestern University Law Review* Vol. 107, No. 1 361 USA. 2012.

Davie, Dave, “Edward Snowden Speaks Out: 'I Haven't and I Won't' Cooperate With Russia” npr. September 19th 2019, web: https://www.npr.org/2019/09/19/761918152/exiled-nsa-contractor-edward-snowden-i-haven-t-and-i-won-t-cooperate-with-russia?t=1581591876947, retrieved on February 13th, 2020.

De Man, Paul, (1971) *Blindness and Insight: Essays in the Rhetoric of Contemporary Criticism*, London: Routledge; 1983.

Dellal, Mohamed, “Globalisation and the Promotion of Democracy: a Trojan Horse or a Genuine Humanitarian Paradigm”, in *Revue Sciences, Language et Communication* Volume 1, N:3, 2017.

Dellal, Mohamed, 2017, *Cybersecurity and International Law: Legal Perspectives; Challenges and Prospects*, Republic of Moldova: Lambert Academic Publishing.

Dellal, Mohamed, Doctoral Dissertation on *L’Ordre Public, le Droit d’Expression et à L’information dans le Cyberespace MENA : le Cas du Maroc* Faculty of Law, Mohamed I University, Oujda, Morocco, Forthcoming.

Frick, Marie-Louisa, *Human Rights Relative Universalism*, USA: Library of Congress, 2019.

Hans, Simran, “XY Chelsea review – in search of the real Chelsea Manning: A documentary about the trans activist and ex-army intelligence officer is intriguing but lacks wider context”, the Guardian, May 26th, 2019. Web: https://www.theguardian.com/film/2019/may/26/xy-chelsea-manning-documentary-film-review. Retrieved February 13th, 2020.

Kasraoui, Safaa “Morocco Sentences 3 Suspects in ‘Hamza Mon BB’ Backmail Case” Web: https://www.moroccoworldnews.com/2020/02/293503/morocco-sentences-3-suspects-in-hamza-mon-bb-blackmail-case/ retrieved on February 13th 2020.

Maulny, Jean-Pierre and Sabine Sarraf, “Assessment and Prospects of Security Threats: Synthesis Report for the International Forum TAC (Technology against Crime) 2016. IRIS, April 2016. Web. http://www.iris-france.org/wp-content/uploads/2016/04/TAC-Report-2016-ENG-V3.pdf, accessed on 06/02/2018.

Merriam Webster, Online Dictionary; web: http://www.merriam-webster.com/dictionary/security, accessed 23rd September, 2016.

Morgenthau, H. *Politics among Nations. The Struggle for Power and Peace*. 2e édit. New York : Knopf. (1954).

Morgenthau, Hans, “A Political Theory of Foreign Aid” in *The American Political Science Review*, Vol. 56, No. 2 (Jun., 1962), pp. 301-309, American Political Science Association Stable, http://www.jstor.org/stable/1952366, accessed on 06/02/2018.

Mutiner, David “Critical Security Studies”, in *The Routledge Handbook of Security Studies*, London and New York: Routledge.2010 pp: 45-55.

Nagan, Winston, P. and Craig Hammer, *Communication Theory and World Public Order: The Anthropomorphic, Jurisprudential Foundations of International Human Rights*, Florida: University of Florida Lavin College of Law, Spring 2007.

Nilsson, Jacob and Sven Olov Wallenstein, *Foucault, Biopolitics, and Governmentalité*, Soderton, Philosophical Studies, Soderton University, The Library, 2013. Web. https://www.diva-portal.org/smash/get/diva2:615362/FULLTEXT03.pdf, visité le 12 May 2018.

Peksen, Dursun et al, “Media-driven Humanitarism? News Media Coverage of Human Rights Abuses and the use of Economic Sanctions”, in *The International Studies Quarterly* V.58, 2014 pp. 855-866. These authors explain that the State has to learn to use a counter discourse to dispel the doubts and suspicions of the public as to some of the news reports relating to public policies.

Rousseau D.L. and Thomas C. Walker, “Liberalism”, in *The Routledge Handbook of Security Studies*, London and New York: Routledge.2010 pp: 21-33.

Schmitt, Carl, The Leviathan in the State Theory of Thomas Hobbes: Meaning and Failure of a Political Symbol, London; Greenwood Press, 1996.

Sharp, Gene, “From Dictatorship to Democrary: A Conceptual Framework for Liberation”, Irenees: *a website of resources* for peace. Web. http://www.irenees.net/bdf_fiche-analyse-953_en.html, Boston, Massachusetts, 2002, visité le 12 mai 2018.

Shaoping, Gan, 2013,” Menschenrechte in China. Von der Idee zur Realität ». In *Trankulturalität der Menschenrechte Arabische, chinesische und europäische Perspektiven*; ed Philippe Brunozzi, Dzarhan Dhouib and Waltr Pfannkuche; 243-254. Freibourg. Karl Alber.

Spencer Jennifer “No Service: Free Speech, the Communications Act, and BART’s Cell Phone Network Shutdown” *in Berkeley Technology Law Journal* Volume 27 Issue 4 Annual Review 2012 Article 20 6-1-2012.

Wholforth, William, C. “Realism and Security Studies”, in *The Routledge Handbook of Security Studies*, London and New York: Routledge.2010. pp: 7-20

Xavier, Inda, Jonathan (ed.) *Anthropologies of Modernity: Foucault, Governmentality, and Life Politics*, USA. Blackwell Publishing, 2005.

Yang, Mirae “The Collision of Social Media and Social Unrest: Why Shutting Down Social Media is the Wrong Response” in *Northwestern Journal of Technology and Intellectual Property* Volume 11 | Issue 7 Article 7 Fall 2013.

Appendix 1. *Quantifying Grid*

1	**Age**	**17-18**	**18-25**	**26- more**	**Other**	**Total**
		60	431	15		581
		11%	74%	15%		
2	**Gender**	**Female**		**Male**	**Other**	
		304		238	39	581
		52%		40,9%	6,7%	
3	**Social Status**	**Student**		**Teacher**	**Nurse**	
		569		11	1	581
		97,9%		1,8%	0,1%	
4	**Users**	**PC**	**SP**	**Both**	**Other**	**Total**
		19	189	325	47	581
		3%	32%	55,9%	8%	
5	**Frequency**	**12h**	**6-3 h**	**1h- less**	**Other**	
		42	282	236	21	581
		7%	48%	40%	3%	
6	**CSM Group**	**Yes**	**No**		**Other**	
		440	122		16	581
		75,7%	20%		3%	
7	**Confidence**	**100**	**80-60**	**40- less**	**Other**	**Total**
		52	247	228	54	581
		9%	42%	39%	9%	
8	**Victim of Hacking**	**Yes**	**No**		**Other**	
		164	344		73	581
		28%	59%		12%	
9	**Use of Data Commercial Reasons**	**Agree**	**Disagree**		**Other**	
		89	390		100	581
		15%	69%		17%	
10	**Political Reasons**	**Agree**	**Disagree**			
		78	399		104	581
		13%	68%		17,9%	
11	**Laws on CMS**	**Yes**	**No**		**Other**	**Total**
		337	193		51	581
		58%	33%		9%	
12	**Types of Speech to Prohibit**	**All Items**	**Porn**		**Other**	
		412	100		69	581
		71%	17%		12%	
13	**Political Speech**	**Agree**	**Disagree**		**Other**	
		317	138		126	581
		317%	23%		21%	
14	**The Protector to be**	**The State**	**SP**		**Other**	
		246	169		166	581
		42%	29%		28%	
15	**Surveillance**	**Agree**	**Disagree**		**Other**	
		239	158		184	581
		41%	27%		31%	
16	**Speaker V Listener**	**Speaker**	**Listener**	**Both**	**Other**	
		250	190	50	10	581
		43%	32.7%	8.6%	1.7%	
17	**Prof, V Amateur**	**Professionals**	**Amateurs**	**Both**	**Other**	
		300	250	24	7	581
		51.6%	43%	4%	1%	

Appendix 2. *Cross-referencing Tab and Charts*

Undecided on Law, Speech and Surveillance	**Laws on CSM**	**Speech Types to Prohibit**	**Political Speech**	**The Protector**	**Surveillance**	**Commercial Use of Data**	**Political Use of Data**
	51	69	126	166	184	100	104
	8,70%	12%	21%	28%	31%	17%	18%
Opiniated Respondents 1 (Yes Agree)	337	512	317	415	239	89	78
	58%	88%	54%	71%	41%	15%	13%
Opiniated Respondents 2 (Nos: Disagree)	193	69	138	166	158	390	399
	33%	11,80%	23%	28%	27%	69%	68%
Cross-referencing user and Frequency	**Non-Owners**	**Other**	**Non-Users**		**Users**	**CSM Groups**	**No Groups**
	47	16	21		560	440	122
	8%	3%	3%		96%	75%	21%

ABBREVIATIONS

AG	**Advocacy Groups**
CNPD	**La Commission Nationale de la Protection des Données (à Caractère Personnel)**
CSM	**Cyber Social Media**
CS	**Civil Society**
DGSSI	**Direction Générale de la Sécurité des Systèmes d'Information**
FEI	**Freedom of Speech and Information**
HR	**Human Rights**
ICCPR	**International Covenant for Cultural and Political Rights**
IPO	**International Public Order**
IS	**Information Society**
ISRI	**International and Strategic Relations Institute**
PO	**Public Order**
SP	**Service Provider**
TD	**Text Document**
UDHR	**Universal Declaration of Human Rights**
UN	**United Nations**
VD	**Video Document**
VPN (Phantom)	**Virtual Private Network**