OPINION ON ZIMBABWE'S CYBER SECURITY AND DATA PROTECTION BILL, 2019

Authored by:
Ms. Catherine Anite, Human Rights Lawyer, Founding Director of the Freedom of Expression Hub in Uganda and member of the High Level Panel of Legal Experts on Media Freedom.

Endorsed by:
Baroness Francoise Tulkens
Justice Manuel Cepeda

Contents

INTRODUCTION

In May 2020, Zimbabwe gazzetted the **Cyber Security and Data Protection Bill** (H.B. 18, 2019)[1] herein referred to as (the "Bill"). The purpose of the Bill is to provide clarity over cyber security and privacy matters. Specifically, it is aimed at "increasing cyber security in order to build confidence and trust in the secure use of information and communication technologies by data controllers, their representatives and data subjects."[2]

The proposed law expands on and amends provisions under sections 162-166 of the Criminal Code (Codification and Reform) Act [*Chapter 9:23*], which were shallow in regards to protection of cyber-crime. The Bill is also intended to create a technology driven business environment and encourage technological development and the lawful use of technology, through providing procedures for investigation and collection of evidence of cyber-crime and unauthorized data collection and breaches, and to provide for admissibility of electronic evidence for such offences. The Bill also establishes a Cyber Security Centre a Data Protection Authority and a Whistleblowing Authority to regulate the proposed sectors under the law.

We note that the proposed cyber security and data law is a positive step by Zimbabwe towards developing its information and communication technology structures, and harnessing ICT's to advance rights of citizens. However, we find that some provisions under the proposed law fail to meet the requisite standards due to their vagueness, unnecessary restrictions and harsh penalties for offences.

Currently, technological advancements are facilitating digital engagements and communication although many countries still struggle to update their laws to address the emerging trends. However, the UN Human Rights Committee, has stated in its General Comment 34 that international guarantees of freedom of expression apply online just as they do offline:

> Paragraph 2 protects all forms of expression and the means of their dissemination. … They include all forms of audio-visual as well as electronic and internet-based modes of expression.[3]

This Opinion contains members of the ***Independent High-Level Panel of Legal Experts on Media Freedom's***'[4] analysis, comments and recommendations on the **Cyber Security and Data Protection Bill 2019** hereinafter referred to as the Bill, premised on Zimbabwe's constitutional standards, international and regional standards and best practices on the guarantee of the right to freedom of expression, access to information, privacy and the media.

Summary of recommendations

1. The interpretation clause should be reviewed and terms clarified and narrowed where necessary.
2. The Cyber Security Centre and the Data Protection Authority should be independent bodies, separate from the Postal and Telecommunications Regulatory Authority.
3. The Bill and/or Regulations should clearly stipulate the manner in which the Authority may waive consent

[1] Cyber Security and Data Protection Bill, 2019
[2] Clause 2 of the Cyber Security and Data Protection Bill
[3] General Comment 34, 12 September 2011/CCPR/C/GC/34 Para 12, https://www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf
[4] The High Level Panel of Legal Experts on Media Freedom, https://www.ibanet.org/IBAHRISecretariat.aspx

4. Clarify the circumstances warranting exception of consent on grounds of national security.
5. Include a provision allowing derogation for processing carried out for journalistic, academic, artistic purposes or literary expression.
6. Clarify what Authority will be in charge of creating a whistleblowing system and ensure independence of that Authority through a clear appointment, and funding process.
7. Clearly state the protection guarantees for whistleblowers including assurance of no civil or criminal sanctions for public interest disclosures
8. Provide defences for persons charged with an offence under the proposed law.

ANALYSIS OF THE BILL

Part I

Definitions and scope of the Bill

This part contains four clauses providing for the title, date and commencement, the objects of the Bill, definitions, and scope respectively. As earlier stated, the object of the Bill under clause 2 is to "*increase cyber security in order to build confidence and trust in the secure use of information and communication technologies by data controllers, their representatives and data subjects*."

Clause 3 defines the terms used in the Bill. We note with concern that some definitions are vague and ambiguous and may be misconstrued, if not amended. In particular, "personal information" is defined as information relating to a data subject including— (h) opinions expressed about an identifiable person; and (i) the individual's personal views or opinions, except if they are about someone else;

While processing personal information, due regard should be accorded to protecting the fundamental rights and freedoms of natural persons, and in particular their right to privacy. The inclusion of *"opinions"* is very subjective. The European Council has defined "personal data" as any information relating to an identified or identifiable natural person hereinafter referred to as "data subject"; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity;[5]

Clause 4 of the Bill spells out the bounds of application. 4 (1) provides that the act … shall be interpreted as being in addition to and not in conflict or inconsistent with the Protection of Personal Information Act [*Chapter*.....]. Currently, there is no Protection of Personal Information Act in Zimbabwe, making it immaterial to state that the bill will conform to a non-existent law. Also, clause 4(2)(a) stipulates in a rather imprecise and vague manner that the act shall be applicable— to the processing of data carried out in the context of the *effective and actual activities of any data controller*, without defining what constitutes "effective and actual activities."

[5] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, Article 2(a), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32001R0045

Recommendations:

- The object of the Bill should specify that the law applies to both natural and legal persons, (Public bodies, corporate bodies and individuals) to avoid doubt within the interpretation clause, especially the imprecise definitions.
- The definition clause should be reviewed and terms clarified and narrowed where necessary.
- We recommend that instead of citing the non-existent Protection of Personal Information Act, the clause should stipulate that this law shall be applied and interpreted in conformity to international standards and best practices on access to information, protection of privacy of information and processing of data.
- A clear definition of effective and actual activities of data controllers should be provided.

PART II and III

Parts two and three will be discussed concurrently as they both create institutional structures to implement the proposed law.

Part II

Establishment of Cyber Security Centre

Clauses 5 and 6 respectively designate the Postal and Telecommunications Regulatory Authority (herein referred to as POTRAZ), established under the Postal and Telecommunications Act [*Chapter 12:05*][6] as the Cyber Security Centre and provides for its functions, which among others includes advising Government and implementing Government policy on cyber-crime and cyber security; establish and operate a protection-assured whistle-blower system that will enable members of the public to confidentially report to the Committee cases of alleged cyber-crime.[7]

Part III

Data Protection Authority

Clause **7** designates the Postal and Telecommunications Regulatory Authority as the Data Protection Authority while **clause 8 (1)** provides for functions of the Authority which include among others to regulate the manner in which personal information may be processed through the establishment of conditions for the lawful processing of data; to promote and enforce fair processing of data in accordance with this Act; to submit to any Court any administrative act which is not compliant with the fundamental principles of the protection of the privacy in the framework of this Act as well as any law containing provisions regarding

[6] Postal and Telecommunications Act, [Chapter 12:05], https://zimlii.org/zw/legislation/act/2000/4
[7] Clause 6 of the Bill

the protection of privacy in relation to the processing of data **in consultation with Minister responsible for Information, Publicity and Broadcasting Services**.

Further, the Data Protection Authority is also mandated to advise the Minister on matters relating to right to privacy and access to information; and facilitate cross border cooperation in consultation with the Minister. **Clause 8 (2)** stipulates that the Authority shall not, in the lawful exercise of its functions be subject to the direction or control of any person or authority.

The Bill has designated the Postal and Telecommunications Regulatory Authority under part II and III as both the Cyber Security Centre and the Data Protection Authority with separate duties of ensuring cyber security as well as data protection.

We however note that the Postal and Telecommunications Regulatory Authority, which is created under the Postal and Telecommunications Act [*Chapter 12:05*] is primarily aimed at ensuring the provision of sufficient domestic and international telecommunication and postal services throughout Zimbabwe,[8] and not created as a cyber security and data protection body. We also note with concern that despite stipulating under clause 8 (2) of the Bill that the Authority (POTRAZ) shall be an independent authority, several sections in the Postal and Telecommunications Act show that POTRAZ **is not an independent body**.

For example, the Minister may give the Board such general directions relating to the policy the Authority is to observe in the exercise of its functions as the Minister considers to be necessary in the national interest,[9] which the Board shall comply with.[10] The Minister can also direct the Board to reverse, suspend or rescind its decisions or actions after consultation with the President,[11] and the Board is mandated to consult the Minister in recruitment of the Director General of the Authority.[12]

In 2015, special international mandates on freedom of expression in their Joint Declaration on Freedom of Expression and Responses to Conflict Situations, stated that:

> Administrative measures which directly limit freedom of expression … should always be applied by an independent body. This should also normally be the case for administrative measures which indirectly limit freedom of expression and, where this is impossible, for example for security reasons, application of the measures should be overseen by an independent body.[13]

In addition, the appointment of the Board under the Post and Telecommunication Act is done by the President after consultation with the Minister, with a bias of experts in postal services and telecommunications.[14] Besides being overwhelmed with executing functions related to postal services,

[8] Postal and Telecommunications Act, Section 4, https://zimlii.org/zw/legislation/num-act/2000/4/Postal_Act.pdf
[9] Postal and Telecommunications Act, Section 25(1), n.8
[10] Postal and Telecommunications Act, Section 25(3), n.8
[11] Postal and Telecommunications Act, Section 26, n.8
[12] Postal and Telecommunications Act, Section 29(1), n.8
[13] Joint Declaration on Freedom of Expression and responses to conflict situations**,** Adopted 15 May 2015, Para 4 (a), https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15921
[14] Section 6

telecommunication, cybercrime and data protection, the constitution of members under the POTRAZ might therefore be inexperienced to fulfil the mandate of the Cyber Security and Data Protection Bill.

Sanctions

The Bill fails to provide for a sanction-regime for the Cyber Security Centre and Data Protection Authority under clauses 6 and 8 respectively. A functional cyber security and data protection mechanism requires appropriate sanctions for offenders and monitoring by an independent supervisory body to ensure rights for data subjects and obligations for those who process personal data.[15]

Recommendations

- The Cyber Security Centre and the Data Protection Authority should be independent bodies, separate from the Postal and Telecommunications Regulatory Authority.
- The recruitment process for the Authority should be clarified and made to comply with the highest standards of professionalism, transparency and equity. The appointment of Board member by the President and Minister under the Postal and Telecommunications Regulatory Authority, without clear guidelines undermines independence.
- A sanctions regime should be elaborated under the functions of the Authority for both the Cyber Security Centre and the Data Protection Authority.

PART IV

Quality of Data and General Rules on the Processing of Data

Clause 9 of the Bill mandates a data controller to process data in an adequate, relevant and non-excessive manner and ensure that it is accurate, kept up-to-date and, where necessary retained in a form that allows for the identification of data subjects, for no longer than necessary with a view to the purposes for which the data is collected or further processed. The data should also be accessible.

PART V

General Rules on the Processing of Data

Clause 10 provides that a data controller shall ensure that the processing of data is necessary, processed fairly and lawfully; clause 11 provides for data to be collected for specified, explicit and legitimate purposes and that further processing of data for historical, statistical or scientific research purposes is not considered incompatible. Clause 12 provides for processing of non-sensitive data, stating that personal information may only be processed if the data subject or a competent person, where the data subject is a child, consents to the processing of such data. However, 12 (2) provides for "implied consent" where the data subject is an adult natural person or has a legal persona and has full legal capacity to consent, while consent is waived

[15] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000, preamble, clause 2, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32001R0045

under 12 (3) for amongst other reasons, proving offences, compliance with an obligation to which the controller is subject by or by virtue of a law; and public interest. The Authority is given broad powers under 12(4) to determine circumstances of waiving consent.

It is commendable that the Bill has adopted the provisions and language from Article 6 of the GDPR, however, there should be emphasis on processing personal data based on consent, and a mandatory explanation on necessity and proportionality in case consent is not obtained.

Art. 5 of the General Data Protection Regulation[16] and Regulation (EC) No 45/2001 of the European Parliament and of the Council,[17] enunciate principles relating to processing of personal data, which the Bill should adopt in its entirety:

1. Personal data shall be:
    1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
    2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, not be considered to be incompatible with the initial purposes ('purpose limitation');
    3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
    4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
    5. 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
    6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
2. The controller shall be responsible for, and be able to demonstrate compliance ('accountability').

Recommendations

- The Bill and/or Regulations should clearly stipulate the manner in which the Authority is deemed to have construed the circumstances under which consent is waived.

[16] GDPR, S.5, https://gdpr-info.eu/art-5-gdpr/
[17] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, Article 4(1) see; https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32001R0045

- The term "public interest" should be clearly defined in the interpretation clause to avoid wanton and arbitrary application.

Sensitive information

Clause 13 prohibits processing of sensitive personal information unless the data subject has given consent in writing although consent shall be waived under circumstances described within clause 13 (2) (a-h). However, the exception involving processing of information necessary to comply with national security laws under 13 (2) (d) is worrisome, especially because states often use "national security" to limit rights, even in circumstances where it does not serve a legitimate purpose, and is unnecessary in restricting rights.

Under the Siracusa Principles, for a State to invoke national security, it must be to justify measures limiting certain rights only when they are taken to protect the existence of the nation or its territorial integrity or political independence against force or threat of force.[18] National security cannot be invoked as a reason for imposing limitations to prevent merely local or relatively isolated threats to law and order,[19] or be used as a pretext for imposing vague or arbitrary limitations and may only be invoked when there exists adequate safeguards and effective remedies against abuse.[20] The Siracusa principles further elucidate that systematic violation of human rights undermines true national security and may jeopardize international peace and security, therefore, a state responsible for such violation shall not invoke national security as a justification for measures aimed at suppressing opposition to such violation or at perpetrating repressive practices against its population.[21]

Recommendation

- Clarify the circumstances warranting exception of consent on grounds of national security.

Processing and freedom of expression and information

The Bill lacks specific provision on processing information in the interest of freedom of expression. International standards make it imperative to reconcile the right to the protection of personal data with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

Article 85 of the GDPR provides that "for processing carried out for journalistic purposes or the purpose of academic, artistic or literary expression, States shall provide for exemptions or derogations from principles, rights of the data subject, controller and processor, transfer of personal data to third countries or international organisations, independent supervisory authorities, cooperation and consistency and specific data processing situations if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

[18] Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights, Annex, UN Doc E/CN.4/1984/, Principle 29, https://www.uio.no/studier/emner/jus/humanrights/HUMR5503/h09/undervisningsmateriale/SiracusaPrinciples.pdf
[19] N18. Principle 30
[20] N.18, Principle 31
[21] N.18, Principle 32

Recommendation:

- Include a provision allowing derogation for processing carried out for journalistic, academic, artistic purposes or literary expression.

PART VI

Duties of the Data Controller and Data Processor

Notification of security breach

Under clause 19, the data controller is required to notify the Authority, without any undue delay of any security breach affecting data he or she processes.

This provision requires expounding in so-far as clarifying the time-frame in which to notify, and how to notify.

Recommendation[22]

- Without undue delay, the data controller shall notify the Authority where feasible within 72 hours after having become aware of the breach, and where it exceeds 72 hours; it shall be accompanied by reasons for the delay.
- The notification shall:
    1. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
    2. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
    3. describe the likely consequences of the personal data breach;
    4. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
- The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with the Act. The process and communication may take the form of the notification above.

PART VII

Data Subject

Clause 25 provides that the data subject shall have the right not to be subject to a decision based solely on automated processing, unless with consent or if the decision is based on law.

[22] N.16, Article 33, GDPR

Recommendation

- Under international standards and best practices, the Data subject has enormous rights[23] including the right to receive without undue delay, concise, transparent, intelligible and easily accessible, clear information from the data controller; right of access, right to be forgotten, rectification, access, object among others. We recommend that these bundles of rights be included within this clause, for easy access.

PART VIII

Code of Conduct

The interpretation clause also defines "code of conduct" to mean the "Data Use Charters drafted by the data controller in order to institute the rightful use of IT resources, the Internet, and electronic communications of the structure concerned, and which have been approved by the Data Protection Authority." A data controller or controller" is defined as "any natural person or legal person who is licensable by the Authority."

Clause 30 of the Bill provides for the Code of Conduct as follows:

> (1) The Authority shall provide guidelines and approve codes of conduct and ethics governing the rules of conduct to be observed by data controllers and categories of data controllers.
> (2) In effecting (1) above, the Authority shall consider trade associations and other bodies representing other categories of controllers who have national codes or have the intention of amending or extending existing national codes and allow them to submit such codes for the approval of the Authority.
> (3) The Authority in considering codes of conduct for approval, shall ascertain, among other things, whether the Codes submitted comply with the provisions of this Act.
> (4) If it deems it fit, the Authority shall seek the views of affected data subjects or their representatives.

The definition of the code of conduct and the process of drafting the codes under clause 30 pause a serious threat in so far as providing enormous powers to data controllers to draft different codes which may vary in standard and fail to conform to constitutional, international and regional standards on data protection. Providing data controllers such powers to make their own guidelines may undermine the legislative and supervisory powers of Parliament and also allow the Data Protection Authority to approve several codes without a clear set standard.

The Authority must ensure that codes of conduct conform to fairness and transparency standards, pursue legitimate interests, collect personal data, pseudonymize personal data, inform the public, notify the authority on breaches, protect children among others.[24]

[23] N.16, GDPR Articles 12-23
[24] N16, GDPR Article 40.

Recommendations:

- The Bill should outline the primary standards of the Code of Conduct that must be set by the Data Protection Authority for adoption by data controllers or in the alternative clarify that the codes of conduct shall be drafted by the Authority and not the data controllers.
- Consistent and homogeneous application of standards under the codes for the protection of individuals' fundamental rights and freedoms with regard to the processing of personal data should be ensured.

PART IX

Whistleblowing

Clause 31 empowers the "Authority" to establish a whistleblowing system in accordance with the principles of fairness, lawfulness, proportionality on the limitation of the scope and accuracy. The clause also sets standards under which information is collected.

Unlike the explicit designation of the Postal and Telecommunications Regulatory Authority as the Cyber Security Centre and the Data Protection Authority, it is unclear whether the Bill intends to create a new Whistleblowing authority, or designate the PROTAZ as a whistleblowing authority as well. This, either way shall overwhelm the PROTAZ, which as it is lacks the independence and perhaps the expertise to metamorphose into a whistleblowing authority.

The Clause also fails to meet the requisite standards of whistleblowing legislation in so far is it fails to spell out the protection guarantees for whistleblowers. For example, in circumstances of public interest disclosures, officials who leak information should be protected by a competent authority.

Protection of whistleblowers is also be consistent with international standards, for example as reflected in the 2015 Joint Declaration on Freedom of Expression and Responses to Conflict Situations of the special international mandates on freedom of expression:

International standards have enunciated that:

> Individuals who expose wrongdoing, serious maladministration, a breach of human rights, humanitarian law violations or other threats to the overall public interest, for example in terms of safety or the environment, should be protected against legal, administrative or employment-related sanction, even if they have otherwise acted in breach of a binding rule or contract, as long as at the time of the disclosure they had reasonable grounds to believe that the information disclosed was substantially true and exposed wrongdoing or the other threats noted above.[25]

[25] Joint Declaration on Freedom of Expression and responses to conflict situations**,** Adopted 15 May 2015, Para 5 (b), https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15921&LangID=E

Recommendations:

- Clarify what Authority will be in charge of creating a whistleblowing system and ensure independence of that Authority through a clear appointment, and funding process.
- The provision should clearly state the protection guarantees for whistleblowers including assurance of no civil or criminal sanctions for public interest disclosures
- The Bill should also make clear the manner in which implicated persons shall be informed, including timeframe, and the "exceptional circumstances" under which information may be withheld from the implicated person under clause 31(4)

PART X AND XI

General Provisions and Consequential Amendments

Part XI provides for offences and penalties while Part XII of the Bill provides for amendments under the Criminal Law (Codification and Reform) Act [*Chapter 9:23*]. Some of the offences herein pose a serious threat to freedom of expression, access to information and privacy rights. We note with concern the ambiguity and harshness of some offences, especially custodial sanctions providing for up-to twenty years imprisonment. For example, unlawful interference with data or data storage medium attracts a sanction of up-to ten years in jail. Under section 163C, "unlawful interference with computer system" by blocking, hindering, impeding, interrupting, altering or impairing the functioning of, access to or the integrity of, a computer device, attracts a jail term of up to twenty years; Transmission of data message with intent to incite violence or damage to Property under section 164 has a penalty of five years in jail; Sending threatening data message under section 164A, also leads to imprisonment of five years while cyber-bullying and harassment attracts a sanction of ten years imprisonment under section 164B.

The lack of independence of the regulatory authority coupled with the harsh penalties is very worrisome, especially because these powers may be abused to crack down on critical voices and legitimate speech.

Recommendations:

- We propose a provision allowing data subjects to file complaints with the Authority if he or she considers that the processing of personal data relating to him or her infringes the Act.
- The Authority should also have clear processes of informing the complainant on the progress and the outcome of the complaint including the available remedies.
- The Bill should provide defences[26] for persons charged with an offence under it to prove that—the obtaining, disclosing, procuring or retaining—

  (a) was necessary for the purposes of preventing or detecting crime,
  (b) was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal, or
  (c) in the particular circumstances, was justified as being in the public interest.

[26] Data Protection Act 2018, section 170.

- It is also a defence for a person charged with an offence under subsection (1) to prove that—

  (a) the person acted in the reasonable belief that the person had a legal right to do the obtaining, disclosing, procuring or retaining,

  (b) the person acted in the reasonable belief that the person would have had the consent of the controller if the controller had known about the obtaining, disclosing, procuring or retaining and the circumstances of it, or

  (c) the person acted—

  (i) for the special purposes,

  (ii) with a view to the publication by a person of any journalistic, academic, artistic or literary material, and

  (iii) in the reasonable belief that in the particular circumstances the obtaining, disclosing, procuring or retaining was justified as being in the public interest.
- The custodial sentences under the Bill are quite excessive and would pose a chilling effect of expression. We propose a reduction to a maximum of five years imprisonment
- We also propose that the offences must be in line with the three-part test where they are provided for in a clear manner, should serve a legitimate purpose and should be necessary in a democratic society and proportional