TELKOMNIKA, Vol.16, No.1, February 2018, pp. 290~301
ISSN: 1693-6930, accredited **A** by DIKTI, Decree No: 58/DIKTI/Kep/2013
DOI: 10.12928/TELKOMNIKA.v16i1.7718

Current State of Personal Data Protection in Electronic Voting: Criteria and Indicator for Effective Implementation

Muharman Lubis*[1], Mira Kartiwi[2], Sonny Zulhuda[3]
[1]Telkom University, Jalan Telekomunikasi No. 1, Bandung 40257, Indonesia
[2,3]International Islamic University Malaysia, 50728 Jalan Gombak, Kuala Lumpur, Malaysia
*Corresponding author, e-mail: muharman.lubis@gmail.com

Abstract

The adoption of electronic voting has been done in various countries related to cost and time reduction operationally. On the other hand, recent publication has been informed several issues occurred such as technicality, reliability, security and privacy due to the compromised system were used. In small scale, there are certain group of people who want to exploit the vulnerabilities for their own benefit in the election, while in the greater scale, it can reduce public confidence to entrust the adoption of e-voting system to augment participation rate, to improve the quality of voting and to aid the political right effectively. This paper aims to investigate the characteristic of people demanding the legislative to address the criteria and indicator for effective implementation in electronic voting. By understanding the perception of voters in viewing current electoral regulation are essential to provide some ideas and opinions for better enhancement, either through recommendation and drafting related legislation to cater the needs.

Keywords*: Personal Data Protection, Fraud, Electronic Voting*

1. Introduction

In general, there are three broad categories of election issue namely security testing, public disclosure and auditing the assembling system from separate components [1]. Based on the recent analysis, lack of proper registration, numerous invalid vote, different speed of vote collection and personal data protection as the common failures occurring in the Indonesian elections [2]. Its main problem lies in the aspect of transparency and the accountability [3]. Fraud is a menace that deserves serious attention and immediate action by both the government organizations and the legislative or governing bodies. The impact of fraud in certain countries can be vary but the long term impact on election culture can be significant. In addition to substantial monetary losses, fraud has damaging effects on a government's reputation, placing at risk the ability to implement programmes effectively, establish partnerships and receive contributions. Effective fraud prevention, detection and response mechanisms, therefore, play a key role in safeguarding organizations' interests against these negative impacts. Consequently, electoral commission must provide the solution to the common failures, which align with the current legal regulation. The issues resided on the weaknesses of legal regulation to fulfil the voters' right and the attempts to anticipate the violation due to circumstances changes [14].

In enforcing legal regulation over privacy protection, the additional safeguard is necessary to minimize potential loss by adopting privacy-enhancing technologies, increasing data transparency and providing data customization. In addition, the lack of a consistent approach may result in lack of legal certainty and predictability, thus it may weakens the position of data subject and impose unnecessary regulatory burdens over activities operating across election body. While critical issues should be addressed by the primary regulation, it should take a note that it cannot regulate every detail but in brief verse. It may be unsuitable to stipulate some of the specific details of election technicality in the law produced by government bodies for administering elections. The important point that can be look in regard the structure, formation and hierarchy of the body that handle the election as well the clear responsibility that allow citizen to request transparency of administration that has been done in every phase of

Received August 19, 2017; Revised December 20, 2017; Accepted January 6, 2018

implementation. Sound laws and regulations are the foundation of law enforcement and the criminal justice system [4]. Another important point with regard to the prevalence of fraud concerns its relationship to financial crises [5]. Thus, this study want to explore the typical legal issues and its demand for personal data protection based on people perception and the importance of legal literacy among them on how they view the current legal for preventing fraud that might occur in the election.

2. Current State of Legal Regulation

There is no single law that provides a comprehensive protection of privacy or personal data in Indonesia but there are certain regulations concerning the use of electronic data of individual for the commercial purpose. The primary sources of electronic information and transaction management are Act No. 11/2008 as amended by Act No. 19/2016 regarding the Amendment of Electronic Information Transaction law, Government Regulation No. 82/2012 regarding Provisions of Electronic system and Transaction and its implementing regulation, Minister of Communications and Informatics Regulation No. 20/2016 regarding the Protection of Personal Data in Electronic System. However, a new draft bill on the Personal Data Protection is being discussed intensively and we can expect single comprehensive regulation can come in 2018 or so, though the exact date remains uncertain and the bill still to be considered by the house of representative in which pressure and socialization from society become essential. There are several serious issues, which cyber law should cover namely cybercrime, digital evidence, intellectual property, standardization, legislation synchronization, privacy protection, e-service and jurisdiction [31]. Meanwhile, the rapid changes of technology might shift the definition of certain terminology and the approach of certain procedure. Furthermore, there are number of regulation with specific issues have been enacted by legislative over decades, which might have different principles, attributes and consideration lead to different interpretation in the court. These aspects complicate the citizen even certain legal experts to understand the regulation.

The legal certainty represents a requirement, which decisions is made according to legal rules linking to the individual autonomy in national jurisprudence. The legal system protects the subject from arbitrary use of state power. In the civil law tradition, legal certainty is defined in terms of maximum predictability of officials' behaviour. Based on establishment of legislation No. 11/2011, verse 96 mentions that citizen can give suggestion either verbal and/or written in establishment of law and regulation through several channels namely public opinion meeting, work visit, socialization and seminar. However, many citizens have no knowledge about this opportunity, as there is a huge gap in education in various cities in Indonesia and less socialization in legal by related institution. The maintenance of law and order is prerequisite to the enjoyment of freedom and happiness in the society. To assure the law enforcement takes place, it requires the mutual respect and understanding between government agency body and citizen of the community. However, there is exists a communication gap between the theory and the practices for it is, either, restrictively protected by reactionary legislation or it is rampantly abused by profit-driven businesses [6, 32].

The engagement of citizen improves the quality of policy being developed, then making it more practical and relevant, also helping the services are delivered in a more effective and efficient way. It is also a way for government to maintain of its relationship with citizens by checking its reputation and status. In contrast, the lack of legal exposure might increase the resistance from the citizen to accept new adopted technology compare remaining in the traditional way. By providing opportunities for a diversity of suggestion and criticism enables citizens to identify priorities. It leads to inspire more ownership of solutions and more responsibility for policy implementation and fosters a sense of mutuality, belonging and a sense of empowerment, which all of them can strengthen resilience. There is no doubt that the role of regulation critical to maintain the public trust and confidence in *e*-voting system. In the Freedom Act No. 14/2008 chapter 6, verse 21 and 22 mention the mechanism to obtain public information based on principle of speed, timely and costly. The Electronic Transaction Act No. 11/2008 (verse 29, 30, 31 & 32) mentions the importance of privacy as human right and the obligation of related organization to protect the integrity, dignity and confidentiality of consumer and individual personal data, while the National Registration Act No. 23/2006 (verse 84) defined the kind of personal data that should be protected. The Banking Act No. 10/1998 (verse 40)

mentions that bank has the obligation to protect the confidentiality of its client personal data and secure his savings besides the exemption purpose stated by the regulation while Bank Indonesia Regulation No. 7/15/PBI/2007 instructs the implementation of risk management in the utilization of information technology in the bank. On the other hand, the Capital Market Act No. 8/1995 (verse 68, 89, 97) mention the procedure for the submissions of confidential and sensitive information while based on Financial Services Authority Regulation No. 1/PJOK.07/2013 instructs the protection of consumers personal data by prohibiting the financial service actor to provide data to third party except when the consumer has provided written consent or when law requires such disclosure. Election is a process in which voters choose their representatives and express their preferences for the way that they will be governed. Thus, the election commissioner should accommodate election requirements namely robustness to fraudulent behaviours, consistency of scheme and mechanism, security and privacy measure and transparency of process. Constitutional Court gave the green light for electronic voting with its verdict No. 147/PUU-VII/2009 as legal basis.

Government introduced SIAK (Residence Administration Information System) based on National Registration Act No. 23/2006 to anticipate common failures in previous election. The system has purpose to increase the accuracy of data population and adjust with government policy such as list of voters data through one integral basis data. Then, the second issue relate to the disfranchisement by the government that prohibit military and police to casting vote as a matter of protecting their neutrality while others argued that every person has same right and responsibility based on constitution. To intercede this issue, constitutional court grant the judicial review in judicial verdict no. 22/PUU-XII/2014 that state military and police have no right to vote in 2014 election due their role of responsibility as country apparatus. Besides that, there are many other issues attached to the previous election such as money politics, children involvement in campaign, election committee neutrality, optimized monitoring process, political violence, etc. that increase the doubt of people in believing the government competency to implement good quality of election while some of them also worry that political interest get involved. Nevertheless, the regulations in the form of content should be constantly updated and adjusted to the latest technology and based on elaborate discussions between the regulators, organizations and stakeholders [7]. But, privacy protection as a social issue has strong need to be simplified by bringing down legislative requirements into technological reality and to design new technical solutions [8]. It is not solely a technical or policy issue rather it depends on behaviour as it is an on-going initiative, not a short-term project or goal [9]. Strong impression might advance the privacy law-related as the regulator perceived its benefits in recognition of privacy rights but the threats and incursions are developing more quickly and in many areas citizen's privacy may be slipping away, particularly disorderly and politicised development of amendments [10].

In Australia, casting a vote for citizen is compulsory by section 245(1) of the Commonwealth Electoral Act 1918, which states: ‘it shall be the duty of every elector to vote at each election’. The Act requires Australian citizens aged 18 years and over to cast a vote except persons who prove to be crazy, prisoners serving more than three years and persons who have been convicted of treason or treachery. Meanwhile, Sweden is generally considered a good democratic example in terms of having well-informed, interested citizens and a high degree of public participation in elections, which at over thirty percent use postal votes. Furthermore, as postal votes must be distributed and placed in return mail before the scheduled Election Day, it is sometimes referred to as a form of early voting and can be used as absentee ballots. There is also allegation that postal votes have been used by the ruling party to secure seats in certain constituencies, which it is more amenable to both fraud and manipulation than voting at polling places. Despite the controversy arises, there has been a strong reluctance by governments to move away from the system as they claim to be proven and secure traditional paper-based methods, while it can also weaken the weight, dignity and symbolic importance of the traditional election day [11]. In order to make electoral commissions able to ascertain the suitability of systems for use in elections, certification procedure are commonly adopted that was begin with the definition of precise characteristics a system should exhibit and must define methods to measure conformance of the system to the reference model [17]. The lack of a coherent and concrete concept of privacy can also hinder the development of technologies, legislations, public policies and practices pertaining to consumers, employees and citizens in both local and global sector [18].

The Philippines Commission on Elections began efforts to automate the electoral process in 1992. Various pilot projects of mixed success eventually saw the 2010 local and national elections employ technology to record ballots and count the vote but there were numerous hitches and allegations of irregularities in which about 465 of 76,000 machines had problems and most of them were replaced [12]. Despite glitches with the new computerized counting machines and violence that claimed at least nine lives, election officials hailed the vote as a success in a country. From the early introduction of voting machines in the Netherlands, which become the reference of Indonesian legal framework, the regulation about electronic machines is remained limited. In 1989, the Electoral Code was revised thoroughly with a few references to *e*-voting. The code explicitly stated local authorities could decide if voting means other than ballot papers are used, that this was only allowed with technical appliances approved by the Home Affairs Ministry and other rules would be determined in the Electoral Decree, although never elaborated further [13]. The Dutch legal framework was inadequate to effectively regulate the development and the utilization of voting machines, especially regarding security safeguards, the certification process and tabulation software. In anticipating the failures of implementation, agencies' best defense against the risk is to pay more attention to their privacy practices and improve their standards of protection [19].

In general, there are numerous studies indicated that IS project management still show its high failure rate, which major issues related to uncertainty of legal concept and lack of focus in the policy [20]. In Great Britain, there were 232 cases of alleged electoral malpractice (38% to voting offences and 34% related to false statement) reported by the police during the election, which one case had resulted in prosecution and conviction but over half of the cases (137 in total) required no further police action [4]. Meanwhile, in US, approximately 24 million voter registrations are no longer valid or significantly inaccurate, which 1.8 million decease individuals are listed as voters and 2.75 million people have registrations in more than one state while researchers estimate at least 51 million (24% of population) eligible US citizens are unregistered [5]. By recognizing the benefits of IT governance and investment are essential for a competitive advantages and to reducing the failure rate of IT projects [21]. Thus, it is better to detect the fraud prior to election either through ecological information of political structure or return sheets on the reported number of electoral violation [6].

3. Research Methodology

The use of ordinal logistic regression is necessary to reveal the hidden fact among the citizen in the sense of their motivation in casting votes decision. Regression coefficient is more informative because it presents by how much the dependent variable changes as the independent variable changes, whereas the correlation coefficient presents only whether or not the two variables move in the same or opposite directions and the degree of linear association [15]. Meanwhile, the standard error measures how sensitive the estimate of the parameter is to changes in a few observations in the sample [16]. The scale that were used for this study consisted six pointer which are (1) strongly disagree/SRD, (2) disagree/D, (3) slightly disagree/SLD, (4) slightly agree/SA, (5) agree/A; and (6) strongly agree/SA. Before run ordinal regression, those scales were changed to three pointers, disagree, neutral and agree to narrow down the result and to have in depth analysis of the direction. There are 12 (twelve) statements to represent legal demand in the context of personal data protection attributes namely complexity, comprehensive, principles, certification, timeframe, security, verification, monitoring, remedies, data type, benchmark and implementation.

a. LR1: In the issue of privacy, the respected regulation in Indonesia is complicated to be understood.
b. LR2: DPR should aware the importance to enact single regulation for personal data protection comprehensively.
c. LR3: Privacy principles are required in voting regulation as the guarantee for successes of implementation.
d. LR4: There must be trusted certification procedures for hardware and software by independent expert stated by voting regulation.
e. LR5: DPR should enact all correspondent regulation at least two-year before the election to see the effectiveness.

f. LR6: Personal data protection regulation should accommodate the secure techniques and methods to be proof secured transparency.
g. LR7: Personal data protection regulation is needed to allow verification process.
h. LR8: Personal data protection regulation is required for monitoring purposes in whole voting activities.
i. LR9: Severe penalties should be applied for any misuse of voters' data.
j. LR10: It should be stated in regulation about the type of data to be used for election purposes.
k. LR11: KPU should learn the other country regulation regard to privacy and data protection.
l. LR12: KPU should learn on how the other countries implement electronic voting.

This study has four kind of results, the first one is the pilot study that has 44 samples to see first the reliability and validity of each items, while the hand to hand survey have done in two biggest city in Indonesia, which are Medan and Jakarta that has 336 and 308 samples respectively. In addition, there are 102 samples from online contributor, in which comprises on total of 790 samples. Due to several criteria, 11 data was eliminated which relate to missing data and invalid data. The missing value in the demographic data except for gender will be predicted based on age, election, education, working and earnings through the code number of survey that reflect the location and field of participants. Meanwhile, for the invalid data, caused by multiple answer, it will be used the median value of total samples in the survey. Meanwhile, the strict number of pieces survey was printed and delivered to avoid snowball effect, which has high return reach 86% with 800 paper delivered offline and reach 51% with 200 invitation online. Most respondent have kind of agreement level with each legal statement in the survey as high indication of their demand as they increasingly become more aware about the importance. From the Table 1, it show the result of LR7 (53.4%), LR3 (52.9%) and LR10 (52.5%) are the highest percentage of agreement (normal) above the other legal demand with more than half of population while, LR2 (8.3%), LR9 (9.9%) and LR6 (10.7%) are the lowest percentage of agreement (slight). Meanwhile, based on Table 2, the education, age and legal literacy became the most frequent demographic factors, which have significant value compare with the others. By having this result, it could predict the tendency of certain eligible voters based on their characteristics and circumstances and provides the general idea of legal demand.

Table 1. Frequency Distribution of Legal Regulation

Items (%)	SRD (1)	D (2)	SLD (3)	SLA (4)	A (5)	SRA (6)
LR1	21 (2.7%)	32 (4.1%)	72 (9.2%)	156 (20%)	334 (42.9%)	164 (21.1%)
LR2	11 (1.4%)	20 (2.6%)	24 (3.1%)	65 (8.3%)	366 (47%)	293 (37.6%)
LR3	11 (1.4%)	10 (1.3%)	35 (4.5%)	88 (11.3%)	412 (52.9%)	223 (28.6%)
LR4	11 (1.4%)	21 (2.7%)	26 (3.3%)	95 (12.2%)	374 (48%)	252 (32.3%)
LR5	9 (1.2%)	21 (2.7%)	33 (4.2%)	111 (14.2%)	381 (48.9%)	224 (28.8%)
LR6	16 (2.1%)	11 (1.4%)	27 (3.5%)	83 (10.7%)	382 (49%)	260 (33.4%)
LR7	15 (1.9%)	13 (1.7%)	29 (3.7%)	107 (13.7%)	416 (53.4%)	199 (25.5%)
LR8	17 (2.2%)	16 (2.1%)	28 (3.6%)	104 (13.4%)	396 (50.8%)	218 (28%)
LR9	31 (4%)	26 (3.3%)	34 (4.4%)	77 (9.9%)	235 (30.2%)	376 (48.3%)
LR10	11 (1.4%)	23 (3%)	36 (4.6%)	115 (14.8%)	409 (52.5%)	185 (23.7%)
LR11	15 (1.9%)	31 (4%)	48 (6.2%)	136 (17.5%)	334 (42.9%)	215 (27.6%)
LR12	14 (1.8%)	16 (2.1%)	32 (4.1%)	95 (12.2%)	321 (41.2%)	301 (38.6%)

Table 2. Ordinal Regression of Legal Regulation

No	Threshold	Estimate	Std. Error	Wald	Sig.
LR1	[LR1R=1.00]	-19.786	1.021	375.277	0.000
	[LR1R=2.00]	-18.619	1.020	333.326	0.000
	[Male]	-0.331	0.161	4.228	0.040
	[under 20]	0.726	0.369	3.876	0.049
	[21-25]	1.163	0.313	13.783	0.000
	[31-35]	0.970	0.318	9.275	0.002
	[36-40]	0.898	0.373	5.807	0.016
	[Diploma]	-17.297	0.399	1880.303	0.000
	[Undergraduate]	-18.098	0.388	2172.477	0.000
	[Postgraduate]	-17.891	0.366	2385.809	0.000
	[Legal Academician]	1.084	0.428	6.404	0.011
	[Legal Legislator]	-1.074	0.471	5.192	0.023
LR2	[LR2R=1.00]	-19.273	1.562	152.216	0.000
	[LR2R=2.00]	-18.359	1.560	138.516	0.000
	[Diploma]	-19.173	1.095	306.813	0.000
	[Undergraduate]	-19.270	1.090	312.476	0.000
	[Postgraduate]	-19.194	1.077	317.452	0.000
LR3	[LR3R=1.00]	-18.292	1.152	252.083	0.000
	[LR3R=2.00]	-17.155	1.150	222.346	0.000
	[21-25]	1.281	0.421	9.267	0.002
	[Diploma]	-17.670	0.534	1095.191	0.000
	[Undergraduate]	-18.346	0.517	1257.184	0.000
	[Postgraduate]	-18.509	0.489	1430.717	0.000
	[Enterpreneur]	1.348	0.646	4.354	0.037
LR4	[LR4R=1.00]	-19.802	1.199	272.866	0.000
	[LR4R=2.00]	-18.673	1.195	244.327	0.000
	[31-35]	0.837	0.408	4.206	0.040
	[Diploma]	-17.441	0.513	1157.452	0.000
	[Undergraduate]	-17.847	0.500	1273.614	0.000
	[Postgraduate]	-17.456	0.480	1321.880	0.000
LR5	[LR5R=1.00]	-2.310	1.676	1.899	0.168
	[LR5R=2.00]	-1.073	1.673	0.412	0.521
	[36-40]	1.126	0.514	4.789	0.029
LR6	[LR6R=1.00]	-19.781	1.363	210.704	0.000
	[LR6R=2.00]	-18.690	1.358	189.289	0.000
	[Less than 3X elected]	0.935	0.369	6.408	0.011
	[3-6X elected]	0.669	0.338	3.914	0.048
	[Diploma]	-16.698	0.576	840.354	0.000
	[Undergraduate]	-17.374	0.561	958.529	0.000
	[Postgraduate]	-16.706	0.541	1018.710	0.000
LR7	[LR7R=1.00]	-19.387	1.188	266.363	0.000
	[LR7R=2.00]	-18.122	1.183	234.466	0.000
	[Diploma]	-17.703	0.570	964.191	0.000
	[Undergraduate]	-17.827	0.566	992.527	0.000
	[Postgraduate]	-17.652	0.546	1044.148	0.000
	[Legal Student]	-0.576	0.273	4.444	0.035
	[Legal Awareness]	-0.665	0.253	6.915	0.009
LR8	[LR8R=1.00]	-19.291	1.215	225.070	0.000
	[LR8R=2.00]	-18.106	1.211	223.517	0.000
	[Diploma]	-17.381	0.603	829.898	0.000
	[Undergraduate]	-17.341	0.601	831.688	0.000
	[Postgraduate]	-17.699	0.578	937.460	0.000
	[Private]	0.636	0.310	4.205	0.040
	[Entrepreneur]	1.384	0.518	7.130	0.008
LR9	[LR9R=1.00]	-19.567	1.257	242.204	0.000
	[LR9R=2.00]	-18.793	1.255	224.249	0.000
	[21-25]	0.817	0.381	4.593	0.032
	[3-6X elected]	-0.710	0.359	3.921	0.048
	[Diploma]	-17.358	0.568	934.984	0.000
	[Undergraduate]	-17.131	0.568	908.381	0.000
	[Postgraduate]	-17.253	0.548	990.694	0.000
LR10	[LR10R=1.00]	-20.692	1.355	233.281	0.000
	[LR10R=2.00]	-19.483	1.350	208.328	0.000
	[Diploma]	-16.959	0.618	753.336	0.000
	[Undergraduate]	-17.268	0.613	794.674	0.000
	[Postgraduate]	-17.252	0.597	833.915	0.000
LR11	[LR11R=1.00]	-20.254	1.137	317.591	0.000
	[LR11R=2.00]	-19.084	1.133	283.690	0.000
	[21-25]	0.943	0.331	8.130	0.004
	[26-30]	0.651	0.313	4.326	0.038
	[Diploma]	-17.377	0.448	1505.635	0.000
	[Undergraduate]	-17.585	0.442	1581.954	0.000
	[Postgraduate]	-17.559	0.419	1760.043	0.000
	[Legal Legislator]	-1.016	0.510	4.118	0.042
LR12	[LR12R=1.00]	-20.341	1.272	255.772	0.000
	[LR12R=2.00]	-19.238	1.268	230.337	0.000
	[Diploma]	-17.176	0.516	1107.135	0.000
	[Undergraduate]	-17.157	0.516	1106.065	0.000
	[Postgraduate]	-17.459	0.486	1288.395	0.000

Education background shows the significant value (0.000) to all LR items except LR5. It explains that educational institution play critical role to shape people mind to support or reject the bill proposed by DPR and to evaluate the effectiveness of certain regulation and its enforcement. Even though, the decision to approve the bill or to amend the legislation completely in the DPR authority, people can give pressure against DPR. Furthermore, being a bachelor student decreases the ordered logit of being in the lower levels of the LR2 category by -19.194 lower than diploma student while the other variables in the model are held constant. The bachelor student is more likely to disagree that DPR should enact supportive legislation for *e*-voting initiative. The DPR should take measured and appropriate steps to evaluate the bill proposed carefully and openly consider any valuable feedback from practitioner and citizens, which is not necessary on single comprehensive act. Also, a decrease by bachelor student with -17.252 (LR10) and -17.459 (LR12) of ordered logit of being lower levels and the other variables in the model are held constant. Based on OLR result, education becomes the highest relationship and solely category, which give the strongest effect on LR2, LR10 and LR12. The reason related to the technical terms and confusing jargon used in the process of enactment, database management and benchmarking only can be understood properly through learning process in educational institution. On the other hand, the second category of age (21-25) and entrepreneur shows sig. value of 0.002 and 0.037 in LR3, which show high relationship and strong effect to realize that privacy principles are important elements in the regulation. They want government to discuss privacy concept and principles carefully before enacting the regulation to avoid misconception among citizen. Essentially, the privacy concept authorized by regulation is the most important part to set the basis in executing the plan and useful element to counter the problem in each implementation phase [22].

4. Factors Influence Privacy Protection Measures

Most privacy protection approach could be improved through the active involvement and participation from users, commissioner and legislative member. People feel that the long vote count can create segregation among community, which might lead to greater scale of conflict. Thus, the use of *e*-voting could prevent this worst possibility by quick and accurate tabulation process so the announcement of election result will be less than a day. Meanwhile, *e*-voting also could save APBN largely into other allocation slot for national growth and poverty eradication. Classic problem from previous election was related to data duplication and manipulation can be solved through this type of voting system. By perceiving benefit from electronic mechanism in casting and tabulating the votes, mostly the people proven to feel confidence and exciting to contribute to the success of *e*-voting. They are also eager to help and look out on the other way to enhance the process to the further level so it can bring more benefit to the nation. People have specific reason, perception and motives to performing their best of practice and action according to their ability to secure the election and its personal data protection.

Table 3. Percentage of Legal Illiteracy from Survey

D/A	L1: In learning Process	L2: Legal Awareness	L3: Political Participation	L4: Public Education on Law	L5: Legal Academician	L6: Legislating the Act
Complexity	15/85	18/82	11/81	24/76	44/56	3/97
Inconclusive	9/91	3/97	4/96	13/87	4/96	3/97
Principles	8/92	6/94	0/100	13/87	4/96	8/92
Certification	9/91	5/95	0/100	13/87	8/92	5/95
Speed	9/91	6/94	4/96	11/89	16/84	3/97
Technicality	7/93	6/94	7/93	7/93	0/100	14/86
Verification	8/92	4/96	0/100	15/85	12/88	16/84
Monitoring	8/92	8/92	11/89	9/81	8/92	8/91
Remedies	13/87	8/92	7/93	16/84	16/84	8/91
Terminology	10/90	8/92	4/96	13/87	0/100	11/89
Literature	12/88	14/86	7/93	15/85	12/88	5/95
Benchmark	8/92	8/92	4/96	16/84	8/92	8/91

In this study, the researcher classifies the citizen based on his/her legal literacy skill into six categories namely in learning process, legal awareness, political participation, public education on law, legal academician and legislating the act. The first number indicated percentage while the next number indicated number of participants. According to the result, L3 have definite agreement upon the privacy principles are required in the related election law. Also, they want to have specific verse about certification procedure for software and hardware and standard verification for vote content in the *e*-voting system. Meanwhile, L5 emphasizes the legal definition and proven technique to be more important compare to the other issues in the *e*-voting system. Interestingly, majority L6 feel the related privacy law are complex to be understood, whereas they involve directly in the parliament drafting process. Majority citizen see the parliament and government respond very slowly to the privacy issue, especially to draft and enact the regulation. The other categories also feel the complexity of the current legal regulation while there is around 44% (56) of L5 say the otherwise. Majority citizen also think that current regulation have not specified the hard punishment to the illegal actor. On the other hand, they want to have comprehensive privacy related law, which has been through comparison study with other relevant country, either its concept or its practice as the important requirement to have national *e*-voting. The enactment of legal regulation can raise the concern of privacy protection from eligible voters but it has no specific effect or relationship to shape the perception of eligible voters upon *e*-voting benefits.

There has been substantial effort to characterize or categorize users according to their privacy concern such as Altman [35], which made significant contributions by initiating a theory of privacy processes with a focus on social interaction, Meanwhile, Staddon, et al., [36] investigate concern, control and sharing and explore on how they are connected to difference behavior and attributes. Most people agreed with the concepts of privacy as a human right but they had more diverse viewpoints on privacy as a right not to be annoyed and they also revealed contradiction between privacy right and privacy norms [38]. However, even with the best attempts at education, many users will be left unqualified to make their own privacy decisions for every scenario because of the problem complexity [34]. The source of information and intensity of communication between citizens can determine the reaction and perception of the importance and objective of *e*-voting, especially the procedure and policy of privacy protection. Designing any privacy protection means the construction of a set of protocols that will satisfy the privacy requirements for the system without compromising the privacy of the individual datasets of the participants [37]. Measuring elections against a free and fair standard suggests a dichotomy when elections are actually political processes more realistically judged along a continuum and placed in context. This focus on the free and fair determination has encouraged international election assessments to make categorical, “bottom-line” judgments that fail to take nuances and context into account. Such judgments imply, inaccurately, that elections in democratic countries are beyond reproach [27]. Incorporating a duty of care into the definition allows for segmentation of malpractice by level of responsibility such as a senior election management official will have a heightened duty relative to the responsibilities of a temporary poll worker [28].

By extracting combining other result from similar project to align with the necessity of regulation, this study develop criteria and indicator [14, 22], which showed privacy protection could be improved through the active involvement and participation from users, committee and legislative member. There are 11 criteria with its indicator to strengthen the process of personal data protection in electronic voting. Mostly, citizens want to know the tabulation result quickly as possible to avoid segregation among community that can lead to greater scale of conflict. Meanwhile, citizen perceived that the implementation of electronic voting could save large national budget into other allocation for national growth. They also aware that classic problem from previous election which is data duplication and manipulation can be solved through electronic adoption. By perceiving benefit from electronic mechanism in casting and tabulating the votes, the citizen feels confidence and exciting to participate in electronic election and look out on how the implementation can bring the nation to further level. These criterions have positive direct influence towards personal data protection significantly. Thus, the citizens have specific reason, perception and motives to performing best of their action according to their ability to secure the general election and its personal data protection.

Table 4. Criteria and Indicator for Personal Data Protection Measures

Criterion	Indicator
Expectation to have quick result through e-voting	Tabulation results are produced and validated at least 24 hours after election has ended
The use of *e*-voting will increase the accuracy of personal information to prevent data duplication on voter's list and vote content	Eligible voters can cast vote wherever they are free without being bound by their address when the authentication take place
The use of *e*-voting will save government budget a lot	Accountability budget report of election implementation shows the savings more than a quarter than previous one.
Confidence to cast vote freely if the machine was proved in its credibility and eligibility through international standard	Testing, checking and certification result of the voting machine is published online that allowed public to look them at
Excitement to see own country to be one step closer in implementing e-voting like other country	Frequent news broadcasts on the progress e-voting implementation
Wonder to know the mechanism to report the privacy violation	Online publication and document provided by election commissioner on operational standard of electronic election in their formal website
The encryption of vote content from plain text to cyphertext will prevent unauthorized party to gain advantages	Comparison test of various encryption methods with different given context
The e-voting system should have simplified its user interface	GUI and accessibility test to ensure they meet specification, sequence and objective
The candidate or party that voters will choose is confidential	All ballot papers have to be sealed in the supreme court under strict condition and safeguards based constitution authorization, while they can only be retrieved by court order
Information on whether voters have casted vote or how they casted vote is secured and have not been published	The voting room/space should not be under surveillance camera
Disconnecting ballots content and identity of voters should preserve secrecy	The principle must be mandated by regulation

There are at least three important concerns from society towards privacy protection in the electronic voting, which are the reporting mechanism, encryption system and graphical user interface. Through decade, some people might witness the privacy infringement occurred next to them but they were reluctant to report to the authorized body. The reason behind it could be varied such as the complexity of channel and procedure for reporting, extreme responsibility being burdened to the one who reported or no further follow-up from election watchdog. Meanwhile, challenges remain with the data encryption security and safety such as modification, corruption and data theft. The concern has been growth among society that quite possible has been triggered by the fear of vandalism, terrorism and infringement. Initially, encryption comes out as double edge sword, which provides protection from malicious access in one side while it also can be used for dangerous reason. Furthermore, citizen also concern on the various aspect of graphical user interface such as component, configuration and features. Considering the multi-ethnic, diverse culture and different education background from nation, the GUI design development must take important note of accessibility, usability and simplicity. Interestingly, technical aspects also gain important spot based on citizen perspective, as they became more knowledgeable due to massive information from media. Citizen want the electronic voting procedure and mechanism value privacy of the user more than anything else, such as the protection of time of votes casted, voter's expression, right fulfilment, etc. All of these criterions became the most important aspect from the responsible committee to define privacy concept and determine privacy requirement into the election system.

In effect, differences in the privacy values of the two parties led to differences in their expectations of the appropriate community because they are not articulated but remain below the surface [28]. Meanwhile, users more often demand quality enhancements (by approximately threefold) than privacy enhancements but privacy features determine their satisfaction with the products [29]. In addition, strong privacy guarantees necessarily obscure information, when the intentional introduction of randomness into published outcomes may require adjustments to specific implementations of scientific replication [30]. In addition, voters' background characteristics have a significant impact on their ability to vote without error, both voters unintentionally cast for the wrong candidate and unintentional undervotes [33]. However, it is important to understand how user privacy concern have evolved over time that increase the intensity of data usage, wherein older people are much less likely to reveal information than younger people and refusals to reveal information have risen over time [39]. The lack of a

coherent and concrete concept of privacy can also hinder the development of technologies, legislations, public policies and practices pertaining to consumers, employees and citizens in both local and global sector [23]. Fundamental changes in information systems and the heavy dependence on computers increased significantly the risk of fraud. While no genuinely new frauds are expected, electronic variations of traditional frauds will be carried out with greater efficiency and effectiveness, will have potentially greater impact and will be more difficult to investigate [24]. According to Brenner [25], someone commits fraud if the following four elements are proved beyond a reasonable doubt, which are *Actus reus* (the perpetrator communicates false statements to the victim), *Mens rea* (the perpetrator communicates what she knows are false statements with the purpose of defrauding the victim), *Attendant circumstances* (the perpetrator's statements are false) and *Harm* (the victim is defrauded out of property or something of value). There are several serious issues, which cyber law should cover namely cybercrime, digital evidence, intellectual property, standardization, legislation synchronization, privacy protection, e-service and jurisdiction [26].

The complexities of legal regulation to be understood by citizen have been directed by the lack of accessibility of specific law information to be learnt properly by relevant agency lead to failure of principle practices and awareness in personal data protection. Therefore, the lack of public participation and discussion in drafting the legislation before regulation enactment resulted to an increase of citizen passiveness towards government attempt in enhance personal data protection in election. Moreover, the lacks of synergize and coherent idea between public interest and government concept implicated to vague and uncertain of verse definition and context. More cooperative and courteous of legal institution to convey the message in creating uniformity of best election practice have positive influence to help citizen better understanding of legal product implication and function. The high risk of exposure to the family might be as the crucial key for the citizen to resist in helping privacy violation precaution as government attempt to protect personal data in electronic election. Less interaction and communication among community increase the opportunities of privacy violation or possibility of privacy incident occurs, and vice versa. By establishing meaningful relationship with the society wherein the leading edge technologies provide high expectation as fortress to block serious threat internally and externally to privacy protection.

5. Conclusion

In the context of election, based on the user perspective through survey, the legal framework was inadequate to effectively regulate the development and use of voting machines, especially regarding security safeguards, the certification process and tabulation software. Meanwhile, people have viewed that current regulation is complicated to understand, which occur because various reasons such as the lack of accessibility, education and awareness. It leads creating misconception and misunderstanding among people of *e*-voting objective and intention. Thus, the election committee should engage people in determining their policy and direction especially related to their legal demands by coordinating them with relevant institution. To ensure the personal data protection, the compliance enforcement towards the guidelines became the critical factor. It has to be capable of extracting relevant security needs from social requirements and determining an acceptable level of residual risk to the community. It also needs to maintain documentation, which provides evidence of the decision maker's due diligence and demonstrates informed risk based decision-making. Thus, the parliament and government should recognize both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of election commission to collect, use or disclose personal data for legitimate and reasonable purposes in e-voting. Then, they should discuss and enact the comprehensive privacy regulation, as it is an essential requirement in the following initiative.

References

[1] Burstein A, Dang S, Hancock G, Lerner J. Legal issues facing election officials in an electronic-voting world. *Social Science Research Network*. 2007.

[2] Azhari R. E-voting. Fakultas Ilmu Komputer Universitas Indonesia 2005. Available at: http://staf.cs.ui.ac.id/WebKuliah/riset/hibah-B/VVCS/pdf/e-Voting.pdf.

[3] Priyono E, Dihan FN. *E-voting: Urgency of transparency and accountability*. Seminal Nasional Informatika. UPN Yogyakarta. 2010.
[4] Spink J, Moyer DC. Defining the Public Health Threat of Food Fraud. *Journal of Food Science*. 2011; 76(9).
[5] Reurink A. Financial Fraud: A Literature Review. MPIfG Discussion Paper. 2016; 16(5).
[6] Leemann L, Bochsler D. A systematic approach to study electoral fraud. *Electoral Studies.* 35; 33-47.
[7] Pearson S, Benameur A. *Privacy, Security and Trust Issues Arising from Cloud Computing*. Proc. IEEE CloudCom. 2010: 693-702.
[8] Bekara K, Laurent M, Nguyen TH. *Technical enforcement of European Privacy Legislation: an access control approach*. Proc. NTMS. 2012: 1-7.
[9] Power EM. Developing a Culture of Privacy: A Case Study. *IEEE Security & Privacy*. 2007; 5(6): 58-60.
[10] Dixon T. Valuing Privacy: An Overview and Introduction. *UNSW Law Journal.* 2001; 24(1): 239-246.
[11] Olsen J, Astrom J. Electronic voting in Sweden: hare or tortoise? In: N Kersting, H Baldersheim. *Editors*. Electronic voting and democracy: a comparative analysis. Basingstoke: Palgrave Macmillan; 2004: 149.
[12] Gomez J. Philippine Election 2010: Filipinos vote amid violence, computer glitches. Retrieved June 25, 2012 from The Huffington Post: http://www.huffingtonpost.com/2010/05/10/philippine-election-2010-_n_569800.html.
[13] Goldsmith B, Ruthfauff H. Case Study Report on Electronic Voting in the Netherlands. National Democratic Institute, IFES. USAID. 2008: 259.
[14] Lubis M, Kartiwi M, Zulhuda S. *Decision to casting a vote: an ordinal regression statistical analysis*. Proc. ICT4M. 2014.
[15] Eboli L, Mazzulla G. An Ordinal Logistic Regression Model for Analysing Airport Passenger Satisfaction. *EuroMed Journal of Business.* 2009; 4(1): 40-57.
[16] Schroeder LD, Sjoquist DL, Stephan PE. Understanding Regression Analysis: An Introductory Guide. Sage Publications, The International Professional Publishers. 1986.
[17] Prandini M, Ramilli M. A Model for E-voting Systems Evaluation Based on International Standards: Definition and Experimental Validation. *e-Service Journal JSTOR*. 2012; 8(3): 42-72.
[18] Dinev T. Why would we care about privacy. *European Journal of Information Systems*. 2014; 23(2): 97-102.
[19] Evans K. Vidal-Hall and Risk Management for Privacy Breaches. *Security & Privacy*. 2015; 13(5): 80-84.
[20] Putra SJ, Subiyakto A, Ahlan AR, Kartiwi M. A Coherent Framework for Understanding the Success of an Information System Project. *TELKOMNIKA Telecommunication Computing Electronics and Control*. 2016; 14(1): 302-308.
[21] Amali LN, Mahmuddin M, Ahmad M. Information Technology Governance Framework in the Public Sector Organizations. *TELKOMNIKA Telecommunication Computing Electronics and Control*. 2014; 12(2): 429-436.
[22] Lubis M, Kartiwi M, Zulhuda S. Privacy and Personal Data Protection in Electronic Voting: Factors and Measures. *TELKOMNIKA Telecommunication Computing Electronics and Control*. 2017; 15(1): 512-521.
[23] Dinev T. Why would we care about privacy. *European Journal of Information Systems.* 2014; 23(2): 97-102.
[24] Lucian V, Warren M, Mackay D. *Defining Fraud: Issues for Organizations from an Information Systems Perspective.* 7th Pacific Asia Conference on Information Systems. Adelaide, South Australia. 2003: 971-979.
[25] Brenner SW. Is There Such a Thing as Virtual Crime?. *California Criminal Law Review*. 2001: 1.
[26] Makarim E. Pengantar Hukum Telematika: Suatu Kompilasi Kajian. 1st Edition. Jakarta, Indonesia: RajaGrafindo Persada. 2005.
[27] Alvarez RM, Hall TE, Hyde SD. Election Fraud: Detecting and Deterring Electoral Manipulation, Brookings Institution Press. 2008.
[28] Codio S, Kafura D, Quiñones MP, Kavanaugh A, Gracanin D. *Identifying Critical Factors of Community Privacy*. ASE International Conference on Privacy, Security, Risk and Trust. Amsterdam. 2012: 666-675.
[29] Preibusch S. The Value of Web Search Privacy. *Computer and Reliability Societies.* 2015: 24-32.
[30] Heffetz O, Ligett K. Privacy and Data-Based Research. *The Journal of Economic Perspectives.* 2014; 28(2): 75-98.
[31] White I, Johnston N. Electoral fraud since 2010. Briefing Paper Number 6255. House of Commons Library. UK. 2017.
[32] pewcenteronthestates. Inaccurate, Costly and Inefficient. Election Initiative. 2012 Issue Brief.
[33] Herrnson PS, Hanmer MJ, Niemi RG. The Impact of Ballot Type on Voter Errors. *American Journal of Political Science.* 2012; 56(3): 716-730.

[34] Allison DS, Capretz MA, Tazi S. *A Privacy Manager for Collaborative Working Environments*. Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises. 2013: 110-116.
[35] Altman I. Privacy Regulation: Culturally Universal or Culturally Specific. *Journal of Social Issues.* 2010; 33(3): 66-84.
[36] Staddon J, Huffaker D, Brown L, Sedley A. *Are privacy concerns a turn-off? Engagement and privacy in social networks*. Symposium on Usable Privacy and Security. 2012: 1-13.
[37] Qusa H. *Does a privacy risk impose a real threat in collaborative environments?*. Palestinian International Conference on Information and Communication Technology. Gaza. 2013: 66-70.
[38] Huang HY, Bashir M. *Is Privacy a Human Right? An Empirical Examination in a Global Context*. Annual Conference on Privacy, Security and Trust. 2015: 77-84.
[39] Goldfarb A, Tucker C. Shifts in Privacy Concerns. *The American Economic Review.* 2012; 102(3): 349-353.