

Original Article

# Reflection on the principles and requirements of a secure electronic voting system

Hosseinali Kalhor\*<sup>1</sup> , Hossein Malakooti Hashajin<sup>2</sup>, Ayat Mulaee<sup>3</sup>, Mohammad Mazhari<sup>4</sup> 

<sup>1</sup> PhD student in Public Law, Faculty of Law and Social Sciences, University of Tabriz, Tabriz, Iran

<sup>2</sup> Assistant Professor, Department of Law, Faculty of Law and Social Sciences, University of Tabriz, Tabriz, Iran

<sup>3</sup> Assistant Professor, Department of Law, Faculty of Law and Social Sciences, University of Tabriz, Tabriz, Iran

<sup>4</sup> Associate Professor, Department of Law, Faculty of Law and Social Sciences, University of Tabriz, Tabriz, Iran



[20.1001.1.24237566.1401.6.2.9.8](https://doi.org/10.22080/LPS.2022.23738.1349)



[10.22080/LPS.2022.23738.1349](https://doi.org/10.22080/LPS.2022.23738.1349)

**Received:**

June 15, 2022

**Accepted:**

October 1, 2022

**Available online:**

December 3, 2022

**Keywords:**

Voting, technology, digital divide, functional requirements, logical integration process.

## Abstract

E-voting is considered to mean the further enhancement and strengthening of democratic processes in the information of modern societies. Electronic voting must first comply with the existing legal and regulatory framework. In addition, e-voting should be technically implemented in a way that specifies the requirements and regulations to reach the maximum number of users. As a result, the purpose of this article is twofold. In the first place (first), to identify the set of general requirements of the Constitution that must be considered when designing an electronic voting system for general elections. This set of requirements will lead to the acceptable design of the specific principles of a law for the electronic voting system. In the second stage (second), by identifying the process of logical integration, the requirements of the electronic voting system are determined. These requirements are the result of design principles that have already been identified. This research seeks to find the answer to the question whether the electronic voting scheme can meet the legal requirements as established in modern information societies. In addition, what differences can be made between different types of electronic voting system requirements? The results using the descriptive-analytical method and collecting library documents show that at present the possibility of electronic voting should be considered only as a complementary tool for traditional electoral processes. The main reason for this phenomenon is the digital divide, the inherent distrust of electronic voting, as well as the inadequacy of existing technology tools to meet certain requirements.

**\*Corresponding Author:** Hosseinali Kalhor

**Address:** PhD student in Public Law, Faculty of Law and Social Sciences, University of Tabriz, Tabriz, Iran

**Email:** [h.k137020@gmail.com](mailto:h.k137020@gmail.com)



## Extended abstract

### 1. Introduction

Despite the various approaches and ideas about how to institutionalize democracy and stabilize it in the national governance system, there is a consensus issue that the procedure and tools of the election should be defined and prepared in such a way as to maximize "transparency" and "impartiality", which are included. It should not be such that these procedures and tools influence people's choices and give them direction, and in practice provide the ground for improper uses and contrary to the general goals and principles of democratic systems. One of the tools that has attracted the attention of governmental and social policy makers in the development and improvement of all aspects of affairs in the last decade is "information and communication technology". The so-called "neutral", flexible and empowering nature of this technology and its tremendous effect in increasing efficiency and effectiveness have made those involved in the micro and macro spheres of society not to hesitate in electronicizing their affairs, and this practice among the countries of the world. An achieved position that has become a criterion for development. One of the topics that has seriously attracted the opinion of policymakers is the way and extent of using this technology in governance. In this regard, there are no exceptions and we try to use all its capacities. In this regard, we can mention topics such as electronic parliament and electronic legislation, which have passed their initial discussions and are approaching their evolution. "Electronic voting" has attracted much attention over the past years due to factors such as the increasing desire of societies to create

electronic government, electronic democracy and electronic governance. In general, electronic voting takes place in various parts of the government, such as the executive branch, parliament, various sectors of industry and universities.

### 2. Methods

The purpose of this article is to discuss whether the e-voting scheme can meet the legal requirements as it is set in modern information societies. This article discusses how to design and implement the electronic voting process in order to comply with the principles and democratic rights of elections as well as other types of human rights that form the cornerstone of international legal civilization. In this regard, the requirements of an electronic voting system are considered as designed principles that are necessary to comply with the legal framework governing general elections. Although technology moves at a faster pace than the legal system, its evolution should be pursued as a means to improve human life and not as an end in itself. In this regard, technological developments and especially those that affect fundamental principles should be carefully examined to ensure their contribution to improving the quality of life of citizens.

The second purpose of this article is to discuss trust in technology. Developers of information systems with electronic voting systems are faced with the prospect of ensuring an adequate level of security. Recent literature has often distinguished between different types of electronic voting system requirements. In the literature (CyberVote, 1999), requirements are usually identified by headings such as legal, technical, and user-oriented—the latter in the form of conditions that the system must meet (e.g., "the system allows

online voting from home"). Other authors choose to derive requirements for electronic voting systems only based on a specific electoral method (such as a paper absentee voting process (United States, 2000).

### 3. Findings

The findings indicated electronic voting systems should currently be considered only as a supplement and not a replacement for the existing paper-based voting systems. We base our offer mainly on the following:

The digital divide, which means the lack of equal access to the Internet and ICT infrastructure tools. Providing new tools and opportunities for participation, based on information and communication technology, in such a case can lead to the opposite result, that is, the removal of "illiterate information and communication technology" voters from the political process. An electoral system itself may organize an individual's unequal access to the electoral process. It is a matter of democracy and equality to ensure that different voting technologies are equal in terms of ease and opportunity of access.

### 4. Conclusion

Technology can help overcome the crisis of trust that representative democracy is experiencing today. The right to vote is a part of the democratic process that is deeply embedded in modern constitutions. In addition, it is considered one of the basic foundations of democracy.

In this paper, we have identified the general design principles of an Internet-based electronic voting system that derives from the relevant constitutional requirements. In addition, we have produced a set of performance requirements for electronic voting

systems that integrate the requirements imposed by existing (traditional) general election systems. To do this, a software engineering method (i.e. logical integrated process) was used, which is based on facilitating use cases. As a result, an electronic voting system is conceptualized in its own institution, in such a way that it limits the number of possible subsequent plans but does not dictate a specific plan.

Thus, it seems that it is really difficult to meet some of the requirements set forth by the law (for example, non-coercion) with the existing technology. In the current socio-technical conditions, the final result of our work is that - at present, electronic voting systems should be considered as a complementary means to traditional general election systems, provided that all necessary legal and technical requirements are adequately met. Therefore, it is expected that the traditional voting system will remain the main means of conducting the general election process, while the additional electronic voting capacity will be introduced only gradually.

### Funding

There is no funding support.

### Authors' contribution

Authors contributed equally to the conceptualization and writing of the article. All of the authors approved the content of the manuscript and agreed on all aspects of the work

### Conflict of interest

Authors declared no conflict of interest.

### Acknowledgments

We are grateful to all the persons for scientific consulting in this paper.

# تأملی بر اصول و الزامات سیستم رای‌گیری الکترونیکی امن

حسینعلی کلهر<sup>۱\*</sup>، سید حسین ملکوتی هاشجین<sup>۲</sup>، آیت مولائی<sup>۳</sup>، محمد مظهری<sup>۴</sup>

<sup>۱</sup> دانشجوی دکتری حقوق عمومی، دانشکده حقوق و علوم اجتماعی، دانشگاه تبریز، تبریز، ایران  
<sup>۲</sup> استادیار گروه حقوق، دانشکده حقوق و علوم اجتماعی، دانشگاه تبریز، تبریز، ایران  
<sup>۳</sup> استادیار گروه حقوق، دانشکده حقوق و علوم اجتماعی، دانشگاه تبریز، تبریز، ایران  
<sup>۴</sup> دانشیار گروه حقوق، دانشکده حقوق و علوم اجتماعی، دانشگاه تبریز، تبریز، ایران



[20.1001.1.24237566.1401.6.2.9.8](https://doi.org/10.22080/LPS.2022.23738.1349)



[10.22080/LPS.2022.23738.1349](https://doi.org/10.22080/LPS.2022.23738.1349)

## چکیده

رای‌گیری الکترونیکی به معنای افزایش و تقویت بیشتر فرآیندهای دموکراتیک در اطلاعات جوامع مدرن تلقی می‌شود. رای‌گیری الکترونیکی ابتدا باید با چارچوب قانونی و نظارتی موجود مطابقت داشته باشد. علاوه بر این، رای‌گیری الکترونیکی باید از نظر فنی به گونه‌ای پیاده‌سازی شود که الزام و مقررات به حدنصاب رسیدن حضور کاربران را مشخص کند. در نتیجه، هدف این مقاله دوگانه است. در وهله نخست، برای شناسایی مجموعه الزامات عمومی قانون اساسی است که بایستی هنگام طراحی سیستم رای‌گیری الکترونیکی برای انتخابات عمومی در نظر گرفته شوند. این مجموعه الزامات منجر به طراحی قابل قبول اصول خاص یک قانون برای سیستم رای‌گیری الکترونیکی خواهد شد. در مرحله دوم، با شناسایی فرآیند یکپارچه‌سازی منطقی، الزامات سیستم رای‌گیری الکترونیکی مشخص می‌شود. این الزامات ناشی از طراحی اصولی است که پیش از این شناسایی شده‌اند. این پژوهش در پی یافتن پاسخ این سؤال است که آیا طرح رای‌گیری الکترونیکی می‌تواند الزامات قانونی را همان‌طور که در جوامع اطلاعاتی مدرن وضع شده است، برآورده کند؟ بعلاوه اینکه چه تفاوت‌هایی بین انواع مختلف الزامات سیستم رای‌گیری الکترونیکی می‌توان قائل شد؟ نتایج این پژوهش با بهره‌گیری از روش توصیفی-تحلیلی و جمع‌آوری اسناد کتابخانه‌ای نشان می‌دهد که در حال حاضر قابلیت رای‌گیری الکترونیکی باید تنها به‌عنوان وسیله‌ای مکمل برای فرآیندهای سنتی انتخابات در نظر گرفته شود. دلیل عمده این پدیده به شکاف دیجیتال، بی‌اعتمادی ذاتی به روش رای‌گیری الکترونیکی و همچنین ناکافی بودن ابزارهای فناوری موجود برای برآوردن برخی الزامات باز می‌گردد. هدف از انجام این تحقیق بررسی اصول و الزامات سیستم رای‌گیری الکترونیکی با نگاهی به الزامات امنیتی و غیر امنیتی کاربران و همچنین کاربردی می‌باشد.

تاریخ دریافت:

۲۵ خرداد ۱۴۰۱

تاریخ پذیرش:

۹ مهر ۱۴۰۱

تاریخ انتشار:

۱۲ آذر ۱۴۰۱

کلیدواژه‌ها:

رای‌گیری، فناوری، شکاف دیجیتال، الزامات عملکردی، فرآیند یکپارچه‌سازی منطقی، انتخابات

\* نویسنده مسئول: حسینعلی کلهر

آدرس: دانشجوی دکتری حقوق عمومی، دانشکده حقوق و علوم ایمیل: [h.k137020@gmail.com](mailto:h.k137020@gmail.com)

اجتماعی، دانشگاه تبریز، تبریز، ایران

## ۱ مقدمه

۱۴۰۰: ۱۸۰-۱۸۱) دلایل زیر منجر به افزایش تمایل جوامع نسبت به اتخاذ روش رأی‌گیری الکترونیکی شده است:

۱- رأی‌گیری الکترونیکی این امکان را برای رأی‌دهندگان فراهم می‌آورد تا رأی خود را از مکانی غیر از مرکز رأی‌گیری در منطقه رأی‌گیری خود، ارائه دهند ۲- تسهیل فرآیند رأی‌گیری ۳- تسهیل مشارکت در انتخابات و همه‌پرسی برای تمامی کسانی که اعم از شهروندان مقیم یا خارج از کشور حق رأی دارند ۴- دسترسی به فرآیند رأی‌دهی برای رأی‌دهندگان دارای معلولیت یا کسانی که برای حضور فیزیکی در مراکز رأی‌دهی از مشکلات دیگری رنج می‌برند. ۵- افزایش مشارکت رأی‌دهندگان به وسیله ایجاد کانال‌های رأی‌گیری مضاعف ۶- کاهش هزینه کلی برای برگزاری انتخابات یا فراندوم ۷- امکان ارائه نتایج به صورت سریع و قابل اعتماد (Report of the Speaker's Commission, 2015; 55-56)

همانگونه که پیش‌تر نیز مورد اشاره قرار گرفت، رأی‌گیری الکترونیکی و استفاده از فناوری‌های دیجیتال فرآیندی است که در بسیاری از بخش‌های حاکمیت از جمله انتخابات پارلمان نیز می‌تواند مورد استفاده قرار گیرد. در انتخابات پارلمان مشارکت رأی‌دهندگان شاخص اصلی سلامت دموکراسی تلقی می‌گردد، حضور اندک رأی‌دهندگان نشانگر کارکرد نه‌چندان مطلوب دموکراسی در یک کشور است. به طور مثال در کشور بریتانیا، پیشتر یکی از دلایل مشارکت پایین مردم در انتخابات پارلمان، عدم نام‌نویسی آنان برای رأی‌گیری بود. لذا در حال حاضر به منظور رفع مانع مذکور در این کشور، از نام‌نویسی آنلاین برای مشارکت در انتخابات استفاده می‌شود. همچنین در این ارتباط از کارهای مهم و تأثیرگذاری که نهادهای دیگری همانند کمیسیون انتخاباتی که یک نهاد مستقل و ناظر بر سیستم انتخاباتی در بریتانیا است برای آموزش مردم در مورد نحوه ثبت نام الکترونیکی به منظور

یکی از ابزارهایی که طی دهه اخیر نظر سیاست‌گذاران حاکمیتی و اجتماعی را در توسعه و ارتقای همه جانبه امور به خود جلب کرده، «فناوری اطلاعات و ارتباطات» است. ماهیت به اصطلاح «خنثی»، انعطاف‌پذیر و تواناساز این فناوری و تأثیر شگرف آن در افزایش کارایی و اثر بخشی باعث شده دست‌اندرکاران حوزه‌های خرد و کلان جامعه در الکترونیکی کردن امور خود تردید نکنند و این رویه در میان کشورهای جهان به جایگاهی دست یافته که به معیاری برای توسعه یافتگی تبدیل شده است.

یکی از موضوعاتی که به طور جدی نظر سیاست‌گذاران را به خود جلب کرده، نحوه و میزان به کارگیری این فناوری در حکمرانی است. در این خصوص هیچ استثنایی هم لحاظ نشده و سعی بر این است که از همه ظرفیت‌های آن استفاده شود. که در این خصوص می‌توان به مباحثی نظیر پارلمان الکترونیکی و قانون‌گذاری الکترونیکی که مباحث نخستین خود را پشت سر گذاشته‌اند و به تکامل خود نزدیک شده‌اند، اشاره کرد. (فتحیان و تقوی، ۱۳۸۷: ۲)

«رأی‌گیری الکترونیکی» طی سالیان گذشته به دلیل عواملی چون افزایش تمایل روزافزون جوامع به ایجاد دولت الکترونیکی، دموکراسی الکترونیکی و نیز حاکمیت الکترونیکی توجه زیادی را به خود جلب کرده است. به صورت کلی رأی‌گیری الکترونیکی در بخش‌های مختلفی از حاکمیت از جمله قوه مجریه، پارلمان، بخش‌های مختلف صنعت و دانشگاه صورت می‌گیرد. اصطلاح رأی‌گیری الکترونیکی، به رأی دادن به صورت الکترونیکی، استفاده از اینترنت برای اظهارنظر در مورد مسائل سیاسی، جدول‌بندی آرا به روش الکترونیکی برای سیستم‌های الکترونیکی یکپارچه از مرحله ثبت نام رأی‌دهندگان و نامزدها تا انتشار نتایج انتخابات، اطلاق می‌گردد. (امیری زرگ آباد و ملکوتی هاشجین،



چارچوب قانونی حاکم بر انتخابات عمومی ضروری است.

هدف دوم این مقاله، بحث درباره اعتماد به فناوری است. توسعه‌دهندگان سیستم‌های اطلاعاتی با سیستم‌های رای الکترونیکی، با چشم‌اندازی برای اطمینان از سطح کافی از امنیت روبه‌رو می‌شوند. (Cramer R., Franklin, 1996; 72-73) ادبیات اخیر، اغلب بین انواع مختلف الزامات سیستم رای‌گیری الکترونیکی تمایز قائل شده است. (CyberVote, 1999) در ادبیات، الزامات، معمولاً با عناوینی چون حقوقی، فنی و کاربرمحور شناسایی می‌شوند-مورد دوم در قالب شرایطی است که سیستم باید رعایت کند (مانند «سیستم اجازه رای‌گیری آنلاین را از خانه می‌دهد»). سایر نویسندگان استخراج الزامات برای سیستم‌های رای‌گیری الکترونیکی را تنها بر اساس روش انتخاباتی خاصی (مانند فرآیند رای‌گیری غیرحضوری کاغذی) (United Sates, 2000) انتخاب می‌کنند.

### ۳ سازماندهی پژوهش

ساختار مقاله به شرح ذیل است: ابتدا به موضوعات اصلی در مورد رای‌گیری الکترونیکی برای انتخابات همگانی اشاره و سپس الزامات عمومی قانون اساسی و طراحی اصول مربوطه که چنین فرآیند انتخاباتی‌ای را باید رعایت کند، خلاصه می‌کند. در ادامه، اصول طراحی سیستم رای‌گیری تحلیل و متعاقب آن به‌طور مختصر روش‌شناسی‌ای را ارائه می‌دهد که برای شناسایی و توصیف نیازهای کاربر سیستم رای‌گیری الکترونیکی استفاده می‌شود.

#### ۳٫۱ مسائل اصلی رای‌گیری الکترونیکی

چالش اساسی دموکراسی الکترونیکی، بهبود و توسعه دموکراسی، نمایندگی و تقویت فرآیندهایی با هدف توانمندسازی شهروندان است (European Commission, 2000) تمدن جدید که جامعه اطلاعاتی آن را به‌وجود آورده است، باید با اصول و ارزش‌های دموکراسی مطابقت داشته باشد. معرفی

رای دادن، حمایت به عمل می‌آید (Report of the Speaker's Commission, 2015; 58)

فناوری دیجیتال می‌تواند در دستیابی بیشتر به اطلاعات مورد نیاز در ارتباط با نامزدها و احزاب سیاسی کمک شایانی نماید. در این راستا وجود وبسایت‌ها و اپلیکیشن‌های ویژه برای کمک به شهروندان در ارتباط با تصمیم‌گیری در مورد رای دادن آنان، بسیار تأثیرگذار می‌باشد. برنامه‌ها و وبسایت‌های مشاوره‌ای می‌توانند به وسیله اقداماتی نظیر أخذ نظرات و دیدگاه‌های شهروندان و تطبیق آنان با سیاست‌های احزاب مختلف، به شهروندان کمک کنند تا تصمیم بگیرند که به چه کسی رای دهند. این فرآیند نباید به وسیله پارلمان و در وبسایت مربوط به آن صورت گیرد زیرا پارلمان در هر صورتی بایستی بیطرفی خویش را حفظ نماید. باین‌حال تمامی افراد جامعه متمایل به استفاده از چنین اپلیکیشن‌هایی نمی‌باشند و بسیاری از آنان این اپلیکیشن‌ها را فقط در صورتی مفید تلقی می‌کنند که آنان را برای دسترسی به اطلاعات مربوط به نامزدها و احزاب یاری نماید (Report of the Speaker's Commission, 2015; 58) جامعه اطلاعاتی در حال ظهور، مردم کشورهای توسعه‌یافته را قادر به انجام چندین فعالیت به‌صورت مستقیم، خودکار، کارآمد و همچنین به‌صورت الکترونیکی می‌سازد.

### ۲ اهداف پژوهش

هدف اول این مقاله، بحث در مورد این است که آیا طرح رای‌گیری الکترونیکی می‌تواند الزامات قانونی را، همان‌طور که در جوامع اطلاعاتی مدرن وضع شده است، برآورده کند؟ این مقاله چگونگی طراحی و اجرای فرآیند رای الکترونیکی را به منظور انطباق با اصول و حقوق دموکراتیک انتخابات و همچنین سایر انواع حقوق بشر که سنگ بنای تمدن حقوقی بین‌المللی را تشکیل می‌دهند، مورد بحث قرار می‌دهد. در این راستا، الزامات یک سیستم رای‌گیری الکترونیکی به عنوان اصول طراحی شده در نظر گرفته می‌شود که رعایت آن‌ها برای انطباق با

اساسی‌اند. بررسی حقوقی نظام انتخاباتی در ایران، در همان گام نخست دو چالش را پیش می‌کشد: نخست انباشتگی قوانین انتخاباتی و دوم کاستی‌های این قوانین. انباشتگی قوانین عادی بدون در نظر داشتن مصوبه‌های پیرامونی مانند دیدگاه‌های تفسیری شورای نگهبان و یا آیین‌نامه‌ها در حوزه انتخابات بیش از اندازه بوده است. با آنکه نظام انتخاباتی در ایران پیشینه‌ای بیش از یک سده دارد و جامعه و دولت ایرانی بارها انتخابات را آزموده و از این در نیازی به قانون‌های پیاپی و دنباله‌دار نبوده، ولی پس از انقلاب بیش از هشتاد قانون عادی در باره انتخابات تصویب شده که نیمی از آنها در باره انتخابات مجلس شورای اسلامی است. سه قانون اصلی درباره نظام انتخابات مجلس شورای اسلامی ۱۳۵۸، ۱۳۶۲ و ۱۳۷۸ و نزدیک به بیست و پنج قانون اصلاحی نسبت به این سه قانون بیانی از وضعیت نظام حقوقی انتخابات در ایران است. (آذر باد، حق شناس، ۱۴۰۰، ۴-۱۲۳) مساله انتخابات الکترونیک در ایران هرچند در پرتو مسائلی چون تسهیل در فرایندهای انتخاباتی، کاهش قابل توجه هزینه‌ها و ایجاد شفافیت ناشی از سرعت شمارش آراء و به تبع آن کاستن از خطر دستکاری انتخاباتی قابل درک است اما سویه مهمتر آن ایجاد بستری برای گذار به دموکراسی از طریق یک نظام انتخاباتی منسجم، در دسترس و قابل اعتمادتر است. از این رو مساله انتخابات الکترونیک در ایران را از چنین منظری باید مورد ملاحظه قرار داد. (همان، ۱۲۸) به‌علاوه این که الزامات بنیادی دموکراسی برای آن‌ها در جهت مجموعه الزامات عمومی رأی‌گیری در قانون اساسی ایجاد می‌شود. این مجموعه به نوبه خود منعکس‌کننده مجموعه اصول اساسی طراحی رأی‌گیری است (جدول ۱). Dimitris A. (Gritzalis, 2002, p.541).

سیستم رأی‌گیری الکترونیکی باید با این قانون مطابق بوده چراکه رأی‌دادن یکی از کارکردهایی است که «شهروندان الکترونیک» ممکن است بخواهند به صورت آنلاین انجام شود. در این راستا، پدیده شکاف دیجیتالی باید مورد توجه قرار گیرد. دسترسی مقرون‌به‌صرفه به اینترنت، کلیدی برای مبارزه با شکاف دیجیتالی بین «غنا (اطلاعات)» و «فقر (اطلاعات)» در یک جامعه اطلاعاتی است. در این راستا باید سیاست‌های خاصی اتخاذ شود. برای مثال، اتحادیه اروپا سه اقدام کلیدی اتخاذ کرده است: الف) انطباق چارچوب قانونی موجود با نیازهای صنعت ارتباطات در اینترنت، ب) تقویت رقابت در شبکه‌های دسترسی محلی، به‌منظور تشویق گسترش اینترنت و دسترسی به اینترنت پرسرعت در اروپا و ج) برای اطمینان از استاندارد بالای حقوق کاربر و حفاظت از حریم خصوصی.

یک سیستم انتخاباتی ممکن است به خودی‌خود دسترسی نابرابر یک فرد را به فرآیند انتخابات تحمیل کند<sup>۱</sup>. تضمین برابری فناوری سنتی و رأی‌گیری الکترونیکی، با توجه به سهولت و فرصت دسترسی، موضوع دموکراسی و برابری است. انتخابات پارلمانی باید آزاد، برابر و مخفی باشد. در عین حال، روند انتخابات باید شفاف و در معرض نظارت عمومی باشد.

قانون اساسی بسیاری از کشورها ایجاد می‌کند که انتخابات عمومی باید به کلیت، آزادی، برابری، رازداری و مستقیم‌بودن احترام بگذارد. همچنانکه نظام حقوقی انتخابات در ایران بر پایه اصل‌های قانون اساسی، گزاره‌های قانونی و رویه‌های انتخاباتی بنیاد گرفته است. این سه خاستگاه، در طول هم جای می‌گیرند و گزاره‌های قانونی پیرو قانون اساسی و رویه‌های انتخاباتی نیز پیرو قانون عادی و قانون

Partizipationsmöglichkeiten (www.tauss.de/bn/e-vote.html).

1. Tauss J., Kollbeck J., e-vote: Die elektronische Briefwahl als ein Beitrag zur Verbesserung der



### جدول ۱ الزامات قانون اساسی و اصول طراحی

| الزامات قانون اساسی | اصول طراحی سیستم‌های رای‌گیری   |
|---------------------|---|
| ۱- اصول کلی         | ۱- از نظر شکل و روابط متناظر یا مشابه با سنت. ۲- شایستگی                            |
| ۲- آزادی            | ۱- عدم اجبار ۲- عدم تبلیغات در سایت رای‌گیری الکترونیکی ۳- قابلیت رای‌گیری غیرمعتبر |
| ۳- برابری           | ۱- برابری نامزدها ۲- برابری رای‌دهندگان ۳- یک رای‌دهنده-یک رای                      |
| ۴- مخفی بودن        | ۱- مخفی بودن ۲- تعادل امنیت در مقابل شفافیت   |
| ۵- مستقیم بودن      | ۱- ثبت و شمارش آرا بدون نظارت   |
| ۶- دموکراسی         | ۱- اعتماد و شفافیت ۲- قابلیت تایید و پاسخگویی ۳- قابلیت اطمینان و امنیت ۴- سادگی    |

## ۳٫۲ اصول طراحی شده سیستم‌های رای‌گیری

همانگونه که ابزارهای مختلفی در نظام‌های سیاسی و حقوقی کشورهای جهان به عنوان مواردی برای طراحی رای‌گیری شناخته می‌شوند. بدین ترتیب می‌توان برای تحقق سیستم‌های رای‌گیری اصول مختلفی را در نظر گرفت و پیشنهاد داد که به شرح ذیل می‌باشد.

### ۳٫۲٫۱ عمومیت

حق رای همگانی، اصلی کلی برای انتخابات دموکراتیک است که درخواست شرکت هر رأی‌دهنده واجد شرایط را در روند انتخابات دارد که هیچ‌کس نتواند طرد یا مورد تبعیض شود. پیامدهای ناشی از این اصل به شرح زیر است:

۱- هر رأی‌دهنده حق دارد در فرآیند انتخابات شرکت کند.

۲- توانایی شرکت در فرآیند انتخاباتی (شرایط صلاحیت) باید مبتنی بر قانون و قابل کنترل باشد.

۳- امکانات و فناوری‌های رای‌گیری باید برای هر رأی‌دهنده قابل دسترسی باشد.

۴- رای‌الکترونیکی باید به عنوان روشی جایگزین برای استفاده از حق رای در نظر گرفته شود.

۵- اصل دموکراتیک (یعنی هر رأی‌دهنده واجد شرایط باید در فرآیند انتخابات حضور داشته باشد) به زیرساخت‌های مناسب در دسترس عموم (مانند کیوسک‌های اینترنتی عمومی، رای‌گیری اینترنتی در ادارات دولتی و غیره) منجر می‌شود تا شهروندان بتوانند از حقوق خود استفاده کنند. ( Dimitris A. Gritzalis, 2002, p.541 )

رای‌گیری الکترونیکی کلیت رویه‌های انتخاباتی را با ارائه گزینه‌ای اضافی برای مشارکت در روند انتخابات بهبود می‌بخشد. موضوعی که مطرح می‌شود این است که آیا شرکت در انتخابات از طریق رای‌گیری الکترونیکی باید مشروط به اثبات شرایطی خاص مانند رای‌گیری پستی باشد؟ در اکثر کشورهای رای‌گیری پستی ایجاد شده است، فقط افراد خاصی مجاز به استفاده از این گزینه هستند.

پذیرش قابلیت رای‌الکترونیکی به عنوان یک استثنا از قاعده (یعنی بر اساس اثبات یک شرط خاص، که از رای دادن واجدین شرایط به صورت فیزیکی جلوگیری می‌کند) به طور کلی قابل قبول تلقی می‌شود. از سوی دیگر، تحول به سمت جامعه اطلاعاتی تأثیر بسزایی بر توانایی شهروندان در اعمال حقوق خود دارد. در پرتو چنین تصمیم سیاسی برای بهبود دولت الکترونیک و مشارکت الکترونیکی،



## ۳،۲،۲ آزادی

اصل انتخابات آزاد ایجاب می‌کند که فرآیند انتخابات بدون اعمال هیچ‌گونه خشونت، اجبار، فشار، مداخله، دستکاری یا هرگونه نفوذ دیگر از سوی دولت یا یک یا چند نفر انجام شود. در رای‌گیری پستی، ممکن است از رای‌دهنده خواسته شود بیانیه‌ای را روی گواهی‌نامه رای‌گیری امضا کرده و تعهد دهد که شخصاً برگه رای را پر کرده است. ارائه چنین امضایی در رای‌گیری الکترونیکی بی‌اهمیت نیست. (IST-2000-29518) e-VOTE (project), 2002 رویه‌های رای‌گیری الکترونیکی، فراتر از رای‌گیری پستی، تهدیدهای جدیدی برای آزادی و یکپارچگی تصمیم رای‌دهندگان ایجاد می‌کند. به عنوان مثال، در محل کار، حتی اگر کارفرما، سرپرست یا همکار بالای سر کارمند رای‌گیری الکترونیکی نایستد، مدیران سیستم می‌توانند فعالیت را در هر حوزه اخذ رای، نظارت یا یک کپی از برگه رأی را ضبط کنند. (Kim A, 2001)

برای عدم اجبار و جلوگیری از خرید و اخاذی رای می‌توان از سیستم رای‌گیری الکترونیکی که به گونه‌ای تضمین‌کننده برای جلوگیری از ثابت کردن استفاده از روشی خاص (عدم ردیابی از طرف رای دهنده)، طراحی شده است، استفاده کرد.<sup>۱</sup> (از آن‌جا که رابطه افراد در محل کار متوازن نیست، پیشنهاد می‌شود از رای‌گیری الکترونیکی در محل کار خودداری شود. به هر ترتیب، به سختی می‌توان از اجبار به رای دادن با فناوری به صورت انفرادی جلوگیری کرد. یک راه حل برای این امر، ایجاد زیرساختی در دسترس عموم است که به رأی‌دهندگان اجازه می‌دهد بدون اجبار هر شخص ثالثی از حقوق خود استفاده کنند.

در صورتی که یک پیام تبلیغاتی در حالی که رای‌دهنده در حال رای دادن الکترونیکی خود است، روی صفحه رایانه نمایش داده شود، آزادی در

معرفی یک قابلیت رای دهی باید به عنوان مکملی از سیستم رای‌گیری سنتی در نظر گرفته شود.

صلاحیت را می‌توان از طریق ثبت‌نام واجدان شرایط و شناسایی آن‌ها در لحظه ثبت‌نام تضمین کرد. ثبت‌نام و احراز هویت رویه‌هایی ضروری برای اطمینان از رعایت اصل حق رأی عمومی و عدم تقلب در انتخابات هستند. هدف از ثبت‌نام رای‌دهندگان تضمین این اصل است که تنها افراد واجد شرایط رای‌دادن، طبق قانون می‌توانند این کار را انجام دهند و هیچ‌کس نمی‌تواند بیش از یک بار رای دهد.

موضوع دیگر این است که آیا در رای‌گیری الکترونیکی نیاز به ثبت‌نام وجود دارد؟ رای‌گیری الکترونیکی به‌نوعی مشابه رای‌گیری پستی است. هنگامی که سیستم رای‌گیری الکترونیکی معرفی می‌شود، معمولاً مراحل ثبت‌نام و اخذ مجوز لازم است. این رویه‌ها به دلایل زیر با اصل انتخابات عمومی مغایرت ندارد: الف) با فرض عدم وجود ثبت‌نام ملی رای‌دهندگان آنلاین، برای جلوگیری از تقلب در رای و حمایت از یکپارچگی انتخابات، پیش‌ثبت‌نام برای رای‌گیری الکترونیکی ضروری است. از سوی دیگر، سیستم ثبت‌نام رای‌دهندگان مبتنی بر اینترنت، می‌تواند در برابر تقلب در مقیاس بزرگ آسیب‌پذیر باشد. (Internet Policy, Institute, 2001) و ب) در صورتی که رای‌گیری الکترونیکی جایگزینی برای رویه سنتی، ثبت‌نام یا اعلامیه‌ای باشد که رای‌دهنده مایل به استفاده از آن است، گزینه رای‌دادن نباید منجر به طرد یا تبعیض شود. علاوه بر این، باید اطمینان حاصل شود که ثبت‌نام، شناسایی و احراز هویت برای رای‌دهندگان الکترونیکی سهل است، زیرا رویه‌های پیچیده می‌تواند برای آن‌ها دشوار باشد. (California Institute of Technology, 2001)

<sup>1</sup> Adler J., Internet Voting Primer (www.votehere.net/adacompliant/whitepapers/primer).



باشند تا بتوانند عملکرد مناسب آن را ایجاد کنند. اصل برابری ایجاب می‌کند هر رأی، چه فیزیکی و چه آنلاین، به‌طور مساوی به نتیجه انتخابات متناسب با آن سنجیده شود. در شرایط رای‌گیری الکترونیکی، رای‌دهندگان خاصی از مزیت دسترسی به فناوری، توانمند و در نتیجه، از قابلیت رای‌گیری الکترونیکی برخوردارند. برخی استدلال می‌کنند که رای‌گیری از راه دور می‌تواند برای دستکاری نتایج انتخابات با مدیریت دسترسی به‌نحوی که به نفع کسانی باشد که بیشترین اتصال به شبکه را دارند مورد استفاده قرار گیرد. (Phillips, 2001; 73-85)

به دلیل ویژگی‌های نوظهور فناوری، حق دسترسی برابر به فرآیند رای‌گیری باید به حق دسترسی برابر به فناوری انتخابات بدل شود.<sup>۲</sup> در نتیجه، باید رویه‌ای بدون تبعیض به رای‌دهندگان ارائه شود که به آن‌ها اجازه دهد بدون هیچ مانعی از حق رای خود استفاده کنند. دسترسی برابر بدین معنا است که سیستم باید کاربرپسند و مستقل از تحصیلات، سن و شرایط فیزیکی رای‌دهنده باشد (برای رای‌دهندگان معلول جسمی).

سیستم رای‌گیری الکترونیکی باید از رعایت اصل یک رای‌دهنده-یک رای اطمینان حاصل کند. یعنی تنها رای‌دهندگان واجد شرایط می‌توانند فقط یک‌بار، چه آنلاین یا آفلاین رای دهند. بنابراین، سیستم رای‌گیری الکترونیکی باید به گونه‌ای طراحی شود که از موارد زیر جلوگیری کند: الف) تکرارپذیری رای (چه توسط خود رای‌دهنده یا توسط شخص دیگری)، ب) از قابلیت استفاده مجدد از رای (چه با رای دادن آنلاین و آفلاین) و ج) تغییر رای شرکت‌کنندگان (بعد از این‌که رای‌دهنده رای خود را ارسال کرد).

تصمیم رای‌دهنده ممکن است نقض شود. در طرح‌های انتخاباتی فعلی، تبلیغات در (مجاورت) محل رای‌گیری مجاز نیست. روش (رویه) رای‌گیری الکترونیکی همچنین باید تبلیغات نهادهای سیاسی در وبسایت رای‌گیری الکترونیکی را از نظر فنی غیرممکن کند. تضمین بیان آزادانه اولویت‌های رای‌دهنده<sup>۱</sup> باید از طریق جلوگیری از امکان انداختن رای آگاهانه باطله (یا کاغذ سفید) انجام شود.

### ۳،۲،۳ برابری

الزام برابری در زمینه انتخابات عمومی، منعکس‌کننده اصل برابری است که یکی از سنگ‌بناهای دموکراسی‌های مدرن را تشکیل می‌دهد. بر اساس اصل حق رای برابر، دو شرط عمده شناسایی شده است: الف) برابری میان احزاب سیاسی شرکت‌کننده و نامزدها و ب) برابری در مورد حق رای هر رای‌دهنده؛ الزامی که از اصل برابری ناشی می‌شود این است که برگه‌های رای الکترونیکی باید به گونه‌ای مشابه آن‌چه که برای برگه‌های رای کاغذی استفاده می‌شود؛ ویرایش و نمایش داده شود. برابری انتخاباتی مستلزم آن است که انحراف معناداری بین ظاهر برگه رای چاپی و معادل الکترونیکی آن وجود نداشته باشد. علاوه بر این، قرار دادن برگه‌های رای الکترونیکی در سایت رای‌گیری (یعنی روی صفحه کامپیوتر) باید دسترسی برابر را تضمین کند. بنابراین، «ظاهر و احساس» وبسایت و برگه‌های رای‌گیری الکترونیکی نباید به نفع یا تبعیض علیه هیچ‌یک از احزاب شرکت‌کننده باشد. یکی دیگر از عناصر برابری در میان احزاب شرکت‌کننده این است که آرای رأی‌دهنده بدون هیچ‌گونه تغییر یا مداخله‌ای ارسال و شمارش می‌شود. رای اخذ شده معتبر نباید در طول فرآیند رای‌گیری تغییر یا حذف شود. بنابراین بایستی از شفافیت نیز حمایت شود. تمام احزاب باید فرصت دسترسی برابر به عناصر روند رای‌گیری را داشته

<sup>2</sup> Burkert H., "Elektronische Demokratie: Einige staats und verfassungsrechtliche Anmerkungen" (<http://www.gmd.de/People/Herbert.Burkert/ARCHIV>).

<sup>1</sup> Rüß O., Wahlen im Internet, quelle multimedia und recht (<http://www.Internetwahlen.de/project/ruess.html>).

مقررات انتخاباتی که برای رای‌گیری پستی و حفاظت از محرمانه بودن ارتباطات قابل اجرا است، می‌تواند مبنایی برای حل مشکل حریم خصوصی سیاسی باشد. با این حال، هیچ تضمینی برای رهایی از نفوذ خارجی توسط اشخاص ثالث در هنگام اخذ آرا وجود ندارد. این یک خطر ذاتی هر نوع رای‌گیری از راه دور یا الکترونیکی است. برای مقابله (مواجهه) با این خطر باید اقداماتی در سطح قانونی و نظارتی انجام شود تا اقدامات کافی در برابر اجبار و تحریم رفتار غیرقانونی اعمال شود. مخفی بودن باید با اصول دموکراتیک برای انتخابات عمومی هماهنگ باشد. محرمانه بودن رای باید با شفافیت و قابلیت حسابرسی کل فرآیند رای‌گیری تطبیق داده شود (منطبق باشد). سیستم انتخاباتی باید اجازه دهد قبل از مشاهده یا شمارش آرا، صحت برگه رای تایید شود. به منظور حفظ محرمانه بودن، برگه‌های رای داده شده باید رمزگشایی و تنها پس از بررسی و حذف اطلاعات احراز هویت، شمارش شوند. سیستم رای‌گیری الکترونیکی باید کنترل و بازشماری آرا را از نظر فنی امکان پذیر کند و در عین حال از غیرقابل شناسایی بودن رای‌دهندگان اطمینان حاصل کند (International Working Group, 2001)

### ۳،۲،۵ مستقیم بودن

اصل انتخاب مستقیم ایجاب می‌کند که هیچ واسطه‌ای در روند تصمیم‌گیری در رای‌گیری وجود نداشته باشد. این اصل ممکن است برای تناسب با روش رای‌گیری الکترونیکی نیز تطبیق داده شود. شرط مربوطه این است که هر برگه رای آنلاین مستقیماً ضبط و شمارش شود.

در صورتی که دوره رای‌گیری با روش رای‌گیری (آنلاین یا آفلاین) که برای رای دادن استفاده می‌شود، متفاوت باشد، ممکن است مشکل ایجاد شود. نتایج رای‌گیری آنلاین ممکن است بر نتیجه کل فرآیند انتخابات تأثیر بگذارد و یکپارچگی و مشروعیت کل فرآیند را محدود کند. برای جلوگیری از این امر، می‌توان سیستمی ایجاد کرد که امکان ضبط و نگهداری آرای کنشگران را فراهم کند، در حالی که

موضوع دیگر، مدت زمان رای‌گیری الکترونیکی است. کارگروه رای‌گیری اینترنتی کالیفرنیا پیشنهاد می‌کند که رای‌گیری اینترنتی در طول روز انتخابات ادامه پیدا نکند، یعنی باید زمانی قبل از روز انتخابات که قانون آن را تعیین کند، وجود داشته باشد که رای‌گیری الکترونیکی قطع شود. از سوی دیگر و به منظور تسهیل در رای‌گیری الکترونیکی، برخی دیگر پیشنهاد تمدید مدت رای‌گیری را به بیش از یک روز مطرح می‌کنند. این امکان ممکن است به دو پیشنهاد منجر شود: الف) در اکثر کشورهای عضو اتحادیه اروپا، انتخابات عمومی فقط در یک روز برگزار می‌شود، بنابراین مقررات قانونی مربوطه باید اصلاح شود و ب) اگر رای‌دهندگان بتوانند بیش از یک روز از این امکان استفاده کنند، اصل برابری زیر سوال می‌رود. (Dimitris A. Gritzalis, 2002, p.542-3)

### ۳،۲،۴ مخفی بودن

مخفی بودن و آزادی اصولی کاملاً مرتبط با یکدیگر هستند. محرمانه بودن، شرط تصمیم‌گیری سیاسی آزادانه رای‌دهندگان است. در انتخابات دموکراتیک پیوند بین رای و رای‌دهنده باید برگشت‌ناپذیر باشد تا اطمینان حاصل شود که رای آزادانه داده می‌شود. در سیستم‌های رای‌گیری سنتی، مخفی بودن از نظر فیزیکی محافظت می‌شود اما این سیستم ممکن است رای‌گیری الکترونیکی را در برابر نقض محرمانه آسیب‌پذیر کند. در نتیجه موارد فوق، الزامات زیر حاصل می‌شود: الف) محرمانه بودن رای باید در هنگام اخذ، انتقال، دریافت، جمع‌آوری و جدول‌بندی آرا تضمین شود، ب) هیچ‌یک از عوامل دخیل در فرآیند رای‌گیری (سازمان‌دهندگان، مقامات انتخاباتی، اشخاص ثالث مورد اعتماد، رای‌دهندگان و غیره) نباید بتوانند رای را با رای‌دهنده قابل شناسایی مرتبط کنند، ج) تشریفات ثبت‌نام و احراز هویت از یک سو و انتقال رای از سوی دیگر باید از هم جدا باشد و د) هیچ رای‌دهنده‌ای نباید بتواند ثابت کند که به روش خاصی رای داده است.



شمارش را قبل از پایان دوره رای‌گیری (آفلاین) ممنوع می‌کند.

### ۳،۲،۶ دموکراسی

یک سیستم رای‌دهی الکترونیکی دموکراتیک حداقل باید الزامات یک سیستم انتخاباتی سنتی را برآورده کند. با این حال، به دلیل ماهیت از راه دور رای‌گیری الکترونیکی الزامات اضافی نیز باید برآورده شود. این الزامات مربوط به حفظ ویژگی‌هایی مانند شفافیت، پاسخگویی، امنیت، دقت و مشروعیت سیستم است. رای‌دهندگان الکترونیکی باید بتوانند نحوه برگزاری انتخابات را درک کنند. رویه‌های رای‌گیری سنتی به گونه‌ای عمل می‌کند که هم برای رای‌دهندگان و هم برای سایر کنشگران انتخابات شفاف باشد. برعکس، رویه‌های رای‌گیری الکترونیکی شفاف نیستند، زیرا رای‌دهندگان عادی دانش لازم برای درک نحوه عملکرد سیستم را ندارند. بنابراین در رای‌گیری الکترونیکی اعتماد بسیار بیشتری به فناوری مورد استفاده و افراد درگیر (مقامات انتخاباتی، ارائه‌دهندگان فناوری و غیره) مورد نیاز رای‌دهندگان است.

سیستم رای‌گیری الکترونیکی باید امکان راستی‌آزمایی آن را توسط رای‌دهندگان (قابلیت تأیید انفرادی) یا مقامات انتخاباتی، احزاب و ناظران مستقل (قابلیت تأیید نهادی) فراهم کند. با این حال، قابلیت تأیید قائم به رازداری (محرمانه بودن) است، به این معنا که تأییدپذیری فردی (یعنی امکان یک رای‌دهنده برای تأیید رأی خود و دریافت تأییدیه در مورد اخذ و شمارش آرا) با شرط رازداری (به عنوان شرط انتخاب آزاد) در تضاد است. پس بنابراین می‌توان گفت که تأییدپذیری با شفافیت در تضاد است.

پاسخگویی نیازی اضافی از سیستم رای‌گیری الکترونیکی است که به معنای ثبت و نظارت بر کلیه عملیات مربوط به آن است. الزامات اطمینان و امنیت از نیاز دموکراتیک ناشی می‌شود بدین معنا که تا اطمینان حاصل شود که نتیجه انتخابات به درستی، اراده رای‌دهنده را منعکس می‌کند. سیستم

قابل‌اعتماد باید اطمینان حاصل کند که نتیجه فرآیند رای‌گیری با آرای داده شده مطابقت دارد. برگه‌ای که به تجهیزات شمارش رای ارسال می‌شود، باید کپی دقیق و غیرقابل تغییر از انتخاب رای‌دهنده باشد (صداقت). علاوه بر این، هم حذف یک رأی معتبر از جدول‌بندی و هم تأیید اعتبار یک رأی غیرمعتبر باید غیرممکن باشد. امنیت مفهومی چندبعدی در زمینه رای‌گیری الکترونیکی است. امنیت عمدتاً فنی تضمین‌شده برای محرمانگی (رازداری)، یکپارچگی و در دسترس بودن اشاره دارد اما همچنین به طیف وسیعی از عملکردها و احراز انتخاباتی مانند ثبت‌نام، واجد شرایط بودن و احراز هویت اشاره دارد. سیستم رای‌گیری الکترونیکی باید در برابر انکار تصادفی یا عمدی خدمات محافظت شود و هر زمان که انتظار می‌رود برای استفاده در دسترس باشد، عملیاتی شود. در دسترس نبودن سیستم (یا یکی از اجزای آن) ممکن است منجر به از دست دادن توانایی رای‌دهنده برای اعمال حقوق اساسی سیاسی خود شود.

سیستم‌های رای‌گیری الکترونیکی به‌طور اجتناب‌ناپذیری پیچیده هستند. علاوه بر این، آن‌ها معمولاً بازیگران بیشتری را نسبت به یک سیستم سنتی درگیر می‌کنند. از دیدگاه رای‌دهندگان، استفاده از سیستم باید آسان بوده و نیاز به مهارت خاصی نداشته باشد. بنابراین، سیستم رای‌گیری الکترونیکی باید به گونه‌ای توسعه یابد که قابلیت استفاده را تسهیل و قابلیت کنترل آن را حفظ کند.

سادگی و دسترسی به یک سیستم، صرفاً مسائل فنی نیستند. آموزش صحیح و مهندسی مجدد فرآیندهای انتخاباتی (مانند میزهای کمک، مقامات انتخابات الکترونیکی و غیره) برای برآورده کردن این الزامات مورد نیاز است.

بر اساس اصول فوق، الزامات زیر مشتق می‌شوند: الف) باید رویه‌های گواهی معتبر برای سخت‌افزار و نرم‌افزار وجود داشته باشد، ب) کل زیرساخت و همچنین هرگونه عملکرد سیستم (مثلاً همه نرم‌افزارهای غیرواسطه باید با منبعی باز ثبت

(Jacobson I, Booch G., Rumbaugh, 1999) خواهد بود. فرآیند یکپارچه منطقی، ترکیبی از فرآیندهای مختلف توسعه نرم‌افزار است. یکی از مهم‌ترین ویژگی‌های آن، این است که در مواردی از آن به عنوان روشی برای گرفتن نیازهای معرفی شده، استفاده می‌شود. هر مورد استفاده، به یک نیاز عملکردی سیستم اشاره دارد. (Simons A, Graham, 1998) الزامات غیرعملکردی که مختص یک مورد استفاده هستند، ممکن است بخشی از توضیحات آن شوند، در حالی که الزامات غیرعملکردی در سراسر سیستم معمولاً به عنوان مشخصات تکمیلی مشخص می‌شوند. (Jacobson, 1993)

شوند، ج) تمام عملیات (احراز هویت، ضبط رأی و غیره) باید با حفظ محرمانگی نظارت شود، د) زیرساخت باید برای بازرسی توسط نهادهای مجاز باز و در دسترس باشد، ت) رأی‌دهندگان، احزاب و نامزدها باید اطمینان حاصل کنند که هیچ تخلفی صورت نگرفته است، ث) امنیت کافی سیستم باید تضمین شود) سیستم باید ساده و کاربرپسند باشد.

## ۴ روش‌شناسی مورد استفاده

در این بخش، الزامات اساسی عمومی (و اصول طراحی مربوطه) به عنوان مبنایی برای استخراج الزامات کاربردی کاربر تسهیل خواهد شد. این استخراج بر اساس فرآیند یکپارچه عقلایی

جدول ۲ الزامات انتخابات قانون اساسی و الزامات کاربران رای الکترونیکی

| نیاز کاربر  | الزامات قانون اساسی   |
|---|---|
| شرکت در فرآیند رای‌گیری باید تایید شود.   | عمومیت :<br>همه شهروندان بالغ حق رای دادن دارند   |
| ۱-عدم اجبار باید تضمین شود.<br>۲-امکان رای آگاهانه غیرمعتبر باید فراهم شود.   | آزادی:<br>هرکس آزاد است به حزبی که مناسب می‌داند رای دهد  |
| ۱-فقط رای‌دهندگان واجد شرایط باید بتوانند رای دهند (واجد شرایط).<br>۲-هر رای‌دهنده واجد شرایط باید فقط یک‌بار بتواند رای دهد (عدم استفاده مجدد).<br>۳-هیچ رأی‌دهنده‌ای نباید بتواند رأی خود یا شخص دیگری را کپی/تغییر دهد (صداقت).<br>۴-رأی‌دهنده باید بتواند تأیید کند که رأی او در شمارش نهایی محاسبه شده است (قابلیت تأیید).<br>۵-رای‌دهندگان باید بتوانند بدون تبعیض به زیرساخت‌های رای‌گیری دسترسی داشته باشند (دسترسی). | برابری:<br>همه آرا برابر در نظر گرفته می‌شود  |
| ۱-مراحل ثبت نام، احراز هویت و رای‌گیری باید آشکارا از هم جدا شوند.<br>۲-آرا باید به‌طور جداگانه و مستقل از احراز هویت رأی‌دهندگان تأیید شود.  | مخفی بودن:<br>هیچ بازیگری که در فرآیند رای‌گیری دخیل است نباید بتواند یک برگه رای را به یک رای‌دهنده مرتبط کند. |
| ۱-هیچ واسطه‌ای نباید در فرآیند رای‌گیری دخالت داشته باشد (یعنی هیچ شخصی نمی‌تواند اجازه رای دادن برای شخص دیگری را داشته باشد).<br>۲-تک‌تک رای‌ها باید به درستی ثبت و شمارش شوند.   | مستقیم بودن:<br>انتخاب‌کننده، نمایندگان خود را بدون دخالت انتخاب می‌کند.  |

(Dimitris A. Gritzalis, 2002, p.546)

از الزامات برای یک سیستم رای‌گیری الکترونیکی امن در ادامه ارائه شده است. موارد استفاده از سیستم معمولاً با موارد استفاده تجاری شناسایی شده در

از آن‌جا که هر قدر توصیفات مورد استفاده جزئی‌تر شوند، شرایط اساسی زیربنایی واضح‌تر و در نتیجه به الزامات غیرکاربردی تبدیل می‌شوند. مجموعه‌ای



موارد استفاده تجاری که در مدل رأی‌گیری سنتی گنجانده شده، شامل موارد زیر است (Ikonomopoulos S., Gritzalis, 2002; 507-520)

۱- **تعریف حوزه‌های انتخاباتی:** پیش از شروع پروسه انتخابات، به منظور تعیین حوزه‌های انتخاباتی و تعداد نامزدهای نمایندگی در هیئت حاکمه انجام می‌شود.

۲- **تعیین انتخاب‌کنندگان:** برای تعیین انتخاب‌کنندگان شرکت‌کننده استفاده می‌شود. به طور کلی، تمام افراد بالغ حق/تعهد دارند که در این فرآیند شرکت کنند.

۳- **ارائه ابزار احراز هویت:** برای ارائه ابزار احراز هویت کافی به انتخاب‌کنندگان و اجازه دادن به آن‌ها برای شناسایی خود در طول فرآیند رأی‌گیری انجام می‌شود. مسئولیت ارائه ابزار احراز هویت می‌تواند با دولت یا انتخاب‌کننده باشد. این فرآیند پس از این‌که رأی‌دهندگان، ابزار احراز هویت مورد نیاز را در روشی غیرتبعیض‌آمیز به دست آوردند، پایان می‌یابد.

۴- **راه‌اندازی مراکز انتخاباتی:** پس از تعیین حوزه‌های انتخاباتی و پیش از دوره زمانی رأی‌گیری انجام می‌شود. هدف آن فراهم کردن زیرساخت‌هایی است که امکان فرآیند انتخابات را فراهم می‌کند. طی این پروسه، کارمندان مجاز مرکز انتخابات، همراه با افراد مجاز برای نظارت بر روند انتخابات برای هر مرکز، شناسایی می‌شوند.

۵- **ایجاد برگه‌های رای:** پس از تعیین حوزه‌های انتخاباتی شروع می‌شود. هر حزب یک قالب رای گسسته و فهرستی از نمایندگان در هر حوزه انتخاباتی ارائه می‌دهد. ایالت برگه‌های رای را تولید کرده و آن‌ها را به تمام مراکز انتخاباتی می‌فرستد.

۶- **احراز هویت انتخاب‌کننده:** زمانی انجام می‌شود که انتخاب‌کننده در مرکز انتخاباتی که در آن ثبت‌نام کرده است، رای دهد. هدف آن اطمینان

مدل دامنه مطابقت دارد، زیرا عملکرد فعلی با معرفی سیستم الکترونیکی تغییر نمی‌کند.

## ۴٫۱ مدل رأی‌گیری سنتی

روند رأی‌گیری به طور کلی در چارچوب انتخابات عمومی قابل بررسی است. با این حال، موقعیت‌های دیگری نیز وجود دارد که رأی‌گیری نقش اصلی را ایفا می‌کند (مثلاً انتخابات داخلی [انتخابات اتحادیه‌های کارگری]، تصمیم‌گیری [به‌عنوان مثال رفراندوم]، نظرسنجی‌هایی با ماهیت اشاره‌ای یا مشورتی و غیره). این رویه‌ها مشابه روشی انتخابات عمومی انجام، اگرچه معمولاً با چارچوب قانونی متفاوتی اداره می‌شوند.

با وجود این، می‌توان استدلال کرد که فرآیند انتخابات عمومی، حتی اگر فعالیت‌های خاص ممکن است متفاوت باشد، فرامجموعه‌ای از سایرین است. در این مقاله، مدل رأی‌گیری با تمرکز ویژه بر روند انتخابات عمومی ارائه خواهد شد. سطح جزئیات این مدل به اندازه کافی عمومی است که در چندین زمینه قابل اجرا باشد. تغییرات جزئی ممکن است در زمینه‌های مختلف وجود داشته باشد، که عمدتاً به دلیل تفاوت بین چارچوب قانونی، قابل اجرا است. به نظر می‌رسد که چنین تغییراتی بر کامل بودن یا صحت مدل تأثیر نمی‌گذارد.

علی‌رغم تنوع گسترده سیستم‌های انتخاباتی، چارچوب قانونی و زیرساخت، الزامات قانون اساسی (اصول طراحی) منجر به الزامات کاربر می‌شود که در جدول ۲ نشان داده شده است. این الزامات به موارد استفاده تجاری مربوطه و تحقق آن‌ها اشاره دارد. رابطه متقابل آن‌ها شامل مدل مورد استفاده تجاری برای فرآیند رأی‌گیری انتخابات عمومی است. مدل رأی‌گیری با مکانیسم‌های به‌کار رفته برای تعیین نامزدها یا معیارهای شرکت برای رأی‌دهندگان سازگار نیست. در نظر گرفته می‌شود که نامزدها تعیین شده‌اند و اطلاعات مربوط به کل جمعیت موجود است.

## ۵ الزامات کاربر:

الف) **رای‌دهندگان:** رای‌دهندگان باید به تعدادی محدود از تلاش‌های ناموفق احراز هویت اجازه داشته باشند. در صورت تجاوز از حد، ابزار احراز هویت آن‌ها باطل می‌شود. برای این‌که شانس شرکت مجدد در فرآیند رای‌گیری را داشته باشند، باید وسیله احراز هویت جدیدی صادر و به رای‌دهنده اختصاص داده شود. طی فرآیند احراز هویت، رای‌دهندگان نباید مستقیماً به سیستم میزبان رای‌گیری دسترسی داشته باشند. فرآیند احراز هویت باید به دسترسی محدود و کنترل‌شده به سیستم رای‌گیری تحت امتیازات، کمتر ممکن یا عدم دسترسی منجر شود. احراز هویت موفقیت‌آمیز باید فقط از طریق رابط کاربری به سیستم رای‌گیری دسترسی داشته باشد.

ب) **عوامل کلیدی:** کاربران باید فقط از پایانه‌های خاص، در بازه زمانی بازتعریف شده، با استفاده از ترکیبی از ابزارهای احراز هویت پیشرفته، مانند بیومتریک یا کارت‌های هوشمند، احراز هویت شوند. بازیگران کلیدی نباید کاربران ممتاز در سطح سیستم باشند. فاصله زمانی بین تلاش‌های ناموفق باید پس از هر شکست افزایش یابد. حداکثر تعداد تلاش باید مجاز باشد (پس از آن، مجوز ویژه باید توسط افسران مجاز انتخابات به منظور باز کردن قفل نهایی داده شود). سیستم باید بتواند روش‌های احراز هویت جایگزین و ابزارهایی با قدرت برابر را با پیشرفت فناوری در این زمینه ترکیب کند. سیستم باید یک قلاب برای یک API باز فراهم کند تا به راحتی ابزارهای احراز هویت جدید را در خود جای دهد.

ج) **برای همه کاربران:** داده‌های احراز هویت باید به روشی امن و قابل اعتماد حتی تحت شبکه‌های عمومی منتقل شوند. دستورالعمل‌های امنیتی که به طور گسترده پذیرفته شده‌اند، باید برای احراز هویت کاربر استفاده شوند. فرآیند احراز هویت باید به عنوان تراکنشی اتمی در نظر گرفته شود. تعامل

حاصل کردن از این است که انتخاب‌کننده خودش رای می‌دهد.

۷- **رای دادن:** پس از احراز هویت رای‌دهنده، رأی خود را به گونه‌ای به صندوق می‌اندازد تا از رازداری محافظت کند. سپس سوابق انتخابات به درستی به روز می‌شود.

۸- **شمارش آرا:** برای تایید آرا و تعیین تعداد آرای که هر حزب به دست آورده است، انجام می‌شود. این روند در هر مرکز انتخاباتی پس از پایان دوره انتخابات صورت می‌گیرد و زمانی پایان می‌یابد که تمام آرا توسط مقامات رسمی و تجمیع شود.

۹- **ادغام آرا:** هدف، تجمیع آرای شمارش‌شده (همراه با لیست افرادی که در مرکز انتخابات داده‌اند) از مراکز انتخاباتی به مخزنی مرکزی است. این روند به طور مستقل برای هر مرکز انتخاباتی پس از پایان انتخابات آغاز می‌شود.

۱۰- **بررسی یکپارچگی نتیجه:** برای تایید درستی مراحل انتخابات از سوی نهاد ذی‌نفع، انجام می‌شود. در این مورد، مقاماتی که از سوابق نگهداری شده طی مراحل مربوطه استفاده می‌کنند، باید این واقعیت را اثبات کنند.

## ۳- الزامات مبتنی بر امنیت کاربر و عملکرد رای‌گیری الکترونیکی

مدل انتخابات عمومی که در بخش قبل توضیح داده شد، مبنای اساسی برای استخراج الزامات سیستم رای‌گیری الکترونیکی را فراهم می‌کند. در راستای موارد استفاده تجاری از مدل انتخابات عمومی، تعدادی از موارد استفاده از سیستم، شناسایی شده است. موارد استفاده تجاری، در رابطه با یک مدل عمومی رای‌گیری الکترونیکی در شکل ۲ نشان و شرح مفصلی از تمام موارد استفاده کسب‌وکار رای‌گیری الکترونیکی در ادامه توضیح داده شده است، به دنبال آن نیازهای کاربری و عملکردی مربوطه، به ویژه آن‌هایی که امنیت سیستم رای‌گیری را هدف قرار می‌دهند. (Dimitris, A. Gritzalis, 2002; 547-552)



دهنده‌ای نباید به بیش از یک حوزه ویا واحد انتخاباتی منصوب شود.

۳- ابزار احراز هویت باید ایجاد، ذخیره و به رای‌دهندگان/نمایندگان احزاب به روشی امن ارسال شود.

۴- سیستم باید بتواند لیست الکترونیکی احزاب را از منابع و فرمت‌های مختلف وارد کند. لیست احزاب باید کامل، صحیح و به‌روز باشد. لیست نباید به سیستم منتقل شود بلکه باید از طریق ابزارهای فیزیکی امن تحویل داده شود. سیستم باید با تعامل نادرست و/یا ورودی غیرمنتظره با موفقیت برخورد کند. سیستم باید تمام اقدامات را ثبت کند.

۵ - سیستم باید بتواند لیست الکترونیکی نامزدها را از منابع و فرمت‌های مختلف وارد کند. لیست تاریخ نامزدها باید کامل، صحیح و به‌روز باشد و هر نامزد باید به یک حزب خاص مرتبط باشد. لیست نباید به سیستم منتقل شود بلکه باید از طریق ابزارهای فیزیکی امن تحویل داده شود. سیستم باید با تعامل نادرست و/یا ورودی غیرمنتظره با موفقیت برخورد کند. سیستم باید تمام اقدامات را ثبت کند.

۶- فقط اطلاعات مربوط به فرآیند رای‌گیری باید در برگه رای ظاهر شود.

۷- فقط اطلاعات در دسترس عموم در مورد طرف باید ارائه شود. و همچنین در الزامات عملکردی، سیستم باید همه اقدامات را ثبت کند.

۸- هیچ رأیی را نمی‌توان به رأی‌دهنده پیوند داد. هیچ رأی‌دهنده‌ای نمی‌تواند دو بار رأی دهد. هیچ‌کس نمی‌تواند رای او یا شخص دیگری را کپی کرده یا تغییر دهد. هیچ‌کس نمی‌تواند آنچه دیگران رای داده‌اند را فاش کند. رای‌دهنده به تنهایی و بدون فشار (عدم اجبار) رای می‌دهد. یک مدرک غیرقابل انکار (رسید) باید به رای‌دهنده تحویل داده شود تا ثابت شود که او رای داده است. هیچ‌کس نمی‌تواند رای دادن را انکار کند. سیستم رای‌گیری باید برای رای‌دهنده شفاف باشد، به گونه‌ای که او بتواند عملاً

غیرعادی یا داده‌های ورودی غیرمنتظره در فرآیند احراز هویت باید به درستی مورد بررسی قرار گیرد. هیچ‌گونه اطلاعات مربوط به برنامه یا سیستم نباید در طول فرآیند احراز هویت، در صورت پایان غیرعادی برنامه یا در هنگام خرابی زیرساخت، فاش شود. تمام تلاش‌های احراز هویت، موفقیت‌آمیز یا غیرموفق، باید ثبت شوند.

الزامات کاربردی: یک API احراز هویت به خوبی تعریف شده را در معرض نمایش قرار دهید (سیستم باید بتواند روش‌ها و ابزارهای احراز هویت جایگزین را با پیشرفت فناوری ترکیب کند). اسناد اعتباری (اعتبارنامه) کنشگران را تأیید کنید (در صورت احراز هویت رای‌دهندگان، یک زیرساخت تقویت‌کننده اعتماد باید وجود داشته باشد تا اعتبارنامه‌های کنشگر با موفقیت تأیید شود). تمام تلاش‌های احراز هویت، موفقیت‌آمیز یا غیرموفق را ثبت کنید. امتیازات تخصیص یافته در بازیگران فقط در سطح برنامه سیستم رای‌گیری معتبر است (سیستم رای‌گیری باید به کنشگران احراز هویت شده، فقط امتیازات گسترده برنامه اعطا کند، در حالی که امتیازات سیستم باید برای همه کنشگران غیرمجاز باشد).

## الف- الزامات کاربر:

۱- تعامل غیرعادی یا داده‌های ورودی غیرمنتظره به فرآیند مدیریت منطقه باید به درستی درمان شود.

۲- سیستم باید بتواند لیست الکترونیکی رای‌دهندگان را از منابع و فرمت‌های مختلف وارد کند. فهرست‌های رای‌دهندگان باید کامل، صحیح و به‌روز باشد و نباید به سیستم مخابره شود بلکه از طریق وسایل فیزیکی امن تحویل داده شود. سیستم باید با تعامل نادرست و/یا ورودی غیرمنتظره با موفقیت برخورد کند. سیستم باید تمام اقدامات را ثبت کند. رای‌دهندگان باید به حوزه‌های صلاحی ویا واحدهای انتخاباتی منصوب شوند. هیچ رای



فهرست رای‌دهندگان باید کامل، صحیح و به‌روز باشد. فهرست رای‌دهندگان نباید به سامانه مخابره شود اما از طریق ابزارهای فیزیکی مطمئن تحویل داده می‌شود). فهرست رای‌دهندگان را بررسی کنید (سیستم باید با تعامل نادرست و/یا ورودی غیرمنتظره با موفقیت برخورد کند). داده‌های ورودی را بررسی کنید (سیستم باید با تعامل نادرست و/یا ورودی غیرمنتظره با موفقیت برخورد کند). فهرست رای‌دهندگان را به روشی امن ذخیره کنید (فهرست باید در سرور امنی غیر از دستگاهی که سیستم رای‌گیری را اجرا می‌کند، ذخیره شود). سیستم باید تمام اقدامات را ثبت کند.

۳- یک API باز ارائه کنید تا به راحتی ابزارهای احراز هویت جدید را در خود جای دهد (برای این که سیستم بتواند با پیشرفت‌های فناوری احراز هویت کنار بیاید). همه تلاش‌ها برای تولید ابزار احراز هویت، موفقیت‌آمیز یا غیرموفق، ثبت شود.

۴- داده‌های ورودی را تایید کنید (ورودی ارائه‌شده توسط کنشگران باید برای سیستم مرتبط و معنادار باشد). سیستم باید تمام اقدامات را ثبت کند.

۵- تغییر لیست نامزدها در مرحله رای‌گیری (در صورتی که کنشگر بخواهد نامزدهای انتخاباتی را در مرحله سیستمی غیر از مرحله قبل از انتخابات تنظیم یا اصلاح کند، باید رویه مناسب فعال شود). فهرست کاندیداهای وارداتی (سیستم باید بتواند لیست الکترونیکی کاندیداها را از منابع و فرمت‌های مختلف وارد کند. فهرست نامزدها باید کامل، صحیح و به‌روز باشد. فهرست کاندیداها نباید به سیستم منتقل شود اما از طریق وسایل فیزیکی ایمن تحویل داده می‌شود). اعتبارسنجی داده‌های نامزدها (سیستم باید با تعامل نادرست و/یا ورودی غیرمنتظره با موفقیت برخورد کند). لیست نامزدها باید در سرور ایمن متفاوت از دستگاهی که سیستم رای‌گیری را اجرا می‌کند، ذخیره شود. سیستم باید تمام اقدامات را ثبت کند.

از همه جا رای دهد. ثبت تمام اقدامات باید انجام شود.

۹- پیش از پایان رسمی فرآیند رای‌گیری، جمع‌آوری آرا باید غیرممکن باشد. آرا و شواهد مربوطه باید به روشی امن ذخیره شوند. ثبت تمام اقدامات انجام می‌شود.

۱۰- تأیید نتایج انتخابات قبل از پایان رسمی شمارش باید غیرممکن باشد. تأیید صحت نتیجه رای‌گیری باید با مشارکت و مشارکت فعال نمایندگان طرف‌های ذی‌نفع در طول فرآیند راستی‌آزمایی تضمین شود. شواهد و نتایج تأیید باید به روشی امن ذخیره شوند. ثبت تمام اقدامات انجام می‌شود.

۱۱- پارامترهای انتخابات باید به روشی امن ذخیره شوند. پارامترهای انتخاباتی به روز شده باید برای شفافیت در میان تمام نهادها و احزاب ذی‌نفع توزیع شود.

۱۲- پارامترهای انتخابات باید به روشی امن ذخیره شوند. پارامترهای انتخابات باید برای شفافیت در میان تمام نهادها و احزاب ذی‌نفع توزیع شود.

## ب- الزامات عملکردی

۱- داده‌های ورودی را تایید کنید (ورودی ارائه‌شده توسط بازیگران باید برای سیستم مرتبط و معنادار باشد). سیستم باید همه اقدامات را ثبت کند.

۲- برای انجام این عملیات، سیستم باید در مرحله تنظیم انتخابات باشد. برای انجام این عملیات در مرحله انتخابات در حال انجام باید مورد استفاده مناسب فعال شود. نیاز به احراز هویت کنشگر کلیدی در مرحله رای‌گیری (اگر کنشگر بخواهد رای‌دهندگان را در مرحله سیستمی غیر از مرحله قبل از انتخابات تنظیم یا تغییر دهد، باید رویه مناسب فعال شود). فهرست رای‌دهندگان وارداتی (سیستم باید بتواند فهرست الکترونیکی رای‌دهندگان را از منابع و فرمت‌های مختلف وارد کند.



(سیستم باید بتواند نشان دهد که تمام آرا به درستی محاسبه شده‌اند). سیستم باید تمام اقدامات را ثبت کند.

۱۰- نمایش گفت‌وگوی تایید (این گفت‌وگو، همراه با اطلاعات اضافی در مورد تاییدیه‌هایی که تاکنون انجام شده است، برای بقیه نویسندگان کلیدی شرکت‌کننده در مورد استفاده نمایش داده می‌شود). سیستم باید تمام اقدامات را ثبت کند.

۱۱- مرحله سیستم را بررسی کنید و به کاربر اطلاع دهید (به منظور تنظیم/تغییر پارامترهای انتخابات، سیستم باید در مرحله قبل از انتخابات باشد). پارامترهای قابل تغییر انتخابات را در مرحله رای‌گیری تعریف کنید. داده‌های پارامتر انتخابات را بررسی کنید (سیستم باید با تعامل نادرست و/یا ورودی غیرمنتظره با موفقیت برخورد کند). پارامترهای انتخابات را به روشی امن ذخیره کنید (پارامترها باید در یک سرور امن، متفاوت از دستگاهی که سیستم رای‌گیری را اجرا می‌کند، ذخیره شود). نیاز به احراز هویت بازیگر کلیدی در مرحله رای‌گیری (در صورتی که بازیگر بخواهد پارامترهای انتخاباتی را در مرحله سیستمی غیر از مرحله قبل از انتخابات تنظیم یا تغییر دهد، این روش باید فعال شود). سیستم باید تمام اقدامات را ثبت کند.

پارامترهای معمول انتخابات شامل فهرست توزیع خروجی، نمایندگان حزب یا سایر احزاب ذی‌نفع، تاریخ شروع/پایان انتخابات، زمان شروع/پایان انتخابات، حداکثر تعداد احزاب، حداکثر تعداد رای‌دهندگان، حداکثر تعداد انتخاب‌های رای‌دهنده، تعداد دقیق انتخاب‌های رای‌دهنده، قالب برگه رای، الزامات برگه رای نامعتبر، حداکثر تعداد تلاش‌های رای ناموفق/ تکمیل نشده بدون احراز هویت مجدد و غیره.

#### ۵- الزامات امنیتی غیرکاربردی رأی الکترونیکی

علاوه بر نیازهای کاربر و عملکردی که از طریق موارد استفاده از سیستم بیان می‌شود، سیستم تعدادی نیاز غیرعملکردی را نشان خواهد داد.

۶- نمایش برگه رای (سیستم باید با تعامل نادرست و/یا ورودی غیرمنتظره با موفقیت برخورد کند، باید حداقل اطلاعات ممکن را به منظور تسهیل فرآیند رای‌گیری در معرض نمایش بگذارد؛ هیچ اطلاعات خاص سیستم/برنامه نباید از طریق برگه رای افشا شود). سیستم باید تمام اقدامات را ثبت کند.

۷- هیچ برگه رای نمی‌تواند به یک رای‌دهنده مرتبط شود، هیچ رای‌دهنده‌ای نمی‌تواند دو بار رای دهد، هیچ کس نمی‌تواند رای دیگران را کپی کند یا تغییر دهد، هیچ کس نمی‌تواند ببیند که دیگران به چه چیزی رای داده‌اند، هیچ کس نمی‌تواند از طرف دیگر رای دهد. نه از شخص دیگری و نه تغییر آنچه که شخص دیگری رای می‌دهد، رای‌دهنده این توانایی را دارد که یک رای باطل به صندوق بیندازد، رأی‌دهنده توانایی (انداختن رای سفید را دارد). ارائه مدرکی مبنی بر رای دادن (نباید مدرک را به انتخاب رای‌دهنده مرتبط کرد). رأی را به روشی امن ذخیره کنید (سیستم رأی‌گیری رأی داده شده را در دستگاهی متفاوت از دستگاهی که سیستم رأی‌گیری را اجرا می‌کند ذخیره می‌کند). سیستم باید تمام اقدامات را ثبت کند.

۸- مرحله انتخابات را بررسی کنید (سیستم باید بتواند مرحله فعلی انتخابات را شناسایی کند و برای انجام این عملیات باید در مرحله نهایی انتخابات باشد). ممنوعیت شمارش آرا، پیش از پایان زمان انتخابات (پیش از پایان رسمی فرآیند رای‌گیری، جمع‌آوری آرا باید غیرممکن باشد). سیستم رای‌گیری را ایزوله کنید (پس از پایان انتخابات، سیستم رای‌گیری باید از هر شبکه خارجی و/یا عمومی (در صورت وجود) جدا شود. ارائه اطلاعات انتخابات را پیش از جمع‌بندی زمان پایان ممنوع کنید (نباید اطلاعات انتخابات را پیش از تاریخ پایانی ارائه کرد، فرآیند محاسبه به پایان می‌رسد). سیستم باید همه اقدامات را ثبت کند.

۹- تضمین معقولی برای یکپارچگی نتیجه انتخابات ارائه دهید. محاسبه رای را تأیید کنید

کار دارند، اشاره می‌کنیم. این الزامات در شرح داده شده است.

جدول ۳ که در آن هر نیاز متمرکز بر امنیت ابتدا با هدف خود مرتبط می‌شود و سپس به طور مختصر شرح داده شده است.

## ۶ پیشنهاد

با توجه به مطالب فوق سیستم‌های رای‌گیری الکترونیکی باید در حال حاضر فقط به عنوان مکمل و نه جایگزین سیستم‌های رای‌گیری مبتنی بر کاغذ موجود در نظر گرفته شوند. ما پیشنهاد خود را عمدتاً بر اساس موارد زیر استوار می‌کنیم:

۱- شکاف دیجیتال، یعنی فقدان فرصت دسترسی برابر به اینترنت و ابزارهای زیرساخت ICT. ارائه ابزارها و امکانات جدید مشارکت، مبتنی بر فناوری اطلاعات و ارتباطات، در چنین حالتی می‌تواند به نتیجه معکوس، یعنی حذف رأی‌دهندگان «بی‌سواد فناوری اطلاعات و ارتباطات» از روند سیاسی منجر شود. خود یک سیستم انتخاباتی ممکن است دسترسی نابرابر یک فرد به فرآیند انتخابات را سازمان دهد. این موضوع دموکراسی و برابری است تا تضمین کنیم که فناوری‌های مختلف رأی‌گیری با توجه به سهولت و فرصت دسترسی برابر هستند.

الزامات غیرعملکردی یا می‌توانند مختص یک مورد استفاده یا ممکن است به کل سیستم مربوط باشند. این الزامات در دسته‌های زیر دسته‌بندی شده‌اند:

امنیت: هدف پشتیبانی از ویژگی‌های امنیتی اصلی، هم در سطح برنامه و هم در سطح سیستم است. آن‌ها همچنین عدم انکار، ناشناس بودن و تأیید منبع را فراهم می‌کنند.

عملکرد: با سرعت، کارایی، در دسترس بودن، دقت، توان عملیاتی، زمان پاسخگویی، زمان بازیابی یا استفاده از منابع و غیره سر و کار داشته باشید.

قابلیت اطمینان: شامل ویژگی‌هایی مانند فراوانی/شدت شکست، قابلیت بازیابی، پیش‌بینی‌پذیری، دقت و میانگین زمان بین خرابی‌ها (MTBF) و غیره باشد.

قابلیت استفاده: با سازگاری در رابط کاربری، کمک آنلاین و حساس به زمینه، کیفیت اسناد کاربر، مواد آموزشی و غیره مقابله کنید.

قابلیت پشتیبانی: الزامات مربوط به نگهداری سیستم، انطباق، نصب و غیره. در این مقاله تنها به آن دسته از الزامات غیرکاربردی که با امنیت سر و

جدول ۳ الزامات امنیتی غیرکاربردی

| هدف          | جزئیات و محدودیت‌ها را مشخص کنید  |
|--------------|---|
| عمل غیرطبیعی | سیستم باید تعامل غیرعادی مناسب یا داده‌های ورودی غیرمنتظره را در تمام عملکردهای سیستم به گونه‌ای مدیریت کند که عملکرد سیستم حفظ شده و هیچ اطلاعات خاص سیستم/برنامه فاش نشود.  |
| مسئولیت      | تمام اقدامات مربوط به سیستم رأی‌گیری، موفقیت‌آمیز یا غیرموفق، باید ثبت شوند. فقط نهادهای کاملاً ضروری باید دسترسی منطقی و/یا فیزیکی به سیستم رأی‌گیری داشته باشند. تفکیک کافی و وظایف باید میان پرسنل مجاز اعمال شود.   |
| کنترل فیزیکی | اعمال تدابیر امنیتی فیزیکی مانند قفل درب، حفاظ، برنامه‌ریزی فیزیکی سایت و غیره.   |
| سرمایه‌ها    | سرمایه‌های داده باید از افشای غیرمجاز، اصلاح و ساخت غیرمجاز و محرومیت از دسترسی مجاز محافظت شوند. تمام سرمایه‌های سخت‌افزاری باید از گم شدن، سرقت، در دسترس نبودن یا غیرقابل استفاده شدن محافظت شوند. تمام سرمایه‌های نرم‌افزاری باید به طور کامل در برابر حذف، گم شدن، دزدیده شدن، اصلاح یا ساختگی محافظت شوند. افراد مسئول عملیات سیستم حیات باید با دقت انتخاب شوند. |



|                      |  |
|----------------------|--|
| گزارش‌های<br>حسابرسی | تمام عملیات سیستم داخلی مربوط به رای‌دهندگان باید بدون به خطر انداختن محرمانه بودن هویت رای‌دهندگان ثبت شود. گزارش‌های دقیق برنامه و سیستم باید در سطح فراخوانی فرآیند نگهداری شوند.   |
| دسترسی               | در حین برگزاری انتخابات باید از دسترس بودن سیستم رای‌گیری اطمینان حاصل شود. در صورت عدم موفقیت، به دلیل اقدامات عمدی یا تصادفی، پشتیبانی عمومی جایگزین (مانند امکانات عقب‌نشینی) و مکان‌های انتخاباتی باید در دسترس باشد. MTBF باید در طول فرآیند انتخابات حداقل باشد. نسخه پشتیبان سیستم رای‌گیری به روز شده باید به راحتی در دسترس باشد تا در صورت بروز فاجعه سیستم را بازیابی کند.  |
| ارتباطات             | اطلاعات مربوط به هر یک از عملکردهای فوق، حتی اگر از طریق شبکه‌های عمومی منتقل شود، باید خصوصی باشد.  |
| حفاظت<br>اطلاعات     | پردازش اطلاعات باید با چارچوب قوانین ملی و بین‌المللی حفاظت از داده‌ها مطابقت داشته باشد. کنترل‌های کافی باید وجود داشته باشد تا با اطمینان معقول اطمینان حاصل شود که اصول حفاظت از داده‌ها به شیوه‌ای مؤثر و کارآمد اجرا می‌شوند.   |
| رمزگذاری             | سیستم باید بتواند از کلیه خدمات رمزگذاری لازم استفاده کند. داده‌های حساس و اطلاعات مبادله شده میان رایانه‌های سیستم رای‌گیری باید به صورت رمزگذاری شده باشد.   |
| تمامیت               | کاربران باید سیستم را فقط از پایانه‌های خاص، در یک پنجره زمانی از پیش تعریف شده، با استفاده از ترکیبی از ابزارهای احراز هویت قوی، مانند بیومتریک یا کارت‌های هوشمند، مدیریت کنند. حداقل قطعات نرم‌افزاری و سخت‌افزاری لازم بر میزبان سیستم رای‌گیری نصب شود. حداکثر سطح ممکن از افزایش امنیت سیستم عامل باید برای تمام ماشین‌های سیستم رای‌گیری اعمال شود. افزایش امتیازات سیستم برای کاربر باید غیرممکن باشد. در شرایط اضطراری خاص باید اجازه داده شود که بخش‌های انتخابی سیستم را در هنگام استفاده اصلاح کند. نقض امنیت مشتری نباید بر امنیت سیستم تأثیر بگذارد. |
| رسانه<br>ذخیره‌سازی  | تمام داده‌ها و اطلاعات مورد استفاده باید (در صورت نیاز و در صورت نیاز) در رسانه‌های ذخیره‌ساز ایمن (محافظت شده و ضد دستکاری) ذخیره شوند.   |
| عدم اجبار            | رای‌دهندگان باید به تنهایی و بدون فشار رای خود را به صندوق بیندازند.   |

استفاده از اینترنت برای اهداف رای‌گیری باید تا به دست آمدن اطمینان که مقامات انتخاباتی و مردم از این فناوری اطمینان داشته باشند، به تدریج اجرا شود.

۳- خطرات امنیتی و عدم کفایت مکانیسم حفاظتی. این استدلال‌های دیگری برای ویژگی تکمیلی سیستم‌های رای‌گیری الکترونیکی است. به نظر می‌رسد خطرات امنیت فرآیند رای‌گیری الکترونیکی به اندازه کافی توسط فناوری‌های موجود مقابله نمی‌شود.

در نتیجه، چنین در نظر گرفته می‌شود تا زمانی که تمامی مسائل و نگرانی‌های فنی، حقوقی و اجتماعی مربوطه به اندازه کافی توسط جوامع

۲- بی‌اعتمادی ذاتی به رویه رای‌گیری الکترونیکی که ناشی از عدم شفافیت در زمینه دیده شدن روند انتخابات است. برخی از عناصر اساسی و الزامات روش سنتی رای‌گیری و مشارکت در یک محیط رای‌گیری الکترونیکی متفاوت است. سطح اعتماد و حمایت عمومی از رای‌گیری الکترونیکی باید در رابطه با تمام رای‌دهندگان بالقوه سنجیده شود، نه فقط با افرادی که احتمالاً از این شکل از رای‌گیری استفاده می‌کنند. ما استدلال می‌کنیم که اگر تعداد زیادی از رای‌دهندگان به رای‌گیری اینترنتی با شک و تردید نگاه کنند، ممکن است اعتماد اساسی به فرآیند دموکراتیک به خطر بیفتد (برای مثال، گروه ویژه رای‌گیری اینترنتی کالیفرنیا توصیه کرد که هر گونه

مربوطه ناشی می‌شود. علاوه بر این، ما مجموعه ای از الزامات عملکردی را برای سیستم های رای گیری الکترونیکی تولید کرده‌ایم که الزامات تحمیل شده توسط سیستم‌های انتخابات عمومی (سنتی) موجود را یکپارچه می‌کند. برای انجام این کار، از یک روش مهندسی نرم‌افزار (یعنی فرآیند یکپارچه منطقی) استفاده شد که مبتنی بر تسهیل موارد استفاده است. در نتیجه، یک سیستم رأی‌گیری الکترونیکی در نهاد خود مفهوم سازی شده است، به گونه‌ای که تعداد طرح‌های ممکن بعدی را محدود کرده اما طرح خاصی را دیکته نمی‌کند. این مجموعه از الزامات، نتیجه اولین تکرار فرآیند استخراج نیازمندی‌ها است. در حال حاضر در مرحله اعتبارسنجی و تقویت این مجموعه، از جمله الزامات غیرعملکردی هستیم و انتظار می‌رود آن در مرحله توسعه سیستم رای‌گیری الکترونیکی قرار گیرد.

بدین ترتیب به نظر می‌رسد برآورده شدن برخی الزامات مطرح شده توسط قانون (مثلاً عدم اجبار) با فناوری موجود واقعا دشوار باشد. در شرایط اجتماعی-فنی کنونی، نتیجه نهایی کار ما این است که در حال حاضر سیستم‌های رای‌گیری الکترونیکی باید به عنوان وسیله‌ای مکمل برای سیستم‌های سنتی انتخابات عمومی در نظر گرفته شود، مشروط بر این که تمام الزامات قانونی و فنی ضروری به اندازه کافی برآورده شد. بنابراین، انتظار می‌رود که سیستم رای‌گیری سنتی به عنوان ابزار اصلی برای انجام فرآیند انتخابات عمومی باقی بماند، در حالی که ظرفیت رای‌گیری الکترونیکی تکمیلی تنها به تدریج معرفی خواهد شد.

اطلاعاتی مدرن مورد توجه قرار نگیرد، رای الکترونیکی را نمی‌توان برای استفاده در انتخابات عمومی ارائه کرد و بنابراین به عنوان اجبار تحمیل نمی‌شود.

## ۷ نتیجه‌گیری

فناوری اطلاعات و ارتباطات ابزار قدرتمندی در دست سیاستمداران و قانونگذاران است که وظیفه دارند روند دموکراتیک را به طور فعال ترویج و شهروندان را به مشارکت تشویق کنند. فناوری می‌تواند به غلبه بر بحران اعتماد، که امروزه دموکراسی نمایندگی در حال تجربه است، کمک کند. حق رای، بخشی از فرآیند دموکراتیک است که عمیقاً در قوانین اساسی مدرن جا افتاده است. علاوه بر این، آن را یکی از پایه‌های اولیه دموکراسی می‌دانند. رأی‌گیری الکترونیکی، برخلاف سایر معاملات الکترونیکی، تنها در صورتی قابل قبول است که ضامن اجرای تمام اصول مربوطه قانون اساسی باشد. علاوه بر این، یک سیستم رای‌گیری الکترونیکی باید در زمینه‌ای اجرا شود که دسترسی برابر به زیرساخت‌های تکنولوژیکی زیربنایی را تضمین کند، که باید باز، کاربرپسند، تعاملی و ایمن باشد تا شهروندان را قادر به مشارکت در زندگی سیاسی کند و تأثیر مستقیم روی آن داشته باشد. (Mitrou L., Gritzalis D., Katsikas, 2002) و (Mercuri, 2000; 176)

در این مقاله، ما طراحی اصول عمومی یک سیستم رأی‌گیری الکترونیکی مبتنی بر اینترنت را شناسایی کرده‌ایم که از الزامات قانون اساسی



## References

- Azarbad, Babak and Haqshanas, Mohammad Javad, (2020) "Electronicization of elections and the transition to democracy, a comparative study of the consequences of this process in the United States and Iran", Islamic World Political Research Quarterly, Year 11, Number 1. (in Persian)
- Amiri Zargabad, Souda and Seyyed Hossein Malkuti Hashtjin, (2021) "Electronic Parliament and its role in the realization of democracy" Journal of Legal Research 2, No. 48. (in Persian)
- Fathian, Mohammad and Taqvi, Muniralsadat (2008), "Electronic Elections (Principles and Practices)", first edition, Research Center of the Islamic Council. (in Persian)
- Namdar Porbanger, Mustafa, Ebadullah Abbasi (2015), Labor Laws, first edition, Shahr Danesh Publications. (In Persian)
- Adler J., **Internet Voting Primer** (www.votehere.net/adacompliant/whitepapers/primer).
- Burkert H., "**Elektronische Demokratie: Einige staats und verfassungsrechtliche Anmerkungen**" (http://www.gmd.de/People/Herbert.Burkert/ARCHIV).
- Buttler R., et al., (2000) "**A national-scale authentication infrastructure**", Computer, Vol. 33, no. 2, pp. 60- 65.
- California Institute of Technology – MIT (2001), Voting: What is, what could be, **Voting Technology Project**.
- Cramer R., Franklin M., Schoenmakers B., Yung M. (1996), "**Multiauthority secret ballot elections with linear work**", Lecture Notes in Computer Science, Vol. 1070, pp. 72-83, Springer-Verlag, Berlin.
- CyberVote (IST-1999-20338 project), **Report on electronic democracy projects, legal issues of Internet voting and users requirements analysis**, European Commission, IST Programme, 1999 (<http://www.eucybervote.org>).
- Digital Democracy Commission, (2015) **Report of the Speaker's Commission on Digital Democracy**.
- European Commission, IST 2000 Programme, **The Information Society for all**, Final Report, Brussels 2000.
- e-VOTE (IST-2000-29518 project) (2000), **Legal and regulatory issues on evoting and data protection in Europe**, Deliverable D3.4, European Commission, IST Programme.
- Hoffman L., Cranor L., (2001) "**Internet voting for public officials**", in Com. of the ACM, Vol. 44, no. 1, pp. 69- 71.
- Ikonomopoulos S., Gritzalis D., Lambrinouidakis C., Kokolakis S., Vassiliou C. (2002), "**Functional requirements for a secure electronic voting system**", in Proc. of the 17th IFIP International Information Security Conference, M. Hadidi, et al. (Eds.), pp. 507-520, Kluwer Academics.
- International Working Group for Data Protection in Telecommunications (2001), **Common Position on the**



- Use of the Internet in the Conduct of Elections**, Berlin, September 2001.
- Internet Policy Institute, **Report of the National Workshop on Internet Voting: Issues and Research Agenda**, March 2001 ([http://www.internetpolicy.org/research/e\\_voting\\_report.pdf](http://www.internetpolicy.org/research/e_voting_report.pdf)).
- Internet Policy Institute (2001), **Report of the National Workshop on Internet Voting: Issues and Research Agenda**.
- Jacobson I., Booch G., Rumbaugh J. (1999), **The Unified Software Development Process**, Addison-Wesley.
- Jacobson I. (1993), **Object-oriented software engineering - a use case driven approach**, Addison-Wesley.
- Jones B. (2000), **A report on the feasibility of Internet voting, Internet Voting Task Force**, State of California.
- Larman G. (1998), **Applying UML and patterns**, Prentice-Hall.
- Mercuri R. (2000), **"Voting automation?"**, in Com. of the ACM, Vol. 43, no. 2, pp. 176.
- Mitrou L., Gritzalis D., Katsikas S. (2002), **"Revisiting legal and regulatory requirements for secure e-voting"**, in Proc. of the 17th IFIP International Information Security Conference, M. Hadidi, et al. (Eds.), pp. 469-480, Kluwer Academics.
- Phillips D., von Spakovsky H. (2001), **"Gauging the risks of Internet elections"**, in Com. of the ACM, Vol. 44, no. 1, pp. 73-85.
- Rational Corporation, **The Rational Unified Process**.  
(<http://www.rational.com/products/rup/index.jsp>)
- Rüß O., **Wahlen im Internet, quelle multimedia und recht**  
(<http://www.Internetwahlen.de/project/ruess.html>).
- Schoenmakers B. (1999), **"A simple publicly verifiable secret sharing scheme and its application to electronic voting"**, in Lecture Notes in Computer Science, Vol. 1666, pp. 148-164, Springer-Verlag.
- Schoenmakers B., **Compensating for a lack of transparency**.  
(<http://citeseer.nj.nec.com/schoenmakers00compensating.html>).
- Simons A., Graham I. (1998), **37 things that don't work in object-oriented modelling with UML**, Technical Report TUM-I9813, Technical University of Munich.
- Tauss J., Kollbeck J., **e-vote: Die elektronische Briefwahl als ein Beitrag zur Verbesserung der Partizipationsmöglichkeiten**  
([www.tauss.de/bn/e-vote.html](http://www.tauss.de/bn/e-vote.html)).
- The Swedish Government, **Internet Voting - Final Report from the Election Technique Commission**, 2000  
([http://www.justitie.regeringen.se/propositionermm/sou/pdf/sou2000\\_125.pdf](http://www.justitie.regeringen.se/propositionermm/sou/pdf/sou2000_125.pdf)).
- Thomas M. Buchsbaum, (2004) **"E-Voting: International Developments and Lessons Learnt, Expatriates Division"**, paper presented on Conference: Electronic Voting in



Europe - *Technology, Law, Politics and Society*, Workshop of the ESF TED Programme together with GI and OCG 4.

United States, State of California, **A Report on the Feasibility of Internet Voting**, January 2000

(<http://www.ss.ca.gov/executive/ivo te/>)