نقد اخلاقی - تکنیکی رأی‌گیری الکترونیکی

دکترفریا نصیری مفخّم*، سیمین نقوی، یاسمن سرلتی

گروه مهندسی فناوری اطلاعات، دانشکده مهندسی کامپیوتر، دانشگاه اصفهان

(تاریخ دریافت: 92/7/30، تاریخ پذیرش: 30 /93/1)

چکیده

زمینه: همسو با جامعه اطلاعاتی، ایران نیز به سوی الکترونیکی‌شدن رأی‌گیری پیش‌می‌رود. رأی‌گیری الکترونیکی می‌تواند از جنبه‌های مختلفی همچون: ابعاد مهندسی، امنیتی، اخلاقی، حقوقی، اجتماعی، اقتصادی، سیاسی، روانشناختی، محیط زیست، و غیره، در به‌کارگیری تجهیزات و رویّه‌های آن مورد مطالعه قرار گیرد. با فرض فراهم‌بودن تمام تجهیزات مربوطه، زیرساخت‌های شبکه‌ای لازم و پهنای باند کافی، بررسی میدانی نشان داده است که؛ با وجود کاهش هزینه‌ها، سادگی و شفافیت تعامل در این نوع مشارکت، موضوعات امنیت اطلاعات و قابلیت اعتماد، به‌عنوان عوامل راهکاری مهم بازدارنده در پذیرش و اقبال عمومی رأی‌گیری الکترونیکی مطرح بوده‌اند. این پژوهش با تحلیل تکنیکی، به این دو دسته نگرانی مطرح برای رأی‌دهنده، نامزد و مجری انتخابات الکترونیکی پاسخ می‌دهد. پاسخگویی و نقد سئوالات مطرح در این مقوله، با بررسی و تحلیل راهکارهای موجود امنیت اطلاعات انجام می‌شود.

نتیجه‌گیری: نتایج بررسی نشانگر آن است که؛ ویژگی‌های مثبت تکنیکی رأی‌گیری الکترونیکی از نظر امنیت اطلاعات و قابلیت اعتماد، گذار از رویکرد سنتی به الکترونیکی را یک ضرورت گریزناپذیر می‌نماید. به هر حال، زیرساخت شبکه‌ای و امنیتی از مهمترین پیش‌نیازهای تکنیکی انتخابات الکترونیکی است.لازم است پژوهش‌های آتی نیز ضمن برشمردن فواید متعدد رأی‌گیری الکترونیکی، به هم‌اندیشی و ارائهٔ راه‌کار برای حل برخی مشکلات آن، رفع سایر موانع و تسهیل به‌کارگیری آن در کشور بپردازند.

کلیدواژگان: *رأی‌گیری الکترونیکی، امنیت اطلاعات، قابلیت اعتماد*

سرآغاز

فرآیند رأی‌گیری، یک روش تصمیم‌گیری در میان گروه‌های مردم است. معروف‌ترین کاربرد رأی‌گیری در انتخاب دولت‌ها و مسئولین دولتی توسط افراد جامعه است. هر رأی، نشان‌دهندهٔ نظر یک فرد در موافقت یا مخالفت با یک ایده، نامزد، یا حزب است. به بیانی دیگر، رأی‌گیری از مظاهر دموکراسی است که به معنی حکومت توسط مردم است. معمول‌ترین نوع آن، دموکراسی پارلمانی است که مردم با شرکت در انتخابات، نمایندگان خود در نوعی مجمع قانون‌گذاری را انتخاب می‌کنند.

در این میان، ظهور فنّاوری‌های نوین اطلاعات و ارتباطات، رابطهٔ دولت و شهروندان و روش ارائهٔ خدمات دولتی را تغییر داده است. دولت الکترونیکی، باعث ایجاد تعاملی ساده، شفاف و ارزان بین دولت و شهروندان، شرکت‌های تجاری و دولت شده است. حرکت از دولت غیرالکترونیکی به دولت الکترونیکی موجب تحقق نوع الکترونیکی از دموکراسی می‌شود (1). از طریق دموکراسی الکترونیکی، فرآیندها و ساختارهای ارتباطات الکترونیکی بین دولت و شهروندان و مشارکت الکترونیکی مردم در فرآیندهای خط‌مشی‌گذاری و به بیانی، حاکمیت شهروند محور شکل می‌گیرد. از این رو، مشارکت الکترونیکی هدف نهایی و کلیدی رأی‌گیری الکترونیکی[1] نیز هست.

در رأی‌گیری دستی، فرد باید مراحلی را پشت سر بگذارد که

* نویسنده مسؤول: نشانی الکترونیکی: fnasiri@ eng. ui.ac.ir

[DOR: 20.1001.1.22517634.1393.9.4.4.4]

می‌تواند موجب هدر رفتن زمان و انرژی بسیاری گردد. فرد رأی‌دهنده باید با دردست‌داشتن مدارک لازم و انتظار در صفوف ثبت تأیید مدارک، رأی خود را نوشته و به صندوق بیندازد. رأی‌گیری الکترونیکی می‌تواند به سه صورت ایستگاهی، اینترنتی و سرویس پیام کوتاه انجام شود (2). هم اکنون، در شعبه‌هایی منتخب از استان‌های کشور، نوع ایستگاهی از رأی‌گیری الکترونیکی به انجام رسیده است. مجری پس از دریافت مدارک لازم از رأی‌دهنده، یک کارت الکترونیکی در اختیار وی قرار می‌دهد. سپس رأی‌دهنده با مراجعه به دستگاه و وارد نمودن کارت، کد نامزد مورد نظر خود را وارد می‌نماید. دستگاه چهرهٔ نامزد انتخابی وی را نمایش می‌دهد تا شخص از درستی انتخاب خود مطمئن شود. در انتهای فرآیند، برگهٔ چاپ‌شدهٔ رأی در اختیار شخص رأی‌دهنده قرار می‌گیرد که در آن، کد انتخاب‌شده قابل ملاحظه است. در پایان، رأی‌دهنده کارت الکترونیکی را به ناظر تحویل داده و کارت شناسایی خود را دریافت می‌نماید. در رأی‌گیری اینترنتی یا از طریق پیام کوتاه، فرد واجد شرایط با واردکردن کد شناسایی نامزد مورد نظر در سایت اینترنتی رأی‌گیری یا ارسال آن به صورت پیام کوتاه به نظام خدمتگزار[2] رأی‌گیری مشارکت می‌کند (2و3).

رأی‌گیری به روش سنتی که برای اولین بار در ایالت ویکتوریای استرالیا در 1856 انجام شد تا امروز تحولات بسیاری را پشت سر گذاشته و به صورت الکترونیکی یا توسط تجهیزات الکترونیکی در آمریکا، هند، بلژیک، برزیل، انگلستان، فرانسه، و استرالیا برگزار می‌شود (4). در ایران نیز اولین تلاش‌ها سال 1372 آغاز شد و پس از پیگیری در سال‌های 1378، 1380 و 1386، این تلاش‌ها هنوز به بهره‌برداری نرسیده و نافرجام مانده است (5). با کاهش نقش عامل انسانی در نظام رأی‌گیری الکترونیکی، ثبت، ذخیره و پردازش داده‌های انتخابات از طریق فناوری های خودکار و الکترونیکی باعث صرفه‌جویی در هزینه‌ها، تسهیل مشارکت مردم و بهبود کیفیت خدمات دولت می‌شود. ولی به هر حال، نگرانی‌های امنیتی به عنوان عاملی بازدارنده در پذیرش رأی‌گیری الکترونیکی مطرح بوده است (2و6). برای برگزاری یک رأی‌گیری مناسب، باید از سه جنبه به رأی‌گیری نگاه کرد و تمهیدات لازم را فراهم نمود. به طوری که، کمترین میزان اعتراض از طرف رأی‌دهنده، مجری و کاندیدا قابل طرح بوده و به بیانی، از سوی همگان قابل اعتماد باشد.

رأی‌گیری الکترونیکی

به‌کارگیری خدمات رأی‌گیری الکترونیکی در فضای فنّاوری اطلاعات نه تنها مستلزم رعایت اخلاق و حقوقی است که همچون؛ سایر علوم و علوم مهندسی برای آن برقرار است ، بلکه، لازم است تمهیداتی فراهم باشد که امکان جرائم از طریق این بستر سایبری به پایین‌ترین مقدار برسد تا مورد اقبال عمومی واقع شود. براساس یافته‌های محققان و صاحبنظران، سه عامل ادراک مفید بودن[3]، سازگاری[4]، و قابلیت اعتماد[5] رأی‌گیری الکترونیکی، در پذیرش آن مؤثر است (7- 10). از سوی دیگر، از میان ویژگی‌های یک سیستم خوب رأی‌گیری الکترونیکی، دقت[6]، حفظ حریم شخصی[7]، و قابلیت تصدیق و تأیید[8]، مواردی هستند که باعث ایجاد دغدغه‌های تکنیکی برای پذیرش این فناوری می‌شوند (11). لازم به ذکر است که؛ در بررسی پیش‌نیازهای انتخابات الکترونیکی در ایران نیز؛ شفافیت[9]، پاسخگویی[10]، فرصت مساوی[11]، آزادی[12] و حریم شخصی، قابلیت اعتماد، تشخیص هویت[13]، امنیت شبکه و اطلاعات[14]، و مدیریت الکترونیکی[15] به عنوان عوامل مؤثر در استقرار رأی‌گیری شناخته شده‌اند که از بُعد تکنیکی مطرح هستند (2). این پژوهش در قالب پرسش‌هایی از دید سه طرف اصلی یعنی رأی‌دهنده، مجری و نامزد در انتخابات الکترونیکی به این دغدغه‌ها می‌پردازد.

رأی‌گیری الکترونیکی از دید رأی‌دهنده

رأی‌دهنده از یک سو می‌خواهد که هویت و رأی او محفوظ بماند و از سوی دیگر مایل است که مشارکت او مخدوش نشده و به حساب بیاید(12و13). نیازهای حقوقی، اخلاقی، اجتماعی و

[DOR: 20.1001.1.22517634.1393.9.4.4.4]

امنیتی یک رأی‌دهنده در اعتماد بـه رأی‌گیـری الکترونیکـی در قالب سؤالات زیر قابل طرح است.

سؤال 1: آیا رأی فـرد مخـدوش شـده اسـت؟ در مخالفـت بـا رأی‌گیری الکترونیکی اولین ایرادی که وارد می‌شود، مـشکلاتی است که احتمال دارد در نرم‌افزارها و سـخت‌افزارهـای مربوطـه وجود داشته باشد. چون مهـم‌تـرین نگرانـی در مـورد انتخابـات الکترونیکـی، امکـان دسـت‌کـاری رأی‌هـا اسـت. در فرآینـد الکترونیکی می‌توان با تهیـه نـسخه پـشتیبان ضـریب اطمینـان سیستم و نتایج را بالاتر برد. ولی این احتمال هست کـه نـسخهٔ پشتیبانِ فرایند رأی‌گیری معدوم شود. به هر حال، صندوق‌هـای رأی سنتی هم ممکن است در یک حادثه از دست بروند و حتـی ممکن است در شمارش دستی آرا هم دچار مشکل شوند و برای بازشماری آراء وقت و انرژی بسیاری صرف شود. با این حال، در روش الکترونیکی ممکن است توسط یک رخنه‌گر[16] تغییـری در رأی فرد رأی‌دهنده اعمال گردد و سپس رأی تغییریافته بـه نـام فرد رأی‌دهنده ثبت شود. ولی در روش سنتی نیـز ممکـن اسـت یک یا چند صندوق رأی در یک یا چند حوزه با صندوق(های) از قبل پُر شده‌ای جا به جا گردد. پس معایب نظـام سـنتی در ایـن خـصوص، کمتـر از روش الکترونیکـی نیـست. چـون، در روش الکترونیکی فرد می‌تواند پس از پایـان رأی‌گیـری، رأی خـود را ببیند و از مخدوش نشدن آن اطمینان حاصل کند (14).

در انتخابات سنتی، از طریق شماره‌های شناسایی که کنـار برگـهٔ آراء هست، امکان وجود تقلب، قابل پیگیری اسـت. در انتخابـات الکترونیکی، می‌توان با اسـتفاده از الگـوریتم‌هـای درهـم‌سـاز[17]، مطمـئن شـد کـه رأی‌دهنـده، همـان رأی را فرسـتاده اسـت و همچنین، مـی‌تـوان از امـضای دیجیتـالی[18] و رمزنگـاری کلیـد عمومی استفاده کرد تا امنیت و محرمانگی اطلاعات حفظ شـود (15).

بنابراین، با استفاده از پروتکل‌هـای امـن مـی‌تـوان از امنیـت در انتخابات الکترونیکی مطمئن شد و برای رسیدن به ایـن هـدف، زیرساخت نباید ضعیف باشد.

مخدوش‌شدن رأی الکترونیکی می‌تواند به‌دلیل تقلـب از طریـق دزدی رأی و حمله‌های تزریـق کـد توسـط ماشـین رأی‌گیـری صـورت گیـرد (16). بـرای نمونـه: یـک ماشـین رأی‌گیـری (AcuuVote Ts) در مقابل حمله‌هـایی کـه رأی‌هـایی از یـک نامزد دزدیده شده و به دیگری داده شود آسیب‌پـذیر اسـت. ایـن حمله‌ها بدون ایـن‌کـه شـواهدی از کـلاه‌بـرداری در ثبـت‌هـای سیستم[19] پیدا شود انجام مـی‌گـردد. بـرای جلـوگیری از کـشف حمله، تعداد رأی‌هایی که از یک کاندید به دیگری داده می‌شـود طوری تنظیم می‌شود که کل رأی‌های داده شده ثابـت مانـده و بازرسین متوجه نشوند. حمله‌هایی که فقـط رأی‌هـایی را اضـافه کرده یا از تعداد آن‌ها می‌کاهند قابل پیگیری هستند. این ماشین دو رکورد از هر رأی به صورت رمزشده نگه می‌دارد که یکـی از آن‌ها در حافظهٔ داخلی و دیگری در حافظـهٔ جـانبی اسـت. ولـی رمزنگاری برای حمله‌های دزدی رأی مناسب نیست چون کلیـد کدگذاری[20] در حافظهٔ ماشـین رأی‌گیـری ذخیـره شـده اسـت و بدافزار[21] به راحتی به آن دسترسی می‌یابـد. بـدافزاری کـه روی ماشین اجرا می‌شود هر دو کپی اضافه رکورد را تغییر می‌دهد. از آنجا که ماشین رأی‌گیری نیز لاگ‌های متعـدد و شـمارنده‌هـای گوناگونی نگه می‌دارد که نشان‌دهندهٔ اسـتفاده متعـدد از ماشـین هستند، یک حملهٔ دزدی موفق باید این رکوردهـا را بـه نحـوی تغییر دهد که با تاریخچه ساخته شده در ماشـین سـازگار باشـد. برخـی از ایـن حملـه‌هـا از طریـق تزریـق کـد اسـت و سـپس حمله‌کننده نرم‌افزار مخرب خود را روی یک یا تعـدادی ماشـین رأی‌گیری نصب می‌کند. اگر او بتواند حتـی یـک دسترسـی بـه ماشین پیدا کند، می‌تواند از حمله‌های شناخته شده بـرای نـصب دستی نرم‌افزار استفاده کرده یا ویروسی نصب کرده که به دیگـر ماشین‌ها منتشر شود و به او اجازهٔ خرابکاری گسترده بدهـد. بـه جای نصب مستقیم کـد مخـرب روی هـر ماشـین بـه صـورت جداگانه، حمله‌کننده می‌تواند ویروسی ایجاد کنـد کـه روی یـک ماشین نصب شود و از یک ماشین رأی‌گیری به ماشین دیگـری منتقل شود و به این ترتیب، تعداد زیـادی از ماشـین‌هـا را آلـوده

[DOR: 20.1001.1.22517634.1393.9.4.4.4]

کند. ویروس می‌تواند به نحوی نوشته شود که برنامه‌های مخرب دیگری مانند: سرقت رأی یا منع خدمت[22] را روی هر ماشین آلوده نصب کند (11و14). هدف حمله‌های منع خدمت که مربوط به سؤال‌های 4 و 11 نیز می‌شود، غیر قابل دسترس کردن ماشین‌های رأی‌گیری در روز رأی‌گیری یا محدود کردن دسترسی افراد مسئول به رأی‌ها پس از رأی‌گیری است. در بیشتر موارد، پیش از رأی‌گیری می‌توان حدس زد که رأی‌دهندگان در بعضی از حوزه‌ها به نسبت خاصی به یک نامزد یا حزب رأی می‌دهند. حمله‌های منع خدمت می‌توانند به طوری طراحی که با افزایش بارکاری پردازش ماشین، مانع ارائه خدمات از طرف آن ماشین‌ها گردند و باعث شوند که نتایج انتخابات تحریف شده یا به نفع یک حزب خاص باشد.

خوشبختانه، استفاده از تکنولوژی و راهکارهای مناسب، ریسک‌ها و خطرات انتخابات الکترونیکی را کاهش می‌دهد. با استفاده از کدهای کپچا[23] می‌توان مانع حملات منع خدمت و تزریق کد شد. همچنین، در سال‌های اخیر، پروتکل‌های انتخابات الکترونیکی مبتنی بر تابلوی اعلانات[24] ابداع شده‌اند که با استفاده از آنها، رأی‌دهنده می‌تواند مراحل مختلفی را که رأی وی از مرحله‌ی تولید تا مرحلهٔ شمارش طی می‌کند بررسی نموده و از مخدوش نشدن آن اطمینان حاصل نماید. از سوی دیگر، استفاده از ابزارها و برنامه‌های جلوگیری از نفوذ و تشخیص نفوذ از یک سو و برنامه‌های ضد بدافزار از سوی دیگر اطمینان بیشتری از سلامت عملکرد ماشین‌های رأی‌گیری به همراه خواهد داشت.

سؤال 2: آیا رأی فرد به حساب آمده و غیر قابل ردگیری است؟ در هر سیستم رأی‌گیری باید محرمانگی حفظ شود. افراد در سیستم رأی معمولی، آراء خودشان را بی‌نام در صندوق می‌ریزند و بدین صورت محرمانگی نیز حفظ می‌شود. این نگرانی در هر دو نوع سنتی و الکترونیکی وجود دارد که رأی فرد با هویت او مطابقت داده شود و احتمال ردگیری یا انتقام وجود داشته باشد.

از آنجا که لازم است برگهٔ رأی ممهور به امضای معتبر برگزارکننده باشند ولی محتوای آنها محرمانه باشد، در رأی‌گیری الکترونیکی از امضای کور[25] به منظور حفظ حریم خصوصی رأی‌دهنده استفاده می‌شود (15). این امضا به فرد اجازه می‌دهد که از فرد دیگری بخواهد که پیامی را بدون دانستن محتوای آن امضا نماید. به این طریق، فرد رأی‌دهنده از به حساب آمدن رأی خود اطمینان می‌یابد و همچنین، به دلیل محفوظ ماندن محتوا می‌داند رأی او غیر قابل ردگیری است و مراجع قانونی مسئول تأیید واجد شرایط بودن رأی‌دهنده، نمی‌توانند به محتوای رأی پی‌ببرند. درحالی‌که، با توجه به شماره‌ی سربرگ‌ها، آراء در رأی‌گیری سنتی قابل ردگیری است و فرد پس از انداختن رأی خود در صندوق رأی نمی‌تواند اطمینان حاصل کند که رأی او مخدوش نشده یا صندوقی که رأی فرد در آن است با صندوق دیگری جابه‌جا نشده است (17-19).

سؤال 3: آیا در صورت تمایل، رای دهنده می‌تواند رأی خود را پس از پایان رأی‌گیری ببیند؟ در رأی‌گیری الکترونیکی فهرستی که توسط نظام‌های خدمتگزار و در نهایت، خدمتگزار شمارش منتشر می‌شود، به رأی‌دهندگان این امکان را می‌دهد که درستی شمارش را بررسی کنند. این فهرست به گونه‌ای است که هر فرد می‌تواند با جست‌وجوی رسید خود در لیست منتشر شده، رأیی که به نام او ثبت شده را بررسی کند و همچنین، سایر آراء را البته بدون اطلاع از نام رأی‌دهنده مشاهده و سلامت نتیجه را بررسی کند. در حالی که، در رأی‌گیری سنتی این امکان برای فرد وجود ندارد (20).

سؤال 4: آیا حق رأی فرد تا آخرین لحظهٔ رأی‌گیری محفوظ است؟ در رأی‌گیری به روش سنتی امکان اتمام تعرفه‌ها در برخی شعب وجود دارد و ممکن است فرد نتواند تا لحظات آخر به دلیل وجود مشکل مذکور از حق رأی خود استفاده کند. اما، در رأی‌گیری الکترونیکی با فرض وجود زیرساخت مناسب (مورد بحث در سؤال 1؛ برای نمونه با جلوگیری از حملات)، حق رأی تا آخرین لحظه محفوظ است. بایستی تا وقتی که مُهر زمانی[26]

[DOR: 20.1001.1.22517634.1393.9.4.4.4]

رأی فرد از زمان اتمام رأی‌گیری کمتر است، فرد حق رأی دادن داشته باشد. از آنجا که تمام شهرهای کشور دارای یک محدوده زمانی[27] هستند، این مورد به سادگی قابل کنترل است.

سؤال 5: آیا فرد می‌تواند از هر جا و در هر زمان رأی بدهد؟ از آنجا که در نوع ایستگاهی رأی‌گیری الکترونیکی نیز لازم است برای رأی دادن به ایستگاه‌ها مراجعه شود، به نظر می‌رسد که مزیتی نسبت به رأی‌گیری دستی ندارد. ولی با نگاهی کلان‌تر به مساله مشخص می‌شود که این روش باعث شده است که محدودیت مکانی حذف شود و برای نمونه، در انتخابات مجلس بتوان به فرد مورد نظر خود که برای حوزهٔ دیگری نامزد شده است رأی داد. درصورتی‌که رأی‌گیری از نوع اینترنتی باشد، فرد با حضور در هر مکانی و زمانی امکان رأی دادن دارد و انتخابات الکترونیکی می‌تواند باعث صرفه‌جویی در زمان افراد شود (14).

اما فرایند رأی‌دهی لحظه‌ای همیشه مطلوب نیست. پردازش سریع آراء وابسته به توانایی پردازش داده‌ای خدمتگزارهای دولت و فراهم‌کنندگان خدمات اینترنت است. اگر یک جمعیت بسیاری از رأی‌دهندگان بخواهند هم‌زمان رأی بدهند، توانایی محاسباتی نیاز به سیستمی دارد که بتواند این ترافیک را مدیریت کند. برگزاری رأی‌دهی در چند روز می‌تواند از این سربار جلوگیری کند. ولی این فرایند چند روزهٔ رأی‌دهی می‌تواند باعث مبارزهٔ سیاسی سختی شود (21).

به هر حال، رأی الکترونیکی با حذف محدودیت مکانی و هزینه ارسال ملزومات فیزیکی رأی‌گیری به کشورهای دیگر برای جمع‌آوری آراء هم‌وطنان، از این جهت برتری دارد. ولی لازم است هر رأی دهنده یک رایانه داشته و یا به تکنولوژی رأی‌دهی دسترسی داشته باشد. با توجه به ضریب نفوذ تلفن همراه و استفاده از پروتکل برنامه کاربردی بی‌سیم (وَپ)[28] دسترسی از همه جا برای رأی‌دهی امکان‌پذیر می‌شود.

رأی‌گیری الکترونیکی از دید مجری انتخابات

سلامت برگزاری رأی‌گیری الکترونیکی از دید مجری نیز اهمیت بسیاری دارد و در قالب پاسخگویی به سؤالات زیر می‌توان این نگرانی‌ها را مطرح نمود.

سؤال1: آیا یک فرد می‌تواند بیشتر از یک بار رأی بدهد؟ در رأی‌گیری الکترونیکی، رأی‌دهنده تنها یک بار در هر یک از سیستم‌های خدمتگزار می‌تواند ثبت نام کند. در نتیجه، تنها یک رسید می‌تواند دریافت کند و با هر رسید هم تنها یک بار می‌توان رأی داد. پس از اتمام گشایش صندوق‌ها، آراء شمارش شده و فهرست حاوی هر رأی و رسید متناظر با آن منتشر می‌گردد. از آنجایی که تمامی سیستم‌های خدمتگزار در مرحله شمارش، لیست امضاهای خود را منتشر می‌کنند می‌توان با بررسی آن‌ها بروز تقلب را کشف نمود. البته، اگر همهٔ خدمتگزارها با هم تبانی کرده باشند، تقلب صورت گرفته کشف نخواهد شد. همچنین، اگر از کارت استفاده شود، زمانی که رأی داده شد، کارت کاربر به‌صورت «رأی داده» نشان‌دار می‌شود و کارت برای رأی‌دهی دوباره نمی‌تواند استفاده شود. اما در رأی‌گیری سنتی، امکان تقلب و جعل شناسنامه و کارت شناسایی وجود دارد و یک فرد می‌تواند با مدارک جعلی در حوزه‌های مختلف در صورت متوجه نشدن مسئولین بیش از یک بار رأی دهد (19و20).

سؤال 2: آیا یک فرد می‌تواند در بیشتر از یک حوزهٔ انتخابی رأی دهد؟ در صورت خرابی دستگاه و یا اگر تمام حوزه‌ها متصل نباشند، پایگاه داده‌های برون‌خط یک حوزه از حوزه دیگر خبر ندارد و ممکن است فردی بتواند بیش از یک رأی بدهد و از این رو، تقلب صورت بگیرد. ولی این نیز بستگی به شرایط نرم‌افزاری دارد و در مورد دستگاه‌های‌خودپرداز نیز مشکل از طریق پایگاه دادهٔ آنلاین حل شده است.

سؤال 3: آیا هویت رأی دهنده قابل تأیید است؟ از آنجایی که ممکن است فردی با کارت فرد دیگری رأی دهد، محرز است که با آن کارت رأی داده شده، ولی این نگرانی هست که نمی‌توان هویت رأی‌دهنده را تأیید کرد. به هر حال، در

[DOR: 20.1001.1.22517634.1393.9.4.4.4]

رأی‌گیری الکترونیکی، رمزگذاری[29] این سری مشکلات را تا حد بسیاری حل کرده است. هویت‌شناسی فرد با استفاده از راهکارهای رمزگذاری و با استفاده از روش‌های زیست‌سنجی[30] قابل اثبات است.

از طریق امضاهای دیجیتالی که توسط گواهی‌های دیجیتالی[31] یکتا و معتبر هستند، محرز می‌شود که یک فرد رأی داده است و هر فرد نیز با ارائهٔ کلید خصوصی[32] می‌تواند از رأی خودش آگاه شود. در راهکارهای زیست‌سنجی تشخیص هویت، به جای خواندن کدهای PIN، ورودی‌های زیست‌سنجی کارت‌خوان‌ها (از طریق تشخیص هویت اثر انگشت، اسکن رگ‌های شبکیه یا قرنیه، تحلیل اندازه و مکان اجزای صورت، یا تشخیص ویژگی‌های خاص صدای کاربر، الگوی امضا کردن یا راه رفتن، یا حتی تحلیل سلول‌های DNA فرد در عرض چند ثانیه) برای تأیید اطلاعات رأی‌دهنده که روی کارت است استفاده نمی‌شود، بلکه به منظور تایید اصالت خود کارت است. به عبارتی، سیستم رأی‌گیری در این زمینه تعاملی با مشخصات زیست‌سنجی رأی‌دهنده ندارد و این فرایند به تأیید خود کارت هوشمند کمک می‌کند. ترکیب دو یا چند تحلیل زیست‌سنجی می‌تواند در بهبود نتیجه و افزایش اعتماد سیستم مؤثر باشد. یک رخنه‌گر می‌تواند تعدادی از الگوهای زیست‌سنجی را با الگوهای دیگر جایگزین کند و باعث شود افرادی سودجو از کارت سایرین استفاده کرده و نتیجهٔ انتخابات تغییر کند. نوع دیگری از حمله نیز وجود دارد که خود دولت با دسترسی مستقیم‌تری، الگوهای زیست‌سنجی ذخیره شده‌ی افراد را تغییر دهد (17و20). مقابله با این دو حمله مستلزم ایجاد انبار داده‌هایی[33] از الگوهای زیست‌سنجی رأی‌دهندگان باید امنیت بسیار بالا و توان پردازش بسیار سریع برای کشف متقلبان از طریق مقایسه با آن داده‌ها است.

سؤال 4: آیا می‌توان نتایج رأی‌گیری را تا قبل از اتمام آن متوجه شد؟ انتشار اخبار عمومی بدون درنگ از نتیجهٔ آراء، نامطلوب است زیرا رأی کسانی که تا آن لحظه رأی داده‌اند بر روی رأی‌گیری اثر خواهد گذاشت. در رأی‌گیری الکترونیکی نیز باید پس از پایان رأی‌گیری و با حضور مسئولان مربوطه، آراء شمارش و نتایج منتشر شود. برای شمارش آراء باید کلیدی خصوصی موجود باشد که می‌توان آن را به چندین قسمت تقسیم کرد و در اختیار مسئولین مختلف (مجریان انتخابات و ناظران نامزدها) قرار داد. دراین صورت، با حضور تمام افراد و ارائهٔ تمام اجزای کلید پس از پایان رأی‌گیری نتایج قابل گشایش و مشاهده است (15). درحالی‌که، در رای‌گیری سنتی در مواقعی که بعضی از صندوق‌ها زودتر باز شوند قسمتی از نتایج می‌تواند قبل از اتمام رأی‌گیری منتشر شود (20).

سؤال 5: آیا افراد مختلف که مسئول هستند می‌توانند بر شمارش آراء نظارت کنند؟ همانگونه که در سؤال قبل اشاره گردید، در رأی‌گیری الکترونیکی با تقسیم کلید خصوصی به چند قسمت جهت شمارش آراء می‌توان کلید را در اختیار افرادی قرار داد که لازم است نظارت را انجام دهند. در حالی‌که، در رأی‌گیری سنتی ممکن است در صورت عدم حضور یکی از مسئولین شمارش صورت گیرد (20).

رأی‌گیری الکترونیکی از دید نامزد انتخابات

نه تنها سلامت انتخابات از دید مجری اهمیت دارد و برای رأی‌دهندگان باید قابل اعتماد باشد، بلکه سئوالاتی نیز از دید یک نامزد انتخاباتی به لحاظ اطلاع از نتایج درست مطرح است.

سؤال1: آیا نامزد انتخابات می‌تواند بر شمارش آراء ناظر باشد؟ همچون رأی‌گیری سنتی، در رأی‌گیری الکترونیکی نیز نامزد انتخابات مایل است که بر شمارش آراء نظارت داشته باشد. برای شمارش آراء باید کلید خصوصی موجود باشد. می‌توان کلید خصوصی را بین نمایندگان نامزدها تسهیم نمود. به‌طوری‌که، هیچ یک هیچ اطلاعاتی در مورد کلید به‌دست نیاورد. اما، اگر همهٔ آنها (یا حداقل تعداد مشخصی از آنها) با هم مشارکت کنند، به کلید رمزگشایی دست یابند. پس از طریق تسهیم راز[34]، نظارت آن‌ها بر صحت شمارش نیز فراهم است. ولی، این

[DOR: 20.1001.1.22517634.1393.9.4.4.4]

نگرانی ممکن است مطرح شود که؛ چون کلید خصوصی نیز در دسترس کسانی است که باید آن را رمز کنند، پس رمزکنندگان کلید خصوصی می‌توانند به آراء دسترسی داشته باشند و تا حدودی امنیت آراء در خطر است (20). انواعی از تسهیم راز و به طور خاص با هدف تسهیم کلیدرمزگشایی در کاربرد رأی‌گیری الکترونیکی پیشنهاد شده است که نیاز به طرف سوم مورد اعتماد ندارد (22). بنابراین، از نظر فنی، امنیت آرا در خطر نیست و محرمانگی رأی اشخاص حفظ می‌شود.

سؤال 2: آیا نامزد انتخابات می‌تواند در شمارش آراء دخیل باشد؟

در رأی‌گیری الکترونیکی نیز همانند رأی‌گیری سنتی نظارت بر شمارش آراء می‌تواند وجود داشته باشد. این امکان توسط کلید خصوصی که به چندین قسمت تقسیم می‌شود صورت می‌گیرد. ممکن است با حضور تعداد کافی از قسمت‌های کلید خصوصی شمارش انجام شود. برای جلوگیری از ایجاد تبانی، باید در این نوع تقسیم‌بندی دقت لازم انجام شود که افراد ضروری به طور حتمی حضور داشته باشند و در صورت مفقود شدن قسمتی از کلید، با حضور و اطلاع مراتب بالا، شمارش صورت گرفته و آراء از دست نرود.

سؤال 3: آیا دیگران می‌توانند تعداد آراء نامزد انتخابات را حدس بزنند؟

با رعایت مسائل امنیتی هیچ کس قبل از شمارش آراء نمی‌تواند تعداد آراء نامزد انتخاباتی را در رأی‌گیری سنتی یا الکترونیکی حدس بزند. زیرا، در روش الکترونیکی بدون وجود تمامی قسمت‌های کلید خصوصی امکان مشاهده نتایج وجود ندارد و در روش سنتی نیز قبل از شمارش این امکان فراهم نمی‌شود.

نتیجه‌گیری

بررسی انجام شده در این پژوهش نشان می‌دهد که؛ برخی از نگرانی‌ها در مورد رأی‌گیری الکترونیکی بسیار قابل تأمل و گاه فراتر از نگرانی‌های مطرح در نظام سنتی است. از دید رأی‌دهنده، داشتن حق رأی و تا آخرین لحظهٔ زمان رأی‌گیری، و غیرقابل ردگیری بودن و نیز مخدوش نشدن رأی او، نیاز اساسی است. به هرحال، از دید مجری انتخابات لازم است محرز شود که هر فرد فقط یک بار و فقط در یک حوزه رأی دهد، در عین اینکه هویت رأی‌دهنده قابل تأیید بوده و جعلی نباشد. نگرانی مجری، امکان نظارت بر سلامت برگزاری انتخابات، مخفی ماندن نتایج رأی‌گیری تا پیش از اتمام آن، و نیز امکان نظارت بر شمارش آراء توسط افراد مسئول است. افزون بر قابل حدس نبودن تعداد آراء نامزدها پیش از پایان انتخابات، نظارت و دخیل بودن نامزد در شمارش آراء برای او اهمیت دارد. پروتکل‌های امن با استفاده از امضاهای کور و دیجیتالی و نیز گواهی‌های دیجیتالی به خوبی به این نیازها پاسخ می‌دهد. این سازوکارهای امنیتی برای حفظ حریم شخصی و حفاظت از آرای افراد و نیز اطمینان از سلامت رأی‌گیری و شفاف بودن فرایند رأی‌گیری بیانگر برتری رأی‌گیری الکترونیکی به لحاظ امنیتی و اعتماد است. ولی بررسی تکنیکی نشان می‌دهد که این امر مستلزم فراهم‌بودن تمام تجهیزات مربوطه، زیرساخت‌های شبکه‌ای لازم و پهنای باند کافی است تا نظام به‌طور مؤثری از حملات امنیتی و سوءاستفاده‌های متقلبانه مصون باشد. جدول 1 این دو روش رأی‌گیری را به‌طور مختصر مقایسه می‌کند.

[DOR: 20.1001.1.22517634.1393.9.4.4.4]

جدول 1: مقایسه رأی‌گیری سنتی و الکترونیکی

سؤال	سادگی و امکان پاسخگویی و رفع نگرانی توسط روش	
	رأی‌گیری سنتی	رأی‌گیری الکترونیکی
آیا رأی فرد مخدوش شده است؟	بلی: پیگیری رأی توسط شماره‌های سربرگ	بلی: امکان پیگیری از طریق نسخه پشتیبان
آیا رأی فرد به حساب آمده و غیر قابل ردگیری است؟	تا حدی: قابل ردگیری بودن از شماره سربرگ‌ها	بلی: اطمینان از به حساب آمدن رأی و غیرقابل ردگیری بودن آن به کمک امضای کور
آیا در صورت تمایل، فرد می‌تواند رأی خود را پس از پایان رأی‌گیری ببیند؟	خیر: این امکان وجود ندارد	بلی: مشاهده رأی با استفاده از رسید رأی‌دهی
آیا حق رأی فرد تا آخرین لحظهٔ رأی‌گیری محفوظ است؟	خیر: در صورت اتمام تعرفه‌ها این امکان وجود ندارد	بلی: وجود این امکان با فرض وجود زیرساخت‌ها
آیا فرد می‌تواند از هر جا و در هر زمان رأی بدهد؟	خیر: وجود محدودیت مکانی	بلی: حذف محدودیت‌ها در صورت اینترنتی بودن
آیا یک فرد می‌تواند بیشتر از یک بار رأی بدهد؟	تا حدی: امکان وجود تقلب	تا حدی: تقلب در صورت تبانی سیستم‌های خدمتگزار
آیا یک فرد می‌تواند در بیشتر از یک حوزهٔ انتخابی رأی دهد؟	بلی: در صورت تقلب و رأی دادن با شناسنامه‌های مختلف	خیر: عدم وجود این امکان به کمک پایگاه داده‌های آنلاین
آیا هویت رأی دهنده قابل تأیید است؟	تاحدی: به کمک شناسنامه و کارت ملی که امکان تقلب هم وجود دارد	بلی: حل این مسئله به کمک مشخصات زیست‌سنجی
آیا می‌توان نتایج رأی‌گیری را تا قبل از اتمام آن متوجه شد؟	بلی: امکان افشای قسمتی از نتایج از طریق زودتر باز شدن بعضی از صندوق‌ها!	تا حدی: امکان شمارش زودهنگام توسط کلید خصوصی با حضور مسئولین
آیا افراد مختلف که مسئول هستند می‌توانند بر شمارش آراء نظارت کنند؟	تا حدی: شمارش در صورت عدم حضور بعضی از مسئولین نیز انجام می‌شود!	بلی: عدم امکان شمارش بدون حضور بعضی از مسئولین یه دلیل تکه‌تکه‌بودن کلید خصوصی
آیا نامزد انتخابات می‌تواند بر شمارش آراء ناظر باشد؟	بلی: این امکان هست	بلی: با قرار دادن تکه‌ای از کلید در اختیار ناظر نامزدها
آیا نامزد انتخابات می‌تواند در شمارش آراء دخیل باشد؟	بلی: نظارت توسط ناظرین	بلی: نظارت ناظرین به کمک تکه‌های کلید خصوصی
آیا دیگران می‌توانند تعداد آراء یک نامزد را حدس بزنند؟	تاحدی: در صورت باز شدن صندوق‌ها	خیر: عدم امکان حدس آراء قبل از شمارش

[DOR: 20.1001.1.22517634.1393.9.4.4.4]

واژه‌نامه

1. e-Voting	رأی‌گیری الکترونیکی
2. Server	خدمتگزار
3. Usability	ادراک مفیدبودن
4. Compatibility	سازگاری
5. Reliability	قابلیت اعتماد
6. Accuracy	دقت
7. Privacy	حفظ حریم شخصی
8. Verifiability	قابلیت تصدیق و تأیید
9. Transparency	شفافیت
10. Responsibility	پاسخگویی
11. Equality of voter influence	فرصت مساوی رأی‌دهنده
12. Freedom	آزادی
13. Ensuring the identity	تشخیص هویت
14. Network & information security	امنیت شبکه و اطلاعات
15. Electronic management	مدیریت الکترونیکی
16. Hacker	رخنه‌گر
17. Hash function	تابع درهم‌ساز
18. Digital signature	امضای دیجیتالی
19. System logs	ثبت‌های سیستم
20. Encoding	کدگذاری
21. Malware	بدافزار
22. DoS (Denial of Service)	مانع از خدمت‌رسانی
23. CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)	کپچا
24. Bulletin board	تابلوی اعلانات
25. Blind signature	امضای کور
26. Time stamp	مُهر زمانی
27. Time zone	محدوه زمانی
28. WAP (Wireless Application Protocol)	پروتکل برنامه بی‌سیم
29. Encryption	رمزگذاری
30. Biometric	زیست‌سنجی
31. Digital certificate	گواهی دیجیتالی
32. Private Key	کلید خصوصی
33. Data warehouse	انبار داده‌ها
34. Secret Sharing	تسهیم راز

منابع

1. Pieters W, Becker MJ. (2005). Ethics of e-voting: An essay on requirements and values in Internet elections. UK: Ethics of New Information Technology: Proceedings of the Sixth International Conference of Computer Ethics.
2. Rahnavard F, Kharestani N. (2005). Prerequisite of e-election in Iran. Journal of Managmnet knowledge; 78: 25-44. (In Persian).
3. Burmester M, Magkos E. (2003). Towards secure and practical e-elections in the new era: Secure electronic voting. US: Springer. P. 63-76
4. Fathian M, Taghavi MS. (2009). E- Voting. Tehran: Islamic Palement Research Center.(In Persian).
5. Capital. (2009). Vacacy of e-election in Iran. Available at: http:// hamvatansalam. com/ news131691.htm. Accessed: 11 Apr. 2014. (In Persian).
6. Robinson D, Halderman J (2012). Ethical issues in e-voting security analysis. Proceedings of international conference on Financial Cryptography and Data Security.
7. Bahadoripoor M. (2006). Note that in engeenering ethics. Ethics in Science & Technology; 1(1): 1-11. (In Persian).
8. Khanifar H, Jandaghi GR, Bordbar H. (2012). Role of ethical climate to utilize information technologies. Ethics in Science & Technology; 7(4): 10-18. (In Persian).
9. Sadeghi Arani Z, Mirghafori SHA, Sabet Z. (2013). Ethical decision making in the cyberspace and demographic factors affecting: study of internet crimes in Yazd province. Ethics in Science & Technology; 8(1): 60-69. (In Persian).
10. Schaupp L, Carter L. (2005). E-voting from apathy to adoption. The Journal of Enterprise Information Management; l8 (5): 586- 60l.
11. Cranor L, Cytron K. (l997). Sensus: A security-conscious electronic polling system for the Internet. IEEE Thirtieth Hawaii International Conference on System Sciences.
12. Shayo M, Harel A. (2012). Non-consequentialist voting. Journal of Economic Behavior & Organization; 81(1): 299-313.

[DOR: 20.1001.1.22517634.1393.9.4.4.4]

13.Guerrero A. (2010). The Paradox of Voting and the Ethics of Political Representation. Philosophy & Public Affairs; 38(3): 272–306.

14.Littlewood B, Bryans JW, Ryan PYA, Strigini L. (2006). E-voting: Dependability Requirements and Design for Dependability. Proceedings of the First International Conference on Availability, Reliability and Security.

15.Sherif MH. (2003). Protocols for Secure Electronic Commerce. 2nd ed. USA: CRC Press.

16.ProCon (2013). Electronic Voting Machines and Related Voting Technology. Available at: http:// votingmachines. procon.org /view.resource. php? resource ID= 000273. Accessed: 11 Apr. 2014.

17.Ferreira P (2007). Traceable Electronic Voting [Dissertação de Doutoramento]. Lisboa: Instituto Superior Técnico–Universidade Técnica de Lisboa.

18.Subariah I, Maznah K, Mazleena S, Shah Rizan A. (2003). Secure E-Voting With Blind Signature. 4th international conference on telecommunication technology.

19.Schneier B. (1996). Applied cryptograhphy. Canada: Katherine Schowalter. P. 125-210.

20.Novotný M. (2009). Design and analysis of a practical e-voting protocol. The Future of Identity in the Information Society; 170-183.

21.Brennan J. (2012). the Ethics of Voting. USA: Princeton University Press.

22.Fouque P, Poupard G, Stern J. (2001). Sharing decryption in the context of voting or lotteries. FC'00 Proceedings of the 4th International Conference on Financial Cryptography.

[DOR: 20.1001.1.22517634.1393.9.4.4.4]