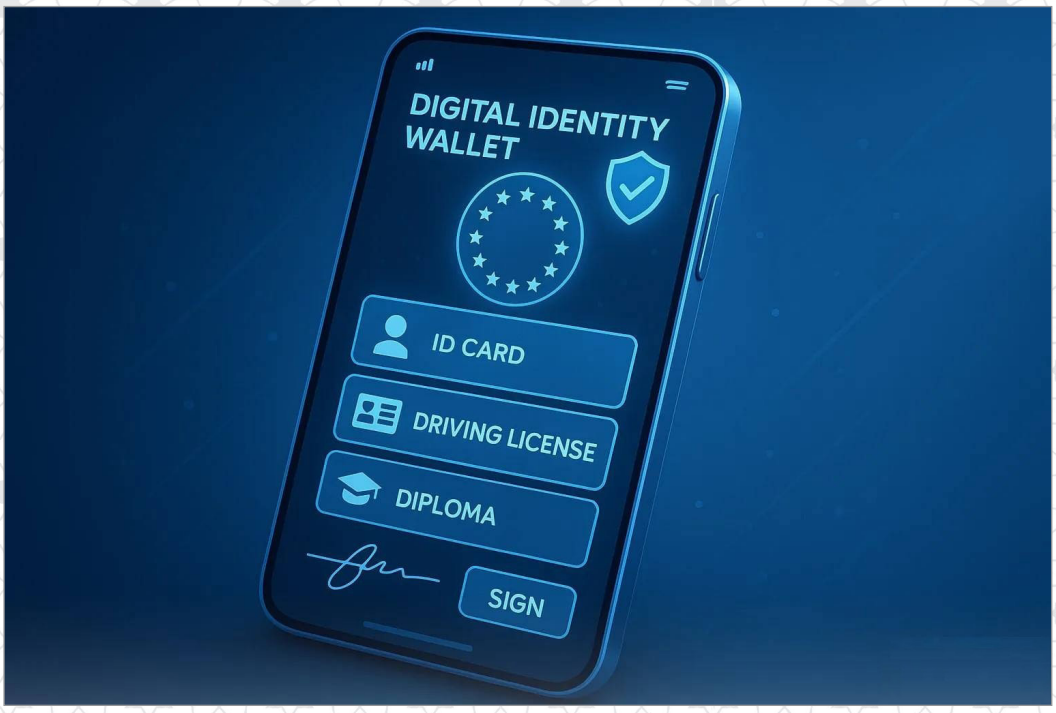
مرکز پژوهش‌های مجلس شورای اسلامی
دفتر مطالعات انرژی، صنعت و معدن
مسلسل: ۲۱۵۵۲ ■ خرداد ۱۴۰۵

مطالعه تطبیقی ابعاد احراز هویت رقومی (دیجیتال)




بسم الله الرحمن الرحيم

تاریخ انتشار:
۱۴۰۵/۳/۳

شماره مسلسل:
۲۱۵۵۲

مرکز پژوهش‌های مجلس شورای اسلامی

عنوان گزارش:
مطالعه تطبیقی ابعاد احراز هویت رقومی (دیجیتال)

نوع گزارش: طرح/ لایحه☐، نظارتی☐، راهبردی■، پیش‌نویس قانونی☐

نام دفتر:
دفتر مطالعات انرژی، صنعت و معدن (گروه مخابرات و فناوری اطلاعات)

مدیر مطالعه:
رسول سلیمانی

تهیه و تدوین کنندگان:
حسن پوراسماعیل، محمدحسن هدایتی، علی میری، سیدمسعود شریفی، حسین عزیزی

اظهار نظر کننده:
علی عبدالاحد (گروه حقوق اساسی و اسناد بالا دستی)

ناظران علمی:
میلاد بیگی، حبیب‌اله ظفریان

گرافیک و صفحه آرایی:
نفیسه حاجی‌صفری

ویراستار ادبی:
مژگان کاظمی

واژه‌های کلیدی:
۱. هویت رقومی (دیجیتال)
۲. احراز هویت
۳. شناسایی

تاریخ شروع مطالعه:
۱۴۰۴/۱/۱

دفتر مطالعات انرژی، صنعت و معدن

فهرست مطالب

فهرست جداول

مطالعه تطبیقی ابعاد احراز هویت رقومی (دیجیتال)

Doi: 10.22034/mrc.report.21552

چکیده

فرایندهای کنونی احراز هویت در ایران، به‌منظور بهره‌مندی از خدمات دولت الکترونیک، نظام بانکی و کسب‌وکارهای نوآورانه همچنان با کندی، هزینه‌های مضاعف و اتکای ناگزیر به مراجعات حضوری روبه‌روست. سامانه‌های موجود از جمله سامانه ثبت احوال، هر یک پایگاه‌های داده هویتی مستقل دارند و روش‌های احراز هویت رقومی مستقلی را پیاده سازی و اجرا می‌کنند. جعل هویت و کلاهبرداری مبتنی بر آن همچنان درحال تداوم است. علاوه‌بر این، نبود چارچوب حقوقی یکپارچه برای فعالیت بازیگران خصوصی، ریسک سرمایه‌گذاری در عرصه خدمات هویت رقومی (دیجیتال) را افزایش داده و سرعت رشد این زیست‌بوم را به‌طور محسوسی کاهش داده است. بررسی تجارب بین‌المللی نشان می‌دهد که بهره‌مندی از راهکارهای نوین و فناوری‌های متنوعی مانند هوش مصنوعی، بلاکچین و رایانش ابری می‌تواند امکان شناسایی و تصدیق هویت کاربران را در هر زمان و مکان با اطمینان بیشتر و هزینه کمتر فراهم آورند. به‌ویژه، مدل‌های جدیدی نظیر هویت غیرمتمرکز یا هویت خود حاکم که با استفاده از رمزنگاری و معماری‌های پیشرفته، اعتماد بین ارائه‌دهنده و دریافت‌کننده خدمات را افزایش داده و موانع موجود در فرآیندهای سنتی را مرتفع می‌کنند.

از بعد تقنینی، تدوین و تصویب نظام جامع احراز هویت رقومی (دیجیتال) ضروری به نظر می‌رسد. با توجه به اهمیت ارایه خدمات هویتی رقومی در اقتصاد رقومی، افزایش بهره‌وری سازمان‌ها و افزایش رضایت کاربران، این گزارش سعی دارد با تحلیل الگوهای موفق جهانی و بررسی قوانین و مقررات جاری، مجموعه‌ای از اقدامات تقنینی و اجرایی را برای استقرار سامانه‌های احراز هویت رقومی یکپارچه، ایمن و مقرون‌به‌صرفه در کشور پیشنهاد کند.

خلاصه مدیریتی

بیان / شرح مسئله

احراز هویت رقومی (دیجیتال) به‌عنوان رکن اساسی در فضای سایبری، جنبه‌های مهمی مانند امنیت، اعتماد عمومی و تحول کسب‌وکارها را به هم پیوند می‌زند. رشد سریع تبادلات الکترونیک نشان داده است که بدون سازوکاری مستحکم و انعطاف‌پذیر برای احراز هویت، نه‌تنها مخاطرات امنیتی (مانند جعل هویت و تقلب) افزایش می‌یابد، بلکه ارائه خدمات برخط نیز دچار محدودیت و بی‌اعتمادی می‌شود. در این میان، توسعه فناوری‌های نوین نظیر بلاکچین، هوش مصنوعی و تحلیل داده‌های کلان فرصتی منحصربه‌فرد را ایجاد نموده تا بهبود فرآیندهای تشخیص هویت، حفظ حریم خصوصی و مدیریت مخاطرات به شکل هم‌زمان میسر شود. ماهیت رقومی (دیجیتال) خدمات احراز هویت به‌ویژه در حوزه‌هایی نظیر فناوری‌های مالی، تجارت الکترونیک و خدمات دولت هوشمند نیازمند چارچوب‌های حقوقی و نظارتی جدیدی است که بتواند هم از حقوق کاربران حفاظت کند و هم انگیزه‌های لازم برای نوآوری را به وجود آورد. بر این اساس توسعه زیست‌بوم احراز هویت رقومی (دیجیتال) در ایران، علیرغم اقدامات و تلاش‌های صورت گرفته با چالش‌هایی همچون خلاءهای قوانین و مقررات جامع، عدم هماهنگی دستگاه‌های ذی‌ربط و ضعف در آشنایی عموم مردم در مورد مزایا و شیوه‌های استفاده از این خدمات مواجه است. این گزارش می‌کوشد، با واکاوی تجارب بین‌المللی و مدل‌های موفق در کشورهای پیشرو، ابعاد حقوقی، فنی و نهادی را بررسی کرده و پیشنهادهایی برای بهبود وضعیت موجود و حرکت به‌سوی نظام احراز هویت رقومی (دیجیتال) فراگیر، قابل اتکاء و اثربخش ارائه دهد.

نقطه‌نظرات / یافته‌های کلیدی

مطالعات و بررسی‌ها نشان می‌دهد که ایجاد و اجرای یک چارچوب جامع قانون‌گذاری هم‌راستا با تحول رقومی (دیجیتال)، نخستین گام برای تثبیت و گسترش احراز هویت رقومی (دیجیتال) در ایران است. در چنین چارچوبی، نقش هماهنگ‌کننده میان نهادهای حاکمیتی و بخش خصوصی برجسته می‌شود و زیرساخت‌های فنی یکپارچه (همچون سامانه‌های گواهی رقومی و پایگاه‌های اطلاعاتی مشترک) زمینه را برای اطمینان‌بخشی به کاربران فراهم می‌کند. افزون بر این، لحاظ کردن شایسته سطوح مختلف اطمینان هویتی، بهره‌گیری از ابزارهای چندعاملی و بیومتریک در فرآیند احراز هویت و استفاده از فناوری‌های نوین(هویت غیرمتمرکز) در راستای تقویت کارایی و امنیت، از اصول ضروری توسعه سازوکارها و نظام احراز هویت رقومی (دیجیتال) کشور قلمداد می‌شود. تجربه کشورهایی که در این زمینه پیشرو هستند نشان می‌دهد طراحی و پیاده‌سازی سازوکارهای ارزیابی و بازرسی مستمر نیز ضرورتی انکارناپذیر برای حفظ اعتماد عمومی خواهد بود.

پیشنهاد راهکار تقنینی، نظارتی یا سیاستی

۱ **طراحی چارچوب قانونی و نظارتی:** تدوین و تصویب قانون جامع احراز هویت رقومی (دیجیتال) با هدف باز آفرینی قوانین و مقررات مرتبط با ابعاد گسترده احراز هویت رقومی، و به‌منظور اصلاح زیست‌بوم فعلی و رفع چالش‌های حوزه مذکور

۲ **تقویت زیرساخت‌های فنی و امنیتی:** ایجاد سامانه‌های متمرکز یا غیرمتمرکز مدیریت هویت، توسعه خدمات ثبت و تأیید هویت مبتنی‌بر نیازمندی هدف و بهره‌گیری از قابلیت‌های فناوری‌هایی مانند بلاکچین و هوش مصنوعی، که اولویتی کلیدی برای ارائه خدمات ایمن محسوب می‌شود.

۳ **ترویج فرهنگ و آموزش:** آگاهی‌بخشی عمومی درباره نحوه استفاده از راهکارهای احراز هویت رقومی (دیجیتال) و مزایای آن، نقش مهمی در پذیرش و گسترش این خدمات دارد.

۴ **تشویق مشارکت بخش خصوصی:** ایجاد فضای رقابتی سالم و ارائه تسهیلات لازم به کسب‌وکارهای ارائه‌دهنده خدمات هویتی رقومی (دیجیتال)، ضمن رعایت الزامات امنیتی و حریم خصوصی، می‌تواند به توسعه این صنعت کمک کند.

۵ توسعه پایش و نظارت مستمر: انتخاب و معرفی نهاد یا کارگروهی مشترک از دستگاه‌های حاکمیتی، بخش خصوصی و کارشناسان مستقل برای بررسی روندهای فناورانه، ارتقای شفافیت و ارتقای سطح اطمینان کاربران، گامی ضروری در حفظ پویایی نظام احراز هویت رقومی (دیجیتال) خواهد بود.

۱. مقدمه

هویت رقومی (دیجیتال)[1] به مجموعه‌ای از ویژگی‌ها، شناسه‌ها و داده‌هایی گفته می‌شود که در فضای مجازی به یک موجودیت اعم از شخص حقیقی، سازمان، ابزار یا نرم‌افزار نسبت داده می‌شود. این ویژگی‌ها می‌تواند دربرگیرنده اطلاعاتی همچون نام، نام کاربری، رمز عبور، شماره ملی، تاریخ تولد، نشانی پست الکترونیک، شماره تلفن همراه، داده‌های زیست‌سنجی (بیومتریک مانند اثر انگشت، عنبیه، چهره)، سوابق تراکنش‌های مالی، الگوهای رفتاری (مانند نحوه تایپ یا استفاده از ماوس) و حتی داده‌های مکانی باشد. بنابراین، هویت رقومی (دیجیتال) تنها به یک شناسه ساده محدود نمی‌شود؛ بلکه گاهی جنبه‌های متعددی از حیات شخص را پوشش می‌دهد و به صورت پراکنده در سامانه‌های گوناگون نگهداری می‌شود.

در رویکرد سنتی، هویت غالباً به‌واسطه اسناد فیزیکی مانند شناسنامه، گذرنامه یا کارت ملی احراز می‌شد. اما در عصر رقومی (دیجیتال)، بخش زیادی از تعاملات انسانی در فضای مجازی و بدون حضور فیزیکی افراد انجام می‌گیرد. درنتیجه، اسناد کاغذی دیگر پاسخگوی الزامات امنیتی و سرعت مورد انتظار در تراکنش‌های برخط نیستند. ازاین‌رو، هویت رقومی (دیجیتال) به‌عنوان جایگزینی پویا و منعطف برای همگام‌شدن با خدمات الکترونیک، ضرورت یافته است.

احراز هویت رقومی (دیجیتال) به‌عنوان رکن اساسی در فضای سایبری، جنبه‌های امنیت، اعتماد عمومی و تحول کسب‌وکارها را به هم پیوند می‌زند. رشد سریع تبادلات الکترونیک نشان داده است که بدون سازوکاری مستحکم و انعطاف‌پذیر برای احراز هویت، نه‌تنها مخاطرات امنیتی (مانند جعل هویت و تقلب) افزایش می‌یابد، بلکه ارائه خدمات برخط نیز دچار محدودیت و بی‌اعتمادی می‌شود. در این میان، توسعه فناوری‌های نوین نظیر بلاکچین، هوش مصنوعی و تحلیل داده‌های کلان فرصتی منحصربه‌فرد را ایجاد نموده تا بهبود فرآیندهای تشخیص هویت، حفظ حریم خصوصی و مدیریت مخاطرات به شکل هم‌زمان میسر شود [۱].

بررسی‌ها نشان می‌دهد طی پنج سال آتی، ارزش بازار هویت رقومی (دیجیتال) در سطح جهانی از مرز ۵۰ میلیارد دلار فراتر خواهد رفت که این رشد، بیانگر تغییرات زیرساختی عمیقی در اقتصاد رقومی (دیجیتال) نیز محسوب می‌شود. همچنین، بنا بر گزارش شرکت تحلیل‌گر فناوری جونیپر ریسرچ[2]، شمار کاربران خدمات احراز هویت رقومی (دیجیتال) در سال ۲۰۲۳ از ۱.۵ میلیارد نفر عبور کرده و روند صعودی آن ادامه خواهد داشت [۲]. آمارها حاکی از آن است که دیدگاه ابزاری و فنی نسبت به موضوع هویت رقومی (دیجیتال) در حال گذار به‌سوی تحول رفتاری و سبک زندگی رقومی (دیجیتال) است.

در ایران نیز برخورداری از ظرفیت بالقوه در حوزه‌هایی مانند خدمات فناورانه مالی، دولت الکترونیک و تجارت الکترونیک، زمینه را برای توسعه راهکارهای احراز هویت رقومی (دیجیتال) مساعد کرده است.

از این‌رو، گزارش حاضر با رویکردی تحلیلی ـ سیاستی، به بررسی مفهوم و الزامات احراز هویت رقومی (دیجیتال) پرداخته و ضمن مرور تحولات جهانی و چارچوب‌های مرجع در این حوزه، وضعیت موجود ایران را از منظر حقوقی، نهادی و اجرایی مورد واکاوی قرار می‌دهد. در این گزارش، قوانین و مقررات بالادستی مرتبط، ساختار نهادی متولیان احراز هویت، و چالش‌های فنی

1. Digital Identity
2. Juniper Research

و حکمرانی داده‌ها بررسی شده و تلاش شده است با شناسایی خلأها و نارسایی‌های موجود، مجموعه‌ای از توصیه‌های تقنینی، نظارتی و سیاستی برای استقرار نظام احراز هویت رقومی (دیجیتال) یکپارچه، ایمن و کارآمد ارائه شود. هدف نهایی گزارش، کمک به تصمیم‌گیران و قانون‌گذاران در طراحی چارچوبی منسجم است که ضمن تسهیل ارائه خدمات الکترونیک، صیانت از حقوق شهروندان و ارتقای اعتماد عمومی در فضای مجازی را تضمین کند.

۲. پیشینه

شناخت سوابق مطالعاتی و تقنینی در زمینه احراز هویت رقومی (دیجیتال) و هویت هوشمند، نقشی کلیدی در ترسیم نقشه راه آینده و هموارسازی مسیر سیاستگذاری ایفا می‌کند. از یک سو، گزارش‌ها و پژوهش‌های انجام شده در مرکز پژوهش‌های مجلس شورای اسلامی، تصویری از اولویت‌ها و چالش‌های اجرایی در پروژه‌های ملی هویت رقومی (دیجیتال) به دست می‌دهد؛ از جمله بررسی میزان پیشرفت استقرار هویت هوشمند در دولت الکترونیک و اهمیت استفاده از شماره ملی در یکپارچگی سامانه‌های دستگاه‌های دولتی. از سوی دیگر، اسناد و مقررات مختلفی که در قالب مصوبات هیئت وزیران، شورای عالی فضای مجازی و دیگر نهادهای تصمیم‌گیر تدوین شده‌اند، نشانگر دغدغه حاکمیت نسبت به ضرورت تکمیل زیرساخت‌های هویت رقومی (دیجیتال) هستند.

۲ـ۱. سوابق مطالعاتی

در مسیر استقرار نظام احراز هویت رقومی (دیجیتال) و هویت هوشمند در ایران، گزارش‌ها و مطالعاتی توسط نهادهای پژوهشی به‌ویژه مرکز پژوهش‌های مجلس شورای اسلامی ارائه شده که در ادامه به سه نمونه مهم اشاره می‌شود:

۱ **بررسی لایحه برنامه هفتم پیشرفت (۷۷): رصد و نظارت بر پروژه استقرار هویت هوشمند اشخاص حقیقی در دولت الکترونیک:** تأکید بر نقش کلیدی سازمان ثبت احوال کشور در ساخت، به‌روزرسانی پایگاه داده جمعیتی و ارائه سرویس‌های احراز هویت رقومی (دیجیتال)، بررسی میزان پیشرفت پروژه‌های مرتبط با هویت هوشمند در دولت الکترونیک، ارزیابی نقاط قوت و ضعف اجرای آن و سرانجام ارائه پیشنهادهایی برای اصلاح مواد مرتبط در لایحه برنامه هفتم پیشرفت، از محورهای اصلی این پژوهش به‌شمار می‌رود.

۲ **استفاده از شماره ملی در نظام احراز هویت و یکپارچگی سامانه‌های دولت:** این مطالعه بر اهمیت تخصیص شماره و کدهای واحد برای شناسایی افراد، اسناد و موجودیت‌ها متمرکز است. بر اساس تجربیات بین‌المللی، داشتن یک شناسه واحد به‌عنوان زیرساخت اصلی احراز هویت الکترونیکی می‌تواند منجر به تبادل مؤثر اطلاعات میان دستگاه‌های اجرایی و کاهش موازی‌کاری شود. گزارش یادشده، با تأکید بر ساده‌سازی فرآیند شناسایی، زمینه‌های ایجاد دولت الکترونیک چابک و پایدار را بررسی می‌کند.

۳ **ارائه خدمات الکترونیکی هویت ملی:** در این گزارش، الزامات توسعه پروژه پایگاه اطلاعات جمعیت کشور و چگونگی اصلاح بسترهای مرتبط با احراز هویت الکترونیکی ملی در سازمان ثبت احوال مورد بحث قرار گرفته است. تدوین و پیاده‌سازی ساختارهای فنی و اجرایی برای تحقق یک سامانه الکترونیکی احراز هویت کارآمد، از جمله نکات محوری این پژوهش محسوب می‌شود.

جدول ۱. تحلیل پیشینه پژوهشی

ردیف	عنوان گزارش	سال انتشار	شماره مسلسل	نام دفتر / سازمان / نهاد	توضیحات
۱	بررسی لایحه برنامه هفتم پیشرفت (۷۷): رصد و نظارت بر پروژه استقرار هویت هوشمند اشخاص حقیقی در دولت الکترونیک [۳]	۱۴۰۲	۱۹۳۷۶	دفتر مطالعات مدیریت	بررسی پروژه استقرار هویت هوشمند اشخاص حقیقی در دولت الکترونیک مطابق با تکالیف هیئت وزیران و قانون برنامه پنج ساله توسعه، که سازمان ثبت احوال کشور متولی ساخت، به‌روزرسانی پایگاه داده و ارائه سرویس‌های احراز هویت اشخاص حقیقی است. در این راستا، پس از نظارت بر اجرای پروژه، پیشنهادهایی جهت اصلاح مواد مرتبط ارائه شده است.
۲	استفاده از شماره ملی در نظام احراز هویت و یکپارچگی سامانه‌های دولت [۴]	۱۳۹۹	۱۷۲۰۶	دفتر مطالعات انرژی، صنعت و معدن	بررسی اهمیت و نقش تخصیص شماره و کدهای واحد در شناسایی اشخاص، اسناد و موجودیت‌ها به عنوان زیرساخت اصلی احراز هویت الکترونیکی و تبادل اطلاعات میان دستگاه‌ها در راستای سامان‌دهی و استفاده بهینه از این کدها برای ایجاد یک دولت الکترونیک چابک و پایدار مبتنی بر تجربیات و اقدامات کشورهای مختلف
۳	ارائه خدمات الکترونیکی هویت ملی [۵]	۱۳۸۵	۸۱۶۵	گروه ارتباطات و فناوری‌های نوین	بررسی الزامات توسعه پروژه پایگاه اطلاعات جمعیت کشور در راستای اصلاح بسترهای ارائه خدمات الکترونیکی احراز هویت ملی در سازمان ثبت احوال کشور

مآخذ: گردآوری توسط نویسندگان

۲-۲. سوابق تقنینی به همراه آسیب‌شناسی[۱]

طی سال‌های اخیر، قوانین و مقررات مختلفی به‌صورت مستقیم یا غیرمستقیم بر لزوم تکمیل زیرساخت‌های احراز هویت رقومی (دیجیتال) و ساماندهی هویت مجازی در کشور تأکید کرده‌اند. بااین‌حال، همچنان یک قانون منسجمی که اختصاصاً نظام هویت رقومی (دیجیتال) را در ایران سامان دهد، وجود ندارد. مهم‌ترین اسناد و مصوبات مرتبط با این حوزه عبارت‌اند از:

مصوبه هیئت وزیران درباره دولت الکترونیک (مورخ ۱۳۹۷/۰۱/۲۲)

در این مصوبه، موضوع تکمیل زیرساخت‌های هویت رقومی (دیجیتال) به‌عنوان یکی از الزامات توسعه دولت الکترونیکی مطرح شده است. این سند بر اهمیت راه‌اندازی سامانه‌های الکترونیکی یکپارچه تأکید کرده و دستگاه‌های دولتی را مکلف به همگرایی در شناسایی و تصدیق هویت کاربران در ارائه خدمات الکترونیک می‌کند [۶].

«نظام هویت معتبر در فضای مجازی کشور»، مصوب جلسه ۴۹ شورای عالی فضای مجازی (مورخ ۱۳۹۸/۰۶/۰۹)

این سند، چارچوبی کلی برای نحوه احراز هویت کاربران در فضای مجازی و تعیین شاخص‌های هویت معتبر ارائه می‌دهد. طبق این مصوبه، دستگاه‌های اجرایی و بخش خصوصی موظف‌اند استانداردهای مشترک در شناسایی رقومی (دیجیتال) را رعایت نموده و از موازی‌کاری در سامانه‌های هویت جلوگیری کنند [۷].

مصوبه یازدهمین جلسه شورای اجرایی فناوری اطلاعات (مورخ ۱۳۹۶/۰۱/۲۸)

این مصوبه، مجموعه‌ای از وظایف و تکالیف دستگاه‌های اجرایی و نهادهای مسئول در حوزه فناوری اطلاعات را تعیین کرده و ضمن اشاره به اهمیت احراز هویت رقومی (دیجیتال)، بر تقویت هماهنگی‌های بین‌بخشی در تبادل داده‌های هویتی تأکید می‌ورزد [۸].

۱. شامل قوانین مصوب مجلس شورای اسلامی و نتایج و ارزیابی از قوانین مصوب و مصوبات شورای عالی (مانند شورای عالی انقلاب فرهنگی و مصوبات هیئت‌وزیران)، ضروری است درخصوص بررسی سوابق در بخش بین‌الملل؛ عنوان موارد بررسی شده، سال اجرای آنها و مهمترین یافته، در قالب یک جدول ذکر شود.

«دستورالعمل ساماندهی واگذاری شناسه ارتباطی» مصوب جلسه ۱۲۵ کمیسیون عالی تنظیم مقررات فضای مجازی کشور (مورخ ۱۴۰۲/۱۱/۱۲)

این دستورالعمل بیشتر جنبه اجرایی و امنیتی دارد و بر کنترل واگذاری غیرقانونی شماره‌های تلفن همراه و شناسه‌های ارتباطی متمرکز است. در آن، لزوم احراز هویت در واگذاری شناسه‌ها، ایجاد سامانه‌های ثبت شکایت و همکاری میان دستگاه‌های انتظامی، وزارت ارتباطات و سکوها مورد تأکید قرار گرفته است. هرچند رویکرد این سند ضروری است، اما همچنان به هویت رقومی (دیجیتال) به‌مثابه ابزاری برای نظارت می‌نگرد، نه یک زیرساخت توسعه‌گرا و حقوق‌محور. تمرکز صرف بر پیشگیری از تخلف، بدون تبیین سازوکارهای مثبت مانند ارتقای تجربه کاربری، صدور گواهی رقومی (دیجیتال) یا ارتقای سطح اطمینان، موجب محدود شدن افق دید سیاست‌گذار شده است.

افزون‌بر این اسناد، قوانین دیگری نیز به‌صورت غیرمستقیم به موضوع هویت و ساماندهی آن در فضای مجازی اشاره دارند؛ اما همان‌گونه که از بررسی کلی مقررات موجود برمی‌آید، خلأ یک قانون اختصاصی در زمینه احراز هویت رقومی (دیجیتال) در ایران همچنان محسوس است. درنتیجه، هرچند در برخی قوانین، مقررات جزئی درباره هویت رقومی (دیجیتال) یا ابعاد گوناگون آن (نظیر امضا و اسناد الکترونیک) وجود دارد، اما برای دستیابی به یک چارچوب همگن و یکپارچه، لازم است قانون‌گذار با همکاری دستگاه‌های اجرایی و کارشناسان حوزه فناوری، نسبت به تدوین و تصویب قانونی اختصاصی و روزآمد اقدام کند تا راه را برای توسعه مطمئن و فراگیر هویت رقومی (دیجیتال) در کشور هموار سازد.

جدول ۲. تحلیل پیشینه تقنینی

ردیف	نام سند	مرجع تصویب	تاریخ تصویب	شماره ماده / صفحه	نکات برجسته / نقاط ضعف و قوت / پیامدهای اجرا
۱	آیین‌نامه اجرایی ماده (۱۴) الحاقی قانون مبارزه با پولشویی مصوب هیئت وزیران [۶]	هیئت وزیران	۱۳۹۸/۰۷/۲۱	مواد (۱۶، ۲۰،۵۰، ۵۵، ۶۱)	تاکید بر لزوم ایجاد سازوکارهای شناسایی و ثبت اطلاعات هویتی اتباع داخلی و خارجی مبتنی بر پایگاه داده اطلاعات
۲	نظام هویت معتبر در فضای مجازی کشور»، مصوب جلسه ۵۹ شورای عالی فضای مجازی	شورای عالی فضای مجازی	۱۳۹۸/۰۶/۰۹	تمامی مواد	تعریف الزامات زیست بوم هویت معتبر در فضای مجازی
۳	مصوبه یازدهمین جلسه شورای اجرایی فناوری اطلاعات با عنوان «الزام ارائه خدمات الکترونیکی به اشخاص با احراز هویت و نشانی محل اقامت»	شورای اجرایی فناوری اطلاعات	۱۳۹۷/۰۲/۰۴	بند «۲»	ارائه اقدامات اجرایی پروژه استقرار هوست هوشمند اشخاص حقیقی در دولت الکترونیک – متولی سازمان ثبت احوال
۴	سند راهبردی نظام جامع فناوری اطلاعات جمهوری اسلامی ایران [۹]	هیئت وزیران	۱۳۸۸/۰۲/۰۸	ه ـ۴ـ۴ـ۳	ایجاد نظام صدور گواهی و احراز هویت الکترونیکی مطمئن
۵	دستورالعمل ساماندهی واگذاری شناسه ارتباطی - مصوب جلسه ۱۲۵ کمیسیون عالی تنظیم مقررات فضای مجازی کشور	کمیسیون عالی تنظیم مقررات فضای مجازی کشور	۱۴۰۲/۰۹/۱۳	تمامی مواد	جلوگیری از واگذاری غیرمجاز شماره‌های ارتباطی (مثل شماره تلفن همراه) و ایجاد سازوکارهای قانونی، فنی و نظارتی برای کنترل، احراز هویت، پیگیری شکایات و اعمال محدودیت علیه واگذارندگان غیرمجاز
۶	الزامات واگذاری شناسه ارتباطی و نحوه برخورد با واگذارنده غیرمجاز - مصوبه شماره ۵ جلسه شماره ۳۵۶ مورخ ۱۴۰۳/۴/۲۴ کمیسیون تنظیم مقررات ارتباطات	کمیسیون تنظیم مقررات ارتباطات	۱۴۰۳/۴/۲۴	تمامی مواد	هرگونه واگذاری شناسه ارتباطی مبنای احراز هویت به اتباع ایرانی یا غیر ایرانی، منوط به احراز هویت متقاضی بر اساس مدارک هویتی، اخذ تاییدیه از سامانه شاهکار و استفاده از یکی از روش‌های زیست سنجی مورد تایید سازمان از قبیل اثر انگشت و تشخیص چهره است؛ در صورت تغییر مالکیت شناسه ارتباطی، این شناسه از مبنای احراز هویت مشترک خارج می‌شود.

مآخذ: گردآوری توسط نویسندگان

۳. هویت رقومی (دیجیتال)

برخلاف هویت سنتی که صدور و تایید آن از طریق نهادهای دولتی (مانند سازمان ثبت احوال) صورت می‌گرفت، هویت رقومی (دیجیتال) می‌تواند توسط مجموعه‌ای از نهادهای گوناگون (بانک‌ها، ارائه‌دهندگان خدمات مخابراتی، سکوهای مجازی و غیره) یا حتی به‌صورت خود حاکم ایجاد و مدیریت شود.

امروزه با توسعه اقتصاد رقومی (دیجیتال) بسیاری از فعالیت‌های اقتصادی، وابسته به تأیید هویت هستند. اگر هویت رقومی (دیجیتال) فرد با دقت و امنیت بررسی و تأیید نگردد، خطراتی همچون جعل هویت، سرقت حساب، کلاهبرداری و سایر جرائم سایبری افزایش می‌یابد. از سوی دیگر، اگر این فرآیند بیش از حد پیچیده یا هزینه‌بر باشد، تجربه کاربری آسیب می‌بیند و مانع از فراگیری خدمات رقومی (دیجیتال) می‌گردد. به همین دلیل، ایجاد تعادل میان امنیت، حریم خصوصی و سهولت استفاده، یکی از چالش‌های اساسی در طراحی سامانه‌های مدیریت هویت رقومی (دیجیتال) است [۱۰].

۳-۱. تمایز مفاهیم شناسایی و احراز هویت

شناسایی، گام مقدماتی در تعاملات رقومی (دیجیتال) است که موجودیت ادعا می‌کند «من چه کسی هستم». این ادعا معمولاً با ارائه یک شناسه یا اطلاعات هویتی (مانند نام کاربری، شماره ملی، شماره همراه) بیان می‌شود. در این مرحله، تنها اعلان هویت صورت می‌گیرد و هیچ سازوکاری برای اثبات یا رد آن وجود ندارد. برای مثال، کاربری که در یک سکو (پلتفرم) فروش آنلاین، نام کاربری انتخاب می‌کند، صرفاً خود را شناسایی کرده است.

احراز هویت رقومی (دیجیتال)، یعنی هویتی در دنیای واقعی وجود دارد که پیش از این شناسایی شده است، و حالا باید مشخص شود فردی که ادعا می‌کند این هویت را راست می‌گوید یا خیر. پس مرحله پیش از احراز، شناسایی هویت است که در همین مرحله چالش‌های اساسی وجود دارد. نمونه‌های بارز آن عبارت‌اند از:

- نوجوانان زیر ۱۵ سال امکان دریافت سیم‌کارت به نام خود را ندارند و والدین به نام خود سیم‌کارت خریداری کرده و به آنان واگذار می‌کنند؛
- افراد می‌توانند به راحتی سیم‌کارت اعتباری دریافت کرده و به شخص دیگری منتقل کنند (در حالی که در بسیاری از کشورها برای خدمات مالی و قضایی تنها سیم‌کارت دائمی با فرایندهای سختگیرانه شناسایی و احراز هویت پذیرفته می‌شود)؛
- تعریف دقیقی از امضا وجود ندارد و اغلب افراد صرفاً علامتی بسیار ساده ترسیم می‌کنند، در حالیکه در بسیاری از کشورها امضا باید همراه با دست‌خط یا نشانه‌ای منحصر به فرد باشد تا قابلیت انتساب قانونی داشته باشد.

بنابراین پیش از این‌که به مرحله احراز برسیم، با ضعف‌های در شناسایی هویت مواجه هستیم که این موضوع مورد بحث این گزارش نیست.

احراز هویت، مرحله دوم و تکمیلی است که در آن درستی ادعای هویت بررسی می‌شود. این اطمینان با استفاده از عوامل احراز هویت مانند رمز عبور (عامل دانسته)، توکن سخت‌افزاری (عامل داشته) یا اثر انگشت (عامل ذاتی) حاصل می‌شود. در اینجا هدف، اثبات این است که فردی که ادعای مالکیت یک حساب یا شناسه را دارد، واقعاً همان شخص باشد.

از این‌رو، در مهندسی سامانه‌های امنیتی، تمایز دقیق میان شناسایی و احراز هویت حیاتی است. شناسایی بدون احراز، یا احراز با شناسایی کم و مخدوش، سطح امنیت را کاهش داده و زمینه‌ساز آسیب‌پذیری در برابر حملات و سوءاستفاده‌های سایبری خواهد بود [۱۱].

نکته مهم دیگری که باید ذکر شود تمایز میان انطباق هویت و احراز هویت است. برای مثال، در سامانه شاهکار در ایران، فرآیند «احراز هویت» در واقع تنها «انطباق» دو داده است (شماره تماس و شماره ملی). این انطباق لزوماً به‌معنای احراز هویت فرد نیست، چرا که ممکن است سیم‌کارت و کد ملی متعلق به فردی باشد، اما شخص دیگری از آن استفاده کند. بنابراین، اتکای صرف به انطباق داده‌ها می‌تواند منجر به خطا و سوءاستفاده شود. احراز هویت متکی به عواملی است که در ادامه به آن اشاره می‌شود.

۲-۳. چارچوب‌ها و مقررات احراز هویت در جهان

۲-۳-۱. چارچوب تضمین احراز هویت موجودیت[1] (ISO/IEC 29115:2013)

چارچوب تضمین احراز هویت موجودیت، استاندارد حاصل همکاری مشترک سازمان بین‌المللی استانداردسازی (ISO) و کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] است و چارچوبی مرجع برای ارزیابی «اطمینان در احراز هویت» فراهم می‌کند. در این چارچوب، سه عامل کلاسیک تصدیق هویت – یعنی آنچه فرد می داند، دارد، یا هست (ویژگی‌های زیستی یا رفتاری) - در چهار سطح اطمینان (طبقه‌بندی می‌شوند. هدف اصلی این استاندارد، یکپارچه‌سازی معیارهای فنی و مدیریتی است تا سازمان‌ها بتوانند براساس میزان ریسک خدمات، سطح اطمینان مناسب را برگزینند و الزامات فناوری، فرایند ثبت و ممیزی را با یک زبان مشترک تعریف کنند. این استاندارد، مبنای تدوین بسیاری از مقررات ملی و بین‌المللی (ازجمله مقررات eIDAS اروپا) برای هم‌ارزسازی سطوح اطمینان بوده است.

۲-۳-۲. دستورالعمل‌های هویت دیجیتال[3] (NIST SP 800-63-4 (Draft 2, 2024))

این سند راهنمای مؤسسه ملی استانداردها و فناوری ایالات متحده مجموعه‌ای به‌روز از الزامات مربوط به چرخه کامل «شناسایی و اثبات هویت رقومی (دیجیتال) » ارائه می‌دهد. جلد-C آن سه سطح تضمین اصالت‌سنجی (AAL1-3) را تشریح می‌کند و درباره فناوری‌های نوینی نظیر احراز بدون گذرواژه، احراز تطبیقی و چندعاملی را راهنمایی می‌کند؛ جلد-B نیز به تشریح فرآیند ثبت هویت و صدور گواهی را در سه سطح پوشش می‌دهد. در نسخه چهارم (پیش‌نویس) واژگان ساده‌تر شده، سازگاری با استانداردهای WebAuthn، FIDO و ISO ۲۹۱۱۵ را تقویت کرده و سناریوهای «احراز پیوسته» و «احراز مرحله‌ای» را وارد ادبیات رسمی می‌کند.

۲-۳-۳. چارچوب تضمین مدیریت هویت پایه[4] (ITU-T X.1254:2020)

این توصیه‌نامه بخش استانداردسازی اتحادیه بین‌المللی مخابرات، با تمرکز بر خدمات جهانی مخابرات و اینترنت، چهارمین عامل «زمینه یا بستر» را به مدل احراز هویت می‌افزاید؛ این عامل، شرایط زمانی، مکانی و رفتاری کاربر را برای تصمیم‌گیری تطبیقی در نظر می‌گیرد. استاندارد X.1254 سه سطح AAL را برای محیط‌های ریسک‌پذیر مخابراتی تعریف و روش امتیازدهی پویا را توصیف می‌کند. جایگاه این توصیه‌نامه در سیاست‌گذاری ملی از آن رو مهم است که سازگاری را میان اپراتورهای مخابرات، ارائه‌دهندگان خدمات ارزش‌افزوده و رگولاتورهای ارتباطات تسهیل می‌کند.

۲-۳-۴. احراز هویت وب (WebAuthn) سطح ۳[5] (W3C)

نسخه سوم استاندارد وب‌اوتن که توسط کنسرسیوم وب جهان‌گستر (W3C)[6] تدوین شده، رابط برنامه‌نویسی کاربردی مرورگرها را برای که احراز هویت مبتنی‌بر جفت کلید عمومی و خصوصی را مستقیم در وب فراهم می‌سازد. این نسخه با پشتیبانی بومی از گذرواژه‌زدایی و «کلید عبور»های همگام‌شونده میان دستگاه‌ها، امنیت فیشینگ-مقاوم را بدون نیاز به افزونه یا نرم‌افزار جانبی ارائه می‌کند. WebAuthn L3 همچنین پروفایل‌های سازگار با FIDO2 را تعریف و سناریوهای احراز چند دستگاهی و بازیابی امن اعتبارنامه را استانداردسازی می‌کند؛ ازاین‌رو، ستون فقرات سامانه‌های مدرن هویت خود سازمان‌یافته (SSI) و بانکداری باز محسوب می‌شود.

۲-۳-۵. پروتکل کلاینت به احراز هویت FIDO -(CTAP)[7]

CTAP مکمل استاندارد احراز هویت وب (WebAuthn) است که توسط کنسرسیوم W3C منتشر شده است. WebAuthn و CTAP خروجی‌های اصلی پروژه FIDO2 هستند که حاصل تلاش مشترک بین FIDO و W3C است. مشخصات CTAP به دو نسخه پروتکل اشاره دارد، پروتکل CTAP1 و پروتکل CTAP 2.2. CTAP2 شیوه ارتباط میان «احرازگر» سخت‌افزاری یا بیومتریک (مانند

1. Entity Authentication Assurance Framework
2. The International ElectrotechnicalCommission
3. Digital Identity Guidelines
4. Baseline Identity Management Assurance Framework
5. Entity Authentication Assurance Framework
6. World Wide Web Consortium (W3C)
7. FIDO Client-to-Authenticator Protocol (CTAP)

YubiKey یا حسگر اثر انگشت گوشی) و «کلاینت» میزبان (مرورگر یا سیستم‌عامل) را مشخص می‌کند. نسخه ۲٫۲ با افزودن قابلیت‌هایی چون «محدودسازی دامنه» و «اعتبارنامه چند کلیدی» امنیت سازمانی را ارتقا و تجربه کاربری «یک-لمس و بدون گذرواژه» را ممکن می‌سازد. این پروتکل همراه با WebAuthn چارچوب فنی FIDO[2] را تکمیل کرده و مهاجرت از گذرواژه‌های سنتی به احراز مقاوم در برابر حملات تکرار یا بازپخش[1] و فیشینگ[2] را تسریع می‌کند.

۶-۲-۳. مقررات هویت دیجیتال اتحادیه اروپا (eIDAS)[3]

مقررات eIDAS، چارچوب قانونی اتحادیه اروپا برای شناسایی الکترونیکی و خدمات اعتماد (مانند امضای الکترونیک، مُهر زمانی، گواهی وب و غیره) است که سه سطح اعتماد پایین (کم)، قابل توجه و بالا را به‌طور مستقیم با ISO 29115 هم‌نقشه می‌کند. نسخه ۲٫۰ مقررات eIDAS مفهوم «کیف پول هویت اروپایی» و سازوکارهای متقابل‌پذیر SSI را وارد قانون کرده، الزام صدور گواهی اعتماد برای کیف پول‌های موبایلی را تعیین و اتحادیه را به یک بازار واحد هویت رقومی (دیجیتال) هدایت می‌کند؛ ازاین‌رو، الگویی جامع برای کشورهایی است که در پی سازگاری فنی و حقوقی خدمات احراز هویت و اعتماد هستند.

۳ـ۳. عوامل و روش‌های احراز هویت

احراز هویت در فضای رقومی (دیجیتال) صرفاً به واردکردن یک رمز عبور خلاصه نمی‌شود. برای مقابله با خطر جعل هویت و افزایش اعتماد کاربران در تراکنش‌های آنلاین، لازم است سطح امنیت متناسب با نیاز و مخاطره هر یک از خدمات اتخاذ گردد. در این چارچوب، درک عوامل احراز هویت و شیوه‌های بهره‌گیری از آن‌ها نقشی کلیدی در طراحی و پیاده‌سازی سامانه‌های امن بر عهده دارد. بر پایه جدیدترین اسناد بین‌المللی اشاره شده در زیر، این هدف با درک دقیق دو بنیان ذیل قابل تحقق است:

الف) عوامل: آنچه برای اثبات هویت به سامانه ارائه می‌شود؛

ب) روش یا الگوهای استفاده از عوامل: چگونگی به‌کارگیری یک یا چند عامل برای رسیدن به سطح اطمینان خواسته شده است.

لذا در ادامه با توجه استانداردهای راهبردی و مرجع ذیل ابتدا عوامل اساسی احراز هویت و سپس مهم‌ترین راهکارها و روش‌های استفاده از این عوامل تشریح می‌گردد.

۱-۳-۳. عوامل احراز هویت

در معماری هر سامانه هویت رقومی (دیجیتال)، نخستین تصمیم راهبردی این است که ادعای هویت کاربر بر پایه چه نوع شواهدی بنا شود. استاندارد ISO/IEC ۲۹۱۱۵ و راهنمای NIST SP ۸۰۰-۶۳-۴ برای پاسخ به این پرسش مجموعه‌ای از عوامل[4] را معرفی کرده‌اند که با اتکای به آنها هویت رقومی (دیجیتال) را تأیید یا رد می‌کنند. این عوامل، اگرچه در متون کلاسیک به سه دسته اصلی تقسیم می‌شوند اما در عمل لایه‌ها و ظرایف بیش‌تری یافته‌اند.

الف) دانسته‌ها

- **تعریف:** هر نوع اطلاعات محرمانه یا خصوصی که کاربر می‌داند و مختص اوست؛ برای مثال رمز عبور، عبارت عبور، پین‌کد یا پاسخ به پرسش‌های امنیتی.
- **نقاط قوت:** راه‌اندازی آسان، هزینه پیاده‌سازی نسبتاً پایین و سادگی درک برای عموم کاربران.
- **نقاط ضعف:**
  - **فراموشی:** کاربر ممکن است رمز عبور را به‌سادگی فراموش کند.

1. Replay
2. Phishing
3. electronic IDentification, Authentication and trust Services
4. Authentication Factors

- **سرقت یا افشای ناخواسته:** احتمال دارد رمز عبور در حملات فیشینگ، بدافزارها یا لو رفتن اطلاعات وب‌سایت[1] فاش شود.
- **ضریب امنیت پایین:** در صورت انتخاب رمز عبور ضعیف یا به اشتراک‌گذاری آن با دیگران، خطر نفوذ بسیار بالا می‌رود.

ب) داشته‌ها

- **تعریف:** هر چیزی که کاربر «دارد» و مختص او باشد؛ مانند تلفن همراه، کارت بانکی، توکن سخت‌افزاری یا کارت هوشمند.
- **نقاط قوت:**
  - **سختی در جعل:** مهاجم برای سوءاستفاده باید واقعاً آن شیء فیزیکی را در اختیار داشته باشد.
  - **افزایش چشمگیر امنیت:** در مقایسه با روش‌های تک‌عاملی دانسته (مثلاً رمز عبور) امنیت بیشتری دارد، زیرا حمله ساده فیشینگ کافی نیست و مهاجم نیازمند دسترسی فیزیکی به دارایی است.
- **نقاط ضعف:**
  - **گم شدن یا سرقت:** در صورت سرقت فیزیکی، عامل امنیتی از دست می‌رود.
  - **هزینه پیاده‌سازی:** اگر نیاز به تولید توکن‌های سخت‌افزاری یا کارت هوشمند باشد، بار مالی بر سازمان تحمیل می‌کند.
  - **نیاز به عامل مکمل:** اغلب به‌تنهایی کافی نیست و ترکیب با رمز عبور یا بیومتریک توصیه می‌شود.

ج) ویژگی‌های ذاتی / بیومتریک

- **تعریف:** مبتنی بر خصوصیات فیزیولوژیک (اثر انگشت، عنبیه چشم، چهره) یا رفتاری (امضای رقومی (دیجیتال) دست‌نویس، صدای کاربر، نحوه تایپ و لمس صفحه) فرد است.
- **نقاط قوت:**
  - **به‌سختی فراموش یا گم می‌شود:** کاربران نیازی به حفظ کردن ندارند و عامل همواره بخشی از وجود خود فرد است.
  - **سختی جعل:** جعل یا سرقت ویژگی‌های بیومتریک دشوارتر از یک رمز عبور است.
- **نقاط ضعف:**
  - **نگرانی‌های حریم خصوصی:** ذخیره الگوهای بیومتریک کاربران، چالش‌های قانونی و اخلاقی به‌همراه دارد و لازم است در بستری امن نگهداری شود.
  - **برگشت‌ناپذیری:** اگر الگوهای بیومتریک نشت کند یا به سرقت برود، برخلاف رمز عبور که قابل تغییر است، جایگزینی آن تقریباً ناممکن خواهد بود.
  - **هزینه پیاده‌سازی:** پیاده‌سازی سیستم‌های بیومتریک (سخت‌افزار اسکنر اثر انگشت، دوربین پیشرفته تشخیص چهره و...) معمولاً مستلزم سرمایه‌گذاری قابل‌توجه است [۱۲].

د) سایر عامل زمینه‌ای یا بستر

هرچند استاندارد ISO سه عامل کلاسیک را برای احراز هویت کافی می‌داند، اما توصیه ITU-T X.1254 و بخش «Risk-Based» در NIST تأکید می‌کند که داده‌های محیطی مانند موقعیت جغرافیایی، زمان دسترسی، نوع مرورگر یا امضای سخت‌افزاری دستگاه می‌تواند در سنجش ریسک بسیار مؤثر باشد.

به‌عنوان نمونه، تراکنشی که از یک دستگاه شناخته‌شده در شهر محل سکونت کاربر آغاز می‌شود، نسبت به درخواستی از قاره‌ای دیگر کم‌ریسک‌تر است و شاید به احراز اضافی نیاز نداشته باشد.

با اتکا به ارزیابی جامع ریسک، روشن است که تکیه بر یک عامل منفرد صرفاً در خدمات کم‌ریسک با سطح اطمینان پایین موجه است و به‌ویژه عوامل دانسته همچون گذرواژه در برابر تهدیدهای فیشینگ و ربودن نشست ایمنی کافی ندارند؛ در مقابل، برای حوزه‌های مالی، مدل ترکیبی

1. Data Breach

«دانسته + داشته» که مبنای الزام‌های احراز قوی مشتری در PSD۲ [۲۰] و دستورالعمل رمز پویاست، حداقل استاندارد پذیرفته‌شده به‌شمار می‌رود. درحالی‌که در خدمات حیاتی دولت هوشمند یا زیرساخت‌های حساس، سیاست‌گذار باید افزوده‌شدن عامل ذاتی (بیومتریک) یا دست‌کم کنترل زمینه‌ای مبتنی‌بر ریسک را الزامی کند تا سطح اطمینان به تراز بالاتر ارتقا یابد.

ازاین‌رو، تدوین مقررات احراز هویت نباید صرفاً به‌عنوان تصمیمی فنی تلقی شود؛ بلکه لازم است چهار بُعد امنیت، حریم خصوصی، هزینه و سهولت کاربری به‌طور هم‌زمان و در چارچوب مدل‌های چندسطحی ISO/IEC 29115 یا نگاشت AAL مستند در NIST SP 800-63-4 ارزیابی شود تا اطمینان حاصل شود تقویت لایه‌های امنیتی با کاهش دسترس‌پذیری یا تعارض با مقررات حفاظت داده‌ها همراه نخواهد بود. در ادامه، مشخص می‌شود که چگونه روش‌هایی نظیر احراز هویت چندعاملی، بدون رمز عبور و تطبیقی مبتنی‌بر ریسک می‌توانند این عوامل را به‌صورت هدفمند ترکیب کنند و سطح اطمینان موردنیاز در سیاست ملی را، با حفظ تجربه کاربری، محقق سازند.

۲-۳-۳. انواع روش‌های احراز هویت

در جدول زیر، انواع روش‌های احراز هویت و مزایا و معایب آنها ذکر شده است [۱۳].

جدول ۳. انواع روش‌های احراز هویت رقومی (دیجیتال) [۱۳]

نام روش	توضیح	مزیت	چالش‌ها	راهبردها
احراز هویت چندعاملی (MFA)	استفاده از حداقل دو عامل مستقل (دانسته، داشته، ذاتی).	امنیت بالا در برابر فیشینگ و مهندسی اجتماعی.	پیچیدگی تجربه کاربری، هزینه سخت‌افزار، نیاز به پشتیبانی.	بانکداری الکترونیک، سامانه‌های سازمانی، خدمات دولتی.
احراز هویت پیوسته[1]	هویت فقط هنگام ورود سنجیده نمی‌شود، بلکه به‌طور مداوم بر اساس رفتار کاربر (مثل تایپ یا موقعیت مکانی) بررسی می‌شود.	افزایش امنیت در طول نشست.	نگرانی‌های حریم خصوصی، بار پردازشی سنگین، خطای الگوریتم‌ها.	بانکداری پیشرفته، سامانه‌های نظامی، سازمان‌های حساس.
احراز هویت بدون رمز عبور[2]	مبتنی بر کلیدهای رمزنگاری ذخیره‌شده در دستگاه کاربر + احراز بیومتریک محلی.	حذف رمز عبور، مصونیت از فیشینگ و سادهشدن تجربه کاربر.	نیاز به سخت‌افزار امن، فرایند بازیابی در صورت از دست رفتن دستگاه، هزینه مهاجرت انبوه.	بانکداری رقومی (دیجیتال)، دولت هوشمند، خودپردازهای آینده.
احراز هویت غیرمتمرکز[3]	داده‌های هویتی در «کیف‌پول رقومی (دیجیتال) » کاربر ذخیره می‌شود و در قالب اعتبارنامه قابل‌وارسی (VC) ارائه می‌گردد.	مالکیت داده در اختیار کاربر، کاهش خطر نشت اطلاعات، اعتبارسنجی برون‌خط.	بازیابی در صورت سرقت دستگاه، نیاز به استانداردسازی حقوقی و زیرساخت دفتر کل.	کیف‌پول هویت ملی، مدارک تحصیلی رقومی (دیجیتال)، گمرک هوشمند.
احراز هویت مرحله‌ای[4]	هنگام عملیات پرریسک، سامانه به‌طور موقت عامل اضافی مطالبه می‌کند.	امنیت هدفمند بدون افزایش دائمی پیچیدگی.	طراحی تجربه کاربری، زمان‌بندی ایمن، دسترس‌پذیری عوامل.	بانکداری برخط، پرتال‌های دولتی، سامانه‌های پرداخت کسب‌وکار.
احراز هویت تطبیقی مبتنی بر مخاطره[5]	سامانه سطح ریسک هر درخواست را می‌سنجد و بر اساس آن شدت احراز را تنظیم می‌کند.	تعادل امنیت و راحتی، مصرف بهینه منابع امنیتی.	دقت مدل‌های مخاطره، حریم خصوصی داده‌ها، بار پردازشی.	پرداخت‌های الکترونیک، ورود کارکنان دولت، سامانه‌های بیمه.

1. Continuous Authentication
2. Passwordless
3. Decentralized Authentication
4. Step-up Authentication
5. Risk-based Adaptive Authentication

۳-۴. سطح اطمینان در احراز هویت

در فضای امنیت اطلاعات، مفهومی به نام «اعتماد مطلق» عملاً وجود ندارد؛ همواره درجاتی از اطمینان یا اطمینان در احراز هویت مطرح است. سطح اطمینان یا LoA[1] بیانگر میزان اعتماد یک سامانه به این امر است که فرد حاضر در نشست یا تراکنش جاری، واقعاً همان فرد مالک هویت اعلام شده است. چارچوب‌های بین‌المللی گوناگونی، مانند NIST SP 800-63 (در آمریکا) و ISO/IEC 29115 (در سطح جهانی)، برای تعریف و طبقه‌بندی LoA تدوین شده‌اند. اغلب این اسناد، چهار سطح کلیدی را به‌ترتیب از سطح اطمینان ۱ (پایین) تا سطح اطمینان ۴ (بسیار بالا) پیشنهاد می‌کنند. هرچه عدد LoA بالاتر باشد، نشان‌دهنده فرآیندی دقیق‌تر، مستندتر و چندلایه‌تر در احراز هویت کاربر است [۱۲, ۱۳].

۱-۴-۳. عوامل مؤثر بر تعیین سطح اطمینان

تعیین سطح اطمینان در یک سیستم احراز هویت مبتنی بر مجموعه‌ای از عوامل صورت می‌پذیرد که در چرخه حیات هویت رقومی (دیجیتال) اعمال می‌گردند بر این اساس نیاز است تا در راستای شناسایی سطح اطمینان مورد نیاز در هر مرحله تمامی عوامل تأثیرگذار مؤثر بر آن سیستم شناسایی گردد.

الف) شدت راستی‌آزمایی در زمان نام‌نویسی

- در فرآیند ثبت‌نام، اگر تنها نام کاربری و رمز عبور از کاربر گرفته شود، LoA نسبتاً پایینی خواهد داشت؛ چراکه فرد بدون ارائه اسناد معتبر می‌تواند خود را هر کسی معرفی کند.
- در رویکردهای دقیق‌تر (مانند مراجعه حضوری به دفاتر صادرکننده گواهی الکترونیک)، بررسی اسناد رسمی یا بهره‌گیری از پایگاه داده دولتی، اطمینان از واقعی‌بودن هویت فرد بالاتر می‌رود. در نتیجه، سامانه در سطوح بالاتری از LoA کار خواهد کرد.

ب) نوع و تعداد عوامل احراز هویت

- یک عامل: مانند رمز عبور ساده، معمولاً در LoA1 یا حداکثر LoA2 قرار می‌گیرد، زیرا حملاتی مانند فیشینگ می‌تواند به‌سرعت رمز عبور را افشا کند.
- چندعاملی: هرچه تعداد عوامل مستقل (نظیر توکن سخت‌افزاری، رمز عبور موقت پیامکی، بیومتریک) بیشتر باشد، احتمال جعل هویت کاهش یافته و LoA افزایش می‌یابد.

ج) حفاظت در برابر جعل و سرقت

- عواملی مانند وجود سخت‌افزار امنیتی یا کارت‌های هوشمند می‌تواند مقاومت سامانه را در برابر جعل یا حملات بالا ببرد. علاوه بر این، استفاده از رمزنگاری قوی (مانند الگوریتم‌های نامتقارن یا امضای رقومی (دیجیتال) رقومی (دیجیتال) (دیجیتال) واجد شرایط) نیز تاثیر بسزایی در تقویت LoA دارد.
- سامانه‌هایی که در برابر حملات رایجی همچون حملات تکرار یا بازپخش و MITM[2] مقاوم‌اند، امتیاز بالاتری در ارزیابی LoA کسب می‌کنند.

د) نظارت و پایش مداوم

- برخی سیستم‌ها رفتار کاربر را به‌شکل مستمر زیر نظر می‌گیرند و در صورت مشاهده تغییرات ناگهانی، مجدداً فرآیند احراز هویت را الزامی می‌کنند. چنین رویکردی می‌تواند LoA را افزایش دهد؛ زیرا حتی اگر نشست کاربر ربوده شود، احتمال تشخیص نفوذ بالا خواهد بود.
- عدم توجه به موضوع پایش مداوم در خدمات حساس، می‌تواند LoA مطلوب را کاهش دهد و ریسک را افزایش دهد.

۲-۴-۳. سطوح متداول در استانداردها

استانداردهای بین‌المللی اغلب از چهار سطح اصلی سخن می‌گویند که هرکدام با توجه به ریسک‌پذیری خدمات و میزان محافظت لازم،

1. Level of Assurance
2. Man-in-the-Middle

مطرح می‌شوند. این چهار سطح رایج، دامنه‌ای از تراکنش‌های بسیار عادی تا تراکنش‌هایی با حساسیت ملی یا مالی کلان را پوشش می‌دهد [۱۰, ۱۳].

الف) اطمینان پایین (LoA1)

- **کاربرد:** سرویس‌های کم‌خطر که نفوذ یا جعل هویت در آن‌ها خسارت زیادی ندارد.
- **خصوصیات:** در این سطح، معمولاً احراز هویت به یک رمز عبور ساده یا تأیید ایمیل محدود می‌شود.

ب) اطمینان متوسط (LoA2)

- **کاربرد:** خدماتی با نیاز امنیتی معقول؛ مثل ورود به حساب کاربری در سایت‌های فروش آنلاین.
- **خصوصیات:** ممکن است مدارک هویتی اولیه درخواست شود، اما الزامات سخت‌گیرانه‌ای مانند تطابق حضوری یا کارت هوشمند الزام‌آور نیست.

ج) اطمینان بالا (LoA3)

- **کاربرد:** مناسب سرویس‌هایی که تبعات مالی یا حقوقی قابل توجهی دارند؛ مانند بانکداری آنلاین یا برخی خدمات دولت الکترونیک.
- **خصوصیات:** احراز هویت بیومتریک یا توکن سخت‌افزاری معمولاً در این سطح رایج است.

د) اطمینان بسیار بالا (LoA4)

- **کاربرد:** تراکنش‌های فوق‌العاده حساس یا مرتبط با داده‌های طبقه‌بندی‌شده (دسترسی به زیرساخت‌های حیاتی ملی یا مدیریت تراکنش‌های مالی کلان.)
- **خصوصیات:** این سطح به‌صورت نظام‌مند بر حضور فیزیکی در مرحله ثبت، نگه‌داری کلید در سخت‌افزار مقاوم، احراز سه‌عاملی، کانال‌های رمزنگاری سطح بالا و پایش پیوسته رفتار متکی است تا ریسک جعل یا نفوذ حتی در سناریوهای دارای داده طبقه‌بندی‌شده یا تراکنش‌های میلیاردی را به حداقل برساند.

۳-۴-۳. اهمیت مدیریت سطح اطمینان

افزون بر تعریف سطح اطمینان، موضوع کلیدی در استقرار موفق سامانه‌های هویت رقومی (دیجیتال)، مدیریت پویای سطح اطمینان است. گزینش نادرست یا انعطاف‌ناپذیر سطوح اطمینان می‌تواند هم امنیت را خدشه‌دار کند و هم تجربه‌کاربری را از بین ببرد.

الف) خطرات تعیین سطح اطمینان پایین

- **جعل هویت و حملات سایبری:** اگر در برخی از خدمات حساس مانند بانکی یا دولتی با LoA1 یا LoA2 عرضه شوند، مهاجمان برای دسترسی غیرمجاز با مانع چندانی روبه‌رو نخواهند بود.
- **عواقب مالی و حقوقی:** در سیستم‌های بانکی، نفوذ موفق می‌تواند به سرقت مبالغ هنگفت یا اختلال در پرداخت‌ها منجر شود. در سامانه‌های دولتی، منجر به افشای داده‌های شخصی شهروندان یا صدور مجوزهای جعلی می‌شود.

ب) خطرات تعیین LoA بالاتر از نیاز

- **پیچیدگی فرآیند:** اگر سرویسی با اهمیت متوسط به بالاترین سطح اطمینان (LoA4) نیازمند شود، کاربران مجبورند مراحل زمان‌بر و چندمرحله‌ای را طی کنند.
- **هزینه‌های اجرایی:** تأمین تجهیزات امنیتی (توکن سخت‌افزاری، راهکارهای بیومتریک سطح بالا) برای LoA4، توجیه اقتصادی نخواهد داشت اگر واقعاً ضرورت نداشته باشد.
- **نارضایتی کاربران:** سختی ورود یا نیاز مستمر به تأییدهای پی‌درپی، ممکن است کاربران را به ترک سرویس یا یافتن جایگزین ساده‌تر ترغیب کند.

۴. جایگاه و اهمیت احراز هویت رقومی (دیجیتال)

در چارچوب حکمرانی داده، احراز هویت رقومی (دیجیتال) در جایگاه «زیرساخت اعتماد ملی» محسوب می‌شود. جایگاهی که گزارش ۲۰۲۴ سازمان همکاری و توسعه اقتصادی (OECD[1]) آن را هم‌ردیف انرژی، حمل‌ونقل و ارتباطات در فهرست زیرساخت‌های حیاتی کشورها قرار داده است [۱۴]. تجربه‌های جهانی نشان می‌دهد در صورت فقدان توسعه زیرساخت هویت رقومی (دیجیتال) فراگیر، ایمن و تعاملی، تحقق دولت هوشمند، رقابت‌پذیری زیست‌بوم فناورانه و توسعه اقتصاد رقومی (دیجیتال) ممکن نخواهد بود.

در ایران، توسعه ضریب نفوذ اینترنت و دسترس‌پذیری به فضای مجازی و پیش‌بینی سهم روبه‌رشد اقتصاد رقومی (دیجیتال) به میزان ۱۰٪ از درآمد سرانه ملی تا سال ۱۴۰۷، فرصتی کم‌سابقه برای تحول رقومی (دیجیتال) ایجاد کرده است [۱۵]. با این وجود، تکثر متولیان داده هویتی، فقدان قانون جامع صیانت داده شخصی و شکاف رقومی (دیجیتال) میان کلان‌شهرها و مناطق کم‌برخوردار، می‌تواند خطر اتلاف سرمایه را افزایش دهد و اعتماد کاربران را کاهش دهد.

بر این اساس و به‌منظور توسعه زیرساخت‌های هویت رقومی (دیجیتال)، تعامل‌پذیر و شهروندمحور بایستی با همکاری میان قوای سه‌گانه، حول کمّی‌سازی منافع احراز هویت رقومی (دیجیتال) در بخش‌های مالی، سلامت، حمل‌ونقل و حکمرانی، تقویت شود و همچنین اهتمام کافی برای رفع چالش‌های حقوقی، نهادی و فناورانه شکل بگیرد.

۴ـ۱. ضرورت و کاربردهای احراز هویت رقومی (دیجیتال)

در دهه گذشته، تحولات فناورانه جایگاه احراز هویت رقومی (دیجیتال) را از یک راهکار جانبی به یک نیاز راهبردی ارتقا داده‌اند. این تحول، صرفاً در سطح فناوری معنا ندارد؛ بلکه نقطه تلاقی سه رکن اساسی نظم رقومی (دیجیتال) معاصر یعنی اعتماد نهادی، شمول رقومی (دیجیتال) و حکمرانی مبتنی بر داده است. به‌عبارت دیگر، هر کشوری که نتواند به‌صورت اثربخش و فراگیر، هویت رقومی (دیجیتال) شهروندان خود را مدیریت کند، نه‌تنها در ارائه خدمات الکترونیک با شکست مواجه می‌شود، بلکه در تأمین عدالت اجتماعی و بهره‌برداری از اقتصاد رقومی (دیجیتال) نیز عقب خواهد ماند.

تحلیل تجربه بیش از ۴۰ کشور (براساس داده‌های ID4D[2] بانک جهانی، ۲۰۲۳) نشان می‌دهد که چهار روند کلان، موجب تسریع سرمایه‌گذاری کشورها در سامانه‌های احراز هویت رقومی (دیجیتال) شده‌اند [۱۶]:

- **الف) دگرگونی خدمات عمومی پساکرونا:** بحران کرونا بزرگ‌ترین آزمون برای توانمندی دولت‌ها در حفظ پیوستگی خدمات بدون تعامل فیزیکی بود. کشورهایی که فاقد نظام احراز هویت رقومی (دیجیتال) بودند، ناگزیر به تعلیق یا کاهش کیفیت خدمات حیاتی نظیر بیمه، سلامت، آموزش و یارانه شدند.
- **ب) رواج اقتصاد سکویی (پلتفرمی) و مالیات رقومی (دیجیتال):** رشد سکوهایی نظیر اوبر[3]، آمازون[4] و تیک تاک[5] در سطح جهانی و نمونه‌های داخلی مانند اسنپ، دیجی‌کالا یا روبیکا، نیاز به شناسایی دقیق ذی‌نفعان حقیقی، گردش مالی و رفتار تراکنشی را دوچندان کرده است. بدون احراز هویت رقومی (دیجیتال) استاندارد، هم نظارت مالیاتی مختل می‌شود و هم سوءاستفاده از زیرساخت‌های رقومی (دیجیتال) افزایش می‌یابد.
- **ج) تهدیدات سایبری و جعل‌های ساختاریافته:** در سال ۲۰۲۲، بیش از ۵.۴ میلیارد دلار فقط در آمریکا بابت کلاهبرداری هویتی

1. Organisation for Economic Co-operation and Development
2. Identification for Development
3. Uber
4. Amazon
5. TikTok

خسارت وارد شد [۱۷]. تحقیقات شرکت امنیت سایبری مندی‌انت[1] نشان می‌دهد حدود ۴۰٪ از حملات سایبری از طریق عبور از سیستم‌های احراز هویت ضعیف صورت می‌گیرد [۱۸]. این ارقام ضرورت ارتقای استانداردهای احراز هویت را از یک توصیه فنی به یک اولویت امنیت ملی بدل کرده‌اند.

- **د) فشارهای تطبیق‌پذیری بین‌المللی:** اتصال به نظام مالی بین‌المللی، تجارت رمزارز، نقل‌وانتقال مرزی، صدور بیمه‌نامه بین‌المللی، همه مستلزم رعایت استانداردهای AML3[3]، KYC2[2] و FATF4[4] هستند. این استانداردها مستقیماً به احراز هویت رقومی (دیجیتال) قابل ردیابی و فریب‌ناپذیر وابسته‌اند.
- **ه) الزامات قانون برنامه هفتم پیشرفت**

با توجه به احکام تدوین شده در قانون برنامه هفتم پیشرفت جمهوری اسلامی ایران، که بر تحول رقومی (دیجیتال)، تمرکززدایی خدمات، رشد بهره‌وری، عدالت در توزیع یارانه‌ها، و شفافیت اقتصادی تأکید دارد، احراز هویت رقومی (دیجیتال) به‌عنوان پیش‌نیاز تحقق بخش قابل توجهی از اهداف برنامه تلقی می‌شود.

با توجه به مواد(۱۰۷) و (۶۹) قانون برنامه هفتم پیشرفت، دو حوزه راهبردی به‌عنوان نقاط ورود کلیدی برای پیاده‌سازی نظام جامع احراز هویت رقومی (دیجیتال) تا افق ۱۴۰۷ شناسایی می‌شود. این دو حوزه به‌طور مستقیم در متن برنامه دارای تکلیف اجرایی مشخص در زمینه احراز هویت، تبادل داده هویتی، و یکپارچه‌سازی خدمات رقومی (دیجیتال) هستند [۱۵]:

۱ حوزه حکمرانی رقومی (دیجیتال) و خدمات دولت هوشمند در قانون برنامه هفتم پیشرفت

- **کاربردها:** اتصال کلیه دستگاه‌های اجرایی به زیرساخت ابری دولت، طراحی پایگاه ملی هویت اشخاص حقیقی توسط سازمان ثبت احوال، الزام به حذف ارائه دستی مدارک هویتی، استعلام آنی اطلاعات پایه، ارائه خدمات بدون دخالت عامل انسانی از طریق پنجره ملی خدمات هوشمند.
- **نقش احراز هویت:** احراز هویت رقومی (دیجیتال) به‌عنوان پیش‌نیاز ارائه خدمات دولت الکترونیکی، نظارت سیستمی، رأی‌گیری الکترونیکی، ثبت اعتراضات و دادخواست‌ها، و پایش برخط عملکرد دستگاه‌ها تعریف شده است.
- **چالش‌ها:** ضعف در تعامل‌پذیری کامل میان پایگاه‌های اطلاعاتی، هم‌پوشانی مأموریت‌های برخی نهادها، ضعف در تبادل برخط داده‌ها و تأخیر در اجرای قانون مدیریت داده‌ها.
- **فرصت‌ها:** ایجاد پایگاه هویت ملی، استقرار احراز هویت پیوسته در پنجره ملی خدمات، کاهش مراجعات حضوری، شفافیت فرآیندها و مشارکت رقومی (دیجیتال) عمومی، کاهش فساد و تقلب اداری.

۲ نظام سلامت و بیمه‌های درمانی در قانون برنامه هفتم پیشرفت

- **کاربردها:** استقرار نظام استحقاق‌سنجی رقومی (دیجیتال) بر پایه احراز هویت، راه‌اندازی پایگاه قواعد سلامت برای کنترل صلاحیت تجویزکنندگان، اتصال کلیه سامانه‌های سلامت به پرونده الکترونیکی یکپارچه، و اعمال امضای رقومی (دیجیتال) بر نسخه‌ها و اسناد پزشکی.
- **نقش احراز هویت:** در بستر پایگاه ملی سلامت، هویت بیمه‌شده و پزشک در زمان ارائه خدمت به‌صورت برخط احراز شده و صحت مدارک و دستورات پزشکی سنجیده می‌شود.
- **چالش‌ها:** تأخیر در راه‌اندازی زیرساخت‌های تبادل امن داده، تداخل مأموریتی میان وزارت بهداشت، بیمه سلامت و تأمین اجتماعی، و عدم شفافیت در صلاحیت حرفه‌ای بعضی ذی‌نفعان.
- **فرصت‌ها:** جلوگیری از تقلب در نسخه‌نویسی و دریافت خدمات، کاهش هزینه‌های بیمه، تسهیل ارائه خدمت در مناطق کم‌برخوردار و تحقق سلامت مبتنی بر داده.

1. Mandiant
2. Know Your Customer
3. Anti Money Laundering
4. Financial Action Task Force

بر این اساس با توجه به اولویت‌های مشخص‌شده در برنامه هفتم، استقرار احراز هویت رقومی (دیجیتال) در حوزه‌های کاربردی مطروحه نه‌تنها با اهداف توسعه‌ای کشور هم‌راستا است، بلکه دارای بیشترین بازده اجتماعی، اقتصادی و نهادی در افق برنامه هفتم خواهد بود.

۲ـ۴. نقش احراز هویت رقومی (دیجیتال) در تحول رقومی (دیجیتال)

احراز هویت رقومی (دیجیتال) صرفاً ابزار فنی نیست، بلکه پیش‌نیاز اصلی تحول رقومی (دیجیتال) و ایجاد لایه اعتماد در همه تعاملات داده‌محور است. بدون آن، ساختارهای حکمرانی و اقتصادی منسجم عمل نخواهند کرد. نقش آن در چهار سطح کلیدی تعریف می‌شود:

الف) سطح فرآیندی

- جایگزینی فرایندهای تمام‌رقومی (دیجیتال) بجای تعامل حضوری، کاغذی و سنتی ؛
- تغییر فرایندها از حالت «متوالی» به «موازی»؛
- کاهش تعامل کارمندان ارایه دهنده خدمت با شهروندان خدمت گیرنده و محدود کردن رانت و تبعیض.

ب) سطح تجربه کاربر

- هویت رقومی (دیجیتال) علاوه بر امنیت، عامل اصلی سادگی، شخصی‌سازی و دسترس‌پذیری است.
- اصول کلیدی: سهولت استفاده، تکرارناپذیری داده، شفافیت، کنترل فردی، دسترس‌پذیری چند بستری.
- اجزای مهم این سطح ورود یکباره و ایمن (SSO[1])، مدیریت رضایت آگاهانه (مالکیت داده توسط کاربر) و تجربه چندکاناله و بدون درز است.

ج) سطح کسب‌وکار و اقتصاد داده

- هویت رقومی (دیجیتال) زیربنای مدل‌های اقتصادی جدید مبتنی بر داده و اعتماد است.
- امکان شناخت عمیق مشتریان بر پایه رفتار و تعاملات، نه صرفاً اطلاعات ایستا.
- بسترساز خدمات مالی، بیمه‌ای، آموزشی و قراردادهای هوشمند مبتنی بر بلاکچین.

د) سطح حکمرانی و دولت هوشمند

- انسجام داده‌ها و فراهم کردن زیرساخت دولت داده‌محور .
- تجمیع و تحلیل داده‌های شهروندی با شناسه یکتا، بهبود تخصیص منابع و نظارت بلادرنگ.
- تقویت شفافیت و مقابله با فساد در مجوزها، معاملات دولتی، رأی‌گیری و بودجه‌ریزی.
- فراهم‌سازی تحلیل پیش‌نگر با ترکیب داده‌های هویتی و هوش مصنوعی.

در نهایت، هویت رقومی (دیجیتال) باید نه صرفاً ابزار امنیتی، بلکه رکن عدالت رقومی (دیجیتال) و کرامت شهروندی باشد؛ در غیر این صورت، خطر تبدیل شدن به ابزار کنترل حاکمیتی وجود دارد. تجربه جهانی نشان داده است که تنها خدمات ساده، سریع، شفاف و تحت کنترل شهروندان پایدار می‌مانند.

۳ـ۴. ملاحظات اجتماعی و فرهنگی

در مسیر استقرار نظام ملی احراز هویت رقومی (دیجیتال)، ابعاد اجتماعی و فرهنگی نقشی بنیادی و چندلایه ایفا می‌کنند. این ابعاد، برخلاف سخت‌افزار یا فناوری‌های رقومی (دیجیتال) که می‌توانند با سرمایه‌گذاری مستقیم تأمین شوند، متکی بر سرمایه اجتماعی، اعتماد عمومی، ادراک فرهنگی و سطح سواد فناورانه هستند. عدم توجه به این مؤلفه‌ها نه‌تنها می‌تواند پروژه‌های ملی را با تأخیر، ناکارآمدی یا شکست مواجه کند، بلکه پیامدهای بلندمدت در شکل‌گیری شکاف رقومی (دیجیتال)، نارضایتی اجتماعی خواهد داشت.

1. Single Sign On

در تحلیل نظام‌مند، چهار محور کلیدی در سطح اجتماعی و فرهنگی باید به‌صورت هم‌افزا در سیاست‌گذاری‌ها مورد توجه قرار گیرد:

الف) اعتماد عمومی به دولت و حاکمیت داده

احراز هویت رقومی (دیجیتال) مبتنی بر داده‌های حساس همچون مشخصات زیست‌سنجی (بیومتریک)، سوابق مالی و الگوهای رفتاری است. در غیاب شفافیت، پاسخ‌گویی و وجود نهادهای ناظر مستقل، شهروندان ممکن است احساس ریسک در قبال سوءِاستفاده، نظارت غیرمجاز یا فروش داده‌های خود داشته باشند. در واقع، اعتماد بیش از آنکه به‌عنوان یک عنصر پیش‌فرض لحاظ گردد ساختنی خواهد بود. در چنین شرایطی، صرفاً تحمیل قانون یا اجبار فنی نمی‌تواند مشارکت همگانی را تضمین کند و طراحی احراز هویت رقومی (دیجیتال) باید مبتنی بر اصول حاکمیت داده، اطلاع‌رسانی مؤثر و دسترسی شفاف به سابقه استفاده از داده‌های فردی باشد. محفوظ ماندن «حق دانستن» و «حق کنترل» برای کاربران دو رکن اعتمادساز هستند که باید نهادینه شوند.

ب) شکاف رقومی (دیجیتال)

نظام‌های هویتی رقومی (دیجیتال) در صورتی موفق‌اند که فراگیر باشند. در ایران نیز مانند سایر کشورها، نوعی شکاف رقومی (دیجیتال) به‌صورت چندبعدی مشهود است:

- تفاوت پوشش و کیفیت اینترنت میان شهر و روستا؛
- تفاوت در سواد رقومی (دیجیتال) میان نسل‌ها؛
- تفاوت میان اقشار دارای دسترسی‌پذیری ویژه (سالمندان، افراد دارای معلولیت، بی‌سوادان).

طبق آمار رسمی وزارت ارتباطات:

- مطابق تکالیف برنامه ششم و هفتم تمرکز دولت بر اتصال روستاهای با جمعیت بیش از ۲۰ خانوار به شبکه ملی اطلاعات است که این امر تاکنون به میزان ۹۵٪ محقق شده است [۱۹]؛
- در نظرسنجی صورت گرفته توسط مرکز پژوهش‌های مجلس مشخص شد که تنها ۱۸ درصد از کاربران تجربه استفاده از پنجره ملی خدمات دولت هوشمند را داشته‌اند [۲۰].

بر این اساس لازم است که طراحی نظام‌های هویتی بصورت عادلانه و با پیش‌بینی ابزارهای جایگزین انجام شود تا اقشار یادشده از دسترسی به خدمات محروم نشوند و شکاف رقومی (دیجیتال) ایجاد نشود.

ج) ملاحظات فرهنگی و دینی

ملاحظاتی نسبت به داده‌پردازی، تصویرسازی چهره، یا تحلیل صدا و حرکت بدن وجود دارد. این ملاحظات در موارد مرتبط با اطلاعات زیستی و بیومتریک مانند تصویر صورت، مطرح هستند. لذا بایستی مولفه‌های فرهنگی و دینی در روش اجرا مورد توجه قرار گیرد.

د) آموزش، توانمندسازی و پذیرش تدریجی

پذیرش اجتماعی فناوری، هم‌زمان با درونی‌سازی مفاهیم امنیت رقومی (دیجیتال)، حریم خصوصی و حقوق رقومی (دیجیتال) رخ می‌دهد. در کشوری با تنوع سواد و سطح آگاهی عمومی، نهادینه‌سازی احراز هویت رقومی (دیجیتال) بدون یک راهبرد آموزشی چندساله میسر نیست. تجربه موفق برخی از کشورهای پیشرو [۱۳] نشان می‌دهد که:

- پیش از اجرای فراگیر هویت رقومی (دیجیتال)، برنامه آموزش سواد رقومی (دیجیتال) برای سالمندان، روستاییان، کارگران و افراد کم‌سواد اجرایی شده؛
- شبکه‌های رسمی (مدارس، رسانه، موسسات فرهنگی) در نقش مروج این سواد عمل کرده‌اند؛
- تمرین عملی با ابزارهای ساده (مثلاً احراز هویت برای دریافت کمک‌های دولتی) راهکار تقویت اعتماد تدریجی بوده است.

با توجه به جمیع موارد ملاحظات اجتماعی–فرهنگی، قلب نرم‌افزاری تحول رقومی (دیجیتال) هستند. در پروژه‌هایی مانند احراز هویت رقومی (دیجیتال) که عمیقاً با اعتماد، هویت، و رفتار شهروندان گره خورده‌اند، عدم توجه به لایه‌های فرهنگی نه‌تنها اثربخشی فناوری را

کاهش می‌دهد، بلکه مشروعیت اجرای آن را نیز زیر سؤال می‌برد.

۴ـ۴. ملاحظات اقتصادی

احراز هویت رقومی (دیجیتال)، نه‌تنها دروازه ورود به اقتصاد داده‌محور و زیربنای تحول رقومی (دیجیتال) در بخش خصوصی و دولتی است، بلکه یک اهرم سیاست‌گذاری اقتصادی راهبردی برای افزایش بهره‌وری، کاهش هزینه‌ها و شکل‌گیری بازارهای نوین خدمات به‌شمار می‌رود. در تحلیل کلان، می‌توان تأثیرات اقتصادی هویت رقومی (دیجیتال) را در چهار سطح بهره‌وری نهادی، بهبود شفافیت مالی و مقابله با فساد، تسهیل نوآوری و رشد اقتصاد رقومی (دیجیتال) و ارتقای تاب‌آوری اقتصادی مورد بررسی قرار داد.

الف) افزایش بهره‌وری نهادی و کاهش هزینه‌های سربار

در ساختارهای اداری سنتی، بخش قابل توجهی از منابع سازمان‌ها صرف فعالیت‌هایی نظیر تطبیق‌های هویتی مکرر، جمع‌آوری و بررسی مستندات فیزیکی، و اجرای کنترل‌های امنیتی وقت‌گیر می‌شود. این رویه‌ها نه‌تنها بهره‌وری را کاهش داده، بلکه منجر به اتلاف سرمایه انسانی، اختلال در جریان خدمت‌رسانی و ایجاد نارضایتی میان کاربران نهایی نیز می‌شوند.

استقرار سامانه‌های احراز هویت رقومی (دیجیتال)، این فرآیندهای پرهزینه و زمان‌بر را به فرآیندهای یکپارچه، سریع و قابل‌پیگیری تبدیل می‌کند. در چنین سامانه‌ای، فرآیندهای اعتبارسنجی و تطبیق اطلاعات به‌صورت برخط و خودکار انجام می‌گیرد و نیازی به ثبت‌نام مکرر یا ارائه اسناد فیزیکی نیست و ارتباط میان دستگاه‌های مختلف نیز مبتنی بر استانداردهای فنی واحد و قابل‌اعتماد خواهد بود.

افزون‌بر این، بهره‌گیری از احراز هویت رقومی (دیجیتال) می‌تواند فشار مالی و فنی وارد بر دستگاه‌های اجرایی را کاهش دهد؛ چراکه دیگر نیازی به توسعه و نگهداری زیرساخت‌های پراکنده تأیید هویت وجود ندارد. به‌عبارت دیگر، با حرکت به‌سوی هویت رقومی (دیجیتال) یکپارچه، دولت می‌تواند منابع آزادشده را به توسعه خدمات هوشمند، بهبود امنیت داده و نوآوری اختصاص دهد.

ب) بهبود شفافیت مالی و مقابله با فساد

احراز هویت رقومی (دیجیتال) می‌تواند به‌صورت بنیادین نظام شفافیت در تعاملات مالی و اقتصادی را متحول سازد. در زیست‌بوم سنتی، نبود یک شناسه هویتی قابل استناد و پایدار، فضا را برای فرار مالیاتی، حساب‌های جعلی و دور زدن مقررات مهیا می‌سازد. در مقابل، با استقرار نظام هویت رقومی (دیجیتال) یکپارچه، هر کنش اقتصادی قابل نسبت‌دادن به یک هویت مشخص و معتبر خواهد بود.

این تحول به نهادهای نظارتی و مالیاتی این امکان را می‌دهد تا زنجیره تراکنش‌ها را با دقت و سرعت بیشتری ردیابی کرده و از بروز تقلب، پول‌شویی، یا دریافت هم‌زمان چندگانه یارانه‌ها و تسهیلات جلوگیری کنند. افزون بر این، هویت رقومی (دیجیتال) می‌تواند به استانداردسازی تعامل میان شهروندان، کسب‌وکارها و دولت کمک کرده و لایه‌ای از پاسخ‌گویی رقومی (دیجیتال) را در نظام حکمرانی مالی نهادینه کند.

ج) تسهیل نوآوری و رشد اقتصاد رقومی (دیجیتال)

در اقتصاد مبتنی بر داده، زیرساخت هویت رقومی (دیجیتال) به‌منزله پیش‌نیاز توسعه محصولات، خدمات و مدل‌های کسب‌وکار نوآورانه است. شرکت‌ها و سکوهای رقومی (دیجیتال)، برای ارائه خدمات شخصی‌سازی‌شده، اعتبارسنجی لحظه‌ای کاربران، و انجام تراکنش‌های امن، نیازمند ابزارهای احراز هویت دقیق و آنی هستند.

هویت رقومی (دیجیتال) امکان خلق خدمات مالی غیرحضوری، بیمه‌نامه‌های هوشمند، قراردادهای رقومی (دیجیتال) و محصولات اشتراکی را فراهم می‌سازد. افزون بر این، کاهش اصطکاک ورود کاربران به زیست‌بوم خدمات رقومی (دیجیتال)، موجب گسترش بازار، افزایش رقابت‌پذیری داخلی و جذب سرمایه‌گذاری در حوزه‌های فین‌تک، سلامت رقومی (دیجیتال) و اقتصاد اشتراکی خواهد شد.

د) ارتقای تاب‌آوری اقتصادی و پشتیبانی از سیاست‌های حمایتی

در شرایط بحران، رکود یا بلایای طبیعی، دسترسی سریع و قابل‌اطمینان به اطلاعات دقیق هویتی شهروندان، یکی از الزامات اجرای سیاست‌های حمایتی هدفمند و کارآمد است. احراز هویت رقومی (دیجیتال) این امکان را فراهم می‌کند تا دولت بتواند در کوتاه‌ترین زمان، کمک‌های دولتی را به افراد مشمول تخصیص دهد، زنجیره‌های آسیب‌پذیر را شناسایی کند، و از توزیع منابع به افراد یا نهادهای غیرمجاز

جلوگیری نماید.

همچنین، وجود یک زیرساخت هویتی رقومی (دیجیتال) منسجم، انعطاف‌پذیری دولت در مدیریت نوسانات اقتصادی، اجرای طرح‌های بازتوزیعی، و مدیریت ریسک‌های کلان را بهبود می‌بخشد. در یک ساختار هوشمند مبتنی بر هویت رقومی (دیجیتال)، دولت قادر خواهد بود با سرعت، دقت و شفافیت بیشتری به تحولات اقتصادی پاسخ دهد و منابع را به شیوه‌ای کارآمد تخصیص دهد.

احراز هویت رقومی (دیجیتال)، یک زیرساخت اقتصادی و فنی چندلایه است که در سطوح مختلف سیاست‌گذاری، سرمایه‌گذاری، و بهره‌برداری اثرگذار است. از کاهش هزینه‌های سربار اداری و هدفمندی یارانه‌ها گرفته تا توسعه بازار خدمات نوین و ارتقای جایگاه بین‌المللی، همگی وابسته به طراحی و استقرار یک نظام هویتی امن، قابل اعتماد و مردم‌محورند.

۴ـ۵. موانع نهادی و اداری

استقرار موفق نظام احراز هویت رقومی (دیجیتال) مستلزم وجود سازوکارهای حکمرانی یکپارچه، همکاری نهادی و قوانین جامع و روزآمد است. با این حال، ممکن است مجموعه‌ای از چالش‌های نهادی، ساختاری و مقرراتی مانع شکل‌گیری یک زیست‌بوم منسجم و مؤثر در این حوزه باشند. تحلیل دقیق این موانع، برای سیاست‌گذاری واقع‌بینانه و اصلاح‌محور ضروری است.

۴ـ۶. رویکردهای فنی و امنیتی

توسعه سامانه احراز هویت رقومی (دیجیتال) نیازمند معماری فنی منعطف، امن و قابل تعامل است. به‌منظور اطمینان از پایداری و امنیت این زیرساخت راهبردی، باید چند اصل فنی و امنیتی به‌صورت همزمان مورد توجه قرار گیرد [۲]:

الف) معماری غیرمتمرکز و توزیع‌شده به‌جای تجمیع تمام داده‌های هویتی در یک پایگاه متمرکز و آسیب‌پذیر، استفاده از معماری توزیع‌شده یا مبتنی بر فناوری زنجیره‌بلوکی توصیه می‌شود. این رویکرد، ضمن افزایش تاب‌آوری سیستم، کنترل داده را در اختیار کاربر قرار می‌دهد.

ب) رعایت استانداردهای باز و تعامل‌پذیر پایبندی به استانداردهای بین‌المللی مانند FIDO2 [۲۱]، OAuth، OpenID Connect و ISO/IEC 29115 2.0 [۱۱]، ضمن تسهیل اتصال سامانه‌ها، تضمین‌کننده امنیت و انطباق‌پذیری سامانه در سطح جهانی است. این استانداردها مبنای اعتماد متقابل در تعاملات بین نهادی را نیز فراهم می‌کنند.

ج) طراحی امنیت‌محور نباید یک افزودنی پسینی باشد، بلکه باید از ابتدا در طراحی سامانه لحاظ شود. استفاده از رمزنگاری انتها به انتها، گواهی رقومی (دیجیتال) معتبر، ذخیره‌سازی مطمئن، احراز هویت دومرحله‌ای، کنترل مجوزها، و پایش رفتارهای مشکوک، عناصر کلیدی این رویکردند.

د) احراز هویت پیوسته و رفتار با بهره‌گیری از الگوریتم‌های یادگیری ماشین، می‌توان رفتار کاربر در زمان استفاده از سامانه (مانند شیوه تایپ، محل و زمان ورود، مسیر حرکتی موس) را برای شناسایی انحرافات امنیتی به‌کار گرفت. این فناوری می‌تواند بدون ایجاد بار شناختی برای کاربر، لایه‌ای دایمی از حفاظت فراهم کند.

هـ) مرکز عملیات امنیتی و تاب‌آوری ملی زیرساخت احراز هویت رقومی (دیجیتال) باید درون یک سامانه جامع پایش امنیتی قرار گیرد تا به‌صورت لحظه‌ای، تهدیدات شناسایی و واکنش متناسب انجام شود. همچنین، طراحی باید به‌گونه‌ای باشد که در برابر قطعی اینترنت، حملات سایبری، یا اختلالات امنیتی، پایداری نسبی حفظ شود.

۴ـ۷. تحلیل مخاطرات و مزایا

احراز هویت رقومی (دیجیتال) به‌عنوان یک فناوری زیرساختی، هم‌زمان فرصت‌های راهبردی و تهدیدهای مهمی به همراه دارد. رویکرد سیاست‌گذاری در این حوزه باید متوازن، چندبُعدی و آینده‌نگر باشد.

مزایا:

- افزایش امنیت خدمات رقومی (دیجیتال) : با حذف کپی کارت ملی و عکس اسکن شده، جعل و کلاهبرداری به حداقل می‌رسد.
- ارتقای سرعت و کیفیت خدمات عمومی و خصوصی: شناسایی فوری، کاهش فرم‌ها و مراجعه حضوری.
- تقویت زیست‌بوم اقتصاد رقومی (دیجیتال) : سکوهای فین‌تک، اینشورتک و سلامت رقومی (دیجیتال) امکان جذب مشتری در لحظه را خواهند داشت.
- افزایش شفافیت و کاهش فساد: هویت قابل رهگیری، ثبت تراکنش‌ها و تحلیل‌پذیری داده.
- تقویت توان حکمرانی داده‌محور: فراهم کردن داده‌های دقیق برای سامانه‌های هوشمند، ارزیابی سیاست‌ها و اجرای عدالت اجتماعی.

مخاطرات:

- نقض حریم خصوصی: در صورت طراحی ناکارآمد، ممکن است داده‌های حساس در معرض سوءاستفاده قرار گیرند.
- تمرکزگرایی خطرناک داده‌ها: تجمیع اطلاعات در یک نقطه می‌تواند هدفی پرجاذبه برای حملات سایبری باشد.
- طرد رقومی (دیجیتال) و شکاف دسترسی: اگر سامانه برای سالمندان، کم‌سوادان یا مناطق محروم مناسب‌سازی نشود، موجب نابرابری می‌شود
- بحران اعتماد عمومی: اجرای شتاب‌زده یا همراه با خطا، منجر به کاهش مشارکت مردم و مقاومت اجتماعی خواهد شد.

۵. مطالعه تطبیقی قوانین و مقررات در سطح بین‌المللی و ایران

در فرآیند قانون‌گذاری نظام احراز هویت رقومی (دیجیتال)، صرف اتکا به تجربیات داخلی خطر بازتولید خلأهای حقوقی، جزیره‌ای‌سازی زیرساخت‌ها و افزایش هزینه‌های انطباق را در پی دارد؛ ازاین‌رو تطبیق مقررات با نمونه‌های موفق بین‌المللی ضرورتی راهبردی محسوب می‌شود. مقایسه تطبیقی نه‌تنها کمک می‌کند استانداردهای فنی و امنیتی ایران با چارچوب‌های جهانی همتراز شود، بلکه امکان شناسایی پیشاپیش چالش‌هایی مانند تعارض حریم خصوصی با احراز هویت زیستی یا نحوه اعمال سطوح اطمینان را فراهم می‌کند. افزون بر این، هماهنگی مقررات داخلی با رویه‌های پذیرفته شده بین‌المللی، مسیر تعامل‌پذیری فرامرزی خدمات مالی و دولتی، جذب سرمایه‌گذاری خارجی و رعایت الزامات مبارزه با پول‌شویی را هموار خواهد کرد.

برای دستیابی به تصویری جامع و متمایز، در این بررسی، کشورها بر پایه سه معیار انتخاب شده‌اند:

- تنوع جغرافیایی: تجربیات اروپا، آسیا (چین، هند و سنگاپور)، غرب آسیا (امارات)، آمریکا و اقیانوسیه (استرالیا) پوشش داده شود؛
- گوناگونی مدل فنی و معماری: الگوی کاملاً متمرکز، معماری فدراتیو و رویکرد غیرمتمرکز و مبتنی‌بر «هویت خود حاکم»؛
- سطح توسعه و بلوغ مقررات: شامل اقتصادهای پیشرفته با چارچوب‌های جاافتاده، اقتصادهای نوظهور با تجربه گسترش سریع نفوذ رقومی (دیجیتال) و کشورهای در حال گذار منطقه‌ای با شرایط نهادی مشابه ایران.

این ترکیب امکان می‌دهد شکاف‌ها و فرصت‌های سیاستی کشور به‌صورت واقع‌بینانه و همه‌جانبه ترسیم شود.

۵ـ۱. چارچوب تطبیق: محورهای کلیدی تحلیل

برای انجام یک مطالعه تطبیقی منسجم و کاربردی میان مقررات احراز هویت رقومی (دیجیتال) در ایران و کشورهای پیشرو، نخستین گام آن است که چارچوب تحلیلی روشنی برای مقایسه انتخاب شود. در این گزارش، شش محور تحلیلی به عنوان ویژگی‌های اصلی مقایسه مقررات انتخاب شده‌اند. این محورها براساس ادبیات معتبر بین‌المللی ازجمله گزارش‌های OECD، کمیسیون اروپا (در تدوین eIDAS و eIDAS 2.0) [۲۲]، اتحادیه بین‌المللی مخابرات و پژوهش‌های مراکز نوآوری سیاستی مانند طرح ابتکاری بانک جهانی با عنوان «شناسایی

برای توسعه (ID4D[1]) « [۱۶] و اتحاد کالاهای عمومی دیجیتال (DPGA)[2] [۱۸] طراحی شده‌اند.

انتخاب این محورها به علت پیوستگی ساختاری آن‌ها با مراحل طراحی، اجرا، و ارزیابی یک نظام احراز هویت رقومی (دیجیتال) ملی صورت گرفته است. این محورها عبارت‌اند از:

دامنه و اهداف قانون

این محور ناظر بر آن است که قانون‌گذار چه اشخاص حقیقی و حقوقی، چه نوع خدماتی، و چه سطوحی از تراکنش‌ها را مشمول قانون دانسته است، و با چه هدفی قانون را وضع کرده است. آیا قانون فقط برای دستگاه‌های دولتی است یا شامل بخش خصوصی نیز می‌شود؟ آیا صرفاً برای امنیت است یا اهدافی چون تسهیل نوآوری، رشد اقتصاد رقومی (دیجیتال)، یا صیانت از حریم خصوصی نیز دنبال می‌شود؟ این محور، چارچوب نظری و دایره شمول قانون را تعیین می‌کند.

مدل نهادی و حکمرانی

نظام‌های احراز هویت رقومی (دیجیتال) معمولاً از سه الگوی نهادی پیروی می‌کنند: متمرکز، فداتیو و غیرمتمرکز خود حاکم. این محور بیان می‌کند که چه نهادی مسئول صدور و اعتباردهی است (دولت، نهاد مستقل، یا کنسرسیوم خصوصی)، ساختار حاکمیتی چگونه تعیین شده (قانون‌گذار، تنظیم‌گر، اجراکننده) و تقسیم کار میان بازیگران کلیدی چگونه است. این بخش همچنین به نقش بخش خصوصی و نهادهای واسط مانند ارائه‌دهندگان اعتبار می‌پردازد.

سطوح اطمینان و عوامل احراز هویت

مطابق استانداردهای بین‌المللی نظیر ISO/IEC 29115، چارچوب‌های معتبر احراز هویت، سطوح مختلفی از اطمینان را تعریف می‌کنند که به میزان دقت شناسایی و کنترل ریسک بستگی دارد. این محور بیان می‌کند که آیا قوانین و مقررات به‌طور شفاف سطوح اطمینان را تعریف کرده است یا خیر، و این‌که چه عوامل احراز هویتی، مجاز یا الزامی هستند. مدل‌های پیشرفته معمولاً از احراز هویت چندعاملی، پیوسته یا زمینه‌محور نیز پشتیبانی می‌کنند.

سازوکار صدور، استفاده و کنترل

در این بخش فرایندهای صدور شناسه رقومی (دیجیتال)، مدیریت اعتبار، و سازوکارهای استفاده از شناسه بررسی می‌شود. مقررات موفق معمولاً به تعریف چرخه عمر شناسه (از ثبت تا تعلیق و ابطال)، قابلیت‌های امضای رقومی (دیجیتال)، یکپارچگی اطلاعات، و روش‌های مقابله با جعل و سوءاستفاده پرداخته‌اند. همچنین نحوه اعمال کنترل کاربر بر شناسه و فرایندهای رضایت‌مندی برای اشتراک داده‌ها از جمله نکات کلیدی در این محور است.

حریم خصوصی و حقوق داده

حفظ حریم خصوصی افراد یکی از حساس‌ترین و بنیادین‌ترین اصول نظام‌های احراز هویت رقومی (دیجیتال) است. این محور به بررسی این می‌پردازد که قانون و مقررات تا چه حد اصول حفاظت داده را رعایت کرده، مانند حداقل‌سازی داده‌ها، محدودیت هدف، شفافیت و اطلاع‌رسانی به کاربر، حق دسترسی و اصلاح داده و نیز حق فراموش‌شدن داده. همچنین بررسی می‌شود که آیا قانون و مقررات سازوکار نظارتی مستقلی برای حفاظت داده (مانند کمیسیون‌های ملی حفاظت داده) پیش‌بینی کرده است یا خیر.

پیاده‌سازی، مشوق‌ها و تعامل‌پذیری

توسعه مقررات و قوانین بدون پیاده‌سازی موفق و ایجاد انگیزه برای پذیرش عمومی، بی‌اثر خواهند بود. این محور به نحوه اجرایی‌سازی قانون و مقررات در عمل، طراحی مسیرهای الزام تدریجی، مشوق‌های مالی یا غیرمالی برای نهادهای مشمول، و تعامل‌پذیری فنی و حقوقی در سطح ملی و بین‌المللی می‌پردازد.

1. Identification for Development (ID4D)

۲. Digital Public Goods Alliance (DPGA): اتحاد کالاهای عمومی دیجیتال، یک ابتکار چندجانبه مورد تایید سازمان ملل متحد است که کشف و استقرار فناوری‌های متن‌باز را تسهیل می‌کند و کشورها و سازمان‌ها را برای ایجاد یک زیست‌بوم جهانی پررونق برای کالاهای عمومی دیجیتال گرد هم می‌آورد.

۲ـ۵. بررسی تطبیقی کشورها و اسناد منتخب جهانی

در این بخش، شش کشور توسعه یافته و پیشرو که در طراحی، پیاده‌سازی، و سیاست‌گذاری نظام‌های احراز هویت رقومی (دیجیتال) سرآمد هستند، مورد بررسی قرار می‌گیرند. معیار انتخاب این نمونه‌ها، تنوع در جغرافیا، سطح توسعه، ساختار حکمرانی رقومی (دیجیتال)، و مدل‌های نهادی است. هدف، استخراج الگوهای موفق و درس‌آموزی از چالش‌هاست.

۱-۲-۵. اتحادیه اروپا – مقررات eIDAS ۲.۰

دامنه و اهداف:

هدف اصلی eIDAS 2.0، ایجاد بازار واحد هویت رقومی (دیجیتال) در سراسر اتحادیه اروپا و تضمین تعامل‌پذیری، شناسایی متقابل و پوشش خدمات خصوصی و عمومی است. این مقررات بر مبنای اصل «کنترل کاربر بر داده» طراحی شده و استفاده از کیف پول هویت رقومی (دیجیتال) اروپا[1] را برای بانک‌ها، بیمارستان‌ها، مراکز آموزشی، خدمات حمل‌ونقل، رأی‌گیری برخط و سایر خدمات کلیدی اجباری می‌داند. برخلاف بسیاری از مدل‌های ملی، هدف آن صرفاً شناسایی نیست بلکه توانمندسازی شهروند در تعاملات رقومی (دیجیتال) بین‌مرزی است.

مدل نهادی:

eIDAS یک مدل فدراتیو میان دولت‌های عضو است که در آن مسئولیت صدور و اعتبارسنجی شناسه رقومی (دیجیتال) میان بازیگران مختلف تقسیم شده است. هماهنگی مرکزی با کمیسیون اروپا است و نظارت نهادی با همکاری ENISA[2]، سازمان‌های ملی، و نهادهای ارزیاب مطابقت انجام می‌شود. نقش شرکت‌های فناوری بزرگ با الزامات صریح محدود شده (مانند الزام اپل و گوگل به پشتیبانی از کیف‌پول اروپایی).

سطوح اطمینان:

مقررات دارای چارچوب دقیق سطوح اطمینان با ارجاع به استانداردهای بین المللی است و الزامات فنی، آزمون‌پذیری و تأیید مستقل برای هر سطح وجود دارد. این سطوح نقش محوری در تفکیک خدمات پُرریسک (مانند سلامت یا مالی) از خدمات کم‌ریسک (مانند انجام نظرسنجی) دارند.

سازوکار صدور و کنترل:

کیف‌پول هویت رقومی (دیجیتال) توسط نهادهای مجاز صادر می‌شود و قابلیت مدیریت داده، صدور، لغو و مشاهده سابقه بهره‌برداری داده برای کاربر در نظر گرفته شده است. هر تراکنش نیازمند رضایت صریح کاربر است. کیف‌پول قابلیت امضای الکترونیکی سطح بالا، ذخیره گواهی، و کاربری چندکشوری دارد. سامانه‌های صدور و مصرف‌کننده باید در سامانه هماهنگی اتحادیه ثبت شده و گواهی انطباق اخذ کنند.

حقوق داده:

eIDAS 2.0 کاملاً با قانون حمایت از داده‌ها (GDPR[3]) هم‌راستا طراحی شده و اصل «کمینه‌سازی داده‌ها[4]» و «محدودیت هدف[5]» را رعایت می‌کند. کاربر در هر مرحله باید رضایت دهد و امکان مشاهده، حذف، و انتقال داده را دارد. کاربر می‌تواند تنظیم کند که کدام داده‌ها به کدام سامانه‌ها ارسال شود. همچنین، مقررات انتقال داده بدون رضایت کاربر یا برای اهداف غیرمرتبط را ممنوع کرده است (اصل محدودیت هدف).

پیاده‌سازی و مشوق‌ها:

اجرای مقررات برای کلیه دولت‌های عضو الزامی است و جدول زمانی اجرایی مرحله‌بندی شده دارد. کمیسیون اروپا متعهد به تأمین بودجه مشترک برای توسعه زیرساخت فنی، آموزش کاربران، و کمک فنی به کشورهای کمتر توسعه‌یافته عضو اتحادیه اروپا شده است. شاخص‌های

1. European Digital Identity Wallet
2. European Union Agency for Cybersecurity
3. General Data Protection Regulation
4. Data Minimization
5. Purpose Limitation

رسمی نظیر «میزان پذیرش در خدمات عمومی»، «نرخ صدور کیف‌پول» و «میزان تراکنش‌های فرامرزی» برای رصد پیشرفت تعریف شده‌اند [۲۲].

۲-۲-۵. هند - مقررات Aadhaar

دامنه و اهداف

Aadhaar با هدف تخصیص یارانه‌های دولتی، کاهش فساد، شمول مالی و ثبت رقومی (دیجیتال) همه مردم طراحی شد. برخلاف مدل‌های اروپایی، تمرکز آن بر جمعیت کم‌برخوردار و تسهیل دسترسی به خدمات پایه بود. دامنه خدمات Aadhaar از یارانه‌های سوخت و غذا تا افتتاح حساب بانکی و دریافت وام را در بر می‌گیرد. با وجود گسترش کاربرد، استفاده از آن در خدمات خصوصی تنها با رضایت کاربر مجاز است.

مدل نهادی:

مدیریت Aadhaar در اختیار «سازمان توسعه شناسه یکتا(UIDAI) [1]» است. ساختار آن کاملاً متمرکز است و شناسه برای هر فرد توسط دولت صادر می‌شود. شرکت‌های خصوصی به‌عنوان ارائه‌دهنده خدمات جانبی و واسط فعالیت دارند، اما چارچوب طراحی و مالکیت داده کاملاً دولتی است.

سطوح اطمینان:

با وجود مقیاس بزرگ پروژه، چارچوب صریح LOA در مقررات Aadhaar دیده نمی‌شود. همه احرازها بر پایه داده‌های زیستی (اثر انگشت، قرنیه، چهره) انجام می‌شود که در بسیاری از مناطق محروم با مشکلات فنی و ناکافی بودن دقت همراه است. نبود طبقه‌بندی خدمات براساس ریسک، موجب شده استفاده از احراز زیستی حتی در خدمات کم‌ریسک نیز اجباری شود.

سازوکار صدور و کنترل:

هر فرد با ثبت‌نام در مراکز رسمی، شناسه یکتای Aadhaar را دریافت می‌کند. کنترل داده در عمل در اختیار سازمان UIDAI و نهادهای دولتی است. کاربر به تاریخچه استفاده یا ابزارهای مدیریت داده دسترسی مستقیم ندارد. لغو یا ابطال شناسه نیز رویه شفاف ندارد.

حقوق داده:

قانون حفاظت از داده‌ها در هند پس از Aadhaar شکل گرفت و اجرای ناقص آن باعث شد انتقادات جدی به این طرح وارد شود. فقدان شفافیت در ذخیره‌سازی داده، عدم رضایت آگاهانه، و نشت اطلاعات زیستی از مهم‌ترین بحران‌های حقوقی Aadhaar بوده‌اند. احکام قضایی متعدد در مورد لزوم داوطلبانه بودن آن صادر شده‌اند.

از زمان راه‌اندازی Aadhaar تاکنون دست‌کم ده‌ها رخداد افشای داده گزارش شده است؛ از فروش غیرقانونی دسترسی به پایگاه اطلاعاتی (گزارش The Tribune در ۲۰۱۸) تا نشت میلیاردها رکورد در مخازن ابری تنظیم نشده سازمان‌های همکار. نبود رمزنگاری کامل داده‌های زیستی در مبدأ، آسیب‌پذیری دستگاه‌های ثبت اثر انگشت در برابر حملات تکرار یا بازپخش و استفاده گسترده از نسخه‌های جعلی اپلیکیشن eKYC، سطح ریسک را تشدید کرده است. دادگاه عالی هند ضمن تأکید بر لزوم «استفاده داوطلبانه»، دولت را ملزم به معرفی ابزار «Virtual ID» و ممیزی امنیتی ادواری کرده است. با این حال، کارشناسان همچنان خطر استفاده اجباری از تک‌عامل زیستی و تمرکز پایگاه داده را برجسته می‌کنند.

پیاده‌سازی و مشوق‌ها:

اجرای Aadhaar با سرمایه‌گذاری عظیم دولت و مشارکت بخش خصوصی در ثبت‌نام و کاربرد همراه بود. انگیزه استفاده از آن در دسترسی به یارانه‌ها و خدمات پایه نهفته است. اما نبود مشوق برای بهبود تجربه کاربری یا نوآوری بخش خصوصی موجب کندی توسعه زیست‌بوم پیرامونی شده است [۲۳].

1. Unique Identification Authority of India - UIDAI

۳-۲-۵. ایالات متحده - پروژه Login.gov و چارچوب NSTIC

دامنه و اهداف:

ایالات متحده برخلاف بسیاری از کشورهای پیشرفته، تاکنون یک سامانه ملی متمرکز برای هویت رقومی (دیجیتال) شهروندان ایجاد نکرده است. تلاش‌ها در قالب چارچوب NSTIC از سال ۲۰۱۱ با هدف افزایش امنیت، کاهش اتکا به رمز عبور و تسهیل دسترسی رقومی (دیجیتال) شهروندان آغاز شد [۲۴]. پروژه Login.gov از سوی GSA به‌عنوان درگاه مرکزی ورود به خدمات فدرال طراحی شد، اما پوشش آن محدود به خدمات دولتی و فدرال باقی مانده است [۲۵]. هدف کلان NSTIC ایجاد زیست‌بوم رقابتی، مبتنی بر انتخاب کاربر و با تعامل بخش خصوصی بود. در آمریکا، هویت افراد بطور سنتی از طریق شماره تأمین اجتماعی (SSN)، گواهی‌نامه رانندگی ایالتی و گذرنامه فدرال اثبات می‌شود. در واقع هیچ شناسه رقومی (دیجیتال) واحدی برای تعامل با خدمات عمومی یا خصوصی وجود ندارد.

مدل نهادی:

مدل حکمرانی آمریکا در حوزه هویت رقومی (دیجیتال) غیرمتمرکز، فدرالی و بازارمحور است. هیچ نهاد مرکزی برای صدور هویت رقومی (دیجیتال) وجود ندارد؛ بخش خصوصی مانند شرکت‌های گوگل، مایکروسافت و ID.me نقش اصلی در ارائه احراز هویت دارند و دولت صرفاً نقش هماهنگ‌کننده، تسهیل‌گر و استانداردگذار را ایفا می‌کند. سامانه Login.gov برای اتصال به خدمات فدرال توسعه یافته، اما بسیاری از ایالت‌ها و آژانس‌ها از راهکارهای متفاوت استفاده می‌کنند. علاوه‌بر این، نهادهای فدرالی نظیر IRS در مالیات، USCIS در مهاجرت و SSA در تأمین اجتماعی سامانه‌های اختصاصی خود را برای احراز هویت دارند.

سطوح اطمینان:

چارچوب NSTIC بر اصل سطوح مختلف اطمینان (LOA) تأکید دارد و چارچوب NIST SP 800-63 را برای تعریف این سطوح در اختیار نهادها قرار داده است. سطوح شامل AAL[2]، IAL[1] و FAL[3] هستند. با این حال، پیاده‌سازی آن به عهده نهادها گذاشته شده و در عمل پراکندگی اجرا وجود دارد.

سازوکار صدور و کنترل:

هیچ سامانه ملی برای صدور شناسه رقومی (دیجیتال) وجود ندارد. سامانه Login.gov به کاربران اجازه می‌دهد با یک حساب کاربری به چند خدمت فدرال دسترسی داشته باشند. در کنار آن، شرکت‌های خصوصی مانند ID.me، Clear و Experian خدمات تجاری احراز هویت رقومی (دیجیتال) ارائه می‌دهند و حتی در برخی پروژه‌ها به سکوهای دولتی متصل شده‌اند (برای مثال، در دوران کووید-۱۹ برخی ایالت‌ها برای توزیع مزایای بیمه بیکاری از ID.me استفاده کردند). در حوزه کیف پول رقومی (دیجیتال) و معماری SSI نیز آمریکا فاقد چارچوب ملی هماهنگ است، اما پروژه‌های آزمایشی مانند گواهی‌نامه رانندگی رقومی (دیجیتال) (mDL) در ایالت‌هایی چون کالیفرنیا و آریزونا جریان دارد. همچنین وزارت امنیت داخلی DHS و NIST در حال ارزیابی راهکارهای مبتنی‌بر اسناد هویتی قابل تایید هستند.

حقوق داده:

ایالات متحده فاقد قانون جامع حریم خصوصی در سطح ملی مشابه GDPR است و مقررات پراکنده‌ای مانند HIPAA در سلامت یا FERPA در آموزش وجود دارد. بسیاری از ارائه‌دهندگان هویت خصوصی تابع سیاست‌های اختصاصی خود هستند و میزان کنترل کاربر بر داده‌ها به آن سیاست‌ها بستگی دارد. این وضعیت نگرانی‌هایی درباره ردیابی، داده‌کاوی و سوءاستفاده از اطلاعات شخصی ایجاد کرده است.

پیاده‌سازی و مشوق‌ها:

دولت فدرال برای گسترش سامانه Login.gov مشوق‌هایی ارائه داده ولی استفاده از آن اجباری نیست. رقابت با ارائه‌دهندگان خصوصی باعث عدم تمرکز در بازار شده است. نبود استاندارد الزامی سراسری، مقاومت ایالت‌ها در برابر فدرالی‌سازی این حوزه و نااعتمادی عمومی،

1. Identity Assurance Level
2. Authenticator Assurance Level
3. Federation Assurance Level

از چالش‌های عمده پیاده‌سازی به شمار می‌رود. مدل حکمرانی آمریکا بر پایه بخش خصوصی قدرتمند، رقابت آزاد و تنظیم‌گری مبتنی بر استاندارد شکل گرفته است؛ مدلی که انعطاف‌پذیر و نوآورانه است، اما به دلیل فقدان رهبری متمرکز، با مشکلاتی چون ناهماهنگی و نابرابری در دسترسی نیز روبه‌روست.

۴-۲-۵. چین – eID و نظام هویت اجتماعی رقومی (دیجیتال)

دامنه و اهداف:

چین از سال ۲۰۱۳ پروژه eID را با هدف تسهیل تراکنش‌های رقومی (دیجیتال)، احراز هویت کاربران اینترنت، و کنترل فعالیت‌های سایبری آغاز کرد. برخلاف بسیاری از کشورها، هدف از ابتدا ترکیبی از خدمات‌رسانی، نظارت حکومتی و تقویت امنیت سایبری ملی بوده است. کاربرد eID در بانکداری، دولت الکترونیک، سلامت، آموزش، سکوهای تجارت الکترونیک و شبکه‌های اجتماعی الزامی است [۲۶].

مدل نهادی:

مدل چین کاملاً دولتی و متمرکز است. نهاد صادرکننده اصلی، وزارت امنیت عمومی (MPS) است که اطلاعات شهروندان را با همکاری اپراتورهای مخابراتی، بانک‌ها و شرکت‌های فناوری ذخیره و پردازش می‌کند. زیرساخت فنی در اختیار شرکت‌های ملی مانند Tencent، Alibaba و China Mobile قرار دارد ولی مالکیت داده و سیاست‌گذاری کلان در اختیار دولت است.

سطوح اطمینان:

سطوح اطمینان در eID براساس تطابق هویت واقعی با منابع رسمی مانند ثبت احوال و سامانه نظارت ملی است. تمامی کاربران سکوهای برخط باید با نام واقعی احراز شوند. با وجود کاربرد گسترده داده‌های زیستی، هیچ چارچوب عمومی شفاف برای سطح‌بندی LOA وجود ندارد. خدمات حساس‌تر مانند مالیات یا سلامت نیازمند احراز بیومتریک پیشرفته هستند.

سازوکار صدور و کنترل:

کاربر با مراجعه به دفاتر ثبت یا از طریق اپ‌های بانکی یا دولتی شناسه رقومی (دیجیتال) دریافت می‌کند. ابزار کنترل کاربر محدود است و گردش داده عمدتاً در اختیار دولت یا شرکت‌های تأیید شده قرار دارد. امکان مشاهده سوابق دسترسی یا لغو مجوزها توسط کاربر به‌صورت عمومی در دسترس نیست. داده‌ها در چارچوب «امنیت سایبری ملی» و قوانین نظارتی طبقه‌بندی می‌شوند.

حقوق داده:

قانون جدید حفاظت از داده‌های شخصی چین (PIPL, 2021) گامی به‌سوی تقویت حقوق داده است، اما همچنان شامل استثنائات گسترده برای دولت و اهداف امنیتی است. کنترل کاربر در برابر بازیگران خصوصی بیشتر از دولت است. رضایت آگاهانه الزامی است ولی در عمل بسیاری از مجوزها به‌صورت پیش‌فرض اخذ می‌شوند.

پیاده‌سازی و مشوق‌ها:

دولت با الزام کسب‌وکارها و سکوها به استفاده از eID و تعیین شاخص‌های عملکردی برای بانک‌ها و اپراتورها، اجرای آن را پیش برده است. همچنین، مزایایی مانند دسترسی سریع به خدمات، امضای رقومی (دیجیتال) معتبر و کاهش هزینه‌های احراز، به‌عنوان مشوق به کاربران ارائه شده‌اند. با این حال، نگرانی‌ها درباره شفافیت، استقلال کاربران، و نظارت دولتی همچنان بالا است [۲۷].

۵-۲-۵. امارات متحده عربی – سامانه UAE PASS

دامنه و اهداف:

سامانه UAE PASS با هدف ایجاد دولت بی‌کاغذ و ساده‌سازی احراز هویت رقومی (دیجیتال) برای تمامی کاربران داخل کشور شامل شهروندان، مقیمان، و حتی گردشگران خارجی طراحی شده است. این سامانه یک شناسه رقومی (دیجیتال) سراسری و امضای رسمی الکترونیکی را فراهم می‌کند که در حوزه‌هایی چون دولت الکترونیک، ثبت شرکت، بانکداری، سلامت، آموزش و گردشگری استفاده می‌شود. هدف کلان، فراهم‌کردن زیرساخت یکپارچه‌ای برای تحول رقومی (دیجیتال) کامل و جذب سرمایه‌گذاران خارجی است [۲۸].

مدل نهادی:

سامانه UAE PASS توسط همکاری میان Smart Dubai، TDRA[1] و Emirates Identity Authority راه‌اندازی شده و از مدل دولتی هماهن‌گشده میان امارات‌های مختلف بهره می‌برد. با این که در سطح فدرال مدیریت می‌شود، اجرا و اتصال نهادها در امارات‌های مختلف گاه با تفاوت‌هایی همراه است. شرکت‌های فناوری ملی نقش پیاده‌ساز را دارند.

سطوح اطمینان:

سامانه UAE PASS از چند سطح احراز هویت استفاده می‌کند:

الف) ورود با رمز عبور ساده

ب) احراز با OTP

ت) تأیید چهره از طریق اپلیکیشن موبایل (Face ID)

ث) امضای رقومی (دیجیتال) معتبر رسمی

سطوح اطمینان برای هر نوع خدمت متناسب با حساسیت آن تعیین شده و چارچوب سطح‌بندی فنی در دستورالعمل‌های TDRA تعریف شده است.

سازوکار صدور و کنترل:

فرایند ثبت‌نام در سامانه UAE PASS از طریق اپلیکیشن موبایل، مراجعه به دفاتر پست، یا اتصال به بانک‌های ملی امکان‌پذیر است. کاربران می‌توانند حساب خود را ارتقا داده و امضای رقومی (دیجیتال) رسمی دریافت کنند. کنترل داده توسط کاربر از طریق اپلیکیشن امکان‌پذیر است که شامل مشاهده سوابق، مدیریت دسترسی، و تأیید یا رد دسترسی‌ها است. شناسه رقومی (دیجیتال) برای مدت معین اعتبار دارد و قابل لغو، تمدید یا بازتنظیم است.

حقوق داده:

امارات دارای قانون فدرال حفاظت از داده شخصی [۲۹] است که اصل رضایت، شفافیت، محدودیت هدف، و دسترسی افراد به داده خود را به رسمیت می‌شناسد. سامانه UAE PASS با این قانون سازگار است و کاربر می‌تواند تعیین کند که کدام نهادها به چه داده‌هایی دسترسی داشته باشند. با این حال، همانند دیگر کشورهای GCC، برخی استثنائات دولتی در حوزه امنیت ملی وجود دارد.

پیاده‌سازی و مشوق‌ها

سامانه UAE PASS در سال‌های اخیر با یک نقشه راه منسجم، شاخص‌های کلیدی و الزام برای دستگاه‌های دولتی پیاده‌سازی شده است. از جمله مشوق‌ها برای شهروندان می‌توان به امکان امضای رسمی اسناد حقوقی، دسترسی به ده‌ها خدمت بدون نیاز به مراجعه حضوری، و ورود سریع به خدمات بخش خصوصی اشاره کرد. همچنین، ارائه قابلیت برای گردشگران خارجی جهت دریافت شناسه موقت رقومی (دیجیتال)، این سامانه را در زمره مدل‌های منحصربه‌فرد جهانی قرار داده است.

۳ـ۵. بررسی مقررات مهم ایران در حوزه احراز هویت رقومی (دیجیتال)

در سال‌های اخیر، ایران مجموعه‌ای از اسناد، آیین‌نامه‌ها و مصوبات را در حوزه احراز هویت رقومی (دیجیتال) تصویب کرده است. این اسناد عمدتاً در پاسخ به نیازهای قانونی در حوزه‌های مبارزه با پول‌شویی، دولت الکترونیک و تنظیم‌گری فضای مجازی تدوین شده‌اند. با این حال، بررسی تطبیقی نشان می‌دهد که این اسناد از نظر یکپارچگی، پوشش خدمات، شفافیت سطح اطمینان، و اصول حریم خصوصی دچار کاستی‌هایی نیز هستند. در ادامه، پنج سند کلیدی بر اساس ۶ محور تطبیقی تحلیل می‌شوند.

1. Telecommunications and Digital Government Regulatory Authority

۱-۳-۵. نظام هویت معتبر در فضای مجازی (مصوب شورای عالی فضای مجازی - ۱۳۹۸/۰۶/۰۹)

دامنه و اهداف:

این سند با هدف کلان ایجاد «نظام هویت معتبر» برای سامان‌دهی تعاملات هویتی در فضای مجازی کشور تدوین شده است. به‌طور مشخص، تلاش دارد سازوکاری رسمی برای تأیید و اعتباردهی به هویت اشخاص حقیقی، حقوقی، دستگاه‌های اجرایی، اشیاء و خدمات در محیط رقومی (دیجیتال) ارائه دهد. در بندهای آغازین، از تحقق اهدافی نظیر ارتقاء اعتماد عمومی، امنیت تعاملات رقومی (دیجیتال)، و مقابله با تخلفات هویتی سخن به میان آمده است. با این حال در این سند، تعیین دقیق دامنه مصادیق خدمات مشمول، نوع خدمات (دولتی یا خصوصی)، یا قلمرو اجرایی الزامات در بخش‌های مختلف اقتصادی و اجتماعی بطور صریح مشخص نشده است.

در واقع، هدف‌گذاری سند همچنان در سطح کلان و سیاستی است و به مباحثی نظیر توسعه دولت رقومی (دیجیتال)، به‌کارگیری هویت در اقتصاد سکویی، یا تسهیل نوآوری در خدمات رقومی (دیجیتال) ورود نکرده است. این در حالیست که در اسناد کشورهای پیشرو، پیوند میان «هویت رقومی (دیجیتال)» و «تحول رقومی (دیجیتال) اقتصادی» به صراحت بیان شده و یکی از معیارهای سنجش موفقیت تلقی می‌شود.

مدل نهادی:

در ساختار اجرایی سند، وظایف اصلی بر عهده مرکز ملی فضای مجازی، سازمان ثبت احوال کشور، و کارگروه‌های ذیل شورای عالی فضای مجازی قرار گرفته است. رویکرد این سند مبتنی بر یک مدل متمرکز و دولتی است که عمدتاً نقش بازیگران غیردولتی، نهادهای واسط، یا اپراتورهای فنی و تجاری را بطور صریح بیان نمی‌کند.

همچنین نقش نهادی مشخص برای تنظیم‌گر حفاظت داده‌ها یا نهاد پاسخگو در برابر نقض‌های هویتی یا اعتراض کاربران پیش‌بینی نشده است.

سطوح اطمینان:

نظام هویت معتبر در فضای مجازی به «اعتبارسنجی متناسب با خدمات» اشاره دارد، اما چارچوب رسمی LOA را معرفی نمی کند. در این سند سازوکاری برای تفکیک خدمات پُرریسک از کم‌ریسک و مطابقت با سطح اطمینان پیش‌بینی نشده است.

سازوکار صدور و کنترل:

سند نظام هویت معتبر در فضای مجازی به «فرآیند صدور شناسه معتبر» اشاره دارد، اما به جزییات مربوط به چرخه حیات هویت رقومی (دیجیتال)، قابلیت ابطال، انتقال‌پذیری، و نحوه نظارت کاربر بر کاربری و اشتراک‌گذاری داده‌ها نمی‌پردازد. مقایسه سند مذکور با مقررات سنگاپور نشان می‌دهد که مقررات سنگاپور دسترسی کامل کاربر به سوابق هویتی و داده‌های مصرف شده را تضمین کرده‌اند.

حقوق داده:

این سند به‌طور کلی از پرداختن به اصول بنیادین حقوق داده خودداری می کند. مفاهیم پایه‌ای مانند رضایت آگاهانه، شفاف‌سازی اهداف پردازش، حداقل‌سازی داده و دسترسی و اصلاح‌پذیری اطلاعات توسط کاربر در این سند ذکر نشده‌اند، و مرجع مستقلی برای رسیدگی به تخلفات داده‌ای معرفی نشده است. پیوند میان نظام هویت رقومی (دیجیتال) و سیاست‌گذاری داده‌محور، از جمله خلأهای این سند سیاست‌گذاری است.

پیاده‌سازی و مشوق‌ها:

در سند نظام هویت معتبر در فضای مجازی به سازوکارهایی مانند ارایه جدول زمانی، فازبندی اجرایی، شاخص ارزیابی یا مشوق برای پذیرش عمومی یا مشارکت بخش خصوصی پرداخته نشده است. اجرای سند مذکور به همکاری داوطلبانه دستگاه‌ها موکول شده که فاقد ضمانت اجرا است [۷].

۲-۳-۵. آیین‌نامه اجرایی ماده (۱۴) قانون مبارزه با پول‌شویی (مصوب هیئت وزیران - ۱۳۹۸/۰۷/۲۱)

دامنه و اهداف:

آیین‌نامه اجرایی ماده (۱۴) الحاقی قانون مبارزه با پولشویی مصوب هیئت وزیران، با هدف اصلی شناسایی هویتی اشخاص حقیقی و حقوقی

در تعامل با نهادهای مالی و حرفه‌ای به‌منظور پیشگیری از تخلفات مالی و ردیابی منشأ منابع مالی تصویب شده است. دامنه اجرایی آن محدود به «اشخاص مشمول» نظیر بانک‌ها، مؤسسات اعتباری، بیمه‌ها، صرافی‌ها و برخی مشاغل خاص (وکلا، حسابداران، دفاتر اسناد رسمی) است. در این مقرره رویکرد یکپارچه، افقی و چندبخشی دنبال نشده است بلکه آیین نامه مذکور صرفاً ناظر بر نیازهای امنیتی بخش مالی است. ازاین‌رو، قابلیت تعمیم‌پذیری به حوزه‌هایی نظیر تجارت الکترونیکی، دولت رقومی (دیجیتال) یا خدمات سلامت وجود ندارد [۶].

مدل نهادی:

ساختار نهادی آیین‌نامه مبتنی بر تمرکز شدید در درون دولت و بانک مرکزی است. واحد اطلاعات مالی (FIU) به‌عنوان نهاد مرکزی گزارش‌گیری، تحلیل و پایش معاملات مشکوک عمل می‌کند، در حالی که بانک مرکزی نقش نظارتی و راهبری برای نهادهای پولی و بانکی دارد. نهادهای خصوصی مشمول (نظیر صرافی‌ها یا مؤسسات مالی غیربانکی) هیچ نقشی در طراحی، استانداردسازی یا نوآوری در مدل احراز هویت ندارند و صرفاً موظف به رعایت الزامات اجرایی‌اند.

سطوح اطمینان:

هرچند آیین‌نامه به‌طور ضمنی بر ارزیابی ریسک مشتری تأکید دارد، اما چارچوب فنی یا سیاستی برای سطوح اطمینان تدوین نکرده است. در آیین‌نامه مذکور مشخص نشده است که در کدام شرایط از احراز هویت ساده، دومرحله‌ای یا زیستی استفاده شود.

سازوکار صدور و کنترل:

فرآیندهای صدور هویت و ثبت اطلاعات مبتنی بر ساختار درونی هر مؤسسه مالی انجام می‌شود. بانک‌ها و مؤسسات برای دریافت اطلاعات هویتی به پایگاه ثبت احوال یا سامانه‌هایی مانند نهاب وابسته‌اند. همچنین، فرآیندهای تأیید، تمدید، لغو یا ابطال هویت رقومی (دیجیتال) به‌صورت رسمی تعریف نشده است.

حقوق داده و حریم خصوصی:

در آیین‌نامه مذکور هیچ‌گونه ارجاع مستقیمی به اصول حفاظت داده‌های شخصی ندارد. تعریفی از رضایت آگاهانه ارائه نشده است. استفاده از داده‌های هویتی در این نظام کاملاً دولت‌محور صورت می‌گیرد.

پیاده‌سازی و مشوق‌ها:

آیین‌نامه از منظر حقوقی الزام‌آور است و نهادهای مشمول مکلف به اجرای آن هستند. بااین‌حال، سازوکار حمایتی، مشوق فناوری، دستورالعمل جزئی پیاده‌سازی یا API متن باز برای تسهیل همگرایی فناوری در آن گنجانده نشده است.

۳-۳-۵. الزام دستگاه‌های اجرایی به ارائه خدمات صرفاً پس از احراز هویت رقومی (مصوب شورای اجرایی فناوری اطلاعات - ۱۳۹۷/۰۲/۰۴)

دامنه و اهداف:

هدف اصلی این مصوبه شورای اجرایی فناوری اطلاعات، تضمین صحت هویت اشخاص حقیقی و نشانی محل اقامت آن‌ها در ارائه خدمات دولت الکترونیک است. این مصوبه، دستگاه‌های اجرایی را ملزم می‌کند تنها پس از انجام موفق احراز هویت رقومی (دیجیتال) و اعتبارسنجی نشانی، خدمت را ارائه دهند [۸].

با وجود این هدف صریح، دامنه اجرایی مصوبه فاقد شمول جامع نسبت به انواع خدمات (مالی، رفاهی، قضایی، آموزشی و...) و بدون تفکیک میان سطوح مختلف ریسک و حساسیت خدمات است. همچنین در این مصوبه اشاره‌ای به پوشش بخش خصوصی، کاربردهای چندمنظوره، یا ارتباط با اقتصاد رقومی (دیجیتال) نشده است.

مدل نهادی:

بر اساس مصوبه، هر دستگاه اجرایی موظف است در فرآیند ارائه خدمت، به سامانه ثبت احوال و شرکت پست متصل شود تا هویت و نشانی کاربر را استعلام کند.

سطوح اطمینان:

مصوبه صرفاً تصریح می‌کند که احراز هویت باید با سطح مناسب اطمینان متناسب با نوع خدمت انجام شود؛ اما هیچ تعریفی از سطح اطمینان، مدل ریسک‌محور، یا شاخص فنی و اجرایی ارائه نمی‌کند.

دستگاه‌ها نیز به‌دلیل نبود چارچوب LOA یا دستورالعمل‌های مرجع مجبور به پیاده‌سازی سلیقه‌ای و نامتوازن شده‌اند. این موضوع، سطح امنیت و کارایی سامانه‌ها را کاهش داده است.

سازوکار صدور و کنترل:

در این مصوبه، فرآیند مشخص و استانداردشده‌ای برای صدور، مدیریت یا ابطال شناسه رقومی (دیجیتال) پیشنهاد نمی‌کند. دستگاه‌ها عمدتاً به‌طور موردی از طریق استعلام‌گیری از سامانه ثبت احوال و پست، به هویت کاربران اطمینان پیدا می‌کنند.

حقوق داده:

مصوبه فاقد هرگونه اشاره‌ای به اصول بنیادین حقوق داده‌ها و حریم خصوصی است. در این مصوبه، از رضایت کاربر برای تبادل داده‌ها و هدفمندی پردازش یا محدودیت در میزان جمع‌آوری داده‌ها موردی ذکر نشده است.

پیاده‌سازی و مشوق‌ها:

در این مصوبه، ساختار مشوقی برای دستگاه‌ها پیش‌بینی نشده است. دستورالعمل اجرایی جزئی برای توسعه‌دهندگان و مجریان ارایه نشده است.

تحلیل تطبیقی اسناد سیاستی و مقرراتی ایران در حوزه احراز هویت رقومی (دیجیتال) نشان می‌دهد که چارچوب‌های موجود، بیشتر حاصل تصمیم‌گیری‌های مقطعی است و انسجام راهبردی آنها ضعیف است. اغلب این اسناد به‌جای طراحی یک زیرساخت بنیادین و فراگیر هویتی، تنها در پاسخ به نیازهای موضعی یا بخشی (مانند مبارزه با پول‌شویی یا تسهیل خدمات دولت الکترونیک) تدوین شده‌اند.

در محورهای کلیدی تحلیل شامل دامنه، مدل نهادی، سطوح اطمینان، سازوکار صدور، حقوق داده و پیاده‌سازی، بیشتر اسناد داخلی با خلأهای مفهومی و اجرایی مواجه‌اند. مهم‌ترین چالش‌ها عبارت‌اند از:

- مشخص نشدن چارچوب سطوح اطمینان (LOA) و تعریف استانداردهای متناسب با حساسیت خدمات؛
- عدم معرفی نهاد تنظیم‌گر واحد و پاسخ‌گو با اختیار تدوین استانداردها، پایش کیفیت و رسیدگی به تخلفات؛
- ضعف در الزامات حمایت از حقوق کاربران
- مشخص نشدن برنامه اجرایی فازبندی‌شده، شاخص‌های عملکردی و مشوق‌های عملیاتی برای دستگاه‌ها و کاربران.

این الگوی سیاست‌گذاری، هم‌افزایی بین‌بخشی لازم در دولت را ایجاد نمی‌کند، همچنین باعث افزایش هزینه‌های انطباق می‌شود، اعتماد عمومی و اقبال کابران را در سطح ضعیفی نگه می‌دارد، و تعامل‌پذیری منطقه‌ای و بین‌المللی نیز دشوار خواهد شد.

۴ـ۵. تحلیل تطبیقی و طراحی پیشران‌های قانون مطلوب احراز هویت رقومی (دیجیتال) در ایران

در شرایطی که گذار به اقتصاد رقومی (دیجیتال) و دولت هوشمند به یکی از اولویت‌های راهبردی کشورها تبدیل شده، «احراز هویت رقومی (دیجیتال)» نه‌تنها یک ابزار فنی، بلکه شالوده‌ای برای اعتماد، حکمرانی داده، و تعاملات ایمن در فضای رقومی (دیجیتال) است. بررسی اسناد و تجارب جهانی نشان می‌دهد که کشورهایی که توانسته‌اند نظام‌های هویت رقومی (دیجیتال) کارآمد، ایمن و مقیاس‌پذیر طراحی کنند، موفق‌تر از دیگران در توسعه خدمات عمومی، رشد زیست‌بوم‌های نوآوری، و تسهیل فعالیت بخش خصوصی عمل کرده‌اند.

در ایران، تلاش‌های پراکنده در سطوح فنی و نهادی انجام شده است اما تاکنون قانون جامع، شفاف، و آینده‌نگر برای احراز هویت رقومی (دیجیتال) تدوین نشده است. مقررات موجود عمدتاً پراکنده و مسئله محور بوده‌اند و نگاه راهبردی، کاربرمحور، یا نوآورانه کمتر مورد توجه بوده‌اند.

بر این اساس، با توجه به مطالعه تطبیقی صورت گرفته در محورهای کلیدی هویت رقومی (دیجیتال) میان ایران و نمونه‌های جهانی، ضعف‌های ساختاری و نهادی موجود شناسایی می‌شود. سپس با مرور عناصر مشترک در الگوهای موفق، اصول بنیادینی برای تدوین یک قانون کارآمد در ایران پیشنهاد می‌گردد؛ قانونی که بتواند همزمان به اعتماد عمومی کاربران، تعامل‌پذیری فنی، رعایت حقوق داده و رشد اقتصادی پاسخ دهد.

۱-۴-۵. تحلیل تطبیقی کشورهای پیشرو و وضعیت ایران

مرور تجربه‌های کشورهای پیشرو در توسعه سامانه‌های احراز هویت رقومی (دیجیتال)، از اروپا گرفته تا سنگاپور، چین و امارات، نشان می‌دهد که با وجود تفاوت در سطح توسعه و ساختار حکمرانی، یک درک مشترک در سیاست‌گذاری آنها وجود دارد: هویت رقومی (دیجیتال) صرفاً ابزار شناسایی یا مدیریت کاربران نیست، بلکه زیرساختی بنیادین برای اعتماد، حکمرانی رقومی (دیجیتال)، شمول مالی، و رشد اقتصاد داده‌محور است.

در مقابل، سیاست‌ها و اسناد ایران بیشتر ناظر به نیازهای اجرایی، مسائل و چالش‌های مقطعی بوده و چارچوب‌های رشدمحور، تعاملی و کاربرمحور کمتر مورد توجه بوده‌اند. این خلأها در مقایسه با استانداردهای جهانی و رویه‌های پیشرفته قابل شناسایی است. جدول ۴ به‌صورت خلاصه، تفاوت‌های ساختاری ایران با کشورها و نهادهای منتخب جهانی را بر اساس شش محور کلیدی تحلیل تطبیقی نشان می‌دهد:

جدول ۴. مقایسه تطبیقی قانون‌گذاری احراز هویت ایران و کشورهای پیشرو

محور تحلیلی	تجربیات بین‌المللی	تجربیات ایران
دامنه و اهداف	شمول خدمات عمومی و خصوصی؛ پوشش فرامرزی (مدل اروپا)، گردشگران (مدل امارات)، جذب سرمایه و کارآفرین (مدل استونی)	محدود به مدیریت دسترسی و خدمات حاکمیتی؛ فاقد افق توسعه رقومی (دیجیتال)
مدل نهادی	مدل‌های فدراتیو (اروپا و استرالیا) یا چندلایه با هماهنگی ملی و خصوصی (سنگاپور و آمریکا)	متمرکز و جزیره‌ای؛ بدون مشارکت رقابتی بخش خصوصی
سطوح اطمینان (LOA)	دارای سطح‌بندی رسمی(ISO, ETSI, NIST)، متناسب‌سازی خدمات با ریسک، ابزارهای آزمون‌پذیر و تأیید مستقل	چارچوب رسمی سطح‌بندی متناسب با ریسک انجام نشده است؛ ارجاعی به استانداردهای بین‌المللی نشده است.
سازوکار صدور و کنترل	امکان مشاهده، لغو، مدیریت مجوزها توسط کاربر (EUDI Wallet اروپا)، شفافیت کامل در مصرف داده‌ها	فاقد ابزارهای مدیریت یکپارچه چرخه حیات و کنترل کاربر بر داده
حقوق داده	مبتنی بر قوانین حمایت از داده (اروپا، PIPL[1] چین، قانون فدرال امارات)، کنترل کاربر بر داده، سیاست رضایت‌محور	عدم پوشش قانون برای تضمین حقوق کاربر؛ عدم پوشش قانون برای رعایت اصول حمایت از داده مانند رضایت، محدودیت هدف و شفافیت
پیاده‌سازی و مشوق‌ها	برنامه اجرایی زمان‌دار، تعریف سنجه‌های کلیدی، مشوق مشارکت زیست‌بوم، بودجه عمومی برای توسعه فنی و آموزشی	عدم صراحت مقررات درباره تعیین شاخص‌های کمی، فازبندی اجرایی، یا مشوق‌های پذیرش عمومی و نوآوری خصوصی

مآخذ: گردآوری توسط نویسندگان

کشورهای موفق از هویت رقومی (دیجیتال) به‌عنوان پیشران تحول رقومی (دیجیتال)، شمول مالی، و قدرت نرم ملی بهره می‌گیرند، استفاده از این تجارب و تدوین و تصویب قانون جامع و آینده‌نگر برای احراز هویت رقومی (دیجیتال) می‌تواند فرصت‌های تحول رقومی در ایران را تقویت کند.

۲-۴-۵. چالش‌های مقررات ایران

تحلیل تطبیقی با کشورهای پیشرو در توسعه سامانه‌های احراز هویت رقومی (دیجیتال) نشان می‌دهد که ایران با چند چالش در حوزه

1. Personal Information Protection Law of the People's Republic of China

سیاست‌گذاری، زیرساخت فنی، حقوق داده، و حکمرانی داده مواجه است. این چالش‌ها از یک طرف سبب بروز موانعی سر راه گسترش و اعتمادپذیری سامانه‌های احراز هویت در کشور شده‌اند و از طرف دیگر توان رقابت‌پذیری ایران در تعاملات رقومی (دیجیتال) فرامرزی را نیز کاهش داده‌اند. مهم‌ترین چالش‌ها به شرح زیر است:

الف) عدم معرفی و انتخاب نهاد تنظیم‌گر فراگیر در حوزه احراز هویت رقومی

در اسناد بالادستی یا آیین‌نامه‌های اجرایی موجود، یک نهاد تخصصی به‌عنوان تنظیم‌گر جامع برای کل زیست‌بوم هویت رقومی (دیجیتال) معرفی و انتخاب نشده است. نقش‌های کلیدی میان نهادهایی نظیر سازمان ثبت‌احوال، سازمان فناوری اطلاعات، مرکز ملی فضای مجازی، و در مواردی وزارت کشور، به‌صورت پراکنده و بدون مرجعیت حقوقی واحد تقسیم شده‌اند. این مسئله منجر به تعارض تصمیم‌گیری، نبود مرجع رسیدگی به اختلافات و عدم امکان تنظیم استانداردهای فنی مشترک میان سامانه‌ها می‌شود. در نتیجه عدم نقش آفرینی یک نهاد بالادستی منسجم باعث گسست در سیاست‌گذاری، پیاده‌سازی ناقص و کاهش اعتماد ذی‌نفعان می‌شود.

ب) فقدان چارچوب فراگیر و رسمی درباره سطح‌بندی اطمینان (LOA)

کشورهای پیشرو یک چارچوب‌های استانداردی مانند NIST SP 800-63 یا ISO/IEC 29115 را برای سطح‌بندی اطمینان به‌کار گرفته‌اند، اما در ایران سازوکار فراگیر، رسمی و هماهنگی، آزمون‌پذیر، و قابل ارجاع برای تعیین سطح ریسک و امنیت احراز هویت تعریف نشده است. بیشتر فرآیندهای احراز هویت صرف‌نظر از سطح ریسک خدمات با الزامات یکسان اجرا می‌شوند. در نتیجه فقدان سازوکار فراگیر و رسمی LOA موجب می‌شود احرازهای کم‌ریسک نیز با هزینه بالا و تجربه کاربری ضعیف انجام شوند یا خدمات پرریسک بدون امنیت کافی عرضه شوند.

ج) ضعف تعامل‌پذیری احراز هویت در سطح ملی

در اغلب سامانه‌های هویت رقومی (دیجیتال) فعال در ایران، از معماری فنی بسته و ناسازگار با همدیگر استفاده شده است. الزامی برای انطباق سامانه‌ها با یکدیگر مصوب نشده است. ضعف در اتصال خدمات احراز هویت نهادهای داخلی با یکدیگر، منجر به کاهش بهره‌وری، عدم مقیاس‌پذیری، و ناکامی در توسعه خدمات ترکیبی می‌شود.

د) فقدان چارچوب جامع حقوق داده و کاربرمحوری

در اسناد فعلی قانون جامع و الزام‌آور برای حفاظت از داده‌های کاربران، رضایت آگاهانه، محدودیت هدف، شفافیت در پردازش داده، یا امکان مدیریت اطلاعات شخصی توسط کاربر وجود ندارد. کنترل کامل داده در اختیار نهادهای صادرکننده است و الزامی برای فراهم کردن ابزارهای مدیریت داده های شخصی برای کاربر لحاظ نشده است. این وضعیت می‌تواند منجر به کاهش اعتماد کاربران شود و خطر پردازش غیرقانونی داده‌های شخصی کاربران توسط اشخاص غیرذیصلاح را افزایش می‌دهد.

ه) فقدان نقشه راه اجرایی، شاخص‌های ارزیابی و مشوق‌ها

در بیشتر اسناد مرتبط با احراز هویت رقومی (دیجیتال) در ایران، برنامه زمان‌بندی، مراحل و ترتیب اجرا، شاخص‌های کمّی عملکرد یا مشوق‌های پذیرش عمومی و نوآوری بخش خصوصی تعریف نشده است. مشارکت دستگاه‌ها نیز به‌جای الزام قانونی، بر همکاری داوطلبانه استوار است. در نتیجه عدم تعبیه این مفاهیم در فرآیندها موجب عدم پیشرفت مناسب پروژه‌ها می‌شود.

۳-۴-۵. اصول بنیادین و پیشران‌های قانون مطلوب برای ایران

پس از بررسی تجربه‌های جهانی و تحلیل شکاف‌های موجود در نظام احراز هویت رقومی (دیجیتال) ایران، اکنون پرسش کلیدی آن است که یک «قانون مطلوب» برای کشور باید بر چه اصولی استوار باشد؟ واقعیت این است که احراز هویت رقومی (دیجیتال) نه‌تنها یک ابزار فنی، بلکه بخشی از «زیرساخت اعتماد ملی در فضای رقومی (دیجیتال) » است و هرگونه سیاست‌گذاری در این حوزه، آثار مستقیمی بر اعتماد عمومی، رشد اقتصاد رقومی (دیجیتال)، و تعاملات فرامرزی خواهد داشت.

بنابراین، طراحی قانون باید نه از مسیر آزمون‌وخطا، بلکه با تکیه بر اصول بنیادین حکمرانی رقومی (دیجیتال)، تجربه‌های موفق بین‌المللی، و

بومی‌سازی هوشمندانه انجام شود. این بخش تلاش دارد مجموعه‌ای از اصول راهبردی و پیشران‌های کلیدی را به‌عنوان نقشه راه سیاست‌گذار برای تدوین قانون اختصاصی، شفاف و آینده‌نگر در ایران معرفی کند.

جدول ۵. اصول راهبردی و پیشران‌های کلیدی قانون مطلوب برای ایران

اصل کلیدی	شرح و ضرورت
رشدگرایی	قانون باید نگاه فرابخشی داشته و هویت رقومی (دیجیتال) را زیرساختی برای توسعه اقتصاد رقومی (دیجیتال)، شمول مالی، و تسهیل خدمات بخش خصوصی تعریف کند.
شفافیت ساختاری	تدوین سطوح اطمینان، ثبت و اعتبارسنجی نهادهای صادرکننده، ایجاد سازوکار آزمون‌پذیر، و طراحی مسیر اجرای فازبندی‌شده، از ارکان ضروری شفافیت و نظارت‌پذیری هستند.
کاربرمحوری	کاربر باید مالک داده خود باشد و بتواند داده‌های خود را مشاهده، لغو، محدود یا منتقل کند. کلیه دسترسی‌ها باید با رضایت روشن کاربر انجام شوند. ابزارهای مدیریت ساده و امن در اختیار کاربر باشد.
تعامل‌پذیری	قانون باید مبتنی بر معماری باز، APIهای استاندارد، و همسویی با زیست‌بوم‌های جهانی طراحی شود تا امکان اتصال داخلی و فرامرزی فراهم شود.
تنظیم‌گری مستقل	یک نهاد تخصصی، مستقل از نهادهای اجرایی، با اختیار مقررات‌گذاری، ارزیابی، صدور مجوز و نظارت بر تمامی لایه‌های صدور تا بکارگیری هویت رقومی (دیجیتال)، ضروری است.

مآخذ: مستخرج از مطالعه تطبیقی و گردآوری شده توسط نویسندگان

بررسی کشورهایی چون هند، ایالات متحده، و چین نشان می‌دهد که حتی کشورهایی با ظرفیت‌های فنی بالا و سرمایه‌گذاری سنگین نیز در صورت بی‌توجهی به حکمرانی داده، شفافیت نهادی، و حقوق کاربران، با بحران‌های ساختاری و مشروعیتی در نظام هویت رقومی (دیجیتال) خود مواجه شده‌اند. این تجربه‌ها نه‌تنها نشانه شکست در اجرا نیستند، بلکه نشان می‌دهند که موفقیت فنی، بدون پذیرش اجتماعی و اعتماد عمومی، فاقد پایداری و اثربخشی بلندمدت خواهد بود. برخی از مهمترین بحران‌های نظام هویت رقومی در سال‌های اخیر عبارتند از:

۱ هند: نشت اطلاعات زیستی و بحران اعتماد عمومی

طرح Aadhaar با هدف تسهیل دسترسی به خدمات و یارانه‌ها در یکی از بزرگ‌ترین پروژه‌های هویت رقومی (دیجیتال) جهان اجرا شد، اما به دلیل فقدان چارچوب‌های محکم حقوق داده و شفافیت نهادی، به‌شدت با چالش مواجه شد. مشکلات کلیدی عبارت‌اند از:

- نشت اطلاعات زیستی میلیون‌ها نفر (اثر انگشت، قرنیه) به رسانه‌ها و بازار سیاه، بدون پاسخگویی مؤثر نهاد صادرکننده.
- نبود رضایت آگاهانه و ابزار کنترلی برای کاربران، به‌ویژه در مناطق روستایی.
- احکام قضایی مکرر مبنی بر ممنوعیت اجبار شهروندان به استفاده از Aadhaar در برخی خدمات به‌دلیل نقض آزادی انتخاب و حقوق اساسی کاربران.

۲ ایالات متحده: پراکندگی نهادی و ضعف حکمرانی داده

با وجود سابقه فنی و زیست‌بوم قوی رقومی (دیجیتال)، ایالات متحده نتوانسته یک نظام هویت رقومی (دیجیتال) ملی و یکپارچه طراحی کند. مشکلات کلیدی عبارت‌اند از:

- نبود نهاد مرکزی تنظیم‌گر و متولی واحد، منجر به رقابت و عدم هم‌افزایی بین راه‌حل‌های فدرال، ایالتی و خصوصی.
- فقدان قانون جامع حریم خصوصی، که موجب شده کاربران بسته به شرکت ارائه‌دهنده (مثلاً شرکت گوگل یا ID.me) با سیاست‌های متفاوت مواجه شوند.
- پراکندگی چارچوب‌های فنی و عدم انطباق استانداردها، علی‌رغم وجود سند مرجع NIST SP 800-63.

۳ چین: تمرکز حکومتی و غیبت حاکمیت فردی بر داده‌ها

چین موفق به طراحی و اجرای نظام گسترده eID شده است، اما به‌دلیل ساختار کنترل‌گرایانه و تمرکز قدرت، این موفقیت فنی با چالش‌های جدی مشروعیتی مواجه است:

- کنترل کامل دولت بر داده‌های شهروندان، بدون ابزار نظارت عمومی یا دسترسی شفاف کاربران به چرخه داده.
- استفاده اجباری از نام واقعی در تمام سکوها، با هدف کنترل محتوا و رفتار برخط کاربران.
- استثنائات گسترده در قانون حفاظت از داده‌ها (PIPL) برای نهادهای امنیتی، که عملاً بسیاری از حقوق کاربر را تعلیق کرده است.

در هر سه نمونه فوق، ضعف در یکی از سه پایه اصلی حکمرانی رقومی (دیجیتال) یعنی حقوق داده، شفافیت نهادی، و اعتماد اجتماعی منجر به بحران‌های دامنه‌دار شده است. اگرچه سطح پیشرفت فنی و مقیاس اجرایی در این کشورها بالا بوده، اما بی‌توجهی به حقوق کاربر و حکمرانی متوازن، نه‌تنها اثربخشی طرح را کاهش داده بلکه آن را در معرض تعلیق، اعتراض یا تحریم اجتماعی قرار داده است. لذا طراحی قانون احراز هویت رقومی (دیجیتال) بدون درنظرگرفتن الزامات حکمرانی داده و مشارکت کاربر، حتی اگر با پیشرفت فنی همراه باشد، نهایتاً با شکست در پذیرش عمومی و ناکامی در توسعه پایدار مواجه خواهد شد.

۶. جمع‌بندی و پیشنهادها

تحلیل تطبیقی نظام‌های احراز هویت رقومی (دیجیتال) در کشورهای پیشرو، تصویری روشن از مؤلفه‌های کلیدی موفقیت در این حوزه به دست می‌دهد: موفقیت نه تنها محصول فناوری‌های نوین یا سرمایه‌گذاری کلان است، بلکه نتیجه طراحی سیاستی بلندمدت، حکمرانی داده کاربرمحور، و اجرای تدریجی در چارچوب یک زیست‌بوم چندبازیگری است. کشورهایی مانند امارات یا اتحادیه اروپا توانسته‌اند از احراز هویت رقومی (دیجیتال) نه‌تنها به‌عنوان یک ابزار شناسایی، بلکه به‌عنوان زیرساخت راهبردی تحول رقومی (دیجیتال)، موتور توانمندسازی اقتصادی، و نقطه اتصال شفاف میان شهروند، دولت و بازار بهره‌برداری کنند.

از طرف دیگر، تجربه ایران نشان می‌دهد که رویکردهای موجود اغلب با نگاه مقطعی، با تمرکز بیشتر بر پاسخ‌گویی به نیازهای دولتی و توجه کمتر به طراحی نهادی بلندمدت و ایجاد بستر مشارکت بخش خصوصی پیش رفته‌اند. عدم معرفی و انتخاب نهاد تنظیم‌گر فراگیر، نبود چارچوب فراگیر و رسمی درباره سطح‌بندی اطمینان (LOA)، پراکندگی در تعامل بین‌دستگاهی، ضعف در پیاده‌سازی حقوق داده، و کم‌توجهی به رضایت کاربر و اختیارات او بر داده‌هایش، از جمله مهم‌ترین موانع تحقق یک سامانه جامع، قابل‌اعتماد و توسعه‌پذیر در ایران بوده‌اند. این شکاف‌ها نه‌تنها پذیرش عمومی را کاهش داده، بلکه موجب شده پروژه‌های متعددی نظیر شاهکار، گذر و کیف پول هویتی ملی در مراحل ابتدایی باقی بمانند یا فاقد تعمیم‌پذیری فرامرزی باشند.

با توجه به این کاستی‌ها، برای عبور از وضعیت فعلی و ایجاد یک نظام احراز هویت رقومی (دیجیتال) مبتنی بر اعتماد، چابکی و مشارکت، تدوین یک بسته سیاستی جامع و چندبعدی ضروری است. چنین بسته‌ای باید بتواند ضمن بازطراحی حکمرانی هویت رقومی (دیجیتال)، پایه‌های تقنینی لازم را فراهم ساخته، زیرساخت‌های فنی تعامل‌پذیر ایجاد کند، و از همه مهم‌تر، شهروند را به‌عنوان بازیگر اصلی در مرکز این نظام بازتعریف نماید.

بر این اساس، در گزارش حاضر، پیشنهادات سیاستی در چهار محور بنیادین ذیل به‌صورت منسجم و قابل اجرا ارائه می‌شود:

- **الزام‌های تقنینی:** ایجاد چارچوب قانونی جامع، مبتنی بر حقوق داده، سطح‌بندی فنی اعتماد و مسئولیت‌پذیری نهادهای مجاز در صدور و بکارگیری هویت رقومی (دیجیتال).
- **الزام‌های اجرایی و نهادی:** طراحی ساختار حکمرانی چندلایه با معرفی نهاد تنظیم‌گر مستقل، نهادهای تخصصی صدور، و معرفی یا ایجاد شورای هماهنگی ملی میان بازیگران کلیدی.

– **راهکارهای فنی و زیرساختی:** توسعه زیرساخت‌های متن‌باز، APIهای استاندارد، کیف‌پول هویتی رقومی (دیجیتال) و ابزارهای مدیریت رضایت داده توسط کاربر.

– **سیاست‌های فرهنگی و آموزشی:** ارتقای سواد رقومی (دیجیتال) عمومی، آموزش کارمندان و مدیران اجرایی و ترویج فرهنگ حفاظت از داده به‌عنوان یک حق شهروندی.

این چهار محور، نه به‌صورت موازی، بلکه در ارتباطی پیوسته و مرحله‌بندی‌شده باید اجرا شوند. تنها در چنین ساختاری است که می‌توان به استقرار یک نظام احراز هویت ملی فراگیر، پایدار، اعتمادمحور و هم‌راستا با استانداردهای بین‌المللی امید داشت.

۱ـ۶. الزام‌های تقنینی: بنیان حقوقی حکمرانی هویت رقومی (دیجیتال) در ایران

استقرار یک نظام احراز هویت رقومی (دیجیتال) فراگیر، قابل اعتماد و تعامل‌پذیر در ایران، در درجه اول مستلزم ایجاد زیربنای حقوقی شفاف، منسجم و روزآمد است. در حال حاضر، چارچوب تقنینی کشور در این حوزه نه‌تنها دارای خلاءهای قانونی است، بلکه متشکل از اسنادی پراکنده، و عمدتاً فاقد ضمانت اجرایی مشخص است. این ضعف‌های نظام احراز هویت رقومی کشور، سبب بلاتکلیفی نهادهای اجرایی، کندی نوآوری و کاهش اعتماد کاربران می‌شود. ازاین‌رو، الزام‌های تقنینی باید در سه محور کلان تحلیل و بازطراحی شوند: (۱) قانونگذاری پایه‌ای (۲) هم‌راستاسازی با قوانین کلیدی موجود و (۳) طراحی ساختارهای الزام‌آور برای سطح‌بندی و حفاظت از داده.

۱-۱-۶. قانون‌گذاری پایه‌ای: گذار از آیین‌نامه‌ها به تدوین قانون ملی هویت رقومی (دیجیتال)

نقطه شروع در مسیر ایجاد یک نظام احراز هویت رقومی (دیجیتال) قابل اتکا در ایران، عبور از وضعیت فعلی مقررات پراکنده و ورود به مرحله تدوین قانونی جامع، فراگیر و الزام‌آور است که نه‌تنها مفاهیم را روشن سازد، بلکه مسئولیت‌ها، حقوق، حدود فنی، سازوکارهای تنظیم‌گری و نیز ضمانت‌های اجرایی را به‌صورت صریح و قابل اجرا مشخص کند. فقدان چنین قانونی، در حال حاضر به سردرگمی نهادی، بلاتکلیفی فنی، کندی نوآوری بخش خصوصی و کاهش اعتماد کاربران انجامیده است. این قانون، باید واجد ابعاد ذیل باشد.

الف) تعریف مفاهیم بنیادین و چارچوب نظری

قانون پیشنهادی باید نخست، تعاریف کلیدی و مشترک را به‌روشنی تبیین کند. این تعاریف، مبنای تفسیر حقوقی، پیاده‌سازی فنی، و هم‌فهمی نهادی خواهند بود. از جمله:

- **هویت رقومی (دیجیتال)** : مجموعه‌ای از داده‌ها، صفات و اعتبارات منتسب به یک فرد، که به‌صورت رقومی (دیجیتال) و از طریق مرجع معتبر صادر می‌شود.
- **احراز هویت چندعاملی:** فرآیندی برای تصدیق هویت از طریق ترکیبی از عوامل دانشی (رمز)، دارایی (توکن یا سیم‌کارت) و بیومتریک.
- **سطح اطمینان:** میزان اعتمادپذیری فرآیند احراز هویت بر حسب ریسک، در چهار سطح اصلی.
- **ارائه‌دهنده خدمات هویتی:** شخص حقیقی یا حقوقی دارای مجوز رسمی برای صدور، نگهداری و تصدیق هویت رقومی (دیجیتال) .
- **شناسه معتبر:** شناسه یکتای حقوقی یا حقیقی که از سوی مرجع صلاحیت‌دار صادر شده و دارای آثار قانونی است.
- **قابلیت تعمیم‌پذیری فرامرزی:** توان نظام هویتی برای پذیرش یا به‌رسمیت‌شناختن استانداردهای بین‌المللی یا هویت‌های خارجی (به‌ویژه در تجارت، سرمایه‌گذاری، سلامت و آموزش).

این تعاریف باید به‌گونه‌ای تدوین شوند که قابلیت رجوع متقن برای نهادهای اجرایی و قضایی را داشته باشند و از تفسیرهای متضاد جلوگیری کنند.

ب) ساختار نهادی و تعیین مسئولیت‌ها در سطوح مختلف

برای جلوگیری از تداخل وظایف و اجرای جزیره‌ای، لازم است قانون، ساختار نهادی منسجمی را برای حکمرانی هویت رقومی (دیجیتال) پیش‌بینی کند:

- **سطح سیاست‌گذاری کلان (نهاد راهبردی):** شورای عالی فضای مجازی یا مرکز ملی فضای مجازی به‌عنوان مرجع سیاست‌گذار ملی و مسئول تصویب راهبردها.
- **سطح تنظیم‌گری فنی و حقوقی:** سازمان فناوری اطلاعات ایران، همراه با تنظیم‌گری حوزه‌های خاص (مانند بانک مرکزی، وزارت ارتباطات، وزارت بهداشت)، با وظیفه تعیین استانداردهای فنی، صدور مجوز فراهم‌آوران ID ها، نظارت بر امنیت داده‌ها، و تضمین رعایت مقررات.
- **سطح اجرایی و عملیاتی:** ثبت‌احوال، دستگاه‌های اجرایی، اپراتورها، بانک‌ها و سکوهای رقومی (دیجیتال) با مسئولیت اجرا، انطباق فنی و به‌کارگیری خدمات احراز هویت.
- **سطح مشارکت خصوصی و نوآوری:** شرکت‌های فناوری و ارائه‌دهندگان خصوصی که از طریق مجوز رسمی، در صدور و تصدیق هویت رقومی (دیجیتال) فعالیت می‌کنند.

این تفکیک، باید همراه با تعیین دقیق حوزه اختیارات، سازوکار تعامل‌پذیری بین نهادها، و سازوکار پاسخ‌گویی حقوقی باشد.

ج) گنجاندن صریح و الزام‌آور حقوق کاربر

یکی از پیش‌شرط‌های جلب اعتماد عمومی، تصدیق و تضمین حقوق کاربران در سطح قانون است. در مدل مطلوب، کاربر نه صرفاً دریافت‌کننده خدمت، بلکه صاحب داده و اختیارکننده مسیر گردش آن تلقی می‌شود. مهم‌ترین حقوقی که باید در متن قانون تضمین شوند عبارت‌اند از:

- رضایت آگاهانه و قابل استناد کاربر پیش از صدور یا استفاده از داده‌های هویتی.
- حق اطلاع‌رسانی درباره نوع، دامنه و هدف استفاده از داده‌ها.
- حق مشاهده و مدیریت داده‌های ذخیره‌شده در پایگاه هویت رقومی (دیجیتال).
- حق اصلاح یا حذف داده‌های هویتی نادرست یا منقضی.
- حق اعتراض و شکایت در برابر استفاده بدون مجوز، نشت یا تبعیض ناشی از تحلیل داده.
- حق جبران خسارت از طریق هیأت‌های داوری، نهادهای تنظیم‌گر یا دادگاه‌های تخصصی.

د) تدوین نظام ضمانت اجرا، پیگیری قضایی و پیشگیری از سوءاستفاده

در فقدان ضمانت اجرا، قانون قابلیت الزام‌آوری ندارد. قانون احراز هویت رقومی (دیجیتال) باید دارای ساختار اجرایی حقوقی در سه سطح باشد:

- **ضمانت‌های مدنی:** امکان شکایت و مطالبه خسارت از فراهم‌آوران ID ها یا دستگاه‌هایی که حقوق افراد را نقض می‌کنند.
- **ضمانت‌های کیفری:** تعریف جرایم خاص مانند جعل هویت رقومی (دیجیتال)، نشت عمدی داده، استفاده غیرمجاز از داده حساس.
- **ضمانت‌های اداری و تنظیم‌گرانه:** تعلیق مجوز، جریمه مالی، محدودیت دسترسی به داده‌ها، تعلیق تعامل بین‌سازمانی برای دستگاه‌های متخلف.

همچنین، پیش‌بینی سازوکار حل اختلاف از طریق نهادهای داوری تخصصی همچون کارگروه تعامل‌پذیری دولت الکترونیک می‌تواند از اطاله دادرسی در دادگاه‌ها جلوگیری کند.

۲-۱-۶. هم‌راستاسازی با قوانین کلیدی موجود

تقنین در حوزه احراز هویت رقومی (دیجیتال) نمی‌تواند و نباید به‌عنوان جزیره‌ای مستقل از سایر قوانین پایه و حاکمیتی عمل کند. تجربه کشورهای موفق در طراحی زیرساخت‌های اعتماد رقومی (دیجیتال)، نظیر مقررات eIDAS اروپا یا الگوی فدراتیو استرالیا، نشان می‌دهد که هم‌راستاسازی دقیق تقنین هویت رقومی (دیجیتال) با قوانین کلان داده، امنیت ملی، اقتصاد رقومی (دیجیتال) و حقوق کاربر، پیش‌نیاز موفقیت اجرایی و مقبولیت اجتماعی چنین نظام‌هایی است.

در ایران نیز، طی سال‌های اخیر چند سند بالادستی و راهبردی تصویب شده است که ظرفیت ممتازی برای «یکپارچه‌سازی حکمرانی داده و هویت رقومی (دیجیتال) » فراهم کرده‌اند. این ظرفیت‌ها اگر به‌درستی در قانون‌گذاری برای احراز هویت رقومی (دیجیتال) لحاظ نشوند، می‌توانند به تداخل و تضاد اجرایی منجر شوند.

الف) قانون مدیریت داده‌ها و اطلاعات ملی: ستون فقرات تعامل‌پذیری بین‌دستگاهی

قانون مدیریت داده‌ها و اطلاعات ملی (مصوب مجلس شورای اسلامی)، به‌عنوان مرجع رسمی تقنینی تعریف داده‌های مرجع، تعامل‌پذیری دستگاه‌ها و تنظیم روابط تبادل داده در ایران محسوب می‌شود. در این قانون:

- داده‌های مرجع (شامل اطلاعات هویتی، مالیاتی، مالکیتی و سازمانی) تعریف و نهادهای مالک داده مشخص شده‌اند (مثلاً ثبت احوال برای اطلاعات تابعیت و هویت پایه).
- کارگروه تعامل‌پذیری به‌عنوان مرجع تنظیم‌گر برای هماهنگی و نظارت بر تبادل داده میان دستگاه‌ها تعیین شده است.
- الزام‌های امنیتی، ثبت رویداد، کنترل دسترسی، و مستندسازی مسیر استفاده از داده‌ها به‌عنوان شرط تعامل داده‌ای مطرح شده‌اند.
- استانداردسازی قالب‌های داده، سطح‌بندی مجوزها، و تفکیک نقش دستگاه‌های منشأ و مصرف‌کننده مورد تأکید قرار گرفته است.

ب) اسناد بالادستی امنیتی و پدافند غیرعامل: بُعد تاب‌آوری و امنیت زیرساختی

مسئله احراز هویت رقومی (دیجیتال) نه‌تنها یک چالش فنی یا خدماتی، بلکه موضوعی راهبردی در امنیت ملی و پایداری حکمرانی رقومی (دیجیتال) کشور است. به‌همین دلیل، اسناد امنیتی نظیر:

- الزام‌های مرکز مدیریت راهبردی افتا برای امنیت سامانه‌های حیاتی؛
- الزام‌های مصوب پدافند غیرعامل در حوزه زیرساخت‌های حیاتی و فضای سایبر؛
- چارچوب‌های امنیتی مرکز ماهر برای حفاظت از داده‌های حساس؛

باید به‌صورت دقیق در تدوین قانون احراز هویت لحاظ شوند. این موضوع به‌ویژه در موارد زیر اهمیت دارد:

- تعیین سطح الزامی اطمینان برای خدمات حیاتی مانند رأی‌گیری رقومی (دیجیتال)، زیرساخت پرداخت الکترونیک، خدمات مالی، بانکی و بورس و نظام سلامت؛
- الزام‌های احراز چندعاملی و استفاده از توکن سخت‌افزاری یا احراز زیستی در سطوح بالا؛
- نیاز به معماری مقاوم در برابر قطع ارتباط، نفوذ، یا نشت گسترده داده‌های هویتی؛
- تعیین سطح دسترسی نهادهای حساس در شرایط بحران یا جنگ سایبری.

بدون پیوست امنیتی و الزام به رعایت استانداردهای امنیتی ملی، زیرساخت هویت رقومی (دیجیتال) کشور ممکن است در برابر تهدیدات داخلی و خارجی آسیب‌پذیر باشد.

۳-۱-۶. طراحی ساختارهای الزام‌آور برای سطح‌بندی و حفاظت از داده‌ها

یکی از مهم‌ترین الزام‌های حکمرانی مؤثر در احراز هویت رقومی (دیجیتال)، تدوین یک چارچوب الزام‌آور و آزمون‌پذیر برای تعیین سطح اطمینان و حفاظت از داده‌های هویتی است. تجربه کشورهای پیشرو نشان می‌دهد که صرفاً تدوین قانون یا ساخت زیرساخت فنی، بدون الزام دستگاه‌ها و ارائه‌دهندگان خدمات به رعایت استانداردهای سطح‌بندی و حفظ داده، به اجرای ناقص و بی‌اعتمادی عمومی منجر خواهد شد. در ایران نیز، فقدان چارچوب فراگیر و رسمی درباره سطح‌بندی اطمینان (LOA) و نبود الزام‌های حقوقی مشخص برای حفاظت از داده‌های هویتی، موجب ابهام در تفکیک ریسک خدمات و رفتار سلیقه‌ای دستگاه‌ها می‌شود. برای رفع این شکاف، طراحی ساختارهای الزام‌آور باید در سه لایه مکمل صورت گیرد:

الف) طراحی و الزام‌آوری چارچوب سطح‌بندی اطمینان بر اساس ریسک خدمت

چارچوب سطح‌بندی اطمینان باید به‌صورت رسمی و با استناد به استانداردهای بین‌المللی در متن مقررات گنجانده شود و کاربرد آن در انواع

خدمات بر اساس سطح حساسیت الزامی شود.

هر سطح باید دارای چک‌لیست اجرایی، آزمون‌پذیر و قابل نظارت باشد و ارائه‌دهندگان خدمات موظف به رعایت آن شوند. سازمان نظارتی مرکزی (پیشنهادی: سازمان فناوری اطلاعات یا تنظیم‌گر بخشی داده‌های هویتی) باید مأمور کنترل انطباق و صدور گواهینامه‌های سطح‌بندی شود.

ب) تعیین الزام‌های حقوقی و فنی حفاظت از داده‌های هویتی

حفاظت از داده‌های هویتی باید در دو لایه حقوقی و فنی صورت گیرد:

از منظر حقوقی:

- الزام به رضایت آگاهانه، محدودیت هدف، تناسب داده و حق لغو یا اصلاح در همه تراکنش‌های هویتی؛
- ممنوعیت ذخیره‌سازی بلندمدت یا پردازش ثانویه بدون مجوز خاص کاربر؛
- پیش‌بینی ضمانت‌های اجرایی و کیفری برای تخطی از مقررات حفظ داده؛
- الزام به تسویه‌حساب رقومی (دیجیتال) داده‌ها در پایان رابطه کاربر و خدمت دهنده؛

از منظر فنی:

- پیاده‌سازی سامانه‌های ثبت مسیر استفاده از داده‌ها با قابلیت رهگیری جزییات دسترسی، تغییر، و تبادل؛
- استفاده از رمزنگاری انتها به انتها، سامانه‌های احراز مبتنی بر سخت‌افزار امن و کیف‌پول‌های رقومی (دیجیتال) امن برای ذخیره شناسه‌ها؛
- محدودسازی دسترسی سطوح پایین سیستمی به داده‌های حساس از طریق معماری تفکیک نقش و حداقل دسترسی؛
- الزام به انجام ارزیابی تأثیر حفاظت از داده‌ها برای هر سامانه بزرگ هویتی؛

این الزام‌ها باید با قانون مدیریت داده‌ها و اطلاعات ملی، اسناد پدافند غیرعامل، و دستورالعمل‌های افتا هم‌راستا شوند.

ج) ایجاد سازوکار نظارت، ارزیابی و انطباق‌سنجی سطح اطمینان

سازوکارهای نظارت مستقل و بازخورد اصلاحی باید شامل موارد ذیل باشند:

- یک مرجع ملی صدور گواهی سطح اطمینان برای ارائه‌دهندگان خدمات هویتی ایجاد شود؛
- گزارش‌های سالانه انطباق، شاخص‌های سطح پذیرش و پایش نشت داده در خدمات عمومی منتشر شود؛
- سازوکار «برچسب سطح اطمینان» برای اپلیکیشن‌ها، سکوها و نهادهای دولتی و خصوصی تعریف و بر اساس آن، مشوق‌های رتبه‌بندی و مجوز بهره‌برداری اعطا گردد؛
- کمیته یا دبیرخانه‌ای مستقل برای بررسی شکایات کاربران، آسیب‌پذیری‌ها و تطبیق سطح‌بندی با شرایط بازار تشکیل شود؛

سطح‌بندی دقیق خدمات، همراه با الزام‌های حفاظت از داده و نظارت مستقل، بنیاد اعتماد رقومی (دیجیتال) میان کاربر، دولت و کسب‌وکارها را شکل می‌دهد. با چنین رویکردی، نظام احراز هویت رقومی (دیجیتال) ایران می‌تواند به ستون فقرات حکمرانی داده و زیربنای امن برای اقتصاد رقومی (دیجیتال)، سلامت هوشمند، دولت رقومی (دیجیتال) و امنیت سایبری تبدیل شود.

۲ـ۶. الزام‌های اجرایی و نهادی: استقرار حکمرانی چندلایه و منعطف

در حوزه احراز هویت رقومی (دیجیتال)، تجارب جهانی مانند نهاد eIDAS Board در اتحادیه اروپا یا RAK Identity Authority در امارات نشان داده‌اند که موفقیت به وجود مرجع تنظیم‌گر مستقل، ساختار بین‌نهادی هماهنگ، و پاسخ‌گویی دقیق نهادی وابسته است.

در ایران نیز، خلاء چنین ساختاری باعث شده اسناد مختلف (از ثبت‌احوال تا کارگروه تعامل‌پذیری و بانک مرکزی) اقدامات جزیره‌ای را به دنبال داشته باشد. برای برون‌رفت از این وضعیت، چهار اقدام کلیدی ضروری است:

الف) انتخاب و معرفی نهاد تنظیم‌گر فراگیر در حوزه احراز هویت رقومی

این نهاد باید:

- مستقل از ساختارهای بخشی موجود (مانند وزارت ارتباطات یا بانک مرکزی) باشد، اما با آن‌ها همکاری نهادی داشته باشد؛
- دارای وظایف مشخص شامل سیاست‌گذاری، صدور مجوز، ارزیابی انطباق، رسیدگی به تخلفات، پایش اجرای سطوح اطمینان و تعامل فراملی باشد؛
- با شخصیت حقوقی عمومی غیردولتی یا در قالب «سازمان تنظیم‌گر تخصصی فضای مجازی» طراحی شود تا استقلال، پاسخ‌گویی و انعطاف لازم را دارا باشد؛

ب) تدوین نقشه راه ملی برای اجرای هویت رقومی (دیجیتال)

این نقشه راه باید شامل موارد ذیل باشد:

- اولویت‌بندی خدمات حساس (بانک، ارتباطات، سلامت، آموزش، رأی‌گیری)؛
- زمان‌بندی فازبندی‌شده، مشخص شدن شاخص‌های عملکرد و تعریف ریسک هر خدمت بر اساس سطح اطمینان موردنیاز؛
- پیش‌بینی منابع مالی پایدار برای اجرای زیرساخت‌های احراز و مشوق برای پیوستن بخش خصوصی به آن؛
- هماهنگی با برنامه هفتم توسعه، مستندات «دولت هوشمند» و مستندات پدافند غیرعامل در حوزه هویت؛

ج) ایجاد ساختار پاسخ‌گویی نهادی به شهروندان

برای این منظور باید اقدامات ذیل انجام شود:

- سامانه ثبت و پیگیری شکایات رقومی (دیجیتال) در حوزه احراز ایجاد شود؛
- سازوکارهای مستقل رسیدگی (شورای داوری یا نهاد ناظر مردمی) برای بررسی تخلفات دستگاه‌ها در برابر کاربران پیش‌بینی شود؛
- ابزارهای عمومی اطلاع‌رسانی، آموزش و ارتقای سواد هویت رقومی (دیجیتال) در جامعه ترویج یابد.

۳ـ۶. راهکارهای فنی و زیرساختی: بنیان رقومی اعتماد و تعامل‌پذیری

قانون و نهاد بدون زیرساخت فناورانه، عملیاتی نمی‌شود. به همین دلیل، طراحی سکوهای ملی، مقیاس‌پذیر، امن و تعامل‌پذیر برای صدور، اعتبارسنجی، و بکارگیری هویت رقومی (دیجیتال)، شرط لازم اجرای موفق هر قانون مرتبط با هویت رقومی است. در ادامه چند راهکار زیرساختی اثربخش ذکر می‌شود.

الف) کاهش وابستگی به سیم‌کارت به‌عنوان عامل شناسایی و احراز

احراز هویت مبتنی بر شماره تلفن همراه به دلیل امکان واگذاری آزاد سیم‌کارت، استفاده از سیم‌کارت‌های غیرمعتبر یا ثبت‌شده به نام دیگران، و نبود الزام به حضور فیزیکی مالک، ناامن و پرریسک است. سامانه‌های ملی نباید سیم‌کارت را «مرجع هویت» تلقی کنند، بلکه صرفاً یک «عامل کمکی» برای ابلاغ اعلان‌ها و ارتباط باشند. لازم است جایگزین‌های امن‌تری مانند کیف پول هویت رقومی (دیجیتال)، گواهی‌های مبتنی بر PKI، و احراز چندعاملی بیومتریک به همراه توکن سخت‌افزاری به‌صورت اجباری برای خدمات حساس طراحی و پیاده‌سازی شوند. تجربه کشورهای پیشرفته نشان داده است که اتکا به سیم‌کارت تنها در کنار یک «شناسه رقومی واحد و رسمی» قابل قبول است، نه به‌عنوان مبنای اصلی شناسایی.

ب) توسعه سکوی ملی مدیریت هویت و امضای رقومی

سامانه‌های صدور هویت رقومی (دیجیتال) با قابلیت اتصال به مرجع‌های مختلف (ثبت‌احوال، ثبت شرکت‌ها، بانک مرکزی،...) طراحی شود. این سامانه باید از قابلیت صدور، تعلیق، و ابطال شناسه‌ها برخوردار باشد و امکان اتصال به کیف‌پول هویت رقومی (دیجیتال)، امضای رقومی (دیجیتال) و سامانه‌های مالی و قضایی را داشته باشد.

ج) طراحی و انتشار APIهای باز (Open API)

برای تحقق تعامل‌پذیری بین‌دستگاهی و بین‌المللی، باید مجموعه‌ای از APIهای استاندارد برای:

- بانک‌ها، بیمه‌ها، سکوهای تجارت الکترونیک، نهادهای عمومی؛
- اپلیکیشن‌های خدمات شهری، سلامت، آموزش، و اشتغال؛
- سکوهای بین‌المللی

ارائه شود. همچنین مستندات فنی، مرکز تست سازگاری، و فرآیند صدور گواهی تعامل‌پذیری باید ایجاد گردد.

د) استقرار سامانه ملی مدیریت رضایت کاربر

با توجه به اصول حکمرانی داده و الزام به رضایت آگاهانه، لازم است:

- سامانه‌ای ایجاد شود که کاربر بتواند مشاهده، لغو، یا محدودسازی دسترسی سازمان‌ها به داده‌های خود را کنترل کند.
- در هر مرحله از احراز، پیامک /اعلان رقومی تأیید رضایت برای کاربر ارسال شود.
- تاریخچه و مسیر استفاده از داده‌های کاربر، به‌صورت شفاف و دائمی قابل مشاهده باشد.

ه) پشتیبانی از تنوع روش‌های احراز متناسب با ریسک خدمت

- سطوح مختلف احراز (از رمز یک‌بار مصرف OTP تا بیومتریک و توکن سخت‌افزاری) باید در زیرساخت در نظر گرفته شود.
- کاربر اختیار انتخاب روش احراز متناسب با سطح خدمات را داشته باشد.
- خدمات حساس مانند افتتاح حساب، رأی‌گیری، یا پرداخت‌های بالای یک حد خاص، احراز چندعاملی بیومتریک به همراه توکن سخت‌افزاری را الزام کنند.

و) هم‌سویی با استانداردهای امنیتی و رمزنگاری

- زیرساخت امضای رقومی (دیجیتال) و کلید عمومی (PKI) باید بر اساس استانداردهای جهانی و اسناد ملی افتا طراحی شود.
- مراکز صدور گواهی رقومی باید دارای گواهینامه امنیتی ملی و در صورت امکان گواهینامه بین‌المللی باشند.
- راهکارهای حفاظت از هویت در برابر حملات جعل، افشا، و مهندسی اجتماعی باید در طراحی سکو لحاظ شوند.

۴ـ۶. سیاست‌های فرهنگی و آموزشی: بسترسازی اجتماعی برای پذیرش، اعتماد و کاربرد

استقرار موفق نظام احراز هویت رقومی (دیجیتال)، صرفاً تابع الزام‌های فنی یا تقنینی نیست، بلکه پذیرش اجتماعی، اعتماد عمومی، و ارتقای فرهنگ داده‌محور نقش بنیادینی در تداوم و اثربخشی آن ایفا می‌کند. تجربه‌های جهانی مانند امارات نشان داده‌اند که هرجا کاربران درک روشن از منافع، حقوق و الزام‌های امنیتی داشته‌اند، میزان استفاده، مشارکت و رضایت‌مندی به‌طور محسوسی افزایش یافته است.

در ایران، سیاست‌های فرهنگی و آموزشی باید به‌عنوان «لایه زیرین حکمرانی هویت رقومی (دیجیتال) » مورد توجه قرار گیرند. سیاست‌های فرهنگی و آموزشی نظام احراز هویت رقومی با اقدامات ذیل قابل پیگیری است:

الف) تدوین برنامه ملی ارتقای سواد داده و آگاهی شهروندی

ایران نیازمند یک برنامه هماهنگ، میان‌مدت و بین‌نهادی در زمینه آموزش عمومی هویت رقومی (دیجیتال) است. این برنامه باید با مشارکت نهادهایی مانند وزارت آموزش و پرورش، صدا و سیما، وزارت علوم، وزارت ارتباطات و مرکز ملی فضای مجازی تدوین شود. این برنامه، مفاهیم پایه‌ای مانند شناسه رقومی (دیجیتال)، رضایت داده، امضای رقومی (دیجیتال)، مخاطرات فیشینگ، ریسک به‌اشتراک‌گذاری داده‌ها، رمز دومرحله‌ای و امنیت بیومتریک را آموزش دهد. همچنین، گروه‌های مختلف (دانش‌آموز، دانشجو، کارمند دولت، سالمند، کاربر عادی اینترنت) را به‌صورت تفکیکی هدف‌گذاری کند. این برنامه باید رسانه‌های عمومی، محتوای ویدیویی، کتابچه راهنما، اینفوگرافیک و شبکه‌های اجتماعی را به‌عنوان بستر آموزش هم‌زمان و فراگیر به‌کار گیرد. همچنین با تدوین چارچوب ارزیابی ملی سواد داده در برنامه مذکور، امکان سنجش

پیشرفت سالانه جامعه در آگاهی رقومی (دیجیتال) فراهم شود.

ب) آموزش تخصصی برای نیروهای کلیدی

به‌منظور افزایش شناخت فنی مشترک و ارتقای توان تخصصی نیروی انسانی، پیشنهاد می‌شود برای کارکنان دولت، بانک‌ها، دفاتر خدمات عمومی، شرکت‌های فناوری اطلاعات، و نهادهای ناظر دوره‌های تخصصی در حوزه‌های زیر برگزار شود:

- آشنایی با قوانین مرتبط با احراز هویت رقومی و حقوق داده؛
- الزام‌های سطح‌بندی اطمینان و روش‌های پیاده‌سازی فنی؛
- تعامل با سامانه‌های احراز در خدمات عمومی (امنیت، سلامت، مالیات، رفاه، انتخابات و...)؛
- ارزیابی انطباق با قانون مدیریت داده‌ها و اطلاعات ملی و مقررات حمایت از داده‌های شخصی؛

لازم است که دانشگاه‌ها، مراکز آموزش مدیریت دولتی، سازمان فناوری اطلاعات، سازمان پدافند غیرعامل این آموزش‌ها را ساختارمند و با ارایه گواهی ارائه کنند. همچنین، دانش‌افزایی مستمر برای توسعه‌دهندگان نرم‌افزار و مدیران امنیت اطلاعات، مورد توجه قرار گیرد.

ج) تولید محتوای بومی‌سازی‌شده، کاربردی و چندرسانه‌ای برای آموزش عمومی

مفاهیم انتزاعی احراز هویت رقومی (دیجیتال) اگر با زبان فنی و رسمی ارائه شوند، نه‌تنها مخاطب را جذب نمی‌کنند، بلکه ممکن است مقاومت ایجاد کنند. بنابراین باید محتوای آموزشی به زبان ساده، تصویری، و حتی داستان‌محور تولید شود تا برای عموم مردم قابل‌فهم، جذاب، و عملیاتی باشد.

د) ترویج فرهنگ احترام به حریم خصوصی و داده‌های شخصی

یکی از خلأها، کم‌توجهی به حقوق داده و مالکیت کاربران بر اطلاعات شخصی است. برای اصلاح این رویکرد، سیاست‌های زیر پیشنهاد می‌شود:

- الزام سازمان‌ها به تدوین کد اخلاق داده و گنجاندن بندهای حقوق کاربر در قراردادها و سیاست‌های خدمات.
- تقویت گفتمان عمومی درباره «حریم خصوصی در عصر رقومی (دیجیتال)» از طریق برنامه‌های تلویزیونی، میزگردهای تخصصی، رسانه‌های اجتماعی، و حضور چهره‌های علمی و فرهنگی.
- آموزش مسئولیت‌پذیری داده در سطوح مختلف مانند: مدیر سیستم، توسعه‌دهنده، ناظر دولتی، و حتی کارمند عادی در سازمان‌ها.
- ارتقای سواد حقوقی کاربران در حوزه رضایت، شکایت، و پیگیری قضایی نقض داده، با همکاری قوه قضائیه، نهادهای حمایت از حقوق مصرف‌کننده، و وکلا.

جدول ۶. پیشنهاد توصیه سیاستی ویژه گزارش‌های راهبردی / نظارتی

ردیف	نوع توصیه		توصیه سیاستی	الزام‌ها و قیود اجرایی	دستگاه متولی	دستگاه معین	زمان‌بندی اجرا (کوتاه‌مدت، میان‌مدت، بلندمدت)	ملاحظات
	تداوم*	اصلاح**						
۱		*	تدوین قانون جامع احراز هویت رقومی (دیجیتال) با تصریح مفاهیم، حقوق کاربر و سطح‌بندی خدمات	هماهنگی با قانون مدیریت داده‌ها و اطلاعات ملی، و اسناد مرتبط با حمایت از داده و اسناد امنیتی	وزارت ارتباطات / مرکز ملی فضای مجازی	سازمان ثبت احوال، بانک مرکزی، مرکز افتا	میان مدت	نیازمند اجماع نخبگانی و بازبینی اسناد قانونی موجود
۲		*	انتخاب و معرفی نهاد مستقل تنظیم‌گر احراز هویت رقومی (دیجیتال) با اختیارات قانونی و تعامل‌بین‌نهادی	تضمین استقلال ساختاری، تأمین بودجه و تصویب جایگاه قانونی	مرکز ملی فضای مجازی	وزارت ارتباطات، بانک مرکزی، ثبت احوال	کوتاه مدت	ریسک تداخل نهادی و مقاومت دستگاه‌های موجود

ردیف	نوع توصیه		توصیه سیاستی	الزام‌ها و قیود اجرایی	دستگاه متولی	دستگاه معین	زمان‌بندی اجرا (کوتاه‌مدت، میان‌مدت، بلندمدت)	ملاحظات
	تداوم*	اصلاح**						
۳	*		توسعه زیرساخت صدور و ابطال هویت رقومی (دیجیتال) با API باز و سامانه مدیریت رضایت	رعایت اصول رابط کاربری، تعامل‌پذیری، و امنیت زیرساخت	سازمان فناوری اطلاعات ایران	وزارت ارتباطات، کاروران، فراهم‌آورندگان IDها	میان مدت	تأمین مالی پروژه‌های زیرساختی و شفافیت در API
۴	*		اجرای برنامه ملی ارتقای سواد داده و آموزش عمومی مفاهیم هویت رقومی (دیجیتال)	پوشش گروه‌های سنی و سواد مختلف، مشارکت نهادهای آموزشی و رسانه‌ها	وزارت آموزش و پرورش / وزارت ارتباطات	صدا و سیما، وزارت علوم، مرکز ملی فضای مجازی	بلندمدت	لزوم تغییر رویکرد فرهنگی به مالکیت داده در سطح جامعه
۵		*	ایجاد مرجع ملی صدور گواهی سطح اطمینان و پایش مستمر نشت احتمالی داده‌ها	استفاده از شاخص‌های سنجش انطباق، گزارش‌گیری عمومی، و نظارت مستقل	سازمان فناوری اطلاعات	مرکز ملی فضای مجازی، دادستانی، شورای عالی فضای مجازی	میان مدت	پایداری نهادی مرجع نظارت و الزام اجرای برچسب اطمینان
۶	*		الزام رعایت الزامات امنیتی و پدافند غیرعامل در طراحی سامانه‌های هویتی	هماهنگی با مرکز افتا، الزام‌های پدافند غیرعامل و طراحی معماری مقاوم	مرکز افتا / سازمان پدافند غیرعامل	مرکز ماهر، شرکت‌های فناوری، وزارت کشور	کوتاه مدت	ضرورت تطبیق با تهدیدات سایبری و تاب‌آوری ملی

* تداوم یا تقویت آیتم‌ها یا اقدام.ات
** اصلاح رویه‌ها یا ایجاد سازوکارها.

منابع و مآخذ

[1] W. E. Forum, “Digital Identity Ecosystems: Unlocking New Value”, 2021. [Online]. Available: https://www3.weforum.org/docs/WEF_Guide_Digital_Identity_Ecosystems_2021.pdf

[2] J. Research, “Digital Identity Verification Market: 2024-2029”, 2024. [Online]. Available: https://www.juniperresearch.com/research/fintech-payments/identity/digital-identity-/verification-research-report

[۳] مرکز پژوهش‌های مجلس، بررسی لایحه برنامه هفتم توسعه (۷۷): رصد و نظارت بر پروژه استقرار هویت هوشمند اشخاص حقیقی در دولت الکترونیک. 1402. [Online]. Available: https://rc.majlis.ir/fa/report/show/1787124

[۴] م. پ. ه. مجلس، «استفاده از شماره ملی در نظام احراز هویت و یکپارچگی سامانه‌های دولت»، ۱۳۹۹. [Online]. Available: https://rc.majlis.ir/fa/report/show/1624832

[۵] م. پ. ه. مجلس، پروژه سازمان ثبت احوال کشور «ارائه خدمات الکترونیکی هویت ملی»، ۱۳۸۵. [Online]. Available: https://rc.majlis.ir/fa/report/show/734220

[۶] آیین‌نامه اجرایی ماده (۱۴) الحاقی قانون مبارزه با پولشویی، ۱۳۹۸.

[۷] نظام هویت معتبر، ۱۳۹۸.

[۸] مصوبات یازدهمین جلسه شورای اجرایی فناوری اطلاعات، ۱۳۹۷.

[۹] هیات وزیران، «سند راهبردی نظام جامع فناوری اطلاعات جمهوری اسلامی ایران»، ۱۳۸۸. [Online]. Available: https://rc.majlis.ir/fa/law/show/136242.

[10] K. Rannenberg, “A framework for identity management (ISO/IEC 24760),” 2011.
[11] C. Sullivan, Digital identity: An emergent legal concept. University of Adelaide Press, 2011.
[12] I. O. f. Standardization, ISO/IEC 27001: 2013: Information Technology--Security Techniques--Information Security Management Systems--Requirements. International Organization for Standardization, 2013.
[13] P. A. Grassi, M. E. Garcia, and J. L. Fenton, “Draft nist special publication 800-63-3 digital identity guidelines, “ National Institute of Standards and Technology, Los Altos, CA, 2017.
[14] OECD, “Digital public infrastructure for digital governments, “ 2024. [Online]. Available: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/12/digital-public-infrastructure-for-digital-governments_11fe17d9/ff525dc8-en.pdf.
[۱۵] قانون برنامه پنجساله هفتم پیشرفت جمهوری اسلامی ایران، ۱۴۰۳.
[16] W. Bank. “Identification for Development.” https://databank.worldbank.org/source/identification-for-development-(id4d)-data (accessed.
[17] FBI, “Internet Crime Complaint Center Releases “, 2022. [Online]. Available: https://www.ic3.gov/AnnualReport/Reports/2022_ic3report.pdf
[18] F. Alliance, “FIDO Alliance White Paper: FIDO for e-Government Services, “ 2022. [Online]. Available: https://fidoalliance.org/wp-content/uploads/2022/12/FIDO-e-Government-White-Paper.pdf
[۱۹] روزنامه ایران, مناطق محروم زیر چتر عدالت ed, 1403.
[۲۰] م. پ. ه. مجلس، «سنجش دیدگاه مردم درباره خدمات الکترونیکی و اینترنتی دولت»، ۱۴۰۳.. [Online]. Available: https://rc.majlis.ir/fa/report/show/1827983
[21] F. Alliance. “FIDO2: Passwordless Authentication Standard.” (accessed.
[22] eIDAS Regulation, 2024.
[23] Aadhaar Act, 2016.
[24] C. Insights. “NSTIC Pilot Common Considerations: 2.” (accessed.
[25] “login.gov.” https://www.login.gov/ (accessed.
[26] S. Reynolds. “China to Verify Citizens’ Identities With New Blockchain-Based Platform.” https://www.coindesk.com/policy/2023/12/12/chinas-ministry-of-public-security-launches-blockchain-based-real-name-decentralized-identifier-system (accessed.
[27] G. Y. Philip Gordon, Morgan Matson, Kwabena Appenteng, and Zoe Argento, “With a Key Deadline Fast Approaching, Now Is the Time to Address the New and Complex Requirements for Data Transfers Outside of China, “ 2023. [Online]. Available: https://www.littler.com/news-analysis/asap/key-deadline-fast-approaching-now-time-address-new-and-complex-requirements-data.
[28] UAE Pass.
[29] UAE Federal Decree Law No. 45/2021, 2021.

گزیده سیاستی

توسعه احراز هویت دیجیتال در ایران نیازمند چارچوب حقوقی جامع، زیرساخت‌های فنی امن، فرهنگ‌سازی عمومی و همکاری هماهنگ دولت و بخش خصوصی است.

مرکز پژوهش‌های مجلس شورای اسلامی

تهران، خیابان پاســـداران، روبروی پـــارک نیاوران (ضلع جنوبی، پلاک ۸۰۲)

تلفن: ۷۵۱۸۳۰۰۰ صندوق پستی: ۱۵۸۷۵-۵۸۵۵ پست الکترونیک: mrc@majles.ir

وب‌سایت: rc@majles.ir