فصلنامه علمی امنیت ملی
سال پانزدهم، شماره پنجاه و پنجم، بهار ۱٤۰٤
مقاله ششم از صفحات ۱۸۰-۱۵۱

مقاله پژوهشی: تدوین راهبردهای حفظ حریم خصوصی داده‌ها در زیرساخت‌های ابری کشور با رویکرد ریسک محور

حمید خضرائیان [۱] شهریار بیژنی[۲] عارف بالی لاشک[۳] و ناصر مدیری [٤]

تاریخ دریافت: ۱٤۰۲/۰۳/۱٤ تاریخ پذیرش: ۱٤۰۲/۱۰/۳۰

چکیده

ظهور رایانش ابری با ویژگی‌هایی چون چند مستاجری، مقیاس‌پذیری و کاهش هزینه، بسیاری از ارائه‌دهندگان فناوری اطلاعات را به استفاده از این فناوری سوق داده است، اما این فناوری با چالش‌های حفظ حریم خصوصی داده‌ها مواجه است. نشت اطلاعات می‌تواند به نقض حریم خصوصی فردی و حتی امنیت ملی منجر شود. باتوجه به فقر در اسناد راهبردی کشور در این زمینه، این پژوهش به بررسی و تدوین راهبردهایی برای حفظ حریم خصوصی در زیرساخت‌های ابری کشور پرداخته است. بدین منظور ضمن بررسی مفاهیم رایانش ابری و حریم خصوصی، تأثیرات بهره‌برداری از رایانش ابری بر روی حریم خصوصی مورد بررسی قرار گرفته و با مطالعه اسناد بین‌المللی و اسناد بالادستی کشور و همچنین استفاده از شبکه مضامین و بر اساس رویکرد PESTLS، ۲۵۰ چالش شناسایی و بعد از دسته‌بندی، ٥٤ چالش عمده احصا و با نظرات خبرگان اولویت‌بندی و ۱۰ چالش با بیشترین مخاطرات نهایی گردید. برای رفع این چالش‌ها، بر اساس چارچوب ITU، ٦ راهبرد اصلی شامل ارتقای فرهنگ، دانش و آگاهی عمومی، طراحی و اجرای نظام جامع، ارتقاء امنیت زیرساخت‌ها، ایجاد سازوکارهای اجرای قوانین، ارتقای همکاری‌های بین‌المللی و فعال‌سازی اقتصاد حریم خصوصی نهایی گردید و در نهایت، ٤۹ راهکار برای حفظ حریم خصوصی در زیرساخت‌های ابری تدوین شد.

کلیدواژه‌ها: حریم خصوصی داده، رایانش ابری، رویکرد ریسک محور، تدوین راهبرد ملی.

[۱] دانش آموخته مقطع دکتری دانشگاه عالی دفاع ملی رایانامه: h.khazraeian@sndu.ac.ir
[۲] استادیار گروه علوم کامپیوتر دانشگاه شاهد، (نویسنده مسئول) رایانامه: bijani@shahed.ac.ir
[۳] استادیار دانشگاه مالک اشتر، رایانامه: a.bali@mut.ac.ir
[٤] دانشیار دانشگاه آزاد زنجان، رایانامه: nassermodiry@chmail.ir

مقدمه و بیان مسئله

با آغاز هزارهٔ سوم، فضای سایبر رشد فزاینده‌ای داشته و این رشد در عرصه‌های مختلف زندگی انسان‌ها تأثیرات غیرقابل انکاری بر جای گذاشته است. با توسعه فضای سایبر و خلق فناوریهای نوظهور در آن، میزان تأثیرگذاری این فناوری به‌صورت تصاعدی افزایش یافته است (کریمی قهرودی، محمدی، و سعادتمند، ۱۴۰۱). رایانش ابری یکی از این فناوریهای نوظهور است.

رایانش ابری[1]در جوامع دانشگاهی و صنعت مورد توجه گسترده‌ای قرار گرفته است. این فناوری تلاش می‌کند تا یک الگوی کارآمد اقتصادی را با توسعه تکاملی بسیاری از رویکردهای موجود و فناوری‌های محاسباتی از جمله خدمات توزیع شده، برنامه‌های کاربردی و زیرساخت‌های اطلاعاتی متشکل از رایانه‌ها، شبکه‌ها و منابع ذخیره‌سازی ادغام کند. برخی ابر را یک انقلاب فنی جدید می‌دانند و برخی دیگر آن را تکامل طبیعی فناوری، اقتصاد و فرهنگ می‌دانند. بااین‌وجود، محاسبات ابری الگوواره[2]بسیار مهمی است که پتانسیل فوق‌العاده‌ای را برای کاهش قابل‌توجه هزینه از طریق بهینه‌سازی و افزایش بهره‌وری اقتصادی و عملیاتی در محاسبات فراهم می‌کند. علاوه بر این، محاسبات ابری این پتانسیل را دارد که همکاری، چابکی و مقیاس‌پذیری را به‌میزان قابل‌توجهی افزایش دهد، بنابراین یک مدل محاسبات جهانی واقعی را بر روی زیرساخت‌های اینترنت امکان‌پذیر می‌کند (Taghavi Zargar, Takabi, & Iyer, 2019).

وزارت امنیت ملی ایالات متحده[3]در سند «مخاطرات امنیتی زیرساخت‌های حیاتی که خدمات ابری استفاده می‌کنند» درصد به‌کارگیری ابر در بعضی از زیرساخت‌های حیاتی آمریکا را در سال ۲۰۱۷ به شرح ذیل اعلام کرده است (DHS, 2017):

1- Cloud Computing
2- Paradigm
3- Department of Homeland Security (DHS)

صنعت ۵۹٪، آموزش ٦۷٪، ارتباطات ۷۸٪، خرده‌فروشی ۷۱٪، بهداشت و درمان ٦۰٪، مالی ۵۵٪، فناوری‌های نوین ۸٦٪

ویژگی‌های ساختاری محیط رایانش ابری عامل اصلی مشکلات امنیتی است. اولاً، گـره‌های درگیر در محاسبات متنوع و پراکنده، توزیع شده‌اند و اغلب قادر به کنترل مؤثر نیستند. دوم، ارائه‌دهندگان خدمات ابری[1](CSP) خطر افشای حریم خصوصی در فرایند انتقال، پردازش و ذخیره‌سازی را دارند. ازآنجاکه محاسبات ابری مبتنی بر فناوری است، آسیب‌پذیری‌های امنیتی فناوری‌های موجود به‌طور مستقیم به یک بستر محاسبات ابری منتقل شده و تهدیدات امنیتی بیشتری ایجاد می‌کند (Sun, 2020).

ممکن است تصور شود دسترسی به اطلاعات خصوصی افراد فقط می‌تواند تأثیرات مخربی برای فرد به‌دنبال داشته باشد، اما تأثیری زیادی بر امنیت ملی ندارد. درحالی‌که سوءاستفاده از اطلاعات کاربران خدمات داخلی، علاوه بر لطمه به کسب و کارهای ارائه‌دهنده خدمات، موجب افزایش عدم اعتماد به خدمات ارائه شده در داخل کشور نیز می‌گردد. همچنین اگر اطلاعات خصوصی مجموعه‌ای از شهروندان مورد دسترسی غیرمجاز قرار گیرد امنیت ملی نیز تحت‌تأثیر قرار می‌گیرد. به‌عنوان مثال درحال حاضر سامانه پایگاه ملی اطلاعات رفاه ایرانیان دربردارنده اطلاعات بسیار مهمی از شهروندان مانند مشخصات فردی، اطلاعات دارایی‌های، اطلاعات شغلی و غیره می‌باشد. نشت این اطلاعات توسط سودجویان یا سرویس‌های اطلاعاتی خارجی منجر به سوءاستفاده‌های آتی آنها و ضربات جبران‌ناپذیری به امنیت و حاکمیت کشور خواهد شد.

در این پژوهش، پژوهشگر با بررسی چالش‌های امنیتی مطرح شده در حوزه حریم خصوصی برای اطلاعات زیرساخت‌های مبتنی بر رایانش ابری، راهکارهای ارتقا امنیت این زیرساخت‌ها در حوزه حریم خصوصی را ارائه و با بررسی وضع موجود، راهبردهای رسیدن به وضع مطلوب را تدوین نموده است.

[1]- Cloud Service Provider (CSP)

اهمیت این پژوهش از آن جهت است که ۱- موجب تدوین راهبردهای ارتقاء امنیت برای اطلاعات زیرساخت‌های ابری کشور و ارائه راهکارهای حفظ حریم خصوصی می‌گردد. ۲- موجب تدوین راهبردهایی می‌شود که متولیان زیرساخت‌های ابری با اشراف بیشتری مسیر بهره‌برداری از فناوری رایانش ابری را طی کنند. ۳- ارائه راهبردها امکان اجرای قوانین صیانت از حریم خصوصی را در محیط ابری کشور ممکن می‌سازد.

از سوی دیگر ضرورت پرداختن به موضوع می‌تواند به دلایل ذیل باشد:

۱- کم‌توجهی به حفظ حریم خصوصی در محیط رایانش ابری باعث تهدیدات جدی علیه اطلاعات زیرساخت‌های ابری کشور و نقض حریم خصوصی داده‌ها در سطح فردی وملی می‌گردد. ۲- عدم وجود راهبردهای حفظ حریم خصوصی اطلاعات در بهره برداری از رایانش ابری و سرویس‌های آن باعث از دست دادن فرصت ارتقا حریم خصوصی اطلاعات زیرساخت‌های ابری کشور و عدم اقبال عمومی در استفاده از ظرفیت‌های داخلی (مانند شبکه‌های اجتماعی) می‌گردد. ۳- حملات علیه محرمانگی و نقض حریم خصوصی که به‌صورت فزاینده‌ای در زیرساخت‌های حیاتی و رایانش ابری در دنیا اتفاق می‌افتد و بخشی از اخبار آن نیز منتشر می‌شود، رغبت و اعتماد کاربران فناوری رایانش ابری را به این فناوری کاهش داده و مانعی جهت بهره‌برداری مطلوب از رایانش ابری در زیرساخت‌های کشور می‌گردد.

۱. مبانی نظری

رایانش ابری

منابع و سرویس‌های مورد درخواست بر روی بستر اینترنت که قابلیت توسعه و اطمینان بالایی دارند را ابر می‌گویند و رایانش ابری یک روش محاسباتی است که در آن منابع با قابلیت گسترش پویا و عموماً به‌شکل مجازی توسط ارائه‌دهندگان خدمات بر روی اینترنت فراهم و تحویل می‌شوند. این روش محاسباتی مزایای بسیاری برای کاربران خود دارد. از جمله؛ می‌توان به عدم نیاز به داشتن دانش فنی یا اعمال کنترل بر روی زیرساخت

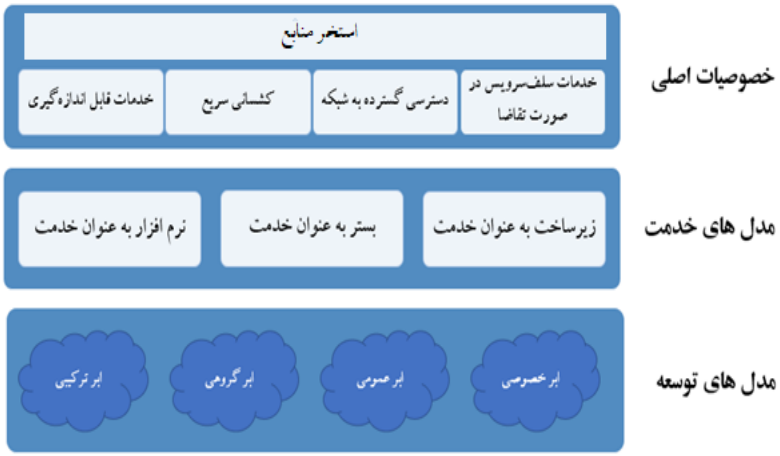
اشاره کرد. در این مدل محاسبات، می‌توان به توان پردازش به‌عنوان یک سرویس یا خدمت توسعه و به‌کارگیری فناوری کامپیوتر بر مبنای اینترنت، اشاره کرد. خدمات ارائه شده در ابر، برنامه‌های کاربردی را به‌صورت برخط فراهم می‌کنند به‌طوری‌که با مرورگرهای وب قابل‌دسترسی هستند. در این زمان نرم‌افزارها و داده‌ها بر روی سرورها ذخیره شده‌اند؛ در طول استفاده از رایانش ابری کاربر بدون اینکه بفهمد سرویس کجاست و یا چگونه آن را تحویل می‌گیرد صورت می‌پذیرد. رایانش ابری دارای ساختاری شبیه توده‌های ابری متشکل از سرویس‌ها و کاربردهای بسیاری است که کاربران از هر جای دنیا و با استفاده از اینترنت پرسرعت و پرداخت هزینه از آنها استفاده می‌کنند و کامپیوتر منفرد جای خود را به ابر با میلیون‌ها کاربر داده است (عبداللهی، سیادت، و اطهری فرد، ۱۳۹٤).

مؤسسه استاندارد ISO در سند ISO/IEC 17788 رایانش ابری را چنین تعریف می‌کند: رایانش ابری یک الگوواره برای فراهم‌کردن دسترسی از طریق شبکه به مجموعه عظیمی از منابع اشتراکی فیزیکی و مجازی با قابلیت مقیاس‌پذیری و انعطاف‌پذیری است که این دسترسی با کمترین نیاز به مدیریت و دخالت فراهم‌کننده سرویس و بر اساس تقاضا می‌باشد (ISO, 2014).

رایانش ابری خصوصیات ویژه و منحصربه‌فردی دارد که خاص سبک خودش است. از خصوصیات آن: ۱- ارائه سرویس مبنی‌بر تقاضا می‌باشد به این معنی که کاربر با پرداخت هزینه از منابع سخت‌افزاری و نرم‌افزاری استفاده می‌کند، ۲- استفاده از اینترنت به‌عنوان بستر جهت تحویل و ارائه سرویس می‌باشد. ۳- غنی‌بودن منابع است. مانند یک استخر پرآب می‌باشد و این منابع به‌وسیله تکنیک مجازی‌سازی از محل فیزیکی خود مستقل شده‌اند؛ بنابراین به‌راحتی می‌توانند در بستر شبکه جابه‌جا شوند؛ ٤- مقیاس فوق وسیع، مجازی‌سازی، چند کاربردی، قابلیت اطمینان و خدمات مبتنی بر تقاضا اشاره کرد (قاسمی و همکاران ، ۱۳۹٦). مؤسسه استاندارد و فناوری‌های ملی آمریکا[1] ویژگی‌های رایانش ابری

[1] NIST

را در سه دسته ارائه نموده است (Mell & Grance, 2011): ۱- پنج خصوصیت کلیدی ابر ۲- چهار مدل استقرار ابر ۳- سه مدل خدمت ابر



شکل شماره ۱: ویژگی‌های ابر (Mell & Grance, 2011).

محاسبات ابری به‌دلیل فواید بالقوه آن به‌نظر می‌رسد یک نیروی غیرقابل توقف باشد. ازاین‌رو، درک مخاطرات امنیتی و حریم خصوصی در محاسبات ابری و ایجاد راه‌حل‌های مؤثر برای موفقیت این الگو واره محاسباتی جدید بسیار مهم است. وقتی اطلاعات را به ابر منتقل می‌شود، ممکن است کنترل آن از دست برود. ابر به ما امکان دسترسی به داده‌ها را می‌دهد، اما چالش اینجاست که اطمینان حاصل شود فقط اشخاص مجاز دسترسی دارند. درک این مسئله دشوار است که چگونه می‌توان از داده‌ها و منابع خود در برابر نقض امنیت در یک ابر که سیستم‌عامل‌ها و خدمات مشترک را ارائه می‌دهد، محافظت نمود (Taghavi Zargar et al., 2019).

حریم خصوصی

با آنکه حریم خصوصی در زبان محاوره و نیز مباحث فلسفی، سیاسی و حقوقی مکرر استعمال می‌شود؛ ولی هنوز تعریف متقن و مشخصی از آن ارائه نشده است. مفهوم حریم خصوصی ریشه‌های عمیقی در مباحث جامعه‌شناختی و انسان‌شناختی دارد که نشان می‌دهد چگونه در فرهنگ‌های مختلف برای آن ارزش قائل شده‌اند. حریم خصوصی

مفهومی سیال است که امروزه از جمله آزادی وجدان و اندیشه، کنترل بر جسم خود، داشتن خلوت و تنهائی در منزل و مکان خصوصی، کنترل بر اطلاعات شخصی، رهایی از نظارت‌های سمعی و بصری دیگران، حمایت از حیثیت و اعتبار خود و حمایت در برابر تفتیش‌ها و تجسس‌ها و رهگیری‌ها را شامل می‌شود (رئوفی، راد، و بافرانی، ۱۳۹۹).

اسلام که زیر بنای هر نوع تربیت و سازندگی را، انسان می‌داند؛ به کرامت و حرمت آدمیان اهمیت فراوان داده و حریم خصوصی افراد را با وسواس و باریک‌بینی فراوان پاس داشته است. در آیات قرآنی و نیز احادیث معصومان (ع) و همچنین در سخنان پیشوایان دینی توصیه‌های فراوانی است که آدمیان را از ورود به حریم خصوصی افراد اکیداً بازداشته است. از همین‌رو است که یکی از شاخصه‌های مهم (رهبر دینی) اصرار او بر امن بودن حریم خصوصی افراد است. امام خمینی (ره) که توانست در تمامی عرصه‌ها با معیارهای اسلامی مشی کند در این وادی نیز با قوت و در حساسیت مثال‌زدنی وارد شد و حریم خصوصی مردم را پیامبرانه پاسداری کرد و همه مسئولان را به رعایت آن فرمان داد. حضرت امام خمینی (ره) در تاریخ ۱۳٦۱/۹/۲٤ یعنی پس از گذشت نزدیک به چهار سال از پیروزی انقلاب اسلامی، فرمان هشت ماده‌ای خطاب به قوه قضائیه و تمام ارگان‌های اجرایی در مورد اسلامی‌شدن قوانین و عملکردها صادر کردند (مهریزی، ۱۳۷۸).

حضرت آیت‌الله خامنه‌ای رهبر معظم انقلاب اسلامی در تاریخ ۱۳۹۷/۱/۲۰ در دیدار جمعی از مسئولان و مدیران نظام با ابراز خرسندی از تبدیل‌شدن مطالبه‌ی ایجاد پیام‌رسان‌ها و شبکه‌های اجتماعی داخلی به مطالبه‌ای عمومی، فرمودند: مسئولان باید امنیت و حریم داخلی مردم و کشور را حفظ کنند. تعرض به امنیت و حریم داخلی مردم «حرام شرعی» است و نباید انجام شود. همچنین ایشان افزودند: متصدیان کار در دستگاه‌های دولتی و قضائی مراقبت کنند تا حریم داخلی زندگی مردم و اسرار آن‌ها محفوظ بماند (دفتر حفظ و نشر آثار آیت الله خامنه ای، ۱۳۹۷)

بیش از دو دهه است که اینترنت و فناوری‌های اطلاعاتی مرتبط با آن منجر به نوآوری بی‌سابقه، ارزش اقتصادی و دسترسی به خدمات اجتماعی گسترده‌ای شده‌اند. بسیاری از

این مزایا توسط داده‌های مربوط به افرادی که از طریق یک زیست‌بوم پیچیده جریان می‌یابند، تغذیه می‌شوند. در نتیجه، ممکن است افراد نتوانند عواقب نقض احتمالی حریم خصوصی خود را در اثر تعامل با سیستم‌ها، محصولات و خدمات درک کنند. سازمان‌ها هم ممکن است پیامدها را کاملاً درک نکنند. عدم مدیریت مخاطرات حریم خصوصی می‌تواند عواقب منفی مستقیمی را در سطح فردی و اجتماعی، با تأثیرات بعدی بر چشم‌اندازهای توسعه‌ای آینده به‌همراه داشته باشد. یافتن راه‌هایی برای ادامه‌یافتن منافع حاصل از پردازش داده‌ها و درعین‌حال محافظت از حریم خصوصی افراد، چالش‌برانگیز است (NIST, 2020).

حریم خصوصی داده‌ها که گاهی اوقات به‌عنوان حریم خصوصی اطلاعات نیز نامیده می‌شود، ناحیه‌ای از حفاظت داده‌ها است که مربوط به مدیریت صحیح داده‌های حساس از جمله و به‌ویژه داده‌های شخصی و بلکه سایر داده‌های محرمانه مانند داده‌های مالی خاص و داده‌های دارایی معنوی، برای برآورده‌کردن الزامات نظارتی و همچنین محافظت از محرمانه بودن و تغییرناپذیری داده‌ها می‌باشد (SINA, 2021).

مؤسسه کلود فلر حریم خصوصی داده‌ها را به‌معنای توانایی شخص در تعیین میزان، زمان، چگونگی اشتراک اطلاعات خودش با دیگران تعریف می‌کند. این اطلاعات شخصی می‌تواند نام، موقعیت مکانی، اطلاعات تماس یا رفتار برخط یا دنیای واقعی فرد باشد. همان‌طور که ممکن است کسی بخواهد افراد را از گفتگوی خصوصی محروم کند، بسیاری از کاربران آنلاین می‌خواهند انواع خاصی از جمع‌آوری اطلاعات شخصی را کنترل یا از آنها جلوگیری کنند (Cloudflare, 2021).

قوانین و اسناد بالادستی حفظ حریم خصوصی داده در ایران

قوانین ایران در ارتباط با حمایت از حریم خصوصی همگام با تحولات پدیدآمده در این زمینه نیست. در سیاست کیفری ایران، چه در قانون اساسی و چه در قوانین عادی، به مفهوم حریم خصوصی صریحاً اشاره نشده و چنین استنباط می‌شود که برخی از مصادیق آنچه در اصطلاح به حریم خصوصی معروف است در برخی مواد موردتوجه قرار نگرفته

است. مجموع احکام پیش‌بینی‌شده در این مواد نشان می‌دهد که اولاً قانون‌گذار تمامی مصادیق حریم خصوصی را مدنظر قرار نداده است. ثانیاً، حتی در آن قسمت که مدنظر قرار داده، حمایت‌های لازم (کیفری و مدنی) از آن به عمل نیاورده است و این میزان از حمایت به‌هیچ‌وجه پاسخگوی نیازهای جامعه امروز و چالش‌های فراروی جامعه در عصر اطلاعات نیست. بنابراین تصویب قوانینی جامع و کامل در خصوص امر یا بازبینی و تکمیل قوانین موجود در کشور که حداقلِ آن ارائه تعریفی صریح و دقیق از مفهوم حریم خصوصی و تاحدامکان تعیین و تعریف دقیق محدوده و مصادیق آن است، امری ضروری و اجتناب‌ناپذیر به‌نظر می‌رسد. شایان‌ذکر است، قوانین تجارت الکترونیکی و جرایم رایانه‌ای دو قانون مهمی است که به منزله نقطه عطف قانون‌گذاری در ایران موردتوجه قرار گرفته و تحولات این دوره را تا حدودی مدنظر قرارداده است (قناد و علیقلی، ۱۳۹۹).

قوانین و مقررات حفظ حریم خصوصی داده در سایر کشورها

دستورالعمل عمومی حفاظت از داده[1] اتحادیه اروپا (2016/679) برای حفاظت از اطلاعات و حفظ حریم خصوصی شهروندان اروپایی -با هدف آن تأمین کنترل افراد بر اطلاعات شخصی خود و تعیین حداقل استانداردهای استفاده از داده‌ها توسط پلیس و دادگستری- در سال ۲۰۱٦ تصویب شد. این دستورالعمل، جایگزین دستورالعمل حفاظت از داده‌های سال ۱۹۹۵ گردید. این دستورالعمل براساس انطباق با محیط دیجیتال و فناوری‌های جدید مانند تلفن‌های هوشمند، شبکه‌های اجتماعی، بانکداری الکترونیکی، سیستم‌های ابری، مدیریت عمومی دیجیتال و خدمات و غیره تدوین شده است (Skendžić, Kovačić, & Tijan, 2018).

در فصل سوم این سند جهت موضوع داده حقوقی را برمی‌شمارد که عبارتست از:

۱- حق مطلع شدن ۲- حق دسترسی ۳- حق اصلاح ٤- حق پاک‌کردن ۵- حق محدودکردن پردازش ٦- حق قابلیت انتقال داده ۷- حق اعتراض ۸- حقوق مربوط به تصمیم‌گیری و پروفایل خودکار

[1] (GDPR) General Data Protection Regulation

در ایالات متحده چندین قانون خاص فدرال و ایالتی برای اطمینان از حقوق حریم خصوصی یک فرد وضع شده است. برخی از این قوانین در ایالات متحده عبارت‌اند از:

۱- قانون حریم خصوصی ارتباطات الکترونیکی (ECPA) از سال ۱۹۸٦ ۲- قانون مسئولیت‌پذیری بیمه سلامت (HIPAA) سال ۱۹۹٦ ۳- قانون محافظت از حریم خصوصی آنلاین کودکان (COPPA) از سال ۲۰۰۰ ٤- قانون محافظت از حریم خصوصی آنلاین کالیفرنیا (CalOPPA) از سال ۲۰۰٤ ٥- فناوری اطلاعات سلامت برای قانون سلامت اقتصادی و بالینی (HITECH) سال ۲۰۰۹ ۷- قانون دفاع از اسرار تجاری (DTSA) از سال ۲۰۱٦ ۸- قانون حریم خصوصی مصرف‌کننده کالیفرنیا (CCPA) اجرا از سال ۲۰۲۰

استانداردهای حفظ حریم خصوصی داده‌ها

مناسب‌ترین سند چارچوب ISO در زمینه حریم خصوصی ISO / IEC 29100 (چارچوب حفظ حریم خصوصی) در سال ۲۰۱۱ و آخرین سند اصلاحیه آن در سال ۲۰۲٤ منتشر شد. این سند به‌صورت آزادانه تحت توافق‌نامه مجوز مشتری ISO در دسترس است. این استاندارد بین‌المللی یک چارچوب سطح بالا برای حفاظت از اطلاعات قابل‌شناسایی شخصی در سیستم‌های فناوری اطلاعات و ارتباطات فراهم می‌کند. این سند ماهیت کلی دارد و جنبه‌های سازمانی، فنی و رویه‌ای را در یک چارچوب کلی حریم خصوصی قرار می‌دهد. چارچوب حفظ حریم خصوصی برای کمک به سازمان‌ها در تعریف الزامات حفاظت از حریم خصوصی مربوط به اطلاعات قابل‌شناسایی شخصی در محیط فناوری اطلاعات و ارتباطات شامل موارد ذیل می‌باشد (ISO 29100," 2024"):

۱- تعریف اصطلاحات مشترک حریم خصوصی ۲- تعیین بازیگران و نقش آنها در پردازش اطلاعات قابل‌شناسایی شخصی ۳- توصیف شرایط حفاظت از حریم خصوصی اصول حاکم بر حریم خصوصی در استاندارد ۲۹۱۰۰ به‌عنوان یک مرجع جهانی شامل موارد ذیل می‌باشد (Quemard, Schallabök, & Kamara, 2019):

جدول شماره ۱: اصول حاکم بر حریم خصوصی در استاندارد ۲۹۱۰۰ (Quemard, & et al, 2019)

ردیف	اصل	شرح
۱	رضایت و انتخاب	ارائه پیشنهاد و قدرت انتخاب صاحب PII[1] (موضوع داده) در خصوص اجازه یا عدم اجازه پردازش PII او، به جز در مواردی که صاحب PII نمی‌تواند آزادانه از رضایت خودداری کند یا در مواردی که قانون پردازش PII بدون رضایت شخص را مجاز می‌داند. انتخاب صاحب PII باید آزادانه، مشخص و بر اساس دانش انجام شود.
۲	مشروعیت و مشخصات هدف	– اطمینان از انطباق هدف (ها) با قانون قابل‌اجرا و تکیه بر مبانی قانونی مجاز؛ – ارتباط اهداف با صاحب PII قبل از اینکه اطلاعات برای اولین‌بار برای هدفی جدید جمع‌آوری یا استفاده شود.
۳	محدودیت جمع‌آوری	محدودکردن جمع‌آوری PII به آنچه در چارچوب قانون قابل‌اجرا است و برای اهداف (اهداف) مشخص کاملاً ضروری است.
٤	کمینه‌سازی داده‌ها	به‌حداقل‌رساندن PII که پردازش می‌شود و تعداد ذینفعان حریم خصوصی و افرادی که PII آنها افشا می‌شود یا به آن دسترسی دارند.
۵	محدودیت استفاده، حفظ و افشا	محدودکردن استفاده، نگهداری و افشای PII به آنچه برای تحقق اهداف خاص، صریح و قانونی ضروری است؛ حفظ PII فقط تا زمانی که برای تحقق اهداف گفته شده لازم باشد و پس از آن به طور ایمن آن را نابود یا ناشناس کنید.
٦	دقت و کیفیت	– اطمینان از دقیق، کامل، به‌روز بودن PII پردازش شده (مگر اینکه مبنای قانونی برای نگهداری داده‌های منسوخ وجود داشته باشد)، کافی و مرتبط باهدف استفاده؛ – اطمینان از اعتبار PII جمع‌آوری شده از منبعی غیر از اصل PII قبل از پردازش؛
۷	آشکار بودن، شفافیت و اعلام	– ارائه اطلاعات واضح و در دسترس به صاحب PII در مورد سیاست‌ها، رویه‌ها و روش‌های کنترل‌کننده PII در رابطه با پردازش PII ؛ – توجه به این واقعیت که PII، برای هدفی که برای این کار انجام می‌شود درحال پردازش است، انواع ذینفعان حریم خصوصی که ممکن است PII و هویت کنترل‌کننده PII از جمله اطلاعاتی در مورد نحوه تماس با کنترل‌کننده PII برای آنها افشا شود.
۸	مشارکت و دسترسی فردی	– دادن امکان دسترسی و بررسی PII به صاحبان PII ، به شرطی که هویت آنها ابتدا با سطح اطمینان مطلوبی تأیید شود و چنین دسترسی توسط قانون منع نشده باشد. – اجازه‌دادن به صاحبان PII برای به چالش کشیدن صحت و تمامیت PII و تغییر یا حذف آن متناسب با شرایط خاص و ممکن؛ – فراهم‌کردن شرایط هرگونه اصلاح یا حذف به پردازنده‌های PII و اشخاص ثالثی که داده‌های شخصی آنها در جایی که شناخته شده‌اند

[1] PII: Personal Identifiable Information

		افشا گردد. – ایجاد روش‌هایی برای اینکه صاحبان PII بتوانند از این حقوق به روشی ساده، سریع و کارآمد استفاده کنند که تأخیر یا هزینه بیجا را به دنبال نداشته باشد.
۹	پاسخگویی	مستندسازی و ابلاغ مناسب کلیه سیاست‌ها، رویه‌ها و روش‌ها مرتبط با حریم خصوصی و واگذاری وظیفه اجرای سیاست‌ها، رویه‌ها و روش‌های مربوط به حریم خصوصی به یک فرد مشخص در سازمان
۱۰	امنیت اطلاعات	محافظت از PII تحت اختیارات خود با کنترل‌های مناسب در سطح عملیاتی، عملکردی و استراتژیک برای اطمینان از یکپارچگی، محرمانه بودن، در دسترس‌بودن PII و محافظت از آن در برابر مخاطراتی مانند دسترسی غیرمجاز، تخریب، استفاده، تغییر، افشا یا ازدست‌دادن در تمام چرخه حیات آن
۱۱	انطباق حریم خصوصی	تأیید و اثبات اینکه پردازش داده‌ها با انجام دوره‌ای نظارت با استفاده از ناظران داخلی یا ناظران شخص ثالث مورداعتماد، از شرایط محافظت از حریم خصوصی و داده‌ها برخوردار است

نمونه‌هایی از نشت اطلاعات و نقض حریم خصوصی

چند نمونه از حوادث برتر نشت اطلاعات در سال ۲۰۱۹ که توسط ENISA منتشر شد در جدول شماره ۲ ارائه می‌گردد (ENISA, 2020):

جدول شماره ۲: چند نمونه از حوادث برتر نشت اطلاعات در سال ۲۰۱۹

ردیف	مصداق نشت اطلاعات در سال ۲۰۱۹
۱	در ژانویه ۲۰۱۹، محقق مستقل Troy Hunt ، ۷۳۷ میلیون آدرس ایمیل و رمز عبور کاربران را در سرویس ذخیره‌سازی ابری MEGA پیدا کرد. هانت این مجموعه داده نقض شده را مجموعه شماره ۱ نام‌گذاری و سرویس «آیا من پسورد شما را می‌دانم؟» را اطلاع‌رسانی کرد، تا بدین روش به صاحبان حساب‌ها اطلاع دهد تا رمزهای ورود به سیستم خود را برای دسترسی به سیستم‌عامل MEGA تغییر دهند.
۲	در ژانویه ۲۰۱۹، افرادی اطلاعات شخصی، ارتباطات خصوصی و اطلاعات مالی صدها سیاستمدار آلمانی را افشا نمودند.
۳	در فوریه ۲۰۱۹، بیش از ٦١ میلیون حساب از وب‌سایت‌ها فاش شد و در وب تاریک برای فروش قرار گرفت. این اطلاعات با کمتر از ۲۰,۰۰۰ دلار به‌صورت بیت‌کوین به فروش می‌رفت.
٤	در مارس ۲۰۱۹، صدها میلیون کاربر فیس‌بوک و اینستاگرام شاهد افشای حساب کاربری خود به دلیل مدیریت ضعیف ذخیره‌سازی رمز عبور، شبکه اجتماعی بودند.
۵	در آوریل ۲۰۱۹ تعداد ۱۲,۵ میلیون پرونده پزشکی زنان باردار در هند، به‌دلیل نشت اطلاعات یک سرور دولتی متعلق به یک آژانس بهداشت و درمان مربوط به اقدامات پیش از بارداری و روش‌های تشخیصی قبل از تولد در معرض دید قرار گرفت. باوجودی که قانونی در هند تصویب شده که تعیین جنسیت قبل از تولد را برای جلوگیری از سقط‌جنین دختران متولد

	شده توسط خانواده‌های هندی ممنوع کرده بود.
٦	در ماه مه ۲۰۱۹ ، DoorDash ، یک سرویس تحویل غذا، با نقض داده‌ها مواجه شد که تقریباً ۵ میلیون کاربر را تحت‌تأثیر قرار داد. تحقیقات بعدی مشخص کرد که اطلاعاتی مانند نام، آدرس ایمیل، آدرس تحویل، تاریخچه سفارش، شماره‌تلفن و رمز عبور قابل‌دسترسی بوده است. این شرکت گفت که چهار رقم آخر کارت‌های اعتباری و شماره‌حساب بانکی برخی از مصرف‌کنندگان نیز قابل‌دسترسی بوده است.
۷	در ژوئن ۲۰۱۹، آژانس جمع‌آوری پزشکی آمریکا (AMCA) درخصوص لورفتن اطلاعات حسابداری برخی از مشتریانش اطلاع‌رسانی کرد. این اطلاعات شامل ۱۱,۹ میلیون پرونده Quest Diagnostics که یکی از بزرگ‌ترین آزمایش خون است بود. طبق پرونده اخیر کمیسیون اوراق بهادار و بورس، هکر از اول آگوست ۲۰۱۸ تا ۳۰ مارس ۲۰۱۹ برای تقریباً هشت ماه به سیستم AMCA دسترسی پیدا کرده بود.

تأثیرات نقض حریم خصوصی داده

به‌طور معمول کاربران برای استفاده از خدمات آنلاین ملزم به افشای اطلاعات شخصی هستند و تنظیماتی که دسترسی به این سرویس‌ها را محافظت یا محدود می‌کنند به‌طور مکرر تغییر می‌کنند. این امر به‌ویژه هنگام استفاده از رسانه‌های اجتماعی گیج‌کننده است، زیرا افراد برای تعامل با دیگران باید به‌طور مداوم اطلاعات مربوط به خود را فاش کنند. طی چند سال گذشته، تحقیقات نشان داده است که حریم خصوصی فقط به تنظیمات پلتفرم یا انتخاب محتوی شخصی برای انتشار آنلاین محدود نمی‌شود. بلکه الگوهای رفتاری فرد (مانند الگوهای زبانی، تعداد دوستان، تعداد دفعات ورود به سیستم) می‌تواند برخی ویژگی‌های جمعیت‌شناختی یا ویژگی‌های شخصیتی را هنگام تجزیه‌وتحلیل توسط الگوریتم‌های رایانه نشان دهد. فرصت مطالعه رفتار انسان از این طریق تحقیقات زیادی را برانگیخته است که درپی پیش‌بینی چگونگی پیش‌بینی دقیق اطلاعات شخصی از ردپای دیجیتالی شخص است. به‌عنوان مثال در مارس ۲۰۱۸، خبر رسوایی فیس‌بوک – کمبریج آنالیتیکا در سرتاسر جهان خبرساز شد. شرکت مشاور داده کمبریج آنالیتیکا[1] بدون اجازه کاربران فیس‌بوک از اطلاعات شخصی آنلاینی که برای اهداف آکادمیک جمع‌آوری شده، در کارزارهای سیاسی استفاده کرده بود. براین‌اساس اطلاعات شخصی بیش از ۸۷ میلیون کاربر فیس‌بوک به شیوه‌ای نامناسب در اختیار شرکت مشاوره سیاسی کمبریج آنالیتیکا قرار

[1] Cambridge Analytica

گرفت. کمبریج آنالیتیکا از این اطلاعات برای تأثیرگذاری بر مبارزات انتخابات ریاست‌جمهوری ایالات متحده آمریکا در سال ۲۰۱٦ به نفع دونالد ترامپ استفاده کرد. این اطلاعات از طریق برنامه اینترنتی «این زندگی دیجیتال شماست» بر روی رایانه ۳۰۵ هزار کاربر فیس‌بوک به‌دست‌آمده بودند. این نرم‌افزار می‌توانست به‌غیر از اطلاعات کاربران فیس‌بوکی که آگاهانه این نرم‌افزار را نصب‌کرده بودند به اطلاعات دیگر کاربرانی که با این کاربر در ارتباط بودند نیز دست یابد (Hinds, Williams, & Joinson, 2020).

آقای اکرمی و رواشد چالش‌های حفظ حریم خصوصی به‌صورت ذیل بیان می نماید. (Akremi & Rouached, 2021):

۱- چند مستأجری ۲- عدم کنترل کاربر ۳- عدم کنترل کاربر ٤- قابلیت نظارت ۵- مجازی‌سازی ٦- ارزیابی صلاحیت[1] ۷- کلان‌داده ۸- جنبه‌های حقوقی ۹- استانداردسازی ۱۰- مدیریت.

۲. روش تحقیق

این پژوهش به‌دلیل اینکه به شناخت چالش‌های وضع موجود و ارائه راهبردها و راهکارهای رفع این چالش‌ها می‌پردازد توسعه‌ای و به‌دلیل اینکه این راهبردها و راهکارها مورد استفاده تصمیم‌گیران واقع می‌گردد کاربردی می‌باشد. بنابراین پژوهش باتوجه به موضوع و هدف تحقیق، از نوع کاربردی-توسعه‌ای و روش تحقیق به کار گرفته شده روش آمیخته است.

جامعهٔ آماری، خبرگانی هستند که ویژگی مشترک آنان داشتن اطلاعات و دانش مناسب در حوزه رایانش ابری و حریم خصوصی، تحصیلات دانشگاهی با مدرک دکتری با حداقل ۱۵ سال سابقه کار اجرایی در این حوزه و دسترسی به اطلاعات طبقه‌بندی شده در لایه‌های حاکمیتی می‌باشد. اینان با روش گلوله برفی، معرفی و تایید جامعه خبرگی و پژوهشی

[1]- due diligence

احصاء شده‌اند. همچنین به‌دلیل ویژگی‌های موردنظر، جامعه نمونه همان جامعه آماری می‌باشد. تحقیق از چارچوب راهنمای تدوین راهبرد ملی ITU برای تدوین راهبرد بهره گرفته است.

- ❖ تحلیل محتوای کیفی: در این پژوهش به تحلیل محتوای کیفی تدابیر و رهنمودهای مقام معظم رهبری (مدظله‌العالی)، اسناد بالادستی، مطالعات تطبیقی، مقالات علمی و پژوهشی و مصاحبه با خبرگان پرداخته شد و با تکنیک شبکه مضامین، چالش‌های موجود بر اساس محیط‌شناسی[1] PESTLS احصا گردید.
- ❖ تکنیک دلفی: در این مرحله با استفاده از روش دلفی، ۲۵۰ مضمون پایه احصا شده در گام اول با اجماع نظر گروه راهبری مورد بازبینی، تلفیق و اصلاح قرار گرفت و مضامین سازمان‌یافته حاصل گردید. در مرحله دوم این مضامین در دو مرحله به خبرگان ارائه و نمره‌دهی گردید و ٥٤ مضمون فراگیر که امتیاز آنها بالاتر از ٦ از ۱۰ بود حاصل شد.
- ❖ پرسش‌نامه: در این مرحله مضامین فراگیر حاصل شده در یک پرسش‌نامه به جامعه آماری ارائه و سپس این مضامین بر اساس ریسک‌های حاصل توسط جامعه آماری به صورت تمام شمار اولویت‌بندی گردیدند. در این پژوهش جهت محاسبه روایی پرسشنامه از شاخص نسبت روایی محتوایی[2] استفاده شد و در پرسشنامه گویه‌هایی که عدد آنها بالاتر از ۰/۸ بود نگه داشته و همچنین جهت محاسبه ضریب پایایی از محاسبه آلفای کرونباخ استفاده شده که این مقدار توسط نرم افزار SPSS برای پرسشنامه ارائه شده مقدار ۰/۸۸ حاصل گردید.
- ❖ راهنمای راهبرد ملی یکی از جامع‌ترین نگرش‌هایی است که راهبردهای موفق را تشکیل می‌دهد. این نتیجه یک تلاش منحصربه‌فرد و مشارکتی است که به دانش، تجربه و تخصص بسیاری از سازمان‌ها در زمینه راهبردهای ملی و سیاست‌های ملی می‌پردازد. به‌طورخاص، این راهنما توسط دوازده عضو از بخش‌های دولتی و

1- Poletical-Economical-Social-Technical-Legal-Security
2Content Validity Ratio (CVR)

خصوصی و همچنین جامعه دانشگاهی و تجاری تولید شده است. تدوین راهبرد ملی از طریق یک رویکرد تعاملی توسعه‌یافته که به‌دنبال رسیدن به توافق از طریق ایجاد اجماع نظری است و بیشترین استفاده را از نظرات خبرگان برای استخراج راهبرد و اولویت‌بندی آن نموده است (ITU, 2021).

چرخه حیات تدوین راهبرد ملی[1]

در شکل شماره دو چرخه حیات تدوین راهبرد ملی نمایش داده شده است.

الف- فاز اول شروع: در این مرحله بر روی فرایندها، منابع، مرجع هدایت، کمیته راهبری و شناسایی خبرگان و ذینفعان کلیدی که باید در تولید راهبرد دخالت و مشارکت داشته باشند تمرکز می‌کند.

- شناسایی مرجع هدایت پروژه

فرایند تدوین و توسعه راهبرد باید توسط یک مرجع معتبر و باصلاحیت هدایت شود. این بخش مهم باید یک نهاد دولتی مانند وزارتخانه یا یک مؤسسه علمی (یا دانشگاهی معتبر) هدایت پروژه علمی را قبول کند.

- ایجاد کمیته راهبری

یک کمیته راهبری برای نظارت و راهبری تحت‌نظر مرجع هدایت پروژه جهت راهبری تشکیل می‌شود. این کمیته باید برای ارائه راهنمایی و نیز ایفای نقش کیفیت، تخصص و اختیار لازم را داشته باشد. این کمیته راهبری بر روی اقدامات و تصمیم‌های مدیر اجرایی تحقیق نظارت و راهنمایی لازم را به‌عمل می‌آورد.

- شناسایی خبرگان و ذینفعان برای مشارکت در تدوین راهبرد

در این مرحله، با همفکری و همکاری کمیته راهبری باید یک مجموعه اولیه از خبرگان و ذینفعان را شناسایی کند تا در تدوین راهبرد مشارکت داشته باشند. باید اطمینان حاصل شود که با این انتخاب خبرگان و ذینفعان، تمام دانش و تخصص مرتبط با مسئله تحقیق

1 Lifecycle of a National Strategy

مورداستفاده قرار می‌گیرد. چنین مکانیسم همفکری و همکاری، می‌تواند شکل کمیته مشورتی و یا پنل خبرگی به خود بگیرد که همفکری و مشاوره مهمی و مؤثری را در مراحل مختلف تحقیق داشته باشد.

- برنامه‌ریزی برای تدوین راهبرد

در برنامه‌ریزی برای تدوین راهبرد مراحل و فعالیت‌های اصلی شناسایی و مشخص می‌شود. در واقع کمیته راهبری، مراحل و گام‌ها را برای مدیر اجرایی طراحی و ترسیم می‌کند.

ب- فاز دوم: برآورد و تحلیل: هدف از این مرحله، جمع‌آوری محتوا و داده‌ها برای تحلیل وضعیت موجود و دورنمای تهدیدات جاری و آتی جهت منظور نمودن برای تدوین راهبرد ملی است.

- ارزیابی از منظر ملی

برای اینکه راهبرد ملی تدوین و مؤثر واقع شود، باید وضعیت کشور را در این حوزه مورد بررسی و مطالعه قرارداد. در این راستا، با تجزیه‌وتحلیل مشکلات، مسائل و ضعف-های موجود در کشور شناسایی می‌شود، در ضمن مطالب و اسناد مرتبط باید در همکاری با خبرگان و ذینفعان مورد بررسی قرار گیرند.

- ارزیابی از منظر دورنمای مخاطرات

باید دورنمای خطراتی را که کشور باتوجه به وابستگی دیجیتال مواجه است، ارزیابی نمود. این موضوع از طریق شناسایی وضع موجود دارایی‌های دیجیتال (دولتی، عمومی و خصوصی)، وابستگی‌های متقابل، آسیب‌پذیری‌ها، تهدیدها، پیامدها، برآوردهای احتمالی و تأثیرات بالقوه، انجام می‌شود.

ج- فاز سوم: تولید راهبرد ملی امنیت سایبری: با شناسایی چالش‌ها در دو بخش قبلی، تدوین و توسعه متن راهبرد با درگیرکردن خبرگان و ذینفعان کلیدی از طریق گروه‌های کاری و یا کانونی صورت می‌گیرد.

- پیش‌نویس راهبرد ملی

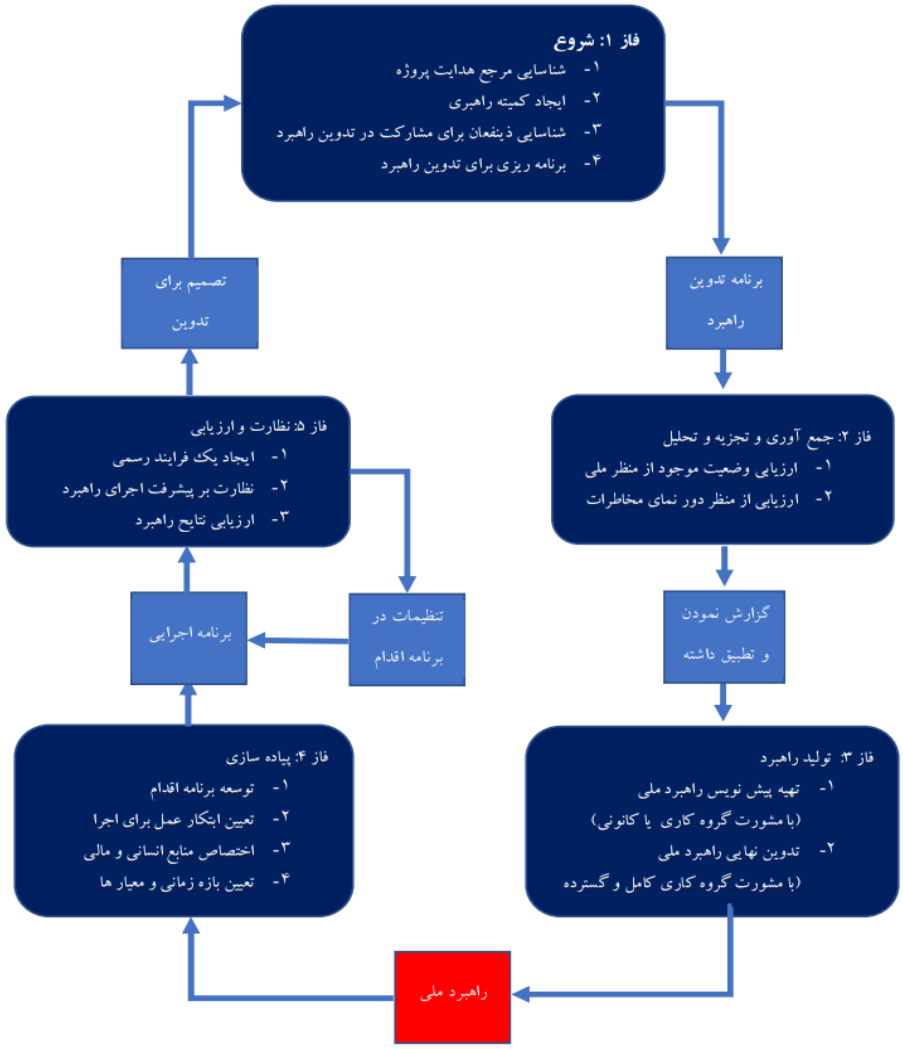
«گروهی کاری» متشکل از خبرگان و ذینفعان (یا گروه کانونی) با نظر کمیته راهبری انتخاب می‌شود. با مشورت، همفکری و تمرکز بر روی موضوعات خاص و چالش‌ها، برای برطرف‌شدن آن‌ها نسبت به تهیه پیش‌نویس بخش‌های مختلف راهبرد اقدام می‌شود. این راهبردها باید پوشش لازم را برای حل مسائل مطرح شده در چالش‌ها را داشته باشد. وجود شفافیت لازم در جهت اهداف و سیاست‌ها ضروری می‌باشد.

- تدوین راهبرد ملی

تعامل با خبرگان و ذینفعان برای موفقیت در تدوین یک راهبرد، حیاتی است. به‌منظور حصول اطمینان از اینکه راهبرد نهایی بر اساس یک دیدگاه مشترک است، پیش‌نویس باید در یک گروه کاملی از خبرگان و ذینفعان مطرح و از نظرات و دیدگاه‌های آنان برای نهایی کردن راهبردها استفاده نمود.

چنانچه امکان حضور همگان در قالب یک گروه بزرگ فراهم نشود، این موضوع می‌تواند از چند طریق از جمله مشاوره (مجازی)، کارگاه‌های اعتبارسنجی، و گروه‌های متخصص نخبگی و ... اتفاق بیفتد. انتظار می‌رود بازخورد و نظرات ناشی از این فرایند برای نهایی کردن راهبرد مورد استفاده قرار گیرد. از نظرات آنان برای اولویت‌سنجی راهبردها نیز استفاده می‌شود.

راهبردهای استخراج شده در گروه کاری این پژوهش؛ بررسی، تنظیم، تدوین و با استفاده روش کمی اولویت‌بندی شده است.



شکل شماره ۲: چرخه حیات تدوین راهبرد ملی (ITU ،۲۰۲۱)

۳. تجزیه و تحلیل یافته‌ها

به‌منظور شناسایی و تعیین عوامل محیطی در سطح کلان و ملی در حوزه عوامل تاثیر گذار بر موضوع، براساس مدل ITU جهت احصاء ریسک، مراحل زیر دنبال گردید:

۱- بررسی مفاهیم تحلیل محیط در منابع علمی ۲- مطالعه اسناد تطبیقی برخی کشورهای پیشرو ۳- تحلیل مضمون در بیانات و ابلاغیه‌ها مقام معظم رهبری و اسناد بالا دستی

منتخب که اشاراتی به چالش محیطی به ابعاد مختلف فضای سایبر کشور وجود داشت. ٤- دسته بندی مضامین پایه جمع آوری شده با تلفیق موارد مشابه به لحاظ معنایی و مفهومی از منابع ذکر شده در ابعاد مختلف PESTLS تحت عنوان مضامین سازمان‌یافته مرحله یک. ٥- انجام مصاحبه و اخذ نظر از خبرگان منتخب و دارای تخصص وتجارب مفید در ابعاد مختلف مرتبط با حفظ حریم خصوصی و رایانش ابری به‌منظور غنا و عمق بخشی بیشتر به مضامین کدگذاری شده سازمان یافته و تمرکز بر هر عاملی اعم از ضعف – تهدید در محیط‌های تحلیل که می‌توانست روندهای عادی را به چالش تبدیل نماید.

در این مرحله ۲۵۰ چالش مرتبط احصا گردید. پس از دسته بندی - تلفیق و پالایش – خبره‌سنجی و رتبه‌بندی مضامین پایه، ٥٤ مضمون سازمان‌یافته حاصل شد.

چالش‌ها و تهدیدات احصا شده به‌صورت پرسش‌نامه در معرض نظر خبرگان قرار گرفت. در این پرسش‌نامه احتمال آسیب‌زا بودن و میزان آسیب احتمالی فاکتورها مورد سنجش قرار گرفت. در پرسش‌نامه از دو طیف لیکرت ٥ سطحی برای احتمال آسیب‌زا بودن چالش و میزان آسیب احتمالی استفاده گردید. حاصل‌ضرب این دو پارامتر به‌عنوان مقدار ریسک محاسبه شد. نتایج به‌دست‌آمده در جدول شماره سه ارائه شده است.

جدول شماره ۳: چالش‌های احصا شده بر اساس محیط شناسی و اولویت بندی بر اساس ریسک

ردیف	میزان ریسک	چالش‌های احصا شده
...	...	...

٤. نتیجه‌گیری و پیشنهاد

پس از احصاء چالش‌های محیطی و محاسبه ریسک، راهبردهای پیشنهاد شده در این تحقیق، حاصل تلاش و مشارکتی می‌باشد که دانش، تجربه و تخصص بسیاری از صاحب‌نظران بخش‌های دولتی و خصوصی و همچنین جامعه دانشگاهی و تجاری که دارای تجارب ارزنده‌ای در زمینه رایانش ابری و حریم خصوصی بودند را برای احصاء راهبردها با نگاهی تعاملی از طریق ایجاد اجماع نظری خبرگان در استخراج راهبردها و

اولویت‌بندی آنها به مشارکت گرفته است. در ادامه ضمن تشریح به‌اختصار مراحل، نتایج حاصل نیز ارائه می‌گردد:

کلیه ٥٤ مضامین فراگیر مرتبط با چالش‌های محیطی که براساس چارچوب تحلیل محیط PESTLS از مطالعه اکتشافی بیانات و ابلاغیه‌های مقام معظم رهبری، اسناد بالادستی و مطالعات تطبیقی احصا و پالایش شده بود توسط پرسشنامه محاسبه ریسک، در معرض نظر خبرگان قرار گرفت و چالش‌ها براساس ریسک حاصله اولویت‌بندی گردید.

جهت ارزیابی از منظر دورنمای مخاطرات با همکاری و مساعدت ۱۰ نفر از خبرگانی که ویژگی مشترک آنان داشتن نگاه داده محور و درک راهبردی از رایانش ابری و حریم خصوصی و همچنین دارای حداقل ۱۵ سال سابقه کار اجرایی در این حوزه بودند ۲۰ عنوان اولیه موضوع چالش ها از ٥٤ مضامین فراگیر استخراج گردید.

پس بررسی مجدد عناوین چالش‌ها و ادغام و اصلاح عناوین در نهایت با تأیید خبرگان با استفاده از روش شبه دلفی ۱۰ عنوان چالش از منظر دورنمای مخاطرات انتخاب و اولویت بندی گردید تا بتوان براین اساس مسیر برای تدوین راهبردها تسهیل گردد.

جدول شماره ٤: عناوین موضوع چالش‌های محیطی منتخب

ردیف	عناوین چالش‌های محیطی منتخب
۱	آموزش – مهارت – نوآوری – فرهنگ‌سازی
۲	سیاست – راهبرد
۳	قوانین و مقررات – نظارت
٤	مدیریت – برنامه‌ریزی – آینده‌نگری
٥	اقتدار – امنیت
٦	**ساختار – برنامه**
۷	دانش و فناوری
۸	تعامل – مشارکت
۹	انسجام‌بخشی – تقویت یکپارچگی – همکاری
۱۰	حمایت هدفمند و سرمایه‌گذاری

براساس مدل ITU گروه کانونی به‌منظور مرتفع نمودن چالش‌های فوق‌الذکر، ۸ راهبرد اولیه ذیل را پیشنهاد دادند.

جدول شماره ۵: جدول راهبردها اولیه بر اساس نظر خبرگان

ردیف	راهبردهای حفظ حریم خصوصی داده ها در زیرساخت‌های حیاتی مبتنی بر رایانش ابری
۱	طراحی و اجرای نظام جامع حفظ حریم خصوصی داده ها در زیرساختهایی ابری حیاتی کشور از طریق تدوین قوانین، مقررات و دستورالعمل‌های مربوطه با استفاده از به کارگیری متخصصین این حوزه و تجارب جهانی
۲	ارتقای فرهنگ، دانش و آگاهی عمومی احاد جامعه از طریق ایجاد دوره‌های آموزشی دانشگاهی ، برگزاری دوره‌های آموزشی کارمندان زیرساخت‌های حیاتی با استفاده از متخصصین داخلی و خارجی به‌منظور آگاهی احاد جامعه از حقوق حریم خصوصی
۳	ایجاد و بهبود ساز و کارهای مورد نیاز به‌منظور اجرای قوانین، مقررات و دستورالعمل‌های حفظ حریم خصوصی داده‌ها و نظارت بر اجرای آنها از طریق بازنگری در ساختار موجود، بهره‌برداری از تجارب جهانی و مبانی بومی
٤	ارتقاء امنیت و تاب‌آوری زیرساخت‌های ابری حیاتی با استفاده از اجرای طرح شبکه ملی اطلاعات، ایجاد مراکز مانیتورینگ و اقدام به‌منظور جلوگیری از درز اطلاعات و سوء استفاده دشمن از اطلاعات زیرساخت‌های حیاتی
۵	فعال‌سازی اقتصاد حریم خصوصی داده از طریق فعال‌سازی شرکت‌های دانش‌بنیان و بخش خصوصی با استفاده از تعریف پروژه‌های تحقیقاتی، اجرایی، نظارتی و توجیه‌پذیر کردن فعالیت‌های بخش خصوصی به‌منظور توسعه و ارتقا خدمات ارزش‌آفرین
٦	استانداردسازی فرآیندها و فعالیت‌های ارتقا حفظ حریم خصوصی داده‌ها در زیرساخت‌های ابری حیاتی از طریق پیاده‌سازی معماری‌های نوین فنی مانند عدم اعتماد
۷	ارتقای همکاری‌های بین‌المللی از طریق مشارکت در کمیته‌ها، کمیسیون‌ها و مجامع بین‌المللی مرتبط، همکاری‌های مشترک علمی، همکاری‌های قضایی به‌منظور مدیریت داده‌های فرامرزی
۸	ارتقا سطح بازدارندگی نقض حریم خصوصی داده‌ها با استفاده از تدوین و اجرای قوانین جزایی مربوطه

راهبردهای پیشنهادی مجدد مورد بررسی – اصلاح و ادغام توسط خبرگان و گروه راهنما قرار گرفت و در نهایت ٦ راهبرد بر اساس اهمیت، انتخاب و اولویت بندی گردید. راهبردهای نهایی بر اساس اولویت بندی در جدول ذیل ارائه شده است.

جدول شماره ٦: جدول اولویت های راهبردها بر اساس نظر خبرگان

ردیف	راهبردهای حفظ حریم خصوصی داده‌ها در زیرساخت‌های حیاتی مبتنی بر رایانش ابری
۱	ارتقای فرهنگ، دانش و آگاهی عمومی آحاد جامعه از طریق ایجاد دوره‌های آموزشی دانشگاهی، برگزاری کارگاه‌ها و دوره‌های آموزشی برای کارمندان زیرساخت‌های حیاتی با

	استفاده از متخصصین داخلی و خارجی به‌منظور آگاهی آحاد جامعه از اهمیت، حقوق حریم خصوصی و ضرورت حفظ آن
۲	طراحی و اجرای نظام جامع حفظ حریم خصوصی داده‌ها در زیرساخت‌هایی ابری حیاتی کشور از طریق تدوین قوانین، مقررات و دستورالعمل‌های مربوطه با استفاده از به‌کارگیری متخصصین این حوزه و تجارب جهانی
۳	ارتقا امنیت و تاب‌آوری زیرساخت‌های ابری حیاتی با محوریت محرمانگی و حفظ حریم خصوصی با استفاده از اجرای طرح شبکه ملی اطلاعات، ایجاد مراکز مانیتورینگ و اقدام، به‌منظور جلوگیری از نشت اطلاعات و سو استفاده دشمن از اطلاعات زیرساخت‌های حیاتی
٤	ایجاد سازوکارهای مورد نیاز به‌منظور اجرای قوانین، مقررات و دستورالعمل‌های حفظ حریم خصوصی داده‌ها و نظارت بر اجرای آن‌ها از طریق بازنگری در ساختار موجود، بهره‌برداری از تجارب جهانی و مبانی بومی
٥	ارتقای همکاری‌های بین‌المللی با استفاده از مشارکت در کمیته‌ها و کمیسیون‌ها و مجامع بین‌المللی مرتبط، همکاری‌های مشترک علمی، همکاری‌های قضایی به‌منظور مدیریت داده‌های فرامرزی
٦	فعال‌سازی اقتصاد حریم خصوصی داده از طریق فعال‌سازی شرکت‌های دانش‌بنیان و بخش خصوصی با استفاده از تعریف پروژه‌های تحقیقاتی، اجرایی، نظارتی و توجیه‌پذیر کردن فعالیت‌های بخش خصوصی به‌منظور توسعه و ارتقا خدمات ارزش‌آفرین

راه کارهای احصا شده

راهبردهای احصا شده جهت تحقق نیازمند راهکار می‌باشند. بدین‌منظور راهبردها در اختیارخبرگان قرار گرفت و با همکاری آنان راهکارهایی برای هر راهبرد پیشنهاد گردید. در مجموع ۸٤ راهکار برای ٦ راهبرد منتخب جمع‌آوری شد. در ادامه با نظر گروه کانونی، راهکارها مورد بازنگری و ادغام قرار گرفت و سپس به خبرگان ارائه گردید. ٤۹ راهکاری که نمره بالاتر از ٦ از ۱۰ را دریافت کردند به عنوان راهکار نهایی تایید شدند.

❖ راهکارهای راهبرد اول

- آگاهی‌بخشی و فرهنگ‌سازی ذینفعان حوزه حفظ حریم خصوصی داده در زیرساخت‌های حیاتی مشتمل بر سرویس‌دهندگان، سرویس‌گیرنده‌ها، پیمانکاران و ...
- ایجاد دوره‌های دانشگاهی مرتبط با حفظ حریم خصوصی داده در مراکز آموزشی و تحصیلات تکمیلی

- ایجاد برنامه‌های مرتبط جهت آگاهی‌رسانی عمومی حفظ حریم خصوصی داده جهت ارتقا دانش عمومی
- ایجاد مراکز تحقیق و پژوهش در حوزه حفظ حریم خصوصی
- برگزاری آموزش‌های دوره‌ای و به‌روز فضای سایبر جهت مدیران ارشد کشور
- آموزش و ترویج فرهنگ مدیریت ریسک (در سطح حاکمیت، دولت و سازمان).

❖ راهکارهای راهبرد دوم

- تدوین قوانین مورد نیاز در خصوص حفظ حریم خصوصی داده در کشور
- جرم‌انگاری نقض حریم خصوصی داده‌ها و تدوین قوانین جزایی مرتبط با نقض حریم خصوصی داده‌ها
- سیاست‌گذاری و تدوین راهبردهای مشخص در خصوص حفظ حریم خصوصی داده در زیرساخت‌های حیاتی
- تدوین نظام حاکمیت داده ملی در کشور
- تلاش جهت ایجاد فضای اعتماد به حاکمیت جهت حفظ حریم خصوصی و صیانت از داده
- استقرار نظام جامع مدیریت هویت و دسترسی در کشور
- تدوین نظام اشتراک اطلاعات در کشور
- تدوین مقرراتی برای انتقال و ذخیره‌سازی داده‌های فرامرزی.

❖ راهکارهای راهبرد سوم

- تکمیل سریع‌تر شبکه ملی اطلاعات به همراه سرویس‌های پایه مانند موتور جستجوی بومی و...
- ایجاد برنامه‌های شناسایی، پاسخگویی و بازیابی تهدیدات

- تدوین سازوکار مدیریت ریسک در این حوزه
- ظرفیت‌سازی جهت قابلیت مقابله با تهدیدات جدید و نوظهور
- ایجاد زیرساخت جهت ذخیره، پردازش یا انتقال داده‌ها در مراکز داده داخلی در محیط ابری
- مدیریت سرویس‌های ارائه شده توسط پلت فرم‌های خارجی
- درنظرگرفتن حفظ حریم خصوصی و صیانت از داده در معماری سازمانی، فعالیت‌های چرخه عمر توسعه سیستم، فرایندهای مهندسی سیستم‌ها و فرایندهای کسب‌وکار
- طراحی و معماری سامانه‌ها مبتنی بر حفظ حریم خصوصی[۱]
- اعمال مناسب مکانیزم‌های رمزنگاری بر روی داده‌های ذخیره شده و در حال انتقال
- پیاده‌سازی معماری عدم اعتماد[۲]در زیرساخت‌های ابری حیاتی اطلاعاتی
- به‌کارگیری فناوری‌های PET [۳]در زیرساخت‌های حیاتی ابری
- فراهم نمودن انواع خدمات ابری قابل‌دسترس مطلوب و رقابتی شامل منابع پردازشی، ذخیره‌سازی و کاربردهای ابری (IaaS، PaaS و SaaS) در سراسر کشور به‌منظور کاهش استقبال از پلت فرم‌های خارجی.

❖ راهکارهای راهبرد چهارم

- ایجاد ساختار سازمانی و یا تدوین شرح وظایفی جهت حفظ حریم خصوصی در زیرساخت‌های حیاتی
- تسریع در راه‌اندازی کامل شبکه ملی اطلاعات و سرویس‌های آن
- تشکیل رگولاتوری حفظ حریم خصوصی در کشور

۱- Privacy base design

۲- Zero Trust

۳ Privacy Enhance Technology

- ایجاد سازوکارهای نظارتی در حوزه مدیریت داده و حفظ حریم خصوصی و صیانت از داده
- ایجاد مرکزی جهت اطلاع، پیگیری و رسیدگی به سو استفاده از داده‌ها (شخصی، تجاری و حاکمیتی)
- حمایت جهت راه‌اندازی شبکه پایدار مطابق با استانداردهای جهانی با سرویس‌های ابری مقیاس‌پذیر و قابل‌توسعه و همچنین تحمل‌پذیر در مقابل انواع خرابی و فاجعه در بستر ارتباطات کشور
- تدوین اصول و چارچوب ارائه خدمات قابل‌قبول با قابلیت تضمین کیفیت در راستای اعتمادسازی
- ایجاد و توسعه مراکز داده و امکانات میزبانی داخلی جهت تولید و عرضه باکیفیت انواع خدمات پهن باند و امن داده.

❖ راهکارهای راهبرد پنجم

- حمایت از سرمایه‌گذاری و ایفای نقش بخش خصوصی در توسعه زیرساخت‌های ابری و سکوهای پایه و خدمات در ابعاد گوناگون
- توجیه‌پذیر نمودن فعالیت بخش خصوصی در حوزه حفظ حریم خصوصی داده
- ایجاد بازار عرضه محصولات و سرویس‌های حوزه حفظ حریم خصوصی و صیانت از داده
- سرمایه‌گذاری هدفمند حاکمیت در حوزه حفظ حریم خصوصی و صیانت از داده
- حمایت از شرکت‌های بخش خصوصی در تصاحب بازارهای بین‌المللی در حوزه حفظ حریم خصوصی
- نقش دادن به بخش خصوصی در تنظیم مقررات حفظ حریم خصوصی.

❖ راهکارهای راهبرد ششم

- اتخاذ رویکردهایی جهت هماهنگی با قوانین متفاوت در کشورهای مختلف
- همکاری‌های قضایی بین‌المللی جهت احقاق حقوق حاکمیت
- داشتن نقش فعال و تأثیرگذار در کمیسیون‌های بین‌المللی با رویکرد ملی و مذهبی
- همکاری‌های مشترک علمی و کاربردی بین‌المللی
- ایجاد ضابطه برای حضور فعالان خارجی در فضای مجازی کشور
- همکاری‌های بین‌المللی در خصوص مدیریت داده‌های فرامرزی

پیشنهادها

پیشنهادهای کاربردی

- تقویت جایگاه شورای‌عالی فضای مجازی و مرکز ملی به‌عنوان نهاد ارشد رصد، سیاست‌گذاری و مدیریت جریان داده بومی در کشور
- تسریع و تلاش ویژه مجلس شورای اسلامی برای تدوین و تصویب قوانین و مقررات حفظ حریم خصوصی، حق مالکیت و کسب‌وکار داده
- توجه و حمایت ویژه و پایدار برای راه‌اندازی شبکه ملی اطلاعات و سرویس‌های آن مانند موتور جستجوی بومی، شبکه اجتماعی فراگیر ملی با پوشش خدمات مالی و تجاری و آموزشی و زیرساخت‌های رایانش ابری برای هدایت داده‌های داخل به‌سوی کلان‌داده‌های بومی
- راه‌اندازی دوره‌های علمی – آموزشی و تخصصی حفظ حریم خصوصی داده
- راه‌اندازی مرکز تخصصی حکمرانی و رگلاتوری داده در عرصه سیاست‌گذاری و نظارت بر جریان داده کشور
- راه‌اندازی مراکز حمایت از سرمایه‌گذاری‌های داخلی و خارجی در حوزه رایانش ابری و حفظ حریم خصوصی داده.

پیشنهادهای پژوهشی

- تدوین نظام حفظ حریم خصوصی در فضای سایبری کشور

- ارائه الگوی مدل بلوغ حریم خصوصی داده‌ها در فضای سایبر کشور
- ارائه الگوی ارزیابی حریم خصوصی داده‌ها در فضای سایبر کشور
- تدوین الزامات اجرای نظام هویت در فضای سایبر کشور
- ارائه متدولوژی ارزیابی حریم خصوصی بر روی داده‌های کشور
- تدوین برنامه‌های عملیاتی حفظ حریم خصوصی داده‌ها در زیرساخت‌های رایانش ابری
- نگاشت نهادی در کشور برای حفظ حریم خصوصی داده‌های کشور
- اولویت‌بندی راهکارهای حفظ حریم خصوصی داده‌ها مبتنی بر کاهش ریسک
- ارزیابی تأثیر فناوری‌های جدید مانند زنجیره بلوکی بر روی حریم خصوصی داده‌ها.

فهرست منابع و مآخذ

الف. منابع فارسی

- دفتر حفظ و نشر آثار آیت الله خامنه ای. (۱۳۹۷). ***دیدار جمعی از مسئولان و مدیران نظام با رهبر انقلاب***. بازیابی ۲۶ آبان ۲۰۲۱، از https://farsi.khamenei.ir/news-content?id=39362
- رئوفی، علی‌اصغر؛ راد، محمد صادق جمشیدی و بافرانی، علیرضاپور. (۱۳۹۹) ***اصول حاکم بر لایحه حریم خصوصی***. مبانی فقهی حقوق اسلامی، ۲۵(۱۳)، ۱۳۵-۱۶۰.
- عبداللهی، علی؛ سیادت، سید حسین و اطهری فرد، علیرضا. (۱۳۹٤) ***رویکردی جامع برای بهبود امنیت سایبری زیرساخت‌های حیاتی کشور***. مقاله ارائه شده در پژوهش‌های کاربردی در مدیریت و حسابداری. دانشگاه شهید بهشتی.
- قاسمی، سجاد؛ کیومرثی، فرشاد و زمانی دهکردی، بهزاد. (۱۳۹٦) ***مروری بر ذخیره‌سازی و انتقال امن پیام در شبکه‌های مبتنی بر رایانش ابری***. مطالعات علوم کاربردی در مهندسی، ٦(۳)، ۱۷۹-۱۷۲.
- قناد، فاطمه و علیقلی، امیره. (۱۳۹۹) ***مفهوم و اهمیت داده‌های شخصی و حریم خصوصی و انواع حمایت از آن در فضای مجازی***. حقوق فناوری‌های نوین، ۱(۱)، ۲۹۷-۳۲۲.

- کریمی قهرودی، محمدرضا؛ محمدی، حافظ و سعادتمند، امیر مسعود. (۱٤۰۱) ***ارائه مدلی برای ارزیابی امنیت سایبری جمهوری اسلامی ایران***. امنیت ملی، ۱۲(٤٥)، ٦۹-۱۰۰.
- مهریزی، مهدی. (۱۳۷۸) ***دولت دینی و حریم خصوصی (بازخوانی فرمان هشت ماده ای امام خمینی(ره))***. پرتال جامع علوم انسانی، ۱۲(٤)، ٤٥-٦۹.

ب. منابع انگلیسی

- Akremi, Aymen; & Rouached, Mohsen. (2021). ***A comprehensive and holistic knowledge model for cloud privacy protection.*** The Journal of Supercomputing, 77(8), 7956-7988. https://doi.org/10.1007/s11227-020-03594-3
- Cloudflare. (2021). ***What is data privacy? | Privacy definition***. Retrieved May 14, 2021, from https://www.cloudflare.com/learning/privacy/what-is-data-privacy/
- DHS. (2017). ***RISKS TO CRITICAL INFRASTRUCTURE THAT USE CLOUD SERVICES***. Department of Homeland Security, Office of Cyber and Infrastructure Analysis.
- ENISA. (2020). ***ENISA Threat Landscape 2020 - Information Leakage.*** european union agency for cybersecurity.
- European Parliament. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation) (2016).
- Hinds, Joanne; Williams, Emma J.; & Joinson, Adam N. (2020). ***"It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal***. International Journal of Human-Computer Studies, 143, 102498. https://doi.org/10.1016/j.ijhcs.2020.102498
- ISO. (2014). ***ISO/IEC 17788 :Information technology*** — Cloud computing — Overview and vocabulary. the International Organization for Standardization.
- ISO. (2024). ***ISO/IEC 29100 :Information technology*** — Security techniques — Privacy framework. the International Organization for Standardization.
- ITU. (2021). ***Guide to Developing a National Cybersecurity Strategy***. The International Telecommunication Union (ITU).
- Mell, Peter; & Grance, Tim. (2011, September 28). ***The NIST Definition of Cloud Computing.*** National Institute of Standards and Technology. https://doi.org/https://doi.org/10.6028/NIST.SP.800-145
- NIST. (2020). ***NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK***

MANAGEMENT, VERSION 1.0. Gaithersburg, MD: National Institute of Standards and Technology.

- Paulsen, Celia; & Byers, Robert. (2019). ***Glossary of key information security terms. Gaithersburg,*** MD: National Institute of Standards and Technology.
- Quemard, Jean-Pierre; Schallabök, Jan; & Kamara, Irene. (2019). ***Guidance and gaps analysis for European standardisation Privacy standards in the information security***. ENISA.
- SINA. (2021). ***What is Data privacy?*** Retrieved May 14, 2021, from https://secure.livechatinc.com/
- Skendžić, A.; Kovačić, B.; & Tijan, E. (2018). ***General data protection regulation*** — Protection of personal data in an organisation. In 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). 1370-1375. https://doi.org/10.23919/MIPRO.2018.8400247
- Sun, PanJun. (2020***). Security and privacy protection in cloud computing: Discussions and challenges.*** Journal of Network and Computer Applications, 160, 102642. https://doi.org/10.1016/j.jnca.2020.102642
- Taghavi Zargar, Saman; Takabi, Hassan; & Iyer, Jay. (2019). ***Security- as- a- Service (SECaaS) in the Cloud.*** In Security, Privacy, and Digital Forensics in the Cloud (189-200). John Wiley & Sons, Ltd.

COPYRIGHTS