"چالش‌ها و راهکارهای مدیریت انتقال داده‌های حساس در صرافی‌های رمزارزی: امنیت، مسئولیت و ضرورت تمرکزگرایی"

داده‌های کسب‌وکارها، به‌ویژه در حوزه رمزارزها، حاوی اطلاعات حساسی نظیر تراکنش‌های مالی، هویت کاربران، و الگوهای رفتاری هستند. اگر سازمان‌ها در فرآیند اخذ این داده‌ها از کسب‌وکارها دچار غفلت شوند و این داده‌ها به‌صورت غیرمجاز یا ناامن افشا شوند، پیامدهای جدی به همراه خواهد داشت. با استفاده از تکنیک‌های داده‌کاوی **(Data Mining)** ، افراد یا گروه‌های غیرمجاز می‌توانند این داده‌ها را تحلیل کرده و از آن‌ها برای اهداف سوءاستفاده کنند. با توجه به شرایط حساس فعلی در کشور و تناقض هایی که میان منافع اشخاص و سازمان های مختلف در تنظیمگری حوزه رمزارز به وجود آمده است، لزوم آگاهی بخشی و صیانت از داده های حیاتی کاربران و صرافی ها در فضای ملتهب کنونی جهت جلوگیری از عدم استفاده دشمنان، کلاهبرداران و سازمان های آموزش دیده در این زمینه از اهمیت بسزایی برخوردار است. لذا از کلیه سازمان ها و کسب و کارهای محترم در فضای تبادل رمزدارایی ها درخواست میکنیم تا با در نظر گرفتن اصول امنیتی و حفاظت صحیح داده ها در فضای حرفه ای اقدام به انتقال داده نمایند.

۱– اهمیت داده‌های صرافی‌های رمزارزی و ضرورت مدیریت صحیح انتقال آنها

داده‌های صرافی‌های رمزارزی هدفی جذاب برای هکرها و مجرمان سایبری هستند. در دنیای پرمخاطره امروز، صرافی‌ها و سازمان‌ها باید با رعایت اصول امنیتی و حقوقی، تبادل داده‌ها را به حداقل رسانده و از انتقال ایمن و متمرکز اطلاعات اطمینان حاصل کنند. این اقدامات به ایجاد اعتماد و تقویت امنیت در بازار رمزارز کمک می‌کند.

۱–۱ داده‌های صرافی‌های رمزارزی: گنجی برای هکرها

داده‌های کاربران و تراکنش‌های صرافی‌های رمزارزی از ارزشمندترین اطلاعات در دنیای امروز هستند. این داده‌ها شامل اطلاعات حساس مانند مشخصات هویتی کاربران، الگوهای تراکنش، دارایی‌های دیجیتال، و روابط مالی می‌باشند. افشای این داده‌ها می‌تواند منجر به سوءاستفاده‌های گسترده، از کلاهبرداری و فیشینگ گرفته تا جرایم مالی پیچیده شود.

جدول ۱- گزارش حملات سایبری مرتبط با صرافی‌های رمزارزی

تاریخ حمله	صرافی/سازمان هدف	جزئیات حمله	پیامدها
2014	Mt. Gox	هک بزرگ اطلاعات کاربران و تراکنش‌ها که منجر به سرقت بیش از ۸۵۰,۰۰۰ بیت‌کوین شد.	اعتماد عمومی به صرافی‌های رمزارزی به شدت کاهش یافت.
2020	Ledger	نشت اطلاعات ۲۷۲,۰۰۰ کاربر شامل نام، ایمیل و آدرس کاربران به دلیل نقض امنیتی.	افزایش حملات فیشینگ و سرقت هویت کاربران.
2022	Binance	دسترسی غیرمجاز به کیف پول‌های کاربران و افشای بخشی از داده‌های تراکنش‌ها به دلیل سوءاستفاده از API.	سرقت ۵۷۰ میلیون دلار دارایی دیجیتال و آسیب جدی به اعتبار صرافی.
2023	Atomic Wallet	حمله به نرم‌افزار کیف پول مرتبط با کاربران صرافی‌ها و سرقت کلیدهای خصوصی آن‌ها.	سرقت میلیون‌ها دلار و افشای اطلاعات حساس کاربران.

خوشبختانه تا به امروز و با گذشت حداقل ۸ سال از فعالیت جدی صرافی های رمزارز در ایران و وجود کاربران پرشمار در این صرافی ها، اصول حفاظت از داده های کاربران در این صرافی ها به درستی رعایت شده است و گزارشی از تخلف و یا از دست رفت داده های کاربران وجود نداشته است. این امر نشان از درک اهمیت داده ها در شرکت های رمزدارایی میباشد و میباید این دستاورد ادامه دار و قابل اهتمام برای همه بازیگران این حوزه باشد.

۱-۲ کاربردهای داده‌کاوی در تحلیل داده‌های افشاشده

۱. تجزیه و تحلیل تراکنش‌ها

- **هدف سوءاستفاده** :شناسایی الگوهای تراکنش مالی کاربران، ردیابی فعالیت‌های اقتصادی، و تحلیل رفتار مالی.
- **پیامدها** :دسترسی غیرمجاز به تاریخچه تراکنش‌ها می‌تواند منجر به کلاهبرداری یا شناسایی اهداف مالی برای حملات سایبری شود.

۲. شناسایی هویت کاربران

- **هدف سوءاستفاده** :استفاده از داده‌های شناسایی مانند نام، شماره تماس، یا آدرس ایمیل برای سرقت هویت یا جعل مدارک.
- **پیامدها** :حملات فیشینگ، سرقت مالی، یا استفاده از هویت افراد در جرایم سایبری.

۳. پروفایل‌سازی رفتاری

- **تکنیک داده‌کاوی** :خوشه‌بندی (Clustering) و دسته‌بندی (Classification) برای ایجاد پروفایل از کاربران.
- **هدف سوءاستفاده** :تحلیل رفتار خرید، علاقه‌مندی‌ها، یا الگوهای استفاده از خدمات مالی.
- **پیامدها** :استفاده از این اطلاعات برای تبلیغات هدفمند غیرقانونی یا حملات مهندسی اجتماعی.

۴. تحلیل شبکه‌های اجتماعی کاربران

- **تکنیک داده‌کاوی** :تحلیل گراف (Graph Analysis) برای شناسایی ارتباطات میان کاربران.
- **هدف سوءاستفاده** :شناسایی روابط افراد، تراکنش‌های مشترک، یا ارتباطات تجاری.
- **پیامدها** :استفاده از این اطلاعات برای اهداف جاسوسی یا آسیب به روابط تجاری و شخصی.

۵. شناسایی نقاط ضعف امنیتی

- **هدف سوءاستفاده** :تحلیل داده‌ها برای یافتن الگوهای ضعف در سیستم‌های امنیتی کسب‌وکارها.
- **پیامدها** :اجرای حملات سایبری گسترده مانند نفوذ به حساب‌های کاربران یا سرقت دارایی‌های دیجیتال.

جدول ۲- چالش‌های سازمان‌ها و صرافی‌ها در مدیریت داده‌ها

چالش	شرح و توضیحات
چالش‌های سازمان‌ها	
ساختارهای قدیمی	بسیاری از سازمان‌ها هنوز از ساختارها و زیرساخت‌های قدیمی استفاده می‌کنند که با نیازهای امنیتی مدرن همخوانی ندارند.
عدم شفافیت	نبود شفافیت در فرآیندهای دریافت و استفاده از داده‌ها باعث کاهش اعتماد کسب‌وکارها به این سازمان‌ها می‌شود.
پیروی از قوانین امنیتی	بسیاری از سازمان‌ها به‌طور کامل از قوانین بین‌المللی و داخلی مرتبط با حریم خصوصی و امنیت داده‌ها تبعیت نمی‌کنند.
چالش‌های صرافی‌ها	
انتقال داده‌های متعدد	ارسال داده‌ها به چندین سازمان، بار عملیاتی و امنیتی زیادی برای صرافی‌ها ایجاد می‌کند و خطر اشتباه یا سوءاستفاده را افزایش می‌دهد.
دید حقوقی محدود	برخی صرافی‌ها دید کافی به تبعات حقوقی مرتبط با انتقال داده‌ها ندارند و این موضوع می‌تواند آن‌ها را در معرض مسئولیت‌های حقوقی قرار دهد.
پیچیدگی امنیتی	تضمین امنیت داده‌ها در هنگام انتقال به چندین سازمان نیازمند زیرساخت‌های پیشرفته و هزینه‌های قابل توجه است.

کاهش تبادل داده‌ها بین سازمان‌ها و تمرکز اطلاعات در یک نهاد واحد، می‌تواند ریسک افشای اطلاعات را کاهش دهد و امنیت کل زنجیره را افزایش دهد. سازمان‌ها باید مسئولیت بیشتری در قبال حفاظت از داده‌ها بپذیرند و صرافی‌ها نیز باید با رویکردی حرفه‌ای و حقوقی، انتقال داده‌ها را تنها در شرایط ایمن و قانونی انجام دهند. در عصر امروز که بسیاری از گروه‌های سایبری در کمین کوچک‌ترین سهل‌انگاری هستند، همکاری صرافی‌ها و سازمان‌ها برای ایجاد زیرساخت‌های امن و شفاف، نه تنها ضرورت بلکه الزامی است. پس در نظر گرفتن اصول کلی زیر قابل ملاحظه میباشد:

- **امنیت اطلاعات** :حفظ محرمانگی(Confidentiality) ، صحت(Integrity) ، و دسترس‌پذیری.(Availability)
- **حفظ حریم خصوصی کاربران** :فقط اطلاعات ضروری و مجاز باید منتقل شود.
- **شفافیت و انطباق قانونی** :هماهنگی با قوانین محلی، بین‌المللی، و چارچوب‌هایی مانند.GDPR

انتقال داده‌های محرمانه و حساس کاربران از سوی کسب‌وکارهای رمزارزی به نهادهای وابسته، چالش‌ها و پیامدهای متعددی به همراه دارد. در اینجا به تحلیل این موضوع، اصولی که باید رعایت شود، و دلایل قانونی که محدودیت‌هایی برای این نوع انتقال داده ایجاد می‌کنند می‌پردازیم.

۲- تحلیل تبعات انتقال داده‌های محرمانه

در این بخش به تبعات افشای داده ها ناشی از سهل انگاری یا نادیده گرفتن درک اهمیت موضوع توسط سازمان ها و کسب و کارها میپردازیم.

۱. نقض حریم خصوصی کاربران:

- اطلاعات کاربران شامل تراکنش‌ها، هویت، و فعالیت‌های مالی، جزء داده‌های حساس طبقه‌بندی می‌شوند. افشای این داده‌ها بدون رضایت کاربران، نقض آشکار حقوق حریم خصوصی است.

- بر اساس قوانین بین‌المللی مانند **GDPR**و اصول مشابه در برخی کشورهای دیگر، انتقال داده‌های شخصی به نهادهای ثالث بدون رضایت صریح ممنوع است.

۲. ریسک‌های امنیتی:

- هر انتقال داده‌ای، به‌ویژه از نوع محرمانه، ممکن است با حملات سایبری یا دسترسی غیرمجاز مواجه شود. زیرساخت‌های شرکت‌های واسطه مانند شاپرک باید برای مقابله با این تهدیدات بسیار قوی باشند.
- اگر این داده‌ها رمزنگاری و حفاظت مناسبی نداشته باشند، ریسک افشای اطلاعات و خسارت‌های مالی و اعتباری بسیار زیاد خواهد بود.

۳. پیامدهای قانونی:

- انتقال داده‌های مشتریان به سازمان‌های دولتی بدون پشتوانه حقوقی مشخص می‌تواند شرکت‌ها را در معرض پیگردهای قانونی قرار دهد.
- تضاد با اصل محرمانگی داده‌ها ممکن است اعتماد عمومی به کسب‌وکارهای رمزارزی را به شدت کاهش دهد.

۴. کاهش اعتماد کاربران:

- ارائه اطلاعات به نهادهای ثالث بدون شفافیت، می‌تواند اعتماد کاربران به کسب‌وکارهای رمزارزی را کاهش دهد.

۵. عدم انطباق با قوانین حمایت از داده:

- در ایران، قوانین مشخصی برای حفاظت از داده‌های شخصی وجود ندارد، اما بسیاری از اصول **حریم خصوصی جهانی** مثل GDPRو **قوانین حفاظت از داده در کشورهای مختلف** باید به‌طور غیرمستقیم رعایت شوند.

۲–۱ تبعات افشای داده‌ها

اکنون به بررسی تبعات افشای داده توسط بازیگران این اکوسیستم میپردازیم و ابعاد آن را از جنبه های مختلف بررسی میکنیم:

۱. برای سازمان دریافت‌کننده (دولتی):

- **پیامدهای قانونی** :اگر افشای داده‌ها به دلیل بی‌احتیاطی یا نقض پروتکل‌های امنیتی سازمان دولتی باشد، این سازمان ممکن است تحت پیگرد قانونی قرار گیرد.
- **کاهش اعتماد عمومی** :افشای داده‌ها می‌تواند به اعتبار سازمان دولتی آسیب بزند و موجب بی‌اعتمادی مردم شود.
- **پیامدهای سیاسی** :در صورت حساسیت داده‌ها، ممکن است این موضوع به یک بحران سیاسی تبدیل شود.

۲. برای کسب‌وکار ارائه‌دهنده داده‌ها:

- **کاهش اعتماد مشتریان** :حتی اگر مسئولیت افشا به عهده سازمان دولتی باشد، مشتریان ممکن است کسب‌وکار را نیز مقصر بدانند.
- **از دست رفتن مشتریان** :بی‌اعتمادی می‌تواند به کاهش مشتریان و آسیب به درآمد منجر شود.
- **پیامدهای حقوقی احتمالی** :اگر کسب‌وکار از ابتدا اطمینان کافی از ایمنی انتقال و ذخیره داده‌ها نگرفته باشد، ممکن است در بخشی از مسئولیت شریک شود.

۳. اگر داده‌ها به رسانه‌ها برسد:

- **آسیب به حریم خصوصی افراد:**
  - انتشار اطلاعات شخصی کاربران (مانند هویت، تراکنش‌های مالی) می‌تواند به سوءاستفاده‌های مختلف مانند کلاهبرداری یا سرقت هویت منجر شود.
- **پیامدهای اجتماعی:**
  - ممکن است نارضایتی عمومی و بحران‌های اجتماعی ایجاد شود.
- **پیامدهای امنیتی:**
  - در صورت حساسیت داده‌ها (مثلاً اطلاعات مالی یا امنیتی)، این افشا می‌تواند تبعات امنیتی برای کشور داشته باشد.

جدول ۳- ضرورت کاهش تبادل داده‌ها بین سازمان‌ها

موضوع	توضیحات
کاهش ریسک افشا	هرچه تعداد انتقال داده‌ها بیشتر باشد، احتمال افشای اطلاعات در یکی از این نقاط بیشتر می‌شود.
	تمرکز داده‌ها در یک سازمان یا نهاد مشخص باعث کاهش نقاط ضعف و افزایش کنترل می‌شود.
تمرکز بر امنیت	به‌جای ارسال داده‌ها به چندین سازمان، یک نهاد واحد می‌تواند با ایجاد زیرساخت‌های امنیتی پیشرفته از اطلاعات به‌طور متمرکز محافظت کند.
کاهش بار حقوقی کسب‌وکارها	کسب‌وکارهای رمزارزی با ارسال داده‌ها به چندین سازمان، در معرض مسئولیت‌های متعدد قرار می‌گیرند.
	انتقال متمرکز داده‌ها به یک نهاد قانونی مشخص، باعث کاهش پیچیدگی‌های حقوقی و ریسک‌های مرتبط می‌شود.

چه کسی پاسخگو است؟

۱. مطابق قوانین بین‌المللی:

- سازمان دریافت‌کننده داده (در اینجا سازمان دولتی) مسئولیت اصلی دارد.
- اگر قصوری از طرف کسب‌وکار ارائه‌دهنده در انتخاب روش انتقال یا بررسی امنیت وجود داشته باشد، ممکن است مسئولیت مشترک باشد.

۲. مطابق قوانین ایران:

- **ماده ۱ قانون مسئولیت مدنی** :اگر سازمان دولتی به دلیل بی‌احتیاطی موجب خسارت شود، مسئول جبران است.
- **ماده ۲۵ قانون جرایم رایانه‌ای** :هر شخص یا نهادی که داده‌ها را افشا کند، مسئولیت قانونی دارد.
- **سازمان‌ها موظف‌اند اقدامات پیشگیرانه انجام دهند:**
  - رمزنگاری داده‌ها.
  - محدودسازی دسترسی.
  - آموزش پرسنل در مورد حفاظت از اطلاعات.

جدول۴- ارزیابی اقتصادی افشای داده‌ها

بعد اقتصادی	توضیحات و جزئیات	پیامدهای افشای داده‌ها
هزینه مستقیم	هزینه‌های جبران خسارت به کاربران، بازیابی زیرساخت‌های امنیتی، و پرداخت جریمه‌های قانونی.	-جریمه‌های مالی سنگین توسط مراجع قانونی.
هزینه غیرمستقیم	از دست دادن اعتماد مشتریان، کاهش ارزش بازار، و افت درآمد.	-کاهش درآمد به دلیل کاهش کاربران و سرمایه‌گذاران.
هزینه‌های بلندمدت	کاهش جذابیت سرمایه‌گذاری در حوزه رمزارزها به دلیل افزایش ریسک امنیتی.	-تضعیف جایگاه رقابتی کسب‌وکار در بازار.

جدول ۵- تحلیل جامعه‌شناختی و روان‌شناختی افشای داده‌ها

جنبه اجتماعی/روانی	تأثیرات افشای داده‌ها	پیامدها و واکنش‌ها
بی‌اعتمادی اجتماعی	کاهش اعتماد عمومی به فناوری‌های جدید و سازمان‌های مرتبط با داده‌های حساس.	-کاهش مشارکت مردم در استفاده از خدمات دیجیتال.
اضطراب کاربران	افزایش نگرانی درباره امنیت اطلاعات شخصی.	-افت تعامل کاربران با صرافی‌ها و کاهش فعالیت در بازار رمزارز.
فشار بر کسب‌وکارها	افزایش انتقادهای عمومی به دلیل سوءمدیریت داده‌ها.	-کاهش سرمایه‌گذاری و تقاضای شفافیت بیشتر در مدیریت داده‌ها.

۲-۲ مسئولیت حفاظت از داده‌ها از سوی نهاد درخواست کننده

۱. مسئولیت اولیه: سازمان دریافت‌کننده داده‌ها

- **قاعده کلی** :سازمانی که داده‌ها را دریافت می‌کند (در اینجا سازمان دولتی)، مسئولیت اصلی حفاظت از داده‌ها و جلوگیری از افشای آن را دارد.
- **دلایل حقوقی:**
  - مطابق قوانین بین‌المللی مانند **GDPR**و اصول مشابه، سازمان دریافت‌کننده باید:
    - اقدامات امنیتی مناسب (مانند رمزنگاری و کنترل دسترسی) را پیاده‌سازی کند.
    - داده‌ها را فقط برای هدف مشخص استفاده کند.
  - در ایران، مطابق **ماده ۲۵ قانون جرایم رایانه‌ای**، هرگونه افشای غیرمجاز اطلاعات کاربران، جرم محسوب می‌شود و سازمان دولتی متخلف نیز مشمول این قانون است.

۲. مسئولیت کسب‌وکار ارائه‌دهنده داده‌ها

- **محدود به رعایت قوانین** :کسب‌وکارها موظفند فقط داده‌های لازم و طبق مقررات قانونی منتقل کنند.
- **مفاد قرارداد** :اگر کسب‌وکار اطمینان حاصل نکرده باشد که سازمان دولتی اقدامات لازم برای حفاظت از داده‌ها را انجام داده است، ممکن است در بخشی از مسئولیت شریک شود.

جدول ۶- پیشنهادات برای پیشگیری از افشای داده‌ها

راهکار	توضیحات
محدودسازی انتقال داده‌ها	انتقال فقط داده‌های ضروری و کمینه‌سازی اطلاعات حساس.
پروتکل‌های امنیتی پیشرفته	رمزنگاری داده‌ها و استفاده از کانال‌های انتقال امنTLS. SFTP
تدوین قرارداد شفاف	تنظیم قرارداد میان کسب‌وکار و سازمان دولتی که مسئولیت حفاظت از داده‌ها را مشخص کند.
ثبت و پایش دقیق	تمامی انتقال‌ها و دسترسی‌ها باید ثبت و پایش شوند.
آموزش پرسنل	آموزش کارکنان سازمان دولتی و کسب‌وکار در زمینه امنیت داده و مدیریت ریسک.

جدول ۷- تبعات قانونی و اجتماعی افشای داده‌ها

ابعاد	توضیحات
قانونی	-مجازات‌های قانونی (جریمه، حبس).
	-احتمال دعاوی حقوقی از سوی مشتریان.
مالی	-کاهش درآمد به دلیل از دست رفتن اعتماد کاربران.
	-پرداخت خسارت به کاربران در صورت شکایت.
اجتماعی	-بحران‌های اجتماعی ناشی از افشای داده‌های حساس.
	-افزایش بی‌اعتمادی عمومی به نهادهای دولتی و کسب‌وکارها.
امنیتی	-احتمال سوءاستفاده از داده‌ها برای جرایم سایبری.

جدول ۸ - تکنولوژی‌های پیشرفته برای مدیریت داده‌ها

تکنولوژی	کاربرد	جزئیات و مزایا
بلاکچین	استفاده برای ذخیره و انتقال امن داده‌ها.	-شفافیت کامل در تراکنش‌ها.
رمزنگاری پیشرفته	حفاظت از داده‌ها در هنگام انتقال و ذخیره‌سازی.	-استفاده از الگوریتم‌هایی مانند AES-256 برای جلوگیری از دسترسی غیرمجاز.
هوش مصنوعی (AI)	تحلیل داده‌ها برای شناسایی الگوهای تهدید.	-تشخیص و پیشگیری از حملات سایبری.
SIEM	مدیریت امنیت اطلاعات و رویدادها.	-یکپارچه‌سازی نظارت بر امنیت و ارائه هشدارهای فوری.

حال که با تبعات انتقال داده و سهل انگاری در پیامدهای آن آشنا شدیم، به موضوع و راه کارهای ساز و کار انتقال داده در بخش های بعدی میپردازیم و پیشنهادها و ملاحظاتی را در این زمینه مطرح مینماییم.

۳– بررسی قوانین انتقال داده میان سازمان ها و کسب و کارها

در این بخش که به نوعی مهمترین عامل جهت درک تبعات حفظ داده و ساز و کار انتقال آن به سازمان های دولتی و خصوصی از منظر کسب و کارها و نهادهای ذیربط میباشد، به قوانین جاری بر نحوه انتقال دیتا در صرافی های رمزارز میپردازیم و مواردی از اقدامات مشابه در سایر کشورها را نیز مرور میکنیم.

۳–۱ مفاد قانونی مرتبط

۱. ماده ۴ قانون حمایت از حقوق مصرف‌کننده:

کسب‌وکارها موظفند داده‌های کاربران را به شیوه‌ای ایمن نگهداری کرده و فقط با رضایت صریح کاربر منتقل کنند.

۲. اصول GDPR:

- **ماده ۶** :انتقال داده فقط در صورت داشتن دلایل قانونی و با رضایت کاربر مجاز است.
- **ماده ۷** :هرگونه رضایت باید مشخص، قابل‌پیگیری، و قابل بازپس‌گیری باشد.
- **ماده ۲۵** :حفاظت از داده‌ها باید از طراحی اولیه رعایت شود.

۳. ماده ۳ قانون تجارت الکترونیکی ایران:

انتقال داده‌های کاربران بدون توافق صریح، مصداق نقض قوانین تجارت الکترونیک است.

۴. مقررات FATF و AML/CFT:

این مقررات بر اساس جلوگیری از پولشویی ممکن است دلایل نظارتی ارائه داده باشند، اما کسب‌وکارها باید مطمئن شوند که اطلاعات فراتر از نیاز، به اشتراک گذاشته نشود.

۵. اصل محرمانگی بانکی:

بانک‌ها و نهادهای مالی، از جمله صرافی‌های رمزارزی، ملزم به رعایت اصل محرمانگی در اطلاعات مشتریان هستند. افشای این اطلاعات تنها با دستور قضایی ممکن است.

۶. تضاد با مسئولیت حرفه‌ای:

- هرگونه افشای اطلاعات بدون رضایت مشتری می‌تواند کسب‌وکارها را در برابر دعاوی حقوقی قرار دهد.

در ادامه جدول شامل قوانین و مقررات کلیدی امنیت داده و انتقال داده در سطح بین‌المللی و ایران را بررسی میکنیم.

جدول۹- قوانین امنیت داده و سازوکار انتقال داده (بین‌المللی و ایران)

قانون/چارچوب	کشور/منطقه	نکات کلیدی و ملاحظات	تبعات عدم رعایت
GDPR	اتحادیه اروپا	-نیاز به رضایت کاربران برای پردازش و انتقال داده.	-جریمه مالی تا ۲۰ میلیون یورو یا ۴٪ از درآمد سالانه.
		-انتقال داده به کشورهای ثالث تنها در صورت رعایت استانداردهای مشابه.	-از دست دادن اعتماد کاربران و مشتریان.
		-اصل Data Minimization) انتقال حداقل داده لازم.)	
CCPA	ایالات متحده (کالیفرنیا)	-حق کاربران برای اطلاع از نحوه استفاده از داده‌هایشان.	-جریمه مالی تا ۷,۵۰۰ دلار برای هر مورد تخلف.
		-الزامات سخت‌گیرانه برای فروش یا انتقال داده به طرف ثالث.	-آسیب به اعتبار شرکت در بازار ایالات متحده.
PIPEDA	کانادا	-تعهد به حفظ حریم خصوصی داده‌ها.	-جریمه تا سقف ۱۰۰,۰۰۰ دلار کانادا برای هر تخلف.
		-سازمان‌ها باید سیاست‌های امنیت داده خود را مستند کنند.	
قانون جرایم رایانه‌ای	ایران	-ماده ۲۵: افشای داده‌های کاربران بدون رضایت یا دستور قضایی جرم محسوب می‌شود.	-مجازات حبس از ۹۱ روز تا ۲ سال یا جریمه نقدی.
		-الزامات برای ثبت و حفاظت از داده‌های کاربران در شرکت‌های فناوری.	
آیین‌نامه اجرایی حمایت از داده‌ها	ایران	-الزامات نگهداری داده‌های مشتریان در سرورهای داخلی ایران.	-تعلیق فعالیت کسب‌وکار و جریمه نقدی.
		-انتقال داده‌های حساس کاربران تنها با مجوز مقامات قضایی امکان‌پذیر است.	
قانون حمایت از مصرف‌کننده	استرالیا	-نیاز به رضایت کاربر برای استفاده از داده‌ها.	-جریمه‌های سنگین و حذف مجوز فعالیت در استرالیا.
قوانین AML/CFT	بین‌المللی	-الزام به ثبت و گزارش تراکنش‌های مشکوک به نهادهای نظارتی.	-ممنوعیت فعالیت در سطح بین‌المللی و جریمه‌های مالی سنگین.
		-الزامات امنیتی برای حفظ حریم کاربران در کنار مقابله با پولشویی.	
PDPA	سنگاپور	-نیاز به شفافیت کامل در نحوه استفاده و انتقال داده‌ها.	-جریمه تا ۱ میلیون دلار سنگاپور.

		-ذخیره و انتقال داده‌های حساس باید مطابق استانداردهای امنیتی مشخص انجام شود.	
قانون حفاظت از داده‌ها	آفریقای جنوبی	-محدودیت‌های شدید برای انتقال داده‌ها به خارج از کشور.	-جریمه تا ۱۰ میلیون رند یا حبس.

با توجه به عملکرد سایر کشورها در وضع قوانین و جرایم روی داده های صرافی ها و اهتمام به صیانت از این داده ها ملاحظاتی مد نظر قرار میگیرد:

۱. **اصل رضایت کاربر** :قوانین بین‌المللی و داخلی به وضوح بر رضایت کاربر برای پردازش یا انتقال داده تأکید دارند.
۲. **محدودیت‌های جغرافیایی** :انتقال داده‌ها به کشورهای دیگر نیازمند رعایت استانداردهای محلی و بین‌المللی است.
۳. **شفافیت و گزارش‌دهی** :کسب‌وکارها باید نحوه استفاده و انتقال داده را شفاف‌سازی کرده و گزارش دهند.
۴. **امنیت داده** :رمزنگاری، کنترل دسترسی، و ثبت فعالیت‌ها از الزامات مشترک همه قوانین است.

چرا رعایت این قوانین ضروری است؟

- **حفظ اعتماد مشتری** :مشتریان انتظار دارند که اطلاعاتشان امن و محرمانه باقی بماند.
- **جلوگیری از مجازات‌های مالی و قضایی** :عدم رعایت قوانین ممکن است به جریمه‌های سنگین و حتی تعلیق فعالیت منجر شود.
- **حفظ اعتبار کسب‌وکار** :نقض قوانین می‌تواند به شدت به شهرت یک شرکت آسیب بزند.

۳–۲ دلایل مخالفت با انتقال داده‌ها به سازمان‌های واسطه و یا بخش خصوصی توسط کسب و کارها:

۱. عدم شفافیت در فرآیند:
- عدم اطلاع کسب و کارها از اینکه داده‌ها به سازمان واسطه منتقل می‌شود، می‌تواند ناقض اصل شفافیت باشد.

۲. عدم رعایت حداقل‌گرایی:
- سازمان ها میبایست دقیقاً مشخص کنند چه داده‌هایی ضروری است و چرا.

۳. تعارض با قوانین حفاظت از داده:
- ارائه داده‌های جزئی کاربران بدون رضایت آن‌ها می‌تواند قوانین بین‌المللی یا ملی را نقض کند.

۴. مشکل حقوقی در احراز صلاحیت:
- شرکت های خصوصی به‌عنوان واسطه میان سازمان های دولتی و کسب و کارها، ممکن است خود توانایی لازم برای حفظ امنیت و حریم خصوصی داده‌ها را نداشته باشد.

۴– ساز و کار انتقال داده میان کسب و کارها و سازمان ها

در این بخش به ساز و کار پیشنهادی انتقال داده میان کسب و کارها و سازمان ها میپردازیم و از اهمیت اهتمام و پایبندی به این ساز و کار خواهیم گفت و همچنین به راه کارهای امنیتی برای اجرای چنین ساز و کارهایی اشاره خواهیم کرد.

جدول۱۰- پروتکل پیشنهادی

بخش	جزئیات و توضیحات
مرحله ۱: درخواست	سازمان درخواست‌کننده باید درخواست رسمی شامل جزئیات داده‌های موردنیاز، هدف استفاده، و مجوزهای قانونی ارائه دهد.
مرحله ۲: شناسایی	بررسی هویت سازمان درخواست‌کننده از طریق احراز هویت دو مرحله‌ای (Two-Factor Authentication) و تأیید اعتبار.
مرحله ۳: انتخاب داده‌ها	داده‌های مورد نیاز بر اساس اصل کمینه‌سازی داده (Data Minimization) انتخاب شوند. اطلاعات اضافی نباید منتقل شود.
مرحله ۴: رمزنگاری	داده‌ها قبل از انتقال با استفاده از الگوریتم‌های رمزنگاری قوی) مانند (AES-256 رمزگذاری شوند.
مرحله ۵: کانال امن	استفاده از پروتکل‌های انتقال امن مانند **HTTPS** یا **SFTP**برای جلوگیری از شنود و دسترسی غیرمجاز.
مرحله ۶: ثبت رویدادها	ثبت کلیه فعالیت‌ها و انتقال‌ها در یک سیستم لاگینگ برای امکان ردیابی.
مرحله ۷: انطباق قانونی	داده‌های منتقل‌شده باید با قوانین مربوطه) مانندGDPR ، (AML/CFTانطباق داشته باشند.
مرحله ۸: تأیید نهایی	تأیید دریافت داده‌ها و تطابق آن با اطلاعات ارسال‌شده توسط سازمان دریافت‌کننده.
مرحله ۹: انقضای دسترسی	داده‌های ارسال‌شده باید فقط برای مدت مشخص استفاده شوند و پس از آن پاک شوند.

۴-۱ مراحل پلکانی دریافت و ارسال داده

گام اول: مراحل دریافت داده توسط سازمان‌ها از کسب‌وکارها

مرحله	شرح مرحله	ملاحظات امنیتی و حرفه‌ای
۱ .درخواست رسمی	سازمان باید درخواست رسمی شامل جزئیات داده‌های مورد نیاز، هدف استفاده، و پشتوانه قانونی ارائه کند.	-درخواست باید شفاف، مستند، و به تایید قانونی رسیده باشد.
۲ .تأیید اعتبار	کسب‌وکار باید هویت و اعتبار سازمان درخواست‌کننده را بررسی و تأیید کند.	-استفاده از احراز هویت دو عاملی یا مجوزهای دیجیتال برای تأیید سازمان درخواست‌کننده.
۳ .بررسی انطباق قانونی	کسب‌وکار باید درخواست را با قوانین محلی و بین‌المللی) مانند GDPR، قانون جرایم رایانه‌ای (تطبیق دهد.	-مشاوره حقوقی برای اطمینان از انطباق قانونی.
۴ .مذاکره و تنظیم قرارداد	کسب‌وکار و سازمان باید قراردادی شفاف برای تعیین مسئولیت‌ها و محدوده داده‌ها تنظیم کنند.	-قرارداد باید شامل بندهای امنیتی، حریم خصوصی، و محدودیت‌های استفاده از داده باشد.
۵ .تأیید رضایت کاربران	در صورت نیاز، کسب‌وکار باید از کاربران رضایت صریح برای انتقال داده‌ها به سازمان دریافت کند.	-ایجاد فرآیند شفاف برای اطلاع‌رسانی به کاربران و اخذ رضایت آن‌ها.

۶ .تأیید نهایی درخواست	کسب‌وکار پس از انجام بررسی‌های لازم، تأییدیه رسمی برای انتقال داده صادر می‌کند.	-مستندسازی کامل تصمیم‌گیری و ثبت آن در سیستم.

گام دوم: مراحل ارسال داده توسط کسب‌وکارها به سازمان‌ها

مرحله	شرح مرحله	ملاحظات امنیتی و حرفه‌ای
۱ .انتخاب داده‌های ضروری	فقط داده‌های ضروری و مرتبط با درخواست انتخاب شوند و از انتقال اطلاعات اضافی جلوگیری شود.	-رعایت اصل Data Minimization برای کاهش ریسک افشا.
۲ .رمزنگاری داده‌ها	داده‌ها باید با الگوریتم‌های قوی) مانند (AES-256 رمزنگاری شوند تا در حین انتقال امن باقی بمانند.	-استفاده از کلیدهای رمزنگاری که تنها برای افراد مجاز در دسترس باشند.
۳ .انتقال از کانال امن	داده‌ها باید از طریق کانال‌های امن مانند **TLS 1.3** یا **SFTP** به سازمان ارسال شوند.	-جلوگیری از استفاده از کانال‌های ناامن مانند ایمیل یا پروتکل‌های قدیمی.
۴ .ثبت رویدادها و گزارش‌دهی	تمامی مراحل انتقال باید در سیستم لاگینگ ثبت شوند تا در صورت نیاز قابل بازبینی باشند.	-ثبت اطلاعاتی مانند زمان انتقال، نوع داده، و هویت افراد مسئول.
۵ .تأیید دریافت	پس از انتقال، سازمان دریافت‌کننده باید تأییدیه‌ای مبنی بر دریافت داده‌ها و صحت آن‌ها ارائه دهد.	-کسب‌وکار باید مستندات دریافت داده‌ها را به‌روزرسانی کند.
۶ .پیگیری پایش و امنیت	کسب‌وکار باید در دوره‌ای مشخص امنیت داده‌های منتقل‌شده و استفاده صحیح از آن‌ها را پایش کند.	-بررسی مستمر تطابق استفاده از داده‌ها با شرایط تعیین‌شده در قرارداد.

۴-۲ اصول امنیتی در انتخاب و انتقال داده:

رعایت اصول امنیتی در انتقال داده‌ها شامل استفاده از پروتکل‌های امن مانند رمزنگاری پیشرفته (AES-256) و کانال‌های امن TLS) یا(SFTP ، کنترل دسترسی به داده‌ها، و ثبت و پایش تمامی فعالیت‌های مرتبط است. این اقدامات نه تنها از افشای اطلاعات و سوءاستفاده جلوگیری می‌کند، بلکه اعتماد کاربران را افزایش داده و کسب‌وکارها را در برابر پیامدهای قانونی و مالی حفاظت می‌کند. رعایت این اصول باید به‌عنوان یک الزام اساسی در هر فرآیند انتقال داده در نظر گرفته شود.

جدول۱۱- اصول امنیتی در انتقال داده ها

حوزه امنیتی	جزئیات
کنترل دسترسی (ACL)	تعیین سطح دسترسی دقیق برای کاربران و سازمان‌ها به داده‌های حساس.
رمزنگاری پیشرفته	استفاده از الگوریتم‌های قوی مانند AES-256 و TLS 1.3 برای انتقال داده.
پایش لحظه‌ای	پایش لحظه‌ای کانال‌های ارتباطی برای شناسایی رفتارهای مشکوک یا نفوذ.
امنیت نقطه پایانی	استفاده از ابزارهای امنیتی مانند VPN و آنتی‌ویروس در هر دو طرف انتقال داده.

جدول۱۲- اصول انتقال داده امن و قانونی

اصل	شرح
محرمانگی (Confidentiality)	داده‌های کاربران فقط باید به نهادهای مجاز و با دلایل قانونی معتبر منتقل شود.
حداقل‌گرایی داده (Data Minimization)	فقط داده‌های ضروری منتقل شود. مثلاً به‌جای انتقال کامل تراکنش‌ها، داده‌های جمع‌آوری‌شده یا ناشناس‌سازی‌شده انتقال یابد. اصل **Data Minimization**: فقط داده‌های ضروری و مشخص منتقل شود و از انتقال کل پایگاه داده اجتناب شود.
شفافیت (Transparency)	کسب‌وکار باید کاربران را مطلع کند که چه داده‌هایی، چرا، و به چه سازمانی منتقل می‌شود.
رمزنگاری قوی / کانال انتقال امن	استفاده از پروتکل‌های رمزنگاری (AES-256) و کانال‌های انتقال امن (HTTPS، SFTP) برای جلوگیری از شنود و نفوذ. استفاده از پروتکل‌های امن مانند **TLS 1.3** یا **SFTP** برای انتقال داده‌ها.
قوانین داده (Data Laws) /انطباق با قانون	کسب‌وکارها باید با قوانین محلی) مانند GDPR، CCPA یا قوانین ملی (انطباق داشته باشند و از انتقال غیرقانونی داده جلوگیری کنند. بررسی قوانین داخلی و بین‌المللی در خصوص انتقال داده و انطباق با آن‌ها.
ثبت رویدادها (Logging)	تمام مراحل انتقال داده باید در سیستم ثبت شود تا امکان پیگیری و تحلیل در صورت بروز مشکل فراهم شود.
محدودیت در استفاده (Purpose Limitation)	داده‌ها فقط باید برای هدف مشخص و قانونی استفاده شوند و بعد از استفاده، حذف شوند.
دوره نگهداری داده	مشخص کردن بازه زمانی نگهداری داده‌ها توسط سازمان دریافت‌کننده و اطمینان از پاک‌سازی آن‌ها پس از انقضا.
کنترل دسترسی	تعیین دسترسی محدود برای افرادی که به داده‌های منتقل‌شده دسترسی دارند.

۴-۳ راهکار پیشنهادی برای انتقال داده‌های محرمانه

پرداختن به راهکارهای انتقال داده‌های محرمانه از اهمیت بالایی برخوردار است، زیرا این داده‌ها قلب اعتماد کاربران به کسب‌وکارها و سازمان‌ها هستند. راهکارهای مناسب نه تنها از افشای اطلاعات و پیامدهای قانونی و مالی جلوگیری می‌کنند، بلکه به بهبود شفافیت، امنیت و اعتبار کسب‌وکار کمک می‌کنند. ارائه روش‌های استاندارد و قابل اجرا برای مدیریت انتقال داده‌ها، به سازمان‌ها امکان می‌دهد تا با رویکردی پیشگیرانه، از بحران‌های احتمالی جلوگیری کرده و اعتماد عمومی را حفظ کنند. این راهکارها به‌ویژه در حوزه‌های حساس مانند رمزارزها، از ارزش استراتژیک برخوردارند.

جدول۱۳- بررسی راه کارهای انتقال امن داده ها

بخش	توضیحات
قرارداد شفاف	-تنظیم قراردادی که شامل موارد زیر باشد:
	-**هدف انتقال داده‌ها**)مانند تحلیل، پایش، یا انطباق قانونی.(
	-**نوع داده‌ها** :فقط داده‌های ضروری (مانند تراکنش‌ها، نه اطلاعات هویتی کامل).
	-**مسئولیت سازمان دریافت‌کننده** :تضمین امنیت داده‌ها و استفاده محدود به هدف مشخص.
	-**نظارت و پایش مداوم** بر نحوه استفاده از داده‌ها.
پروتکل‌های امنیتی	-استفاده از موارد زیر برای اطمینان از امنیت انتقال داده:
	-**رمزنگاری داده‌ها** :رمزنگاری با استاندارد.AES-256
	-**کانال انتقال امن** :استفاده از TLS 1.3 یا.SFTP
	-**ثبت فعالیت‌ها** :لاگینگ تمام فعالیت‌های انتقال و دسترسی به داده‌ها.
رضایت کاربران	-اخذ رضایت صریح از کاربران پیش از انتقال داده‌ها.
	-کاربران باید از **ماهیت داده‌های انتقالی**، **هدف استفاده** و **سازمان دریافت‌کننده** مطلع باشند.
	-ایجاد گزینه‌ای برای **رد یا تأیید انتقال** در پروفایل کاربری یا قرارداد.
تطابق قانونی	-بررسی و انطباق فرایند انتقال داده با قوانین محلی و بین‌المللی:
	-**قوانین داخلی** :مانند قوانین حمایت از داده‌ها یا اصول بانکی.
	-**چارچوب‌های بین‌المللی** :مانند) GDPR رعایت حقوق داده‌های شخصی.(
نظارت و گزارش‌دهی	-ایجاد سیستم نظارت بر فرآیند انتقال داده:
	-**ثبت گزارشات منظم** از میزان داده‌های منتقل‌شده.
	-بررسی تطابق داده‌های منتقل‌شده با اهداف ذکرشده در قرارداد.
	-نظارت بر امنیت و عدم وجود نقض یا افشای اطلاعات.
دوره نگهداری داده‌ها	-تعیین دوره زمانی مشخص برای نگهداری داده‌های منتقل‌شده توسط سازمان دریافت‌کننده.
	-حذف داده‌ها پس از پایان دوره.
	-تضمین **عدم بازنشر یا استفاده اضافی** از داده‌ها.

جدول ۱۴- تقسیم‌بندی جزئی‌تر پروتکل‌های امنیتی

مرحله	راهکار امنیتی
پیش از انتقال	-تأیید هویت سازمان درخواست‌کننده.
	-انتخاب دقیق داده‌های ضروری برای انتقال.
	-آماده‌سازی گزارش اولیه از داده‌ها.
حین انتقال	-رمزنگاری داده‌ها با استاندارد AES-256.
	-انتقال داده‌ها از کانال امن (TLS 1.3 یا SFTP).
	-نظارت لحظه‌ای برای شناسایی نفوذ احتمالی.
پس از انتقال	-تأیید دریافت داده‌ها توسط سازمان مقصد.
	-تطبیق داده‌های منتقل‌شده با موارد تعریف‌شده در قرارداد.
	-ثبت فعالیت‌ها در سیستم لاگینگ برای امکان بازبینی.