Submit Date: 15 June 2024
Revise Date: 10 August 2024
Accept Date: 17 August 2024
Publish Date: 10 September 2024

The Encyclopedia of Comparative Jurisprudence and Law



# Analysis of the Civil Liability of Information Technology Contractors for Cyberattacks on Industrial Control Systems in the South Pars Refineries

Naser Mohammadnejad[1]*, Seyed Mostafa Hashemi[2]

1. Master's Student and Researcher in Private Law, Department of Law, Yas.C., Islamic Azad University, Yasuj, Iran
2. Assistant Professor, Department of law, Yas.C., Islamic Azad University, Yasuj, Iran

* Corresponding Author's Email: nasermohamadnejhad@iau.ir

## ABSTRACT

Digital transformation in the oil and gas industry, particularly in critical infrastructure such as the South Pars refineries, has increased efficiency, data integration, automation, and reduced operational costs. At the same time, however, it has significantly expanded the cyberattack surface. In this context, information technology contractors, who play a central role in the design, installation, maintenance, updating, support, and integration of operational technology systems and industrial control systems, may incur civil liability when cyberattacks occur. The principal question addressed in this article is: What is the legal basis for the civil liability of these contractors for damage arising from attacks on industrial control systems in the South Pars refineries? Employing a descriptive-analytical method and an argumentative approach, and drawing on legal sources, industrial cybersecurity standards, and experience gained from major cyberattacks, this study demonstrates that a contractor's mere reliance on technical complexity or the professional nature of the risks is insufficient to exempt it from liability. Rather, civil liability may be established whenever negligence is proven in secure system design, network segmentation, security patch management, access control, event logging, continuous monitoring, or user training. The article further concludes that, in information technology contracts concerning critical infrastructure, the traditional obligation-of-means model should be reconceptualized in favor of a heightened professional duty of care. This approach should be complemented by stronger contractual mechanisms, including risk allocation, cyber insurance, explicit obligations to comply with applicable standards, and security-audit clauses.

***Keywords:*** *civil liability, information technology contractor, cyberattack, industrial control systems, South Pars refineries.*

How to cite: Mohammadnejad, N. & Hashemi, S. M. (2024). Analysis of the Civil Liability of Information Technology Contractors for Cyberattacks on Industrial Control Systems in the South Pars Refineries. *The Encyclopedia of Comparative Jurisprudence and Law*, *2*(2), 430-447.

تاریخ ارسال: ۲۶ خرداد ۱۴۰۳
تاریخ بازنگری: ۲۰ مرداد ۱۴۰۳
تاریخ پذیرش: ۲۷ مرداد ۱۴۰۳
تاریخ چاپ: ۲۰ شهریور ۱۴۰۳

دانشنامه فقه و حقوق تطبیقی

# تحلیل مسئولیت مدنی پیمانکاران فناوری اطلاعات در برابر حملات سایبری به سیستم‌های کنترل صنعتی در پالایشگاه‌های پارس جنوبی

ناصر محمدنژاد[1*]، سید مصطفی هاشمی[2]

۱. دانشجوی کارشناسی ارشد و پژوهشگر حقوق خصوصی، گروه حقوق، واحد یاسوج، دانشگاه آزاد اسلامی، یاسوج، ایران
۲. استادیار، گروه حقوق، واحد یاسوج، دانشگاه آزاد اسلامی، یاسوج، ایران
* پست الکترونیک نویسنده مسئول: nasermohamadnejhad@iau.ir

## چکیده

تحول دیجیتال در صنعت نفت و گاز، به‌ویژه در زیرساخت‌های حساس نظیر پالایشگاه‌های پارس جنوبی، اگرچه موجب افزایش بهره‌وری، یکپارچگی داده‌ها، اتوماسیون و کاهش هزینه‌های عملیاتی شده است، اما هم‌زمان سطح حمله سایبری را نیز به‌طور معناداری گسترش داده است. در این میان، پیمانکاران فناوری اطلاعات که در طراحی، نصب، نگهداری، به‌روزرسانی، پشتیبانی و یکپارچه‌سازی سامانه‌های فناوری عملیاتی و سیستم‌های کنترل صنعتی نقش محوری دارند، در صورت وقوع حملات سایبری می‌توانند در معرض مسئولیت مدنی قرار گیرند. مسئله اصلی این مقاله آن است که مبنای مسئولیت مدنی این پیمانکاران در برابر خسارات ناشی از حمله به سامانه‌های کنترل صنعتی در پالایشگاه‌های پارس جنوبی چیست؟ این پژوهش با روش توصیفی-تحلیلی و رویکردی استدلالی، ضمن بهره‌گیری از منابع حقوقی، استانداردهای امنیت صنعتی و تجربه حملات مهم سایبری، نشان می‌دهد که صرف استناد پیمانکار به پیچیدگی فنی یا حرفه‌ای بودن مخاطرات، برای رهایی از مسئولیت کفایت نمی‌کند؛ بلکه هرگاه قصور در طراحی امن، تفکیک شبکه، مدیریت وصله‌های امنیتی، کنترل دسترسی، ثبت رخداد، پایش مستمر یا آموزش کاربران اثبات شود، مسئولیت مدنی وی قابل استقرار خواهد بود. همچنین مقاله نتیجه می‌گیرد که در قراردادهای فناوری اطلاعات مربوط به زیرساخت‌های حیاتی، باید الگوی سنتی تعهد به وسیله به نفع تعهد حرفه‌ایِ مشدد بازخوانی شود و در کنار آن، سازوکارهای قراردادی نظیر تقسیم ریسک، بیمه سایبری، تعهدات صریح انطباق با استانداردها و شروط بازرسی امنیتی تقویت گردد.

**کلیدواژگان:** *مسئولیت مدنی، پیمانکار فناوری اطلاعات، حمله سایبری، سیستم‌های کنترل صنعتی، پالایشگاه‌های پارس جنوبی.*

**نحوه استناددهی:** محمدنژاد، ناصر.، و هاشمی، سید مصطفی. (۱۴۰۳). تحلیل مسئولیت مدنی پیمانکاران فناوری اطلاعات در برابر حملات سایبری به سیستم‌های کنترل صنعتی در پالایشگاه‌های پارس جنوبی. *دانشنامه فقه و حقوق تطبیقی*، ۲ (۲)، ۴۴۷-۴۳۰.

**مقدمه**

دیجیتالی‌شدن زیرساخت‌های صنعتی، مرزهای سنتی میان فناوری اطلاعات (IT) و فناوری عملیاتی (OT) را کم‌رنگ کرده است. در پالایشگاه‌ها، سامانه‌های کنترل توزیع‌شده، اسکادا، کنترلرهای منطقی برنامه‌پذیر، سامانه‌های ایمنی ابزار دقیق و بسترهای تبادل داده صنعتی، اکنون نه‌تنها مأموریت کنترلی دارند، بلکه با سامانه‌های مدیریتی، انبار، تعمیرات، برنامه‌ریزی و حتی خدمات ابری نیز تعامل می‌کنند. این همگرایی، کارایی را افزایش داده، اما آسیب‌پذیری را نیز تشدید کرده است؛ زیرا هر نقطه اتصال جدید می‌تواند دریچه‌ای برای نفوذ باشد (Stouffer et al., 2023).

پالایشگاه‌های پارس جنوبی، به‌عنوان بخش مهمی از زنجیره انرژی کشور، نمونه بارز زیرساخت حیاتی‌اند. هرگونه اختلال در سامانه‌های کنترل صنعتی (ISC) این مجموعه، صرفاً یک رویداد فنی محدود نیست، بلکه می‌تواند به توقف تولید، انفجار، آتش‌سوزی، نشت مواد خطرناک، آسیب به کارکنان، خسارت به اشخاص ثالث، لطمه به محیط‌زیست و حتی تهدید امنیت انرژی منجر شود. ازاین‌رو، ارزیابی حقوقی رفتار بازیگران فنیِ دخیل در این سامانه‌ها اهمیت ویژه دارد.

در این میان، پیمانکاران فناوری اطلاعات و شرکت‌های یکپارچه‌ساز سیستم‌ها، به‌دلیل نقش مستقیم در معماری شبکه، پیکربندی تجهیزات، راه‌اندازی نرم‌افزارهای نظارت و کنترل، ایجاد دسترسی‌های راه دور، به‌روزرسانی سیستم‌ها و رفع اشکال، عملاً در قلب زنجیره اعتماد سایبری قرار دارند. اگر حمله‌ای از طریق ضعف در این لایه‌ها تحقق یابد، این پرسش مطرح می‌شود که آیا پیمانکار را باید صرفاً در حدود مفاد قرارداد سنجید یا آنکه به‌سبب ماهیت خطرناک و تخصصی موضوع، تکالیف حرفه‌ای گسترده‌تری بر عهده اوست؟ این مقاله، با تأکید بر مسئولیت مدنی پیمانکاران فناوری اطلاعات در حوزه پالایشگاه‌های پارس جنوبی، بر آن است که پاسخ دهد: نخست، مبانی قانونی و قراردادی مسئولیت چیست؛ دوم، معیار احراز تقصیر در محیط صنعتی چگونه باید تفسیر شود؛ سوم، چه خساراتی قابل مطالبه‌اند؛ و چهارم، چه تدابیر قراردادی و تقنینی برای کاهش منازعات آینده ضروری است.

**تبیین مفاهیم و چارچوب مسئله**

**مفهوم پیمانکار فناوری اطلاعات در محیط صنعتی**

مراد از پیمانکار فناوری اطلاعات در این مقاله، هر شخص حقوقی یا حقیقی متخصصی است که در قالب قرارداد، مسئولیت طراحی، تأمین، استقرار، پشتیبانی، نگهداری، یکپارچه‌سازی، ارتقا یا امنیت سامانه‌های اطلاعاتی و کنترلی پالایشگاهی را بر عهده می‌گیرد. این عنوان می‌تواند شرکت نرم‌افزاری، پیمانکار زیرساخت شبکه، شرکت امنیت سایبری، یکپارچه‌ساز OT/IT، پیمانکار تعمیر و نگهداری سامانه‌های کنترل، یا ارائه‌دهنده خدمات دسترسی از راه دور باشد.

اهمیت این تعریف در آن است که مسئولیت مدنی تنها بر پایه نام قراردادی اشخاص تعیین نمی‌شود، بلکه نقش واقعی آنان در ایجاد یا پیشگیری از خطر نیز تعیین‌کننده است. بدین‌ترتیب، هر پیمانکاری که به‌طور مؤثر بر محرمانگی، تمامیت و دسترس‌پذیری سامانه‌های کنترل صنعتی اثر می‌گذارد، ممکن است در صورت بروز حادثه، مسئول شناخته شود.

**مفهوم حمله سایبری به سیستم‌های کنترل صنعتی**

حمله سایبری به سیستم‌های کنترل صنعتی، مجموعه‌ای از اقدامات تعمدی است که از طریق دسترسی غیرمجاز، دست‌کاری نرم‌افزار، بدافزار، تخریب یا اخلال در شبکه، جعل داده، اختلال در حسگرها یا فرماندهی و سوءاستفاده از آسیب‌پذیری‌های ارتباطی، عملکرد سامانه کنترل را مختل می‌کند (Stouffer et al., 2023). برخلاف حملات متعارف به سامانه‌های اداری، در سامانه‌های کنترل نظارت و داده (SCADA) و سیستم‌های کنترل صنعتی (ISC)، نتیجه حمله ممکن است مستقیماً در جهان فیزیکی ظهور

یابد؛ مثلاً افزایش فشار، خاموشی اضطراری، توقف فرایند، باز و بسته‌شدن نامنظم شیرها یا ازکارافتادن سامانه ایمنی.

**جایگاه خاص پالایشگاه‌های پارس جنوبی**

پارس جنوبی صرفاً یک مجتمع صنعتی معمولی نیست؛ بلکه بخشی از زیرساخت حیاتی ملی است. در چنین فضایی، هر کاستی امنیتی، نه‌فقط نقض یک تعهد قراردادی، بلکه ایجاد مخاطره‌ای با دامنه عمومی محسوب می‌شود. به‌همین‌دلیل، استاندارد مورد انتظار از پیمانکار فناوری اطلاعات در این محیط باید بالاتر از پروژه‌های عادی تجاری باشد.

**ویژگی‌های فنی سیستم‌های کنترل صنعتی و اثر آن بر تحلیل حقوقی**

**تفاوت میان فناوری اطلاعات (IT) و فناوری عملیاتی (OT)**

در محیط فناوری اطلاعات، محرمانگی غالباً اهمیت محوری دارد؛ اما در فناوری عملیاتی، دسترس‌پذیری و ایمنی در اولویت‌اند. خاموش‌کردن یک سرور اداری برای نصب وصله امنیتی ممکن است قابل تحمل باشد، اما توقف کنترلر یک واحد فرایندی در پالایشگاه می‌تواند پیامدهای جدی ایمنی داشته باشد. بنابراین، تحلیل رفتار پیمانکار در سیستم‌های کنترل صنعتی باید با درک تفاوت میان این دو قلمرو صورت گیرد (Stouffer et al., 2023).

این تفاوت بر مسئولیت مدنی اثر مستقیم دارد؛ زیرا پیمانکار نمی‌تواند به بهانه اجرای یک قاعده عمومی فناوری اطلاعات، اقدامی را انجام دهد که در محیط فناوری عملیاتی غیرحرفه‌ای یا خطرناک تلقی می‌شود. برای مثال، نصب شتاب‌زده یک وصله بدون آزمون در محیط شبیه‌سازی، اگر موجب اختلال در فرایند شود، خود می‌تواند مبنای مسئولیت باشد.

**سطح بالای وابستگی به زنجیره تأمین**

بخش مهمی از مخاطرات سایبری در صنعت نفت و گاز ناشی از زنجیره تأمین است: نرم‌افزارهای شخص ثالث، تجهیزات دارای میان‌افزار، پیمانکاران نگهداری، دسترسی فروشندگان خارجی یا داخلی و به‌روزرسانی‌های وابسته به سازندگان. حملات بزرگ سال‌های گذشته نشان داده است که نفوذ از طریق تأمین‌کنندگان یا پیمانکاران، یکی از مؤثرترین روش‌ها برای عبور از لایه‌های دفاعی است (Stouffer et al., 2023). از این حیث، پیمانکار فناوری اطلاعات، در عین آنکه مجری پروژه است، خود نیز بخشی از سطح حمله محسوب می‌شود.

**دشواری انتساب فنی و اهمیت مستندسازی**

در بسیاری از حملات سایبری، اثبات اینکه منشأ خسارت دقیقاً کدام ضعف یا قصور بوده، دشوار است. لاگ‌های ناقص، تأخیر در کشف رخداد، مداخله هم‌زمان چند پیمانکار و ضعف در ثبت تغییرات، احراز رابطه سببیت را پیچیده می‌کند. به‌همین‌دلیل، مستندسازی معماری، ثبت دسترسی‌ها، نگهداری سوابق تغییرات و رعایت فرایندهای مدیریت پیکربندی، نه‌فقط تکلیف فنی، بلکه وسیله‌ای برای تعیین یا دفع مسئولیت حقوقی است.

**مبانی مسئولیت مدنی پیمانکاران فناوری اطلاعات در حقوق ایران**

مسئولیت مدنی در حقوق ایران بر این اندیشه بنیادین استوار است که هیچ‌کس نباید بدون مجوز قانونی، زیانی به دیگری وارد کند و در صورت ورود ضرر، باید آن را جبران نماید. این قاعده در زمینه پیمانکاران فناوری اطلاعات، به‌ویژه در محیط‌های صنعتی حساسی مانند پالایشگاه‌های پارس جنوبی، اهمیتی دوچندان می‌یابد؛ زیرا رفتار فنی پیمانکار ممکن است از سطح یک تخلف قراردادی فراتر رود و به خسارات مالی، جانی، زیست‌محیطی و حتی لطمه به منافع عمومی منجر شود. در حقوق ایران، مبانی مسئولیت مدنی را می‌توان در چند محور اصلی بررسی کرد: مبنای تقصیر، مبنای قراردادی، مبنای تسبیب و اتلاف، اصل لاضرر و گرایش به حمایت از زیان‌دیده در فعالیت‌های تخصصی و پرخطر (Katouzian, 2007; Safaei & Rahimi, 2012).

**مبنای تقصیر در مسئولیت مدنی**

مهم‌ترین مبنای سنتی مسئولیت مدنی در حقوق ایران، نظریه تقصیر است. مطابق این دیدگاه، هرگاه شخص در نتیجه عمد، بی‌احتیاطی، بی‌مبالاتی، عدم مهارت یا عدم رعایت نظامات، زیانی به دیگری وارد کند، مسئول جبران خسارت خواهد بود. این مبنا در ماده ۱ قانون مسئولیت مدنی به‌روشنی انعکاس یافته است؛ آنجا که مقرر می‌دارد هرکس بدون مجوز قانونی، عمداً یا در نتیجه بی‌احتیاطی، به جان یا مال یا حقوق دیگران لطمه وارد کند، مسئول جبران خسارت است (Ibn-Najjar, 2019).

در حوزه امنیت سایبری و سامانه‌های کنترل صنعتی، تقصیر پیمانکار فناوری اطلاعات می‌تواند در قالب‌های مختلفی ظهور کند: طراحی ناامن شبکه، فقدان کنترل دسترسی مناسب، به‌روزرسانی‌نکردن سامانه‌های حساس، بی‌توجهی به هشدارهای فنی یا عدم پیش‌بینی تمهیدات متعارف دفاعی. ازآنجاکه پیمانکار در اینجا یک متخصص حرفه‌ای است، معیار تقصیر درباره او، معیار انسان متعارف عادی نیست، بلکه معیار «متخصص محتاط و آگاه» است؛ یعنی کسی که با توجه به دانش فنی و حساسیت محیط عملیاتی، باید سطح بالاتری از مراقبت را اعمال کند (Katouzian, 2007; Pour-Ostad, 2018).

بنابراین، در حقوق ایران نیز می‌توان استدلال کرد که هرچه فعالیت تخصصی‌تر و خطرات ناشی از آن شدیدتر باشد، دامنه تکلیف به احتیاط گسترش می‌یابد. از این منظر، پیمانکار فناوری اطلاعات در پالایشگاه نمی‌تواند به حداقل رفتار فنی اکتفا کند، بلکه باید کلیه مراقبت‌های متناسب با ماهیت زیرساخت حیاتی را به‌کار گیرد.

**مبنای قراردادی مسئولیت**

یکی دیگر از مهم‌ترین مبانی مسئولیت مدنی در حقوق ایران، نقض تعهد قراردادی است. مطابق اصل لزوم قراردادها، هرگاه شخص تعهدی را در برابر دیگری بپذیرد و از اجرای آن خودداری کند یا آن را ناقص و معیوب انجام دهد و از این رهگذر خسارتی وارد شود، مسئول جبران آن خواهد بود (Katouzian, 2009). در روابط میان پالایشگاه و پیمانکار فناوری اطلاعات، بخش بزرگی از مسئولیت در همین حوزه قرار می‌گیرد.

پیمانکار ممکن است به موجب قرارداد متعهد شده باشد که سامانه‌ای ایمن، پایدار، دارای تفکیک شبکه، با قابلیت ثبت رخداد، یا منطبق با استانداردهای امنیتی مشخص تحویل دهد. در این صورت، اگر حمله سایبری از ضعف همان تعهدات ناشی شود، مسئولیت او پیش از هر چیز، مسئولیت قراردادی است. مزیت تحلیل قراردادی آن است که حدود وظایف، معیارهای عملکرد، زمان‌بندی، سطح خدمت و تعهدات امنیتی غالباً در متن قرارداد یا اسناد فنی پروژه قابل احراز است (Taghizadeh, 2022).

بااین‌حال، مسئولیت قراردادی در این زمینه صرفاً به نقض صریح بندهای قرارداد محدود نمی‌شود. در حقوق ایران، حسن اجرای تعهد نیز اهمیت دارد؛ بدین‌معنا که متعهد باید تعهد خود را به‌گونه‌ای اجرا کند که هدف مشروع قرارداد تأمین شود. پس اگر پیمانکار سامانه‌ای را ظاهراً نصب کند، اما به‌لحاظ امنیتی آن را در وضعیت آسیب‌پذیر رها سازد، نمی‌تواند مدعی شود صرف تحویل شکلی موضوع قرارداد، او را از مسئولیت معاف می‌کند (Katouzian, 2009).

**اتلاف و تسبیب به‌عنوان مبانی فقهی و قانونی**

از مهم‌ترین مبانی مسئولیت مدنی در حقوق ایران، قواعد فقهی و قانونی اتلاف و تسبیب است. قاعده اتلاف بر این اصل مبتنی است که «هرکس مال دیگری را تلف کند، ضامن است»؛ اعم از اینکه این اتلاف مستقیم باشد یا در نتیجه فعل او تحقق یابد. همچنین، در تسبیب، اگر شخص سبب ورود زیان را فراهم آورد، در صورتی که عرفاً ورود ضرر به او منتسب باشد، مسئول شناخته می‌شود (Mohaqeq Damad, 2010).

در حملات سایبری به سامانه‌های کنترل صنعتی، پیمانکار غالباً مباشر مستقیم خسارت نیست، بلکه با ایجاد ضعف امنیتی یا ترک اقدام لازم، سبب وقوع زیان می‌شود. ازاین‌رو، تحلیل مسئولیت او با قاعده تسبیب سازگاری بیشتری دارد. برای نمونه، اگر پیمانکار به‌دلیل سهل‌انگاری، درگاه دسترسی ناامن ایجاد کند و مهاجم از همان مسیر وارد سامانه شود، هرچند عامل مستقیم خسارت مهاجم است، اما پیمانکار نیز عرفاً سبب ورود ضرر شناخته می‌شود؛ زیرا زمینه مؤثر و قابل پیش‌بینی وقوع حمله را فراهم کرده است (Jafari Langroudi, 2008).

در واقع، یکی از نقاط قوت حقوق ایران در تحلیل این مسئله آن است که برای استقرار مسئولیت، لزوماً نیازی به مباشرت مستقیم وجود ندارد، بلکه فراهم‌آوردن مقدمات زیان‌بار نیز می‌تواند منشأ ضمان باشد. این مبنا در محیط‌های سایبری و صنعتی اهمیت زیادی دارد؛ چون در بیشتر حملات، زیان از رهگذر زنجیره‌ای از اسباب محقق می‌شود، نه از یک فعل مستقیم و منفرد.

**اصل لاضرر و منع اضرار به غیر**

یکی از پشتوانه‌های مهم مسئولیت مدنی در حقوق ایران، قاعده فقهی لاضرر است. بر اساس این قاعده، هیچ‌کس نمی‌تواند به دیگری ضرر وارد کند و نظم حقوقی نیز نباید وضعی را بپذیرد که زیان ناروایی بر اشخاص تحمیل شود (Makarem Shirazi, 1990). هرچند قاعده لاضرر بیش از آنکه مستقیماً یک ماده قانونی اجرایی باشد، مبنایی تفسیری و اصولی برای تحلیل احکام است، اما در حوزه مسئولیت مدنی نقش تقویت‌کننده دارد.

در زمینه پیمانکاران فناوری اطلاعات، اصل لاضرر اقتضا می‌کند که هرگاه فعالیت تخصصی آنان در زیرساخت حیاتی، بدون رعایت احتیاط‌های لازم، موجب تحمیل خسارت به کارفرما، کارکنان، اشخاص ثالث یا محیط‌زیست شود، نظام حقوقی از زیان‌دیده حمایت کند. این مبنا به‌ویژه در مواردی اهمیت دارد که برخی پیمانکاران می‌کوشند با استناد به شروط محدودکننده مسئولیت یا پیچیدگی فنی موضوع، از پاسخ‌گویی فرار کنند. قاعده لاضرر مانع از آن است که قرارداد یا تفسیر فنی، به ابزاری برای توجیه اضرار ناروا تبدیل شود (Safaei & Rahimi, 2012).

**مسئولیت ناشی از بی‌احتیاطی حرفه‌ای**

حقوق ایران، اگرچه به‌صراحت از اصطلاح «مسئولیت حرفه‌ای» در همه حوزه‌ها استفاده نکرده است، اما در عمل، برای صاحبان مشاغل تخصصی استاندارد بالاتری از دقت و مهارت قائل است. پزشک، مهندس، کارشناس رسمی و پیمانکار متخصص، همگی در حدود دانش و مهارت حرفه‌ای خود سنجیده می‌شوند، نه بر پایه رفتار اشخاص عادی (Pour-Ostad, 2018).

در نتیجه، پیمانکار فناوری اطلاعات در پروژه‌ای مانند امنیت سامانه‌های کنترل صنعتی پالایشگاه، صرفاً یک فروشنده خدمات عادی نیست، بلکه متخصصی است که کارفرما با اتکا به دانش فنی او تصمیم می‌گیرد. ازاین‌رو، هرگاه او از استانداردهای حرفه‌ای شناخته‌شده عدول کند، مثلاً بدون ارزیابی ریسک، ارتباط شبکه اداری و عملیاتی را برقرار سازد یا تجهیزات را با تنظیمات پیش‌فرض رها کند، این رفتار می‌تواند مصداق بی‌احتیاطی حرفه‌ای باشد. استدلال مهم در اینجا آن است که مسئولیت چنین پیمانکاری نباید با معیار حداقلی ارزیابی شود، زیرا موضوع تعهد او مستقیماً با ایمنی، تولید و منافع عمومی پیوند دارد (Hosseini, 2020).

**رابطه سببیت در حقوق ایران**

برای تحقق مسئولیت مدنی، صرف وجود تقصیر کافی نیست، بلکه باید میان فعل زیان‌بار و خسارت، رابطه سببیت احراز شود. در حقوق ایران نیز، همانند بسیاری از نظام‌های حقوقی، احراز این رابطه در موارد پیچیده، تابع تشخیص عرف، اوضاع‌واحوال پرونده و نظر کارشناسی است (Katouzian, 2007). در دعاوی سایبری، این شرط دشوارتر می‌شود؛ زیرا خسارت معمولاً حاصل تعامل چند عامل است: مهاجم، ضعف فنی، تصمیم‌های مدیریتی، رفتار اپراتور و شاید نقص تجهیز.

بااین‌حال، دشواری اثبات سببیت نباید به مصونیت پیمانکار بینجامد. هرگاه ثابت شود که قصور پیمانکار، یکی از اسباب مؤثر و متعارف در تحقق حمله بوده است، برای انتساب مسئولیت کفایت می‌کند. در این موارد، فعل مهاجم معمولاً سببیت پیمانکار را قطع نمی‌کند، زیرا اصل وقوع تهدید سایبری در زیرساخت حیاتی، امری قابل پیش‌بینی است. بنابراین، اگر پیمانکار باید احتمال چنین حمله‌ای را می‌داده و تدابیر مناسب اتخاذ می‌کرده، نمی‌تواند به مداخله شخص ثالث به‌عنوان عامل رافع مسئولیت تمسک جوید (Salehi, 2022).

**جبران کامل خسارت و حمایت از زیان‌دیده**

یکی از اهداف بنیادین مسئولیت مدنی در حقوق ایران، جبران کامل خسارت زیان‌دیده است. این جبران می‌تواند شامل خسارت‌های مالی مستقیم، منافع فوت‌شده، هزینه‌های بازسازی، خسارات ناشی از توقف عملیات و، در موارد مقتضی، خسارات بدنی و معنوی باشد (Ibn-Najjar, 2019). در زمینه حملات سایبری به پالایشگاه، این اصل اهمیت ویژه دارد؛ زیرا زیان‌ها غالباً محدود به خرابی نرم‌افزار یا ازبین‌رفتن داده نیست، بلکه ممکن است توقف خط تولید، آسیب به تجهیزات گران‌قیمت، بروز حادثه صنعتی یا خسارت به محیط‌زیست را نیز دربر گیرد.

از منظر استدلالی، اگر مبانی مسئولیت مدنی را به‌گونه‌ای مضیق تفسیر کنیم که پیمانکار متخصص تنها در صورت اثبات تقصیر بسیار آشکار پاسخ‌گو باشد، زیان‌دیده در بسیاری از موارد بدون جبران مؤثر باقی می‌ماند. این نتیجه با فلسفه حمایتی مسئولیت مدنی ناسازگار است. بنابراین، در تفسیر مقررات و قراردادها باید به‌گونه‌ای عمل کرد که تعادل میان حمایت از نوآوری فنی و حمایت از زیان‌دیدگان برقرار شود، نه اینکه پیچیدگی فناوری به سپری برای فرار از مسئولیت تبدیل گردد.

**مبنای مناسب‌تر برای تحلیل مسئولیت پیمانکاران فناوری اطلاعات**

با ملاحظه مجموعه مبانی حقوق ایران، می‌توان گفت مسئولیت پیمانکاران فناوری اطلاعات در حملات سایبری به سیستم‌های کنترل صنعتی، ماهیتی مرکب دارد؛ بدین‌معنا که هم‌زمان می‌تواند بر مبنای تقصیر، نقض قرارداد، تسبیب و اصول عمومی منع اضرار تحلیل شود. در نتیجه، مناسب‌ترین رویکرد آن نیست که مسئولیت این پیمانکاران صرفاً در چهارچوب مضیق تعهدات لفظی قرارداد محدود شود، بلکه باید با توجه به تخصص حرفه‌ای، حساسیت زیرساخت، پیش‌بینی‌پذیری خطر و دامنه خسارات محتمل، تفسیری موسع و حمایتی از مسئولیت ارائه کرد.

بر این اساس، در حقوق ایران می‌توان از این گزاره دفاع کرد که پیمانکار فناوری اطلاعات در پالایشگاه‌های پارس جنوبی، در صورت قصور در رعایت الزامات حرفه‌ای امنیت سایبری، نه‌تنها در برابر کارفرما از حیث قراردادی، بلکه در برابر اشخاص ثالث زیان‌دیده نیز از حیث قواعد عام مسئولیت مدنی پاسخ‌گو است. این تحلیل، هم با مبانی قانونی موجود سازگار است و هم با مقتضیات عصر دیجیتال و ضرورت حمایت از زیرساخت‌های حیاتی.

**مسئولیت قراردادی**

اولین مبنای مسئولیت، قرارداد است. هرگاه پیمانکار متعهد شده باشد سامانه‌ای با سطح معینی از امنیت، پایداری، تفکیک شبکه یا قابلیت بازیابی طراحی و نگهداری کند و در انجام آن تعهد کوتاهی کند، مسئولیت قراردادی وی قابل استقرار است. در حقوق ایران، اصل لزوم قراردادها و الزام متعهد به اجرای مفاد عقد، مبنای مهمی برای مطالبه خسارت است (Katouzian, 2009). اگر در قرارداد، رعایت استانداردهای مشخصی مانند IEC 62443، NIST SP 800-82 یا الزامات کارفرما پیش‌بینی شده باشد، انحراف از آن‌ها قرینه قوی بر تقصیر قراردادی خواهد بود.

در پروژه‌های صنعتی، تعهدات پیمانکار غالباً صرفاً تحویل سخت‌افزار یا نرم‌افزار نیست، بلکه شامل طراحی امن، مستندسازی، آزمون امنیتی، آموزش، مدیریت رخداد و پشتیبانی نیز می‌شود. ازاین‌رو، محدودکردن مسئولیت وی به «تحویل فنی اولیه» اغلب با واقعیت نقش او سازگار نیست.

**مسئولیت قهری یا غیرقراردادی**

در مواردی، خسارت به اشخاصی وارد می‌شود که طرف قرارداد با پیمانکار نیستند؛ مانند کارکنان، پیمانکاران دیگر، ساکنان محلی یا حتی شرکت‌های پایین‌دستی که از توقف پالایشگاه زیان می‌بینند. در این موارد، مسئولیت پیمانکار می‌تواند بر مبنای قواعد عام اتلاف، تسبیب و قانون مسئولیت مدنی تحلیل شود. مطابق ماده ۱ قانون مسئولیت مدنی، هرکس بدون مجوز قانونی، عمداً یا در نتیجه بی‌احتیاطی، به جان، سلامت، مال، آزادی، حیثیت یا هر حق دیگر اشخاص لطمه وارد کند، مسئول جبران خسارت ناشی از عمل خود است. در نتیجه، قصور سایبری، اگر به خسارت بدنی، مالی یا معنوی منجر شود، از شمول این قاعده خارج نیست.

**پیوند مسئولیت قراردادی و قهری**

در عمل، حمله سایبری به پالایشگاه می‌تواند هم‌زمان چند نوع مسئولیت ایجاد کند: در برابر کارفرما، مسئولیت قراردادی؛ و در برابر ثالث، مسئولیت قهری. این دو الزاماً یکدیگر را نفی نمی‌کنند، بلکه ممکن است یک رفتار واحد ــ مثلاً عدم تفکیک شبکه کنترل از شبکه اداری ــ هم نقض تعهد قراردادی باشد و هم سبب ورود زیان به اشخاص ثالث. از این منظر، پیمانکار نمی‌تواند با استناد به اینکه «قرارداد فقط با کارفرما داشته»، از آثار زیان‌بار رفتار حرفه‌ای خود در قبال ثالث بگریزد.

**ضرورت تشدید معیار تقصیر در زیرساخت‌های حیاتی**

**کفایت‌نداشتن معیار متعارف تقصیر**

در روابط عادی تجاری، تقصیر غالباً با معیار رفتار «متعارف» سنجیده می‌شود. اما در زیرساخت‌های حیاتی، این معیار باید با ملاحظات شدت خطر بازتفسیر شود. پرسش اساسی این است که آیا برای پیمانکار فناوری اطلاعات در پالایشگاهی مانند پارس جنوبی، همان سطح دقتی کافی است که در یک سازمان غیرحساس انتظار می‌رود؟ پاسخ قطعاً منفی است.

زیرا اولاً، پیمانکار حرفه‌ای از حساسیت محیط آگاه است یا باید آگاه باشد. ثانیاً، دامنه خسارات بالقوه بسیار فراتر از زیان مالی قراردادی است. ثالثاً، استانداردها و رویه‌های حرفه‌ای مشخصی برای ایمن‌سازی سیستم‌های کنترل صنعتی وجود دارد و نمی‌توان به بهانه فقدان نص خاص، از رعایت آن‌ها عدول کرد. بنابراین، «رفتار متعارف» در این حوزه، مساوی با رعایت استانداردهای حرفه‌ایِ تشدیدشده است، نه صرف عرف عمومی بازار.

**تعهد به وسیله یا تعهد به نتیجه؟**

در حقوق قراردادها، غالباً میان تعهد به وسیله و تعهد به نتیجه تفکیک می‌شود. برخی ممکن است ادعا کنند که امنیت سایبری هرگز به‌طور کامل قابل تضمین نیست، پس پیمانکار فقط به «به‌کارگیری تلاش متعارف» متعهد است. این استدلال در سطح کلی درست به‌نظر می‌رسد، اما در محیط پالایشگاهی کافی نیست. درست است که پیمانکار نمی‌تواند عدم وقوع مطلق هیچ حمله‌ای را تضمین کند، ولی بی‌تردید متعهد است که حداقل‌های حرفه‌ای و استانداردهای لازم را به‌طور کامل رعایت کند. ازاین‌رو، هرچند اصل تعهد ممکن است به‌ظاهر تعهد به وسیله باشد، اما «وسیله» در اینجا یک وسیله عادی نیست، بلکه وسیله‌ای حرفه‌ای، تخصصی و سخت‌گیرانه است.

به‌بیان‌دیگر، پیمانکار نمی‌تواند به این دفاع اکتفا کند که «حمله سایبری ذاتاً غیرقابل پیش‌بینی است». اگر حمله از مسیر رمز عبور پیش‌فرض، نبود تفکیک شبکه، دسترسی از راه دورِ بدون احراز هویت چندمرحله‌ای، یا وصله‌نشدن آسیب‌پذیری شناخته‌شده رخ داده باشد، سخن از غیرقابل پیش‌بینی‌بودن، مسموع نیست (Stouffer et al., 2023).

**الگوی مسئولیت حرفه‌ای مشدد**

به‌نظر می‌رسد در تحلیل مسئولیت پیمانکاران فناوری اطلاعات در صنایع حساس، باید از الگوی «مسئولیت حرفه‌ای مشدد» دفاع کرد. مبنای این الگو آن است که متخصصی که در محیط پرخطر فعالیت می‌کند، نسبت به مخاطرات شناخته‌شده، تکلیف مضاعف به مراقبت دارد. مشابه این تحلیل در مسئولیت پزشکان، مهندسان و دارندگان مشاغل تخصصی نیز دیده می‌شود. در نتیجه، هرچه تخصص بیشتر و خطر شدیدتر باشد، آستانه تحمل حقوقی نسبت به سهل‌انگاری پایین‌تر خواهد بود.

**مصادیق تقصیر پیمانکاران فناوری اطلاعات در حملات سایبری به سیستم‌های کنترل صنعتی**

**طراحی ناامن معماری شبکه**

یکی از مهم‌ترین مصادیق تقصیر، عدم تفکیک مناسب میان شبکه اداری، شبکه کنترل، منطقه غیرنظامی و سامانه‌های حیاتی است. استانداردهای امنیت صنعتی بر اصل ناحیه‌بندی و مجراهای کنترل‌شده تأکید دارند (Stouffer et al., 2023). اگر پیمانکار سامانه را به‌گونه‌ای طراحی کند که نفوذ از شبکه اداری به فناوری عملیاتی، بدون مانع مؤثر ممکن باشد، قصور وی آشکار است.

در پالایشگاه، این نقص صرفاً یک خطای معماری نیست، بلکه ایجاد امکان سرایت حمله به تجهیزات فیزیکی است. لذا در صورت تحقق زیان، چنین رفتاری می‌تواند از بارزترین نمونه‌های تسبیب در ورود خسارت باشد.

**مدیریت نامناسب وصله‌ها و آسیب‌پذیری‌ها**

یکی از چالش‌های سامانه‌های کنترل صنعتی، تعادل میان امنیت و تداوم عملیات است. پیمانکار باید برای شناسایی، ارزیابی، آزمون و اعمال وصله‌ها، روندی مرحله‌ای و مستند داشته باشد. اگر آسیب‌پذیری شناخته‌شده و بحرانی، مدت‌ها بدون تمهید جبرانی رها شود و حمله از همان مسیر انجام گیرد، تقصیر پیمانکار قابل انتساب خواهد بود، مگر آنکه اثبات کند اختیار اعمال وصله یا تمهید جایگزین از او سلب شده یا تصمیم نهایی، برخلاف هشدار صریح وی، از سوی کارفرما اتخاذ شده است.

**ایجاد یا تداوم دسترسی ناامن از راه دور**

در بسیاری از حوادث صنعتی، دسترسی‌های از راه دورِ فاقد کنترل کافی نقش اساسی داشته‌اند. استفاده از فیلترشکن ناامن، رمزهای عبور مشترک، فقدان احراز هویت چندمرحله‌ای، نگهداری حساب‌های فعال بلااستفاده و عدم ثبت کامل نشست‌های پشتیبانی، همگی می‌توانند تقصیر محسوب شوند؛ به‌ویژه زمانی که پیمانکار برای سهولت پشتیبانی، درگاه‌هایی باز بگذارد که پس از اتمام عملیات نیز بسته نشوند.

**استفاده از پیکربندی‌های پیش‌فرض و ضعیف**

باقی‌گذاشتن گذرواژه‌های پیش‌فرض، پورت‌های غیرضروری، سرویس‌های بلااستفاده، یا تنظیمات کارخانه‌ای در تجهیزات صنعتی و سرورها، با معیارهای حرفه‌ای ناسازگار است. اگر حمله از چنین منافذ ابتدایی رخ دهد، پیمانکار به‌دشواری می‌تواند فقدان تقصیر را اثبات کند.

**قصور در ثبت رخداد و پایش امنیتی**

عدم فعال‌سازی لاگ‌ها، نگهداری نامناسب سوابق، نبود هشداردهی مؤثر، یا فقدان سامانه نظارت بر رفتار غیرعادی، دو پیامد حقوقی دارد: نخست، احتمالاً خود زمینه‌ساز تشدید خسارت می‌شود؛ دوم، امکان کشف و انتساب حادثه را دشوار می‌کند. چنین ضعفی در محیط حیاتی، قصوری مضاعف به‌شمار می‌آید.

**آموزش ناکافی کاربران و اپراتورها**

بخش مهمی از حملات از رهگذر خطای انسانی، فیشینگ، اتصال حافظه‌های آلوده یا نقض رویه‌های عملیاتی رخ می‌دهد. اگر آموزش کاربران، کنترل رسانه‌های قابل حمل و تدوین دستورالعمل‌های واکنش بر عهده پیمانکار باشد و وی در این زمینه کوتاهی کند، نمی‌توان همه بار مسئولیت را بر دوش بهره‌بردار نهاد.

**رابطه سببیت در حملات سایبری**

**دشواری اثبات سببیت**

یکی از مهم‌ترین چالش‌های حقوقی در دعاوی سایبری، اثبات رابطه سببیت میان رفتار پیمانکار و خسارت نهایی است. حمله ممکن است توسط مهاجم خارجی انجام شده باشد، اما این امر به‌خودی‌خود سببیت رفتار پیمانکار را منتفی نمی‌کند. در حقوق مسئولیت مدنی، وجود عامل انسانی ثالث زمانی سببیت اولیه را قطع می‌کند که رفتارش کاملاً مستقل، غیرقابل پیش‌بینی و قاهرانه باشد. حال‌آنکه در امنیت سایبری، اصل بر پیش‌بینی‌پذیری تهدید است؛ به‌ویژه در زیرساخت‌های انرژی که همواره در معرض مخاطرات جدی قرار دارند (Stouffer et al., 2023).

ازاین‌رو، اگر پیمانکار منفذی فراهم کرده باشد که عرفاً مسیر محتمل بهره‌برداری مهاجم است، نمی‌تواند صرفاً با اشاره به «عمل مجرمانه مهاجم» از مسئولیت رها شود. حمله سایبری در اینجا نه عاملی قاطع، بلکه حلقه‌ای از زنجیره‌ای است که با قصور پیشین ممکن شده است.

**سببیت در فرض تعدد عامل**

در پالایشگاه، معمولاً چندین بازیگر دخیل‌اند: کارفرما، پیمانکار اصلی، پیمانکار فرعی، فروشنده تجهیز، تیم بهره‌برداری، مشاور و گاه ارائه‌دهنده خدمات ارتباطی. در چنین شرایطی، خسارت ممکن است محصول جمع اسباب باشد. راه‌حل منطقی، تحلیل سهم هر عامل در ایجاد خطر و تشدید خسارت است. هرچند تعیین دقیق سهم ممکن است دشوار باشد، اما دشواری اثبات نباید به مصونیت عملی پیمانکار متخصص بینجامد.

**نقش کارشناسی فنی در احراز سببیت**

به‌دلیل تخصصی‌بودن موضوع، رسیدگی قضایی بدون کارشناسی فنی دقیق ممکن نیست. بررسی لاگ‌ها، توپولوژی شبکه، سوابق تغییرات، نسخه‌های سیستم، گزارش‌های آسیب‌پذیری، قراردادهای سطح خدمات (SLA) و رویه‌های مدیریت رخداد، در تعیین سببیت نقش کلیدی دارند. بنابراین، توصیه می‌شود در قراردادها، تکلیف نگهداری ادله دیجیتال و همکاری در تحقیقات حادثه تصریح شود.

**خسارات قابل مطالبه**

**خسارات مستقیم**

خسارات مستقیم شامل هزینه بازگردانی سامانه، بازیابی داده‌ها، تعمیر تجهیزات آسیب‌دیده، توقف تولید، ازدست‌رفتن مواد، هزینه کارشناسی، پاک‌سازی بدافزار و ارتقای اضطراری سامانه است. در محیط پالایشگاهی، توقف چندساعته یا چندروزه می‌تواند خسارات هنگفتی ایجاد کند. هرجا این خسارات نتیجه متعارف نقض تعهدات امنیتی پیمانکار باشد، قابلیت مطالبه دارند.

**خسارات بدنی و جانی**

اگر حمله سایبری موجب انفجار، آتش‌سوزی، نشت گاز یا اختلال در سامانه‌های ایمنی شود و به کارکنان یا اشخاص ثالث صدمه وارد آید، مسئولیت پیمانکار می‌تواند از سطح زیان مالی صرف فراتر رود. این نکته جایگاه تحلیل مقاله را تقویت می‌کند؛ زیرا در اینجا امنیت سایبری مستقیماً با حق حیات و سلامت پیوند می‌خورد. هر تفسیر سهل‌گیرانه از مسئولیت پیمانکار در چنین وضعی، با فلسفه حمایت‌گر مسئولیت مدنی سازگار نیست.

**خسارات زیست‌محیطی و اعتباری**

در صنعت نفت و گاز، نشت مواد آلاینده، آلودگی محیط و خسارات اکولوژیک از پیامدهای محتمل حملات سایبری‌اند. افزون بر آن، لطمه به اعتبار شرکت بهره‌بردار، کاهش اعتماد عمومی و پیامدهای تجاری نیز قابل توجه است. هرچند ارزیابی و اثبات خسارات اعتباری دشوارتر است، اما اصل قابلیت جبران آن، در صورت احراز شرایط، قابل دفاع است.

### دفاعیات احتمالی پیمانکار و نقد آن‌ها

#### دفاع مبتنی بر غیرقابل پیش‌بینی‌بودن حمله

رایج‌ترین دفاع آن است که حمله سایبری ماهیتی پیشرفته و غیرقابل پیش‌بینی داشته است. این دفاع تنها زمانی می‌تواند مؤثر باشد که پیمانکار نشان دهد همه تدابیر متعارف و حرفه‌ای را رعایت کرده و حمله واقعاً فراتر از سطح انتظار معقول بوده است. اما در مواردی که ضعف‌های اولیه و شناخته‌شده وجود داشته، این دفاع مردود است.

#### دفاع مبتنی بر قصور کارفرما

گاه پیمانکار ادعا می‌کند که کارفرما توصیه‌های امنیتی را نپذیرفته، بودجه کافی نداده یا برای جلوگیری از توقف تولید، با اعمال کنترل‌ها مخالفت کرده است. این دفاع در صورتی می‌تواند مسئولیت را کاهش دهد که مستند، روشن و مکتوب باشد. سکوت پیمانکار در برابر تصمیم پرخطر کارفرما، یا ادامه همکاری بدون ثبت هشدارهای فنی، او را از مسئولیت نمی‌رهاند. متخصص حرفه‌ای باید خطر را صریح، مستدل و قابل اثبات اعلام کند.

#### دفاع مبتنی بر فعل شخص ثالث

پیمانکار ممکن است به فروشنده تجهیز، اپراتور شیفت، پیمانکار فرعی یا مهاجم استناد کند. این دفاع نیز زمانی پذیرفتنی است که رفتار ثالث سببیت اصلی را قطع کرده باشد. اما در اکثر موارد، فعل ثالث با قصور پیمانکار جمع می‌شود، نه اینکه آن را محو کند.

#### دفاع مبتنی بر شرط محدودکننده مسئولیت

در بسیاری از قراردادها، شروطی برای تحدید یا سقف‌گذاری مسئولیت پیش‌بینی می‌شود. هرچند اصل این شروط در حقوق قراردادها قابل تصور است، اما در حوزه زیرساخت‌های حیاتی باید با تفسیر مضیق نگریسته شوند؛ به‌ویژه جایی که تقصیر سنگین، بی‌مبالاتی حرفه‌ای یا خسارات بدنی و عمومی مطرح است. شرط قراردادی نباید به ابزاری برای بی‌اثرکردن حداقل‌های ایمنی تبدیل شود.

### نقش استانداردها در تعیین معیار تقصیر

#### استاندارد به‌عنوان شاخص رفتار حرفه‌ای

استانداردهایی مانند NIST SP 800-82، سری IEC 62443، راهنماهای «انجمن بین‌المللی اتوماسیون (ISA)» و استانداردهای بخش انرژی، هرچند در همه نظام‌های حقوقی الزام‌آور به‌معنای قانون نیستند، اما در تعیین رفتار حرفه‌ای متعارف نقش اساسی دارند. دادرس و کارشناس می‌توانند از این استانداردها برای سنجش اینکه «پیمانکار محتاط و متخصص» چه باید می‌کرده، استفاده کنند.

#### انطباق صوری در برابر انطباق واقعی

یکی از مشکلات عملی، اتکای صوری به استانداردهاست. ممکن است پیمانکار ادعا کند که پروژه بر مبنای چارچوب خاصی اجرا شده، اما در عمل، کنترل‌ها ناقص یا نمایشی بوده‌اند. بنابراین، مسئولیت مدنی با ارائه چند سند انطباق صوری منتفی نمی‌شود. ملاک، کارآمدی واقعی کنترل‌ها در مدیریت خطر است.

#### استانداردها و بار اثبات

هرگاه پیمانکار از استانداردهای شناخته‌شده عدول کرده باشد، بار توجیه فنی و حقوقی رفتار او سنگین‌تر می‌شود. برعکس، رعایت مستند و واقعی استانداردها می‌تواند قرینه‌ای به نفع او باشد، هرچند مصونیت مطلق ایجاد نمی‌کند.

### مطالعه تطبیقی و درس‌آموخته‌های حملات مهم سایبری

#### استاکس‌نت و تغییر پارادایم مسئولیت

حمله استاکس‌نت نشان داد که بدافزارها می‌توانند فراتر از سرقت داده، به تخریب فیزیکی تجهیزات صنعتی منجر شوند (Langner, 2011). این رخداد پارادایم حقوقی را نیز تغییر داد: دیگر نمی‌توان امنیت سایبری را یک موضوع صرفاً اداری یا محرمانگی‌محور دانست. در نتیجه، پیمانکاران فناوری اطلاعات در محیط صنعتی باید خطرات فیزیکی ناشی از طراحی ضعیف را نیز در محاسبات حرفه‌ای خود وارد کنند.

**تهدید علیه سامانه‌های ایمنی**

حمله بدافزار تریتون/تریسیس (Triton/Trisis) به سامانه‌های ایمنی ابزار دقیق، اهمیت ویژه‌ای دارد؛ زیرا هدف آن عبور از لایه‌های ایمنی و ایجاد امکان حادثه فاجعه‌بار بود (Miller & Rowe, 2012). اگر پیمانکار در طراحی یا نگهداری سامانه‌ای که به SIS متصل است، استانداردهای جداسازی و کنترل دسترسی را رعایت نکند، از نظر حقوقی در معرض مسئولیتی به‌مراتب سنگین‌تر قرار می‌گیرد.

**مفهوم اختلال عملیاتی ناشی از فناوری اطلاعات**

حادثه کلونیال پایپ‌لاین (Colonial Pipeline) نشان داد حتی حمله‌ای که لزوماً مستقیماً فناوری عملیاتی را هدف نگرفته، می‌تواند به توقف عملیات زیرساخت انرژی منجر شود (Stouffer et al., 2023). این نکته برای پالایشگاه‌ها مهم است: بی‌احتیاطی در سامانه‌های اداری یا تجاری نیز ممکن است اثر عملیاتی جدی بر کنترل صنعتی بگذارد. بنابراین، مسئولیت پیمانکار محدود به دیوار فناوری عملیاتی نیست.

**تحلیل خاص مسئولیت در پالایشگاه‌های پارس جنوبی**

**ویژگی‌های خاص محیط بومی**

در پالایشگاه‌های پارس جنوبی، افزون بر مخاطرات عمومی سیستم‌های کنترل صنعتی، عوامل بومی نیز اهمیت دارند: پیچیدگی زنجیره پیمانکاری، تنوع تجهیزات با نسل‌های مختلف، محدودیت‌های ناشی از تحریم و دشواری به‌روزرسانی برخی سامانه‌ها، وابستگی به راه‌حل‌های بومی یا ترکیبی و گاه شکاف میان الزامات امنیتی و اقتضائات تداوم تولید. این شرایط، اگرچه واقعیت‌های مدیریتی‌اند، اما مسئولیت پیمانکار را زایل نمی‌کنند. برعکس، اقتضا دارند پیمانکار با دقت بیشتری مدیریت ریسک را مستند کند.

**انتظار مشروع از پیمانکار حرفه‌ای**

در چنین محیطی، از پیمانکار حرفه‌ای انتظار می‌رود:

ارزیابی ریسک اولیه و ادواری انجام دهد؛

دارایی‌های حیاتی و وابستگی‌ها را شناسایی کند؛

معماری تفکیک‌شده و قابل دفاع طراحی کند؛

کنترل‌های جبرانی برای سامانه‌های قدیمی پیش‌بینی نماید؛

دسترسی‌های موقت و دائمی را دقیقاً مدیریت کند؛

برنامه واکنش به رخداد و بازیابی داشته باشد؛

هشدارهای فنی را به‌صورت مکتوب به کارفرما اعلام کند.

اگر پیمانکار این تکالیف را انجام ندهد، استناد به دشواری‌های محیطی بیش از آنکه دفاع باشد، اقرار ضمنی به عدم کفایت نظام حرفه‌ای اوست.

**مسئولیت در قبال امنیت ملی و منافع عمومی**

هرچند موضوع این مقاله مسئولیت مدنی است، نه کیفری یا اداری، اما نباید از این نکته غفلت کرد که اختلال در پالایشگاه‌های پارس جنوبی می‌تواند آثار عمومی و ملی داشته باشد. بنابراین، تحلیل مسئولیت مدنی در این حوزه باید با ملاحظه منافع عمومی انجام شود. از همین رو، تفسیر مضیق مسئولیت پیمانکار با اقتضائات حمایت از زیرساخت حیاتی سازگار نیست.

**پیشنهادهای حقوقی و قراردادی**

**تصریح تعهدات امنیتی در قرارداد**

قراردادهای پیمانکاری فناوری اطلاعات در حوزه پالایشگاهی باید به‌صراحت شامل تعهدات امنیتی باشند: استاندارد مرجع، سطح خدمت امنیتی، الزامات مدیریت وصله، ثبت لاگ، گزارش‌دهی رخداد، آزمون نفوذ مجاز، مدیریت دسترسی و تکالیف نگهداری ادله دیجیتال. ابهام در این حوزه، بستر اختلاف و فرار از مسئولیت را فراهم می‌کند.

**پیش‌بینی سازوکار هشدار و ثبت مخالفت**

اگر پیمانکار به‌دلیل ملاحظات عملیاتی کارفرما نتواند کنترل‌های پیشنهادی را اعمال کند، باید سازوکاری برای ثبت هشدار رسمی

و پذیرش ریسک از سوی کارفرما در قرارداد پیش‌بینی شود. نبود این سازوکار، اثبات دفاع پیمانکار را دشوار می‌کند.

**بیمه مسئولیت و بیمه سایبری**

با توجه به ابعاد بالقوه خسارت، استفاده از بیمه مسئولیت حرفه‌ای و بیمه سایبری برای پیمانکاران و کارفرمایان ضروری است. بیمه جایگزین مسئولیت نیست، اما ابزار مهمی برای مدیریت پیامدهای اقتصادی آن است.

**نظام ارزیابی و ممیزی مستقل**

پذیرش صرف ادعای پیمانکار درباره ایمن‌بودن سامانه کافی نیست. لازم است در پروژه‌های حساس، ممیزی امنیتی مستقل در دوره‌های معین پیش‌بینی شود. این ممیزی‌ها هم به پیشگیری کمک می‌کنند و هم در صورت بروز اختلاف، مبنای ارزیابی تقصیر قرار می‌گیرند.

**اصلاح تقنینی و تدوین دستورالعمل‌های بخشی**

در سطح کلان، ضرورت دارد برای مسئولیت فعالان سایبری در زیرساخت‌های حیاتی، دستورالعمل‌های بخشی روشن‌تری تدوین شود تا حدود تکلیف حرفه‌ای، نحوه مستندسازی، الزامات گزارش‌دهی و آثار حقوقی نقض استانداردها مشخص‌تر شود.

**نتیجه‌گیری**

مسئولیت مدنی پیمانکاران فناوری اطلاعات در برابر حملات سایبری به سیستم‌های کنترل صنعتی در پالایشگاه‌های پارس جنوبی، موضوعی صرفاً قراردادی یا فنی نیست، بلکه در تقاطع حقوق خصوصی، ایمنی صنعتی، حکمرانی سایبری و منافع عمومی قرار دارد. یافته اصلی این مقاله آن است که در زیرساخت‌های حیاتی، معیار سنجش تقصیر پیمانکار باید تشدید شود؛ زیرا خطرات بالقوه ناشی از سهل‌انگاری در این حوزه، تنها به نقض یک تعهد مالی محدود نمی‌شود و می‌تواند به خسارات جانی، زیست‌محیطی، تولیدی و ملی بینجامد.

از نظر تحلیلی، پیمانکار فناوری اطلاعات، هرچند معمولاً متعهد به دفع مطلق همه حملات نیست، اما بدون تردید متعهد به رعایت کامل استانداردهای حرفه‌ای، طراحی امن، مدیریت معقول آسیب‌پذیری‌ها، مستندسازی دقیق، کنترل دسترسی، پایش مؤثر و هشداردهی شفاف است. هرگاه حمله سایبری از مسیر ضعف‌هایی رخ دهد که به‌طور حرفه‌ای شناخته‌شده و قابل پیشگیری بوده‌اند، مسئولیت مدنی او قابل استقرار است و دفاع به غیرقابل پیش‌بینی‌بودن حمله یا مجرمانه‌بودن فعل مهاجم، در اغلب موارد کفایت نمی‌کند.

همچنین، مقاله استدلال کرد که تفکیک سنتی میان تعهد به وسیله و تعهد به نتیجه باید در این حوزه با احتیاط بازخوانی شود. هرچند امنیت مطلق ناممکن است، ولی در محیطی همچون پالایشگاه‌های پارس جنوبی، تعهد پیمانکار به «وسیله حرفه‌ای مشدد» نزدیک می‌شود؛ بدین‌معنا که سطح مراقبت مورد انتظار از وی، به‌مراتب بالاتر از پیمانکاری در محیط‌های عادی است.

سرانجام، برای کاهش اختلافات و افزایش پاسخ‌گویی، باید قراردادهای فناوری اطلاعات در صنعت نفت و گاز از حیث امنیت سایبری بازطراحی شوند؛ استانداردهای مرجع در آن‌ها تصریح گردد؛ ممیزی مستقل، بیمه سایبری، شروط روشن تقسیم ریسک و سازوکار ثبت هشدارهای فنی پیش‌بینی شود. تنها در چنین صورتی است که می‌توان میان نوآوری دیجیتال، تداوم تولید و مسئولیت‌پذیری حقوقی توازن برقرار کرد.

**مشارکت نویسندگان**

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

**تعارض منافع**

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافعی وجود ندارد.

## EXTENDED ABSTRACT

The rapid digitalization of the oil and gas industry has fundamentally altered the operational architecture of refineries by integrating information technology systems with operational technology, industrial control systems, supervisory control and data acquisition platforms, programmable logic controllers, safety instrumented systems, and remote monitoring infrastructures. This transformation has enhanced efficiency, process integration, production continuity, data exchange, predictive maintenance, and real-time decision-making; however, it has simultaneously expanded the cyberattack surface of critical energy infrastructure. In the South Pars refineries, where industrial processes are closely connected to national energy security, a cyber incident may extend far beyond data loss or temporary service disruption and may cause production shutdowns, physical equipment damage, explosions, fires, toxic releases, environmental contamination, bodily injury, financial loss, and widespread disruption of downstream energy activities. Industrial control systems are particularly sensitive because cyber intrusions may directly manipulate physical processes rather than merely compromise information confidentiality. The convergence of information technology and operational technology therefore creates a complex legal environment in which technical errors may produce extensive physical and economic consequences (Stouffer et al., 2023; Weaver, 2014). Information technology contractors and system integrators occupy a central position within this environment because they may be responsible for network architecture, system deployment, equipment configuration, cybersecurity controls, remote access, software updates, patch management, event logging, technical support, system integration, and incident response. Their access to critical components places them at the center of the cybersecurity trust chain and makes their professional conduct legally significant. Accordingly, the principal objective of this study is to determine the legal foundations, conditions, and scope of the civil liability of information technology contractors for damage resulting from cyberattacks against industrial control systems in the South Pars refineries. The study also examines whether the traditional contractual distinction between an obligation of means and an obligation of result remains adequate in relation to cybersecurity duties in critical infrastructure, or whether the dangerous and highly specialized nature of the activity requires a heightened professional standard of care.

This study adopts a descriptive-analytical legal methodology combined with an argumentative approach. It analyzes the general principles of Iranian civil liability law, contractual obligations, professional negligence, causation, compensation, jurisprudential rules, and the legal significance of industrial cybersecurity standards. The analysis is based on the premise that the designation used in a contract does not, by itself, determine the contractor's civil liability; rather, the contractor's actual technical role in creating, controlling, increasing, or preventing cyber risk must be assessed. An information technology contractor may include a software company, network infrastructure provider, cybersecurity service provider, system integrator, operational technology maintenance contractor, industrial automation specialist, or remote-access service provider. Any such contractor whose activities materially affect the confidentiality, integrity, availability, safety, or resilience of industrial control systems may be exposed to liability where professional misconduct contributes to damage. The study also distinguishes between cyberattacks against ordinary administrative systems and attacks against operational technology environments. In conventional information systems,

confidentiality often receives the greatest attention, whereas in operational technology environments, availability, continuity, process integrity, and physical safety are frequently prioritized. A technical intervention that is acceptable in an administrative network, such as the immediate shutdown of a system for patch installation, may be hazardous in a refinery control environment. Therefore, the legal assessment of conduct must reflect the operational context and cannot be based solely on general information technology practices (Stouffer et al., 2023). The study further considers the importance of supply-chain dependencies, legacy equipment, third-party software, remote vendor connections, outdated firmware, multiple subcontractors, and the limited availability of updates. These factors complicate both technical attribution and legal causation, particularly when several contractors or operators have simultaneously contributed to the vulnerability. Consequently, the preservation of logs, configuration records, access histories, architecture diagrams, vulnerability reports, change-management records, service-level agreements, and incident-response documentation becomes essential not only for cybersecurity governance but also for establishing or rebutting legal responsibility.

The findings demonstrate that the civil liability of information technology contractors under Iranian law has a composite legal basis. First, liability may arise from fault where the contractor, through intent, negligence, recklessness, lack of skill, failure to comply with professional regulations, or omission of necessary precautions, causes damage to another person. The professional status of the contractor significantly affects the applicable standard of conduct. An information technology contractor operating in a refinery should not be assessed according to the behavior of an ordinary person, but according to the conduct expected of a cautious, competent, and informed professional possessing specialized knowledge of industrial cybersecurity and the dangers of critical infrastructure (Katouzian, 2007; Pour-Ostad, 2018). Second, contractual liability may arise where the contractor fails to perform express or implied security obligations. Such obligations may concern secure architecture, network segmentation, patch management, access control, incident logging, system recovery, vulnerability assessment, compliance with agreed technical standards, or the maintenance of operational continuity. Contractual liability is not limited to literal nonperformance; defective performance that formally satisfies delivery requirements but leaves the system materially insecure may also constitute a breach, because contractual obligations must be performed in a manner that fulfills the legitimate purpose of the agreement (Katouzian, 2009; Taghizadeh, 2022). Third, the jurisprudential and legal doctrines of direct destruction and causation provide an additional foundation for liability. A contractor is rarely the direct perpetrator of the cyberattack, but may create the conditions through which the attacker causes harm. Where an insecure remote-access channel, unpatched vulnerability, default password, inadequate network boundary, or defective security configuration constitutes an effective and foreseeable cause of the damage, the contractor may be regarded as a legally relevant cause even though the immediate harmful act was committed by a third-party attacker (Jafari Langroudi, 2008; Mohaqeq Damad, 2010). The principle against causing harm also reinforces the protective orientation of civil liability and prevents technical complexity or contractual limitations from being used as instruments for unjustly transferring the consequences of professional negligence to victims (Makarem Shirazi, 1990; Safaei & Rahimi, 2012).

The analysis identifies several technical and professional failures that may constitute legally relevant negligence. One of the most significant is the insecure design of network architecture, particularly the failure to properly separate administrative systems, control networks, critical assets, remote-access gateways, and industrial demilitarized zones. If a contractor creates an architecture through which compromise of the administrative network can easily spread to operational technology, such conduct may constitute both a breach of contractual duties and a cause of the resulting physical damage. Other important forms of negligence include inadequate patch and vulnerability management, failure to assess or test updates before deployment, prolonged exposure to known critical vulnerabilities, absence of compensating controls for legacy systems, and failure to document the reasons for delaying security updates. Insecure remote access is another major source of liability, especially where contractors use shared credentials, weak passwords, unsafe communication tools, permanent vendor accounts, or connections lacking multifactor authentication and session monitoring. The use of default configurations, unnecessary ports, unused services, factory-set passwords, and poorly secured maintenance accounts also falls below the expected standard of professional care. Failure to activate, preserve, and review logs may increase damage by delaying detection and may also obstruct later investigation, thereby complicating the determination of causation and responsibility. Inadequate training of operators and users may similarly create liability where the contractor was responsible for awareness programs, removable-media controls, phishing prevention, access protocols, or incident-response procedures. These duties are particularly significant because many industrial attacks exploit a combination of technical vulnerabilities and human error. The professional standard applicable in critical infrastructure must therefore be stricter than that applied to ordinary commercial projects. Although cybersecurity cannot guarantee the absolute prevention of every attack, a contractor cannot rely on the inherent uncertainty of cyber threats where the intrusion occurred through a well-known and preventable weakness. Historical incidents such as Stuxnet demonstrated that malicious code can manipulate industrial processes and produce physical consequences, thereby transforming cybersecurity from an information-protection concern into a matter of operational safety and physical risk (Langner, 2011). Research concerning industrial control system incidents likewise confirms that vulnerabilities in supervisory and control environments may produce effects that extend far beyond conventional data breaches (Miller & Rowe, 2012).

A central legal issue concerns causation and the extent to which the criminal act of an external attacker interrupts the causal connection between the contractor's negligence and the resulting loss. The study concludes that the intervention of a malicious third party should not automatically exempt the contractor from liability. In critical energy infrastructure, cyberattack is generally foreseeable, and cybersecurity contractors are specifically engaged to identify, reduce, and manage such threats. Therefore, where the contractor creates or fails to eliminate a vulnerability that constitutes a normal and foreseeable route of exploitation, the attacker's conduct forms part of the causal chain rather than necessarily breaking it. The contractor may be liable if its omission was an effective and legally relevant factor in the occurrence or aggravation of the damage, even when other factors also contributed (Salehi, 2022). The determination of causation in such cases requires detailed technical expertise and

careful evaluation of logs, access records, network topology, system versions, vulnerability assessments, maintenance reports, contractor warnings, employer decisions, and the sequence of events. Liability may also be distributed among several actors, including the employer, main contractor, subcontractor, equipment manufacturer, software vendor, system operator, and communications provider. The presence of multiple causes should not create practical immunity for a professional contractor whose failure materially increased the risk. The compensable losses resulting from such attacks may include system restoration costs, data recovery expenses, emergency upgrades, malware removal, equipment repair, production interruption, loss of materials, expert investigation costs, lost profits, bodily injury, death, environmental damage, reputational harm, and damage sustained by third parties. In contractual relationships, the contractor may be responsible to the refinery operator, whereas in relation to employees, neighboring communities, downstream companies, or other third parties, noncontractual liability may arise. Contractual clauses limiting liability should be interpreted narrowly in the context of critical infrastructure, particularly where gross negligence, professional recklessness, bodily injury, environmental harm, or public interests are involved. Compliance with recognized standards may constitute evidence that the contractor exercised professional care, but formal or documentary compliance alone is insufficient. The decisive issue is whether the implemented controls were real, effective, properly maintained, and appropriate to the actual risks of the refinery environment (Amini, 2021; Hosseini, 2020; Nobakht, 2021).

In conclusion, the civil liability of information technology contractors for cyberattacks against industrial control systems in the South Pars refineries should be understood as a multidimensional form of responsibility located at the intersection of contract law, tort law, professional liability, industrial safety, cybersecurity governance, and the protection of public interests. The dangerous nature of refinery operations, the national significance of energy infrastructure, and the potential for cyber incidents to produce physical, environmental, human, and economic harm justify the application of a heightened professional standard of care. Contractors cannot reasonably be required to guarantee that no cyberattack will ever occur, but they must fully perform all professional duties relating to secure design, network segmentation, vulnerability management, controlled remote access, event logging, continuous monitoring, user training, risk assessment, incident response, system recovery, and transparent warning. The conventional obligation-of-means model should therefore be reformulated as a heightened professional obligation of means, under which the contractor is expected to demonstrate not merely ordinary effort but specialized, documented, risk-sensitive, and standards-based conduct. Effective risk allocation also requires the redesign of information technology contracts in the oil and gas sector. Such contracts should expressly define security obligations, reference applicable standards, allocate responsibility among contractors and subcontractors, regulate remote access, require the preservation of digital evidence, establish formal warning and risk-acceptance procedures, provide for independent security audits, and require adequate professional liability and cyber insurance. Clearer sector-specific regulations are also necessary to define the duties of cybersecurity actors in critical infrastructure and to reduce uncertainty concerning documentation, reporting, inspection, causation, and compensation. Through these measures, it is

possible to establish a more appropriate balance among technological innovation, continuity of production, protection of victims, and legal accountability.

**References**


Amini, R. (2021). *Cyber Law and Liability Arising from Information Security Breaches*. Jangal.

Hosseini, S. M. (2020). Legal Analysis of Critical Infrastructure Security in Iran. *Journal of Public Law Studies*, *21*(3), 133-160.

Ibn-Najjar, M. (2019). *Civil Liability and Compensation for Damage in Iranian Law*. Mizan.

Jafari Langroudi, M. J. (2008). *Legal Terminology*. Ganj Danesh.

Katouzian, N. (2007). *Extra-Contractual Obligations: Civil Liability*. University of Tehran Press.

Katouzian, N. (2009). *General Rules of Contracts*. Sherkat-e Sahami Enteshar.

Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security & Privacy*, *9*(3), 49-51.

Makarem Shirazi, N. (1990). *Al-Qawa'id al-Fiqhiyyah*. Imam Ali ibn Abi Talib School.

Miller, B., & Rowe, D. (2012). A Survey of SCADA and Critical Infrastructure Incidents. Proceedings of the 1st Annual Conference on Research in Information Technology,

Mohaqeq Damad, S. M. (2010). *Rules of Jurisprudence, Civil Section*. Center for Islamic Sciences Publishing.

Nobakht, S. (2021). *Civil Liability Arising from Data Breach and Cybersecurity*. SAMT.

Pour-Ostad, A. (2018). *Foundations of Professional Civil Liability*. Khorsandi.

Safaei, S. H., & Rahimi, H. (2012). *Civil Liability and Compensation for Damage*. SAMT.

Salehi, H. (2022). Civil Liability Arising from Emerging Technology Risks. *Journal of the Faculty of Law and Political Science*, *51*(4), 57-84.

Stouffer, K., Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., & Thompson, M. (2023). *Guide to Operational Technology (OT) Security* (NIST Special Publication 800-82 Rev. 3, Issue.

Taghizadeh, M. (2022). Contractual Liability in Information Technology Projects. *Quarterly Journal of Private Law Research*, *19*(2), 85-112.

Weaver, N. (2014). ICS Security: Industrial Control Systems in the Digital Age. *Communications of the Acm*, *57*(7), 28-30.