O PAPEL DA CIBERSEGURANÇA NA TRANSIÇÃO PARA A ECONOMIA CIRCULAR EM UMA INDÚSTRIA AUTOMOTIVA

1 INTRODUÇÃO

A Economia Circular tem sido adotada na indústria como estratégia voltada à sustentabilidade (MURRAY; SKENE; HAYNES, 2017), com destaque para iniciativas da Fundação Ellen MacArthur (BOCKEN et al., 2016). O conceito abrange práticas como reutilização, remanufatura e uso de energias renováveis (GEISSDOERFER et al., 2017), além de modelos circulares (LACY; LONG; SPINDLER, 2020), dimensões de aplicação (BOYER et al., 2021) e abordagens setoriais, como na indústria automotiva (ESTEVA et al., 2021). Entre os principais referenciais estão o modelo ReSOLVE (EMF, 2015; LEWANDOWSKI, 2016) e o Diagrama Borboleta (EMF, 2015).

A indústria automotiva, inserida em cadeias upstream e downstream, apresenta demanda crescente em países emergentes (BHATTACHARYA; MUKHOPADHYAY; GIRI, 2014). Nesse cenário, a Economia Circular é apoiada por tecnologias da Indústria 4.0 voltadas à eficiência e redução de desperdícios (RAJPUT; SINGH, 2019). A cibersegurança é apontada como elemento essencial para garantir integridade e disponibilidade de dados em sistemas automatizados (RÜßMANN et al., 2015), contribuindo para maior agilidade nas cadeias de suprimentos (JABBOUR et al., 2018).

A convergência entre Economia Circular e Indústria 4.0 ainda é limitada (MASSARO et al., 2021), com estudos sobre seus facilitadores (SU et al., 2013; TURA et al., 2019) e interações (JABBOUR et al., 2018; RAJPUT; SINGH, 2019). A articulação entre tecnologias da Indústria 4.0 (RÜßMANN et al., 2015; SAUCEDO-MARTÍNEZ et al., 2018) e modelos circulares como o ReSOLVE requer aprofundamento, especialmente no setor automotivo (ESTEVA et al., 2021). Esta pesquisa, por meio de estudo de caso, analisa como a cibersegurança pode contribuir para a Economia Circular na indústria automotiva (JABBOUR et al., 2018; RAJPUT; SINGH, 2019), considerando sua relação com estratégias do modelo ReSOLVE (EMF, 2015; LEWANDOWSKI, 2016).

2 FUNDAMENTAÇÃO TEÓRICA

A Economia Circular propõe uma abordagem restaurativa, com foco na conservação de recursos e redução de desperdícios (GHISELLINI; CIALANI; ULGIATI, 2016; EMF, 2015), substituindo o modelo linear por práticas de design circular e gestão eficiente de materiais (GENG; SARKIS; ULGIATI, 2016; LEWANDOWSKI, 2016). Essa transição exige considerar toda a cadeia de suprimentos e dissociar crescimento econômico de impactos ambientais (LINDER; SARASINI; LOON, 2017), com ações em níveis micro, meso e macro (GHISELLINI; CIALANI; ULGIATI, 2016).

Modelos de negócios circulares e estratégias como recirculação e resistência dos produtos são destacados (LACY; LONG; SPINDLER, 2020; BOYER et al., 2021), além do Diagrama Borboleta e do modelo ReSOLVE, com seis estratégias aplicáveis a diversos setores (EMF, 2015; LEWANDOWSKI, 2016; DEV; SHANKAR; QAISER, 2020). No setor automotivo, há modelo baseado nos ciclos de vida dos veículos e em pilares como energia renovável e materiais recicláveis (ESTEVA et al., 2021). Tecnologias digitais ampliam a circularidade na manufatura (ROSA et al., 2020), com destaque para a Indústria 4.0 como facilitadora da transição (TSENG et al., 2018; RAJPUT; SINGH, 2019).

A Indústria 4.0, oficializada em 2013, baseia-se em nove tecnologias habilitadoras que transformam sistemas produtivos em estruturas integradas e autônomas (XU; XU; LI, 2018; RÜßMANN et al., 2015; SAUCEDO-MARTÍNEZ et al., 2018). Essas tecnologias contribuem

para a circularidade nas cadeias de suprimentos (JABBOUR et al., 2018) e são incorporadas a políticas ambientais (DOS SANTOS; COTI-ZELATI; DE ARAÚJO, 2020).

A cibersegurança é considerada tecnologia habilitadora essencial, garantindo integridade, confiabilidade e disponibilidade de dados (RÜßMANN et al., 2015; SAUCEDO-MARTÍNEZ et al., 2018). Sua implementação envolve ferramentas específicas (SARKER et al., 2020) e Sistemas Físicos Cibernéticos (BAGHERI et al., 2015; XU; XU; LI, 2018), com sensores e automação (MOHAMMADIAN; HATZINAKOS, 2009).

A cibersegurança é fundamental para a circularidade em contextos hiperconectados (SULICH et al., 2021), protegendo dados ambientais e produtivos (ESMAEILIAN et al., 2020). Na indústria automotiva, tecnologias digitais promovem integração e automação (RÜßMANN et al., 2015; DOS SANTOS; COTI-ZELATI; DE ARAÚJO, 2020), com sistemas conectados que ampliam rastreabilidade e agilidade (MRABTI; NOURI, 2023).

A cibersegurança protege todo o ciclo veicular, incluindo dados de fornecedores e sistemas de resposta a incidentes (ARROYABE; WATSON; ANGELOPOULOU, 2023), sendo essencial diante da exposição a ameaças digitais nas fábricas inteligentes e veículos conectados (ÖZARPA; İSA, 2022).

3 METODOLOGIA

O estudo é de natureza aplicada, com abordagem qualitativa interpretativa, baseado em estudo de caso (CRESWELL, 2010). A pesquisa foi conduzida em uma fabricante de veículos comerciais que adota tecnologias da Indústria 4.0 e práticas de Economia Circular, com objetivo exploratório de gerar insights sobre eficiência produtiva e circularidade de materiais (COLLIS; HUSSEY, 2005). Foram realizadas entrevistas semiestruturadas com profissionais das áreas de desenvolvimento e manufatura, abordando temas ligados à Cibersegurança e à circularidade (FLICK, 2009).

A escolha do estudo de caso permitiu análise contextualizada do fenômeno (YIN, 2015), sendo a empresa selecionada por sua relevância e disponibilidade de dados públicos sobre ferramentas da Indústria 4.0 (AUTOCARPRO, 2018; HANNOVERMESSE, 2018). A pesquisa seguiu três etapas: definição do protocolo, coleta e análise de dados, e interpretação das evidências (YIN, 2015). O mapeamento dos processos organizacionais orientou a definição das unidades de análise e permitiu identificar estratégias ReSOLVE e avaliar os impactos das tecnologias habilitadoras.

As fontes de evidência incluíram documentos internos e públicos, registros organizacionais, observações diretas e entrevistas (CRESWELL, 2010; YIN, 2015; FLICK, 2009). As evidências foram organizadas e categorizadas conforme Bardin (2011), com base nas fases do ciclo de vida automotivo: Design e Manufatura, Uso e Final de Vida. As unidades de análise foram estruturadas em macroprocessos organizacionais (MPG, MPAC, MPCP, MPAP, MPS), abrangendo áreas como gestão, produção, atendimento e suporte.

A análise considerou a aplicação da Cibersegurança em diferentes áreas da empresa, relacionando suas contribuições às estratégias circulares e às tecnologias da Indústria 4.0, com foco na aderência das práticas organizacionais às teorias investigadas. A confidencialidade da empresa foi preservada por meio da codificação dos documentos internos.

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

Diante de um mercado automotivo global cada vez mais competitivo, aspectos como reputação corporativa — tanto no que diz respeito às operações quanto aos produtos — e a eficiência operacional tornaram-se determinantes para a sustentabilidade do negócio. Embora os sistemas de gestão contribuam para esse desempenho, a inovação e a adoção de tecnologias

avançadas mostraram-se indispensáveis para alcançar maior produtividade com menor consumo de recursos e o investimento em tecnologias da Indústria 4.0 como estratégia prioritária para elevar a competitividade da organização. A implementação das tecnologias habilitadoras da Indústria 4.0 passou a ser tratada como um diferencial competitivo pela organização. A empresa realizou uma ampla reestruturação em seus processos de manufatura, com revisão de linhas de produção e automação de equipamentos. Para guiar esse processo de maneira sistêmica, a organização adotou um modelo composto por nove tecnologias habilitadoras, conforme referência da literatura: big data e analytics, robôs autônomos, simulação, integração horizontal e vertical de sistemas, internet das coisas (IoT), cibersegurança, manufatura aditiva, realidade aumentada e computação em nuvem (RÜßMANN et al., 2015; SAUCEDO-MARTÍNEZ et al., 2018).

Com a incorporação dessas tecnologias às atividades organizacionais, aumentaram as preocupações quanto à governança de dados e sua segurança. A área de Tecnologia da Informação, pertencente à unidade de análise de Suporte, ficou responsável por apoiar a categorização das informações, que passaram a ser classificadas como públicas, internas, confidenciais ou secretas. A partir dessa classificação, são aplicadas políticas de proteção específicas, sendo os dados secretos submetidos aos mecanismos mais rigorosos de segurança.

Reconhecendo a importância estratégica da proteção digital frente à digitalização intensiva e à ampliação da superfície de ataque, a organização instituiu o Business Information Office, dedicado exclusivamente à gestão da cibersegurança. Uma das principais iniciativas conduzidas por essa área é o Sistema de Segurança de TI de Chão de Fábrica.Embora a proteção da informação abarque todos os processos organizacionais, o enfoque nas operações fabris deve-se à crescente conectividade dos dispositivos no ambiente de produção. Apenas em uma planta, estima-se que existam cerca de 8 mil dispositivos conectados à rede, todos requerendo monitoramento e controle contínuos para garantir a disponibilidade e integridade dos dados. Diante do aumento da automação e das interconexões, a exposição a riscos cibernéticos torna-se mais acentuada, razão pela qual foi desenvolvido o Sistema de Segurança de TI de Chão de Fábrica.

Tal sistema busca fortalecer a comunicação e a gestão de riscos relacionados à segurança cibernética no ambiente produtivo. Ele é estruturado em torno de cinco domínios principais: Identificação, compreensão organizacional sobre riscos cibernéticos; Detecção, atividades de monitoramento de eventos adversos; Resposta, ações frente a incidentes de segurança; Proteção, medidas preventivas para assegurar serviços críticos; e Recuperação: processos de restauração de recursos comprometidos. O desempenho dessas atividades é monitorado por meio de um software que fornece indicadores relevantes, como o número de incidentes, localização dos ativos afetados, média de restaurações, vulnerabilidades mapeadas, alertas por tipo de dispositivo, status de ativos inventariados, controle de acessos e aplicações de antivírus.

As evidências do estudo demonstraram que a cibersegurança é essencial para garantir tanto a proteção da informação quanto a disponibilidade dos dados em cada uma das tecnologias habilitadoras da Indústria 4.0. Na tecnologia de Big Data e Analytics, a cibersegurança assegura que os dados processados sejam protegidos contra acessos não autorizados e manipulações, garantindo integridade, confidencialidade e a disponibilidade dos sistemas analíticos para suporte à tomada de decisões. Para Robôs Autônomos, a cibersegurança protege os sistemas de controle e comunicação contra invasões e sabotagens, preservando a precisão das operações e garantindo que os dados estejam sempre acessíveis para monitoramento seguro. Nas aplicações de Simulação, a cibersegurança impede alterações maliciosas nos modelos computacionais e nos dados utilizados, garantindo que os resultados simulados sejam confiáveis e que os sistemas virtuais estejam disponíveis para uso estratégico. Na Integração Horizontal e Vertical de Sistemas, a cibersegurança previne interceptações e distorções nos fluxos de dados entre departamentos e parceiros, além de garantir que as informações essenciais estejam disponíveis

para operações integradas. Em ambientes com Internet das Coisas (IoT), a cibersegurança protege os dados gerados por sensores conectados, impede interferências externas e assegura que as redes estejam disponíveis e seguras para análise e controle em tempo real. Como tecnologia transversal, a própria cibersegurança sustenta todas as demais ao definir infraestruturas seguras, mitigar riscos digitais e preservar a disponibilidade e a confiabilidade dos ativos informacionais industriais. Na Manufatura Aditiva, a cibersegurança garante que arquivos digitais de projeto sejam protegidos contra corrupção ou acesso indevido, além de manter os sistemas operacionais disponíveis para produção precisa e segura. Nas soluções de Realidade Aumentada, a cibersegurança assegura que os dados projetados nas interfaces estejam íntegros e protegidos contra manipulações, mantendo a confiabilidade e disponibilidade das informações visuais. Por fim, na Computação em Nuvem, a cibersegurança protege dados armazenados e transmitidos em ambientes distribuídos, garantindo acesso apenas a usuários autorizados e preservando a disponibilidade dos serviços em escala industrial.

No contexto da Economia Circular, essa tecnologia habilitadora contribui para a implementação de todas as estratégias do modelo ReSOLVE (EMF, 2015; LEWANDOWSKI, 2016). Com o processo de digitalização via IoT, análises baseadas em Big Data e gestão em nuvem, a Cibersegurança assegura a proteção e disponibilidade de dados, sendo de grande relevância para as estratégias de Regeneração, Compartilhamento, Otimização, Loop, Virtualização e Substituição. Sob a ótica ambiental, a Cibersegurança oferece suporte à eficiência organizacional ao garantir a confiabilidade e a disponibilidade de dados em rede, possibilitando decisões mais assertivas que reduzem o consumo de recursos naturais e a geração de resíduos. Além disso, contribui para a gestão de aspectos e impactos ambientais associados ao ciclo de vida apresentado no modelo automotivo de Economia Circular (ESTEVA et al., 2021).

6 CONSIDERAÇÕES FINAIS

O estudo teve como objetivo analisar as contribuições da cibersegurança na transição para a Economia Circular em uma indústria automotiva, com foco na implementação das tecnologias habilitadoras da Indústria 4.0 e na relação com as estratégias do modelo ReSOLVE (EMF, 2015; LEWANDOWSKI, 2016). As evidências obtidas permitiram associar essas tecnologias às estratégias circulares ao longo das fases do ciclo de vida do veículo: desenvolvimento, manufatura, uso e fim de vida. A cibersegurança destacou-se como tecnologia transversal, essencial para garantir integridade, disponibilidade e confidencialidade dos dados digitais, sustentando sistemas interconectados que viabilizam práticas circulares. Tecnologias como manufatura aditiva, robôs colaborativos, realidade aumentada, simulação, computação em nuvem, integração de sistemas, Internet das Coisas e Big Data demonstraram potencial para apoiar estratégias como otimização, compartilhamento, virtualização e substituição, desde que operem sobre infraestrutura digital protegida.

A cibersegurança viabiliza o rastreamento de componentes (loop), o compartilhamento seguro de informações (compartilhamento), decisões em tempo real (otimização), proteção de dados sensoriais (virtualização), suporte a plataformas digitais (substituição) e integridade de dados críticos (regeneração). As tecnologias mais recorrentes foram Internet das Coisas, Big Data e cibersegurança, que juntas sustentam a aplicação das estratégias ReSOLVE em todas as fases do ciclo de vida veicular.

A análise confirmou que a cibersegurança atua como infraestrutura estratégica para a operacionalização segura e integrada das demais tecnologias habilitadoras da Indústria 4.0. A contribuição prática do estudo está na identificação de processos organizacionais com maior aderência à cibersegurança, enquanto a contribuição teórica reside na articulação entre segurança digital e práticas circulares no setor automotivo.

Como as tecnologias estão em diferentes estágios de maturidade, alguns benefícios observados são potenciais. Recomenda-se que estudos futuros explorem tecnologias emergentes, como blockchain e inteligência artificial, e investiguem possíveis externalidades negativas, como o consumo energético e a demanda por resfriamento de datacenters.

REFERÊNCIAS

ARROYABE, Ignacio Fernandez de; WATSON, Tim; ANGELOPOULOU, Olga. Cybersecurity in the Automotive Industry: A Systematic Literature Review (SLR). **Journal of Computer Information Systems**, v. 63, n. 3, p. 716-734, 2023.

AUTOCARPRO. **Daimler Trucks implements Industry 4.0 at Brazilian plant**. 2018. Disponível em: <https://www.autocarpro.in/news-international/daimler-trucks-implements-industry-brazilian-plant-28839>. Acesso em: 07 abr. 2023.

BAGHERI, Behrad et al. Cyber-physical systems architecture for self-aware machines in industry 4.0 environment. **IFAC-PapersOnLine**, v. 48, n. 3, p. 1622-1627, dez. 2015.

BHATTACHARYA, Souresh; MUKHOPADHYAY, D.; GIRI, Sunil. Supply chain management in Indian automotive industry: Complexities, challenges and way ahead. **International Journal of Managing Value and Supply Chains**, v. 5, n. 2, p. 49-62, jun. 2014.

BOCKEN, Nancy MP et al. Product design and business model strategies for a circular economy. **Journal of industrial and production engineering**, v. 33, n. 5, p. 308-320, abr. 2016.

BOYER, Robert H. W. et al. Three-dimensional product circularity. **Journal of Industrial Ecology**, v. 25, n. 4, p. 824-833, fev. 2021.

COLLIS, Jill; HUSSEY, Roger. **Pesquisa em Administração**. 2. ed. São Paulo: Bookman, 2005.

CRESWELL, J. W. **Projeto de pesquisa**: método qualitativo, quantitativo e misto. Porto Alegre: Artmed, 2010.

DANTAS, Thales Eduardo Tavares et al. How the combination of Circular Economy and Industry 4.0 can contribute towards achieving the Sustainable Development Goals. **Sustainable Production and Consumption**, v. 26, p. 213-227, abr. 2021.

DEV, Navin K.; SHANKAR, Ravi; QAISER, Fahham Hasan. Industry 4.0 and circular economy: Operational excellence for sustainable reverse supply chain performance. **Resources, Conservation and Recycling**, v. 153, n. 2, fev. 2020.

DOS SANTOS, Leonardo Pezenatto dos; COTI-ZELATI, Paolo Edoardo; ARAÚJO, Davi Lucas Arruda de. Industry 4.0 and Sustainable Development in the Automotive Sector. **Revista Liceu On-Line**, v. 10, n. 1, p. 26-54, maio 2020.

EMF - ELLEN MACARTHUR FOUNDATION. **Towards the circular economy:** Business rationale for an accelerated transition. Isle of Wight: EMF, 2015.

ESMAEILIAN, Behzad et al. Blockchain for the future of sustainable supply chain management in Industry 4.0. **Resources, Conservation and Recycling**, v. 163, dez. 2020.

ESTEVA, Laura C. Aguilar et al. Circular economy framework for automobiles: Closing energy and material loops. **Journal of Industrial Ecology**, v. 25, n. 4, p. 877-889, ago. 2021.

FLICK, U. **Introdução à pesquisa qualitativa**. Porto Alegre: Artmed, 2009.

GEISSDOERFER, Martin et al. The Circular Economy - A new sustainability paradigm?. **Journal of cleaner production**, v. 143, p. 757-768, fev. 2017.

GENG, Yong; SARKIS, Joseph; ULGIATI, Sergio. Sustainability, well-being, and the circular economy in China and worldwide. **Science**, Washington, v. 6278, n. Suppl., p. 73-76, mar. 2016.

GHISELLINI, Patrizia; CIALANI, Catia; ULGIATI, Sergio. A review on circular economy: the expected transition to a balanced interplay of environmental and economic systems. **Journal of Cleaner Production**, v. 114, p. 11-32, fev. 2016.

HANNOVERMESSE. **Daimler commissions high-tech assembly line in Brazil**. 2018. Disponível em: <https://www.hannovermesse.de/en/news/news-articles/daimler-commissions-high-tech-assembly-line-in-brazil>. Acesso em: 06 abr. 2023.
HEYES, Graeme et al. Developing and implementing circular economy business models in service-oriented technology companies. **Journal of Cleaner Production**, v. 177, p. 621-632, mar. 2018.
JABBOUR, A. B. L. D. S. et al. Industry 4.0 and the circular economy: a proposed research agenda and original roadmap for sustainable operations. **Annals of Operations Research**, v. 270, n. 1, p. 273-286, nov. 2018.
LACY, Peter; LONG, Jessica; SPINDLER, Wesley. The Circular Business Models. In: LACY, P.; LONG, J.; SPINDLER, W. **The Circular Economy Handbook**. London: Palgrave Macmillan, 2020. p. 17-42.
LEWANDOWSKI, Mateusz. Designing the Business Models for Circular Economy—Towards the Conceptual Framework. **Sustainability**, Basel, v. 8, n. 1, p. 43-70, jan. 2016.
LINDER, Marcus; SARASINI, Steven; LOON, Patricia. A Metric for Quantifying Product-Level Circularity. **Journal of Industrial Ecology**, Hoboken, v. 21, n. 3, p. 545-558, fev. 2017.
MOHAMMADIAN, Masoud; HATZINAKOS, Dimitrios. Data classification process for security and privacy based on a fuzzy logic classifier. **International Journal of Electronic Finance**, v. 3, n. 4, p. 374-386, out. 2009.
MRABTI, Abdelaziz; NOURI, Khaled. Smart manufacturing production line connectivity–case study in automotive sector. **ITM Web of Conferences,**.v. 52, p. 1-10, maio 2023.
MURRAY, Alan; SKENE, Keith; HAYNES, Kathryn. The circular economy: an interdisciplinary exploration of the concept and application in a global context. **Journal of business ethics**, v. 140, n. 3, p. 369-380, maio 2017.
ÖZARPA, Cevat; İSA, A. V. C. I. Industry 4.0 and Cybersecurity at Automobile Manufacturing in Smart Factories. **Düzce University Journal of Science & Technology**, v. 10, n. 4, p. 2120-2132, out. 2022.
RAJPUT, Shubhangini; SINGH, Surya Prakash**.** Connecting circular economy and industry 4.0. **International Journal of Information Management**, v. 49, p. 98-113, dez. 2019.
ROSA P. et al. Assessing Relations between Circular Economy and Industry 4.0: A Sistematic Literature Review. **International Journal of Production Research**, v. 58, n. 6, p. 1662-1687, mar. 2020.
RÜßMANN, Michael et al. Industry 4.0: The future of productivity and growth in manufacturing industries. **Boston consulting group**, v. 9, n. 1, p. 54-89, abr. 2015.
SARKER, Iqbal H. et al. Cybersecurity data science: an overview from machine learning perspective. **Journal of Big data**, v. 7, p. 1-29, jul. 2020.
SAUCEDO-MARTÍNEZ, Jania Astrid et al. Industry 4.0 framework for management and operations: a review. **Journal of ambient intelligence and humanized computing**, v. 9, n. 3, p. 789-801, jun. 2018.
SU, B. et al. A review of the circular economy in China: moving from rhetoric to implementation. **Journal of Cleaner Production**, v. 42, p. 215-227, mar. 2013.
SULICH, Adam et al. Cybersecurity and sustainable development. **Procedia Computer Science**, v. 192, p. 20-28, out. 2021.
TSENG, Ming-Lang et al. Circular economy meets industry 4.0: Can big data drive industrial symbiosis?. **Resources, conservation and recycling**, v. 131, p. 146-147, abr. 2018.
TURA, N. et al. Unlocking circular business: A framework of barriers and drivers. **Journal of Cleaner Production**, Lappeenranta, v. 212, p. 90–98, mar. 2019.
YIN, R. K. **Estudo de Caso - Planejamento e Métodos**. 5. ed. Porto Alegre: Bookman, 2015.
XU, Li Da; XU, Eric L.; LI, Ling. Industry 4.0: state of the art and future trends. **International Journal of Production Research**, v. 56, n. 8, p. 2941-2962, mar. 2018.