The European Union Artificial Intelligence Act in 2026: Regulatory Stasis, Economic Imperatives, and the Specter of Historical Protectionism

1. Introduction: The Digital Crossroads of February 2026

As the European Union moves through the first quarter of 2026, the continent finds itself at a pivotal moment in the governance of the digital age. The implementation of the landmark **EU Artificial Intelligence Act (AI Act)**, once heralded as the world's first comprehensive constitution for artificial intelligence, has encountered significant structural and political headwinds. While the initial prohibitions on "unacceptable risk" AI practices successfully entered into force in February 2025, the broader machinery of the regulation is straining under the weight of technical complexity, economic anxiety, and intense geopolitical pressure.

The current landscape is defined by a tension between the EU's foundational commitment to a "human-centric" digital ecosystem and the terrified realization that Europe may be regulating itself out of the global technological arms race. This sentiment, often described in policy circles as "AI FOMO" (Fear Of Missing Out), has precipitated a dramatic legislative pivot in early 2026: the introduction of the **"Digital Omnibus"**, a sweeping deregulation package intended to simplify compliance and delay the most burdensome aspects of the AI Act.

To fully understand the gravity and the potential trajectory of this moment, it is necessary to look beyond the immediate bureaucratic struggles of Brussels and examine the historical precedents of technological restriction. The current debates regarding "digital sovereignty," "protectionism," and the "Digital Iron Curtain" echo with striking fidelity the technological policies of the 1980s. Specifically, the draconian import restrictions on personal computers in **socialist Malta under Dom Mintoff** and the broader **Eastern Bloc** offer a compelling historical mirror. In both eras, the state attempted to centrally manage the influx of a disruptive technology—the personal computer in the 1980s, and generative AI in the 2020s—ostensibly to protect social stability and labor, but often resulting in stagnation, illicit markets, and a frantic game of catch-up.

This report provides an exhaustive analysis of the status of the EU AI Act as of February 2026, dissecting the arguments for and against its current trajectory. It then synthesizes these modern regulatory challenges with a detailed historical audit of the 1980s computer bans, revealing deep structural continuities in how political regimes respond to the "threat" of

uncontrolled technological proliferation.

---

2. The State of the AI Act in 2026: A System Under Stress

2.1 The Implementation Timeline and Emerging Bottlenecks

The AI Act was designed to be implemented in a phased approach, a strategy intended to allow the market sufficient time to adapt to the new "high-risk" obligations. However, as of February 2026, this timeline has fractured. While the regulatory architecture for the most extreme risks is in place, the mechanisms for the broader market have stalled.

The Act officially entered into force in **August 2024**, triggering a countdown for various provisions. The first major milestone was successfully met on **February 2, 2025**, when the prohibitions on AI practices deemed to pose an "unacceptable risk" became active.[1] This effectively outlawed systems capable of subliminal manipulation, social scoring by public authorities, and real-time remote biometric identification in public spaces for law enforcement purposes (with narrow exceptions for serious crimes and terrorism).

Following this, in **August 2025**, the governance rules for **General-Purpose AI (GPAI)** models came into effect. This obligated providers of powerful foundation models (such as the successors to GPT-4 and Claude 3) to adhere to transparency requirements and, for those with systemic risks, to conduct adversarial testing and model evaluations.[3] By this date, Member States were also required to designate their national competent authorities (NCAs) to oversee enforcement.

However, the momentum began to falter as the timeline approached **February 2026**. This date was the deadline for the European Commission to provide crucial guidelines on the practical implementation of **Article 6**, which defines the classification rules for high-risk AI systems. As reported by the International Association of Privacy Professionals (IAPP), the Commission missed this deadline.[5] This failure has left operators of high-risk systems—ranging from medical devices to recruitment software—in a state of legal uncertainty. Without clear guidance on how to determine if their specific application counts as high-risk, companies cannot prepare the necessary technical documentation or conformity assessments required for the upcoming August 2026 deadline.

Table 1: The Fractured Implementation Timeline of the EU AI Act (Status: Feb 2026)

Milestone Date	Regulatory Provision	Current Status	Implications
August 2024	Entry into Force	**Completed**	The Act became binding EU law.
February 2025	**Prohibited Practices** (Art. 5)	**Enforced**	Bans on social scoring, biometric categorization, and manipulative AI are active.
August 2025	**GPAI Governance** (Ch. V)	**Partially Effective**	Governance rules apply, but technical standards for compliance are still in flux.
February 2026	**High-Risk Guidance** (Art. 6)	**MISSED**	The Commission failed to publish crucial classification guidelines, creating market confusion.[5]
August 2026	**High-Risk Obligations** (Annex III)	**Delayed / At Risk**	Originally the full application date. The "Digital Omnibus" proposes delaying this to late 2027.[6]
August 2027	**Product Safety Component** (Annex I)	**Pending**	Rules for AI embedded in regulated products (e.g., cars, machinery) remain scheduled for 2027/2028.

2.2 The "Digital Omnibus" Intervention

In response to these delays and the growing chorus of industry concern regarding preparedness, the European Commission unveiled a significant legislative intervention in **January 2026**: the **Digital Omnibus** package. This proposal represents a tacit admission that the original implementation schedule was overly ambitious relative to the bureaucratic capacity of the EU's standardization bodies.[6]

The centerpiece of the Digital Omnibus is the **"stop-the-clock" mechanism**. This provision conditions the application of high-risk AI obligations on the availability of harmonized technical standards. The European Committee for Standardization (CEN) and the European Electrotechnical Committee for Standardization (CENELEC) were originally tasked with producing these standards by Fall 2025 but failed to meet the deadline, with estimates now pushing their completion to the end of 2026.[5]

Under the "stop-the-clock" rule, the compliance deadline for high-risk systems listed in **Annex III** (biometrics, critical infrastructure, education, employment, etc.) is pushed back by a transition period of **six months** *after* the standards are officially confirmed. This effectively shifts the compliance deadline from August 2026 to potentially **December 2, 2027**.[6] For AI systems embedded in products covered by **Annex I** (machinery, toys, elevators), the transition is even longer, with a 12-month period pushing the deadline to **August 2028**.

This delay is framed by the Commission as a necessary measure to provide "legal certainty" and allow businesses "breathing room".[5] However, it also introduces a period of "legal limbo" where high-risk systems may be placed on the market without the safeguards originally envisioned by the legislators.

2.3 The Deregulatory Pivot and "Simplification"

The Digital Omnibus is not merely a scheduling adjustment; it is part of a broader "simplification" agenda championed by Commission President Ursula von der Leyen. This agenda aims to reduce administrative burdens on European businesses by an estimated **€5 billion** by 2029.[6]

The package proposes several substantive changes to the AI Act and related digital laws (like the GDPR) that critics argue amount to deregulation:

- **Voluntary Monitoring:** The obligation for mandatory post-market monitoring for certain AI providers has been softened, allowing them to rely on voluntary guidance rather than strict harmonized standards.[6]
- **SME Exemptions:** The Omnibus extends simplified compliance requirements to Small and Medium-sized Enterprises (SMEs) and even "Small Mid-Cap" companies (SMCs). This includes replacing mandatory AI literacy training with state-supported training programs, shifting the burden from the private sector to the public purse.[6]

- **Removal of Registration:** Providers of AI systems that self-assess as "not high-risk" (despite falling under high-risk categories in Annex III) are no longer required to register in the EU database, removing a key transparency mechanism.[7]

This pivot reflects a shift in the Commission's priorities from pure regulation to industrial competitiveness, driven by the fear that Europe is falling behind the United States and China in the AI sector.

---

3. The Ideological Battlefield: Arguments in Favor of the AI Act

Despite the implementation struggles, a robust coalition of civil society organizations, ethical AI researchers, and fundamental rights advocates continues to defend the AI Act. Their arguments center on the necessity of a rights-based framework to prevent the excesses of "surveillance capitalism" and authoritarian control.

3.1 Defending Fundamental Rights and Human Dignity

The core argument in favor of the AI Act is that it is the only global legislation that prioritizes **human dignity** over corporate profit or state efficiency. Proponents argue that without these rules, the deployment of AI would inevitably lead to a "race to the bottom" where privacy and non-discrimination are sacrificed for speed and scale.

- **Preventing the Panopticon:** The ban on real-time remote biometric identification in publicly accessible spaces is viewed as a civilizational firewall. Advocates like Amnesty International argue that without this prohibition, European cities would essentially become open-air prisons where every citizen's movement is tracked, logged, and analyzed, mirroring the surveillance state models seen in authoritarian regimes.[8] The Act ensures that anonymity in public spaces remains a right, not a privilege.
- **Protecting the Marginalized:** High-risk AI systems are disproportionately used to manage vulnerable populations—in welfare distribution, migration control, and policing. Civil society groups argue that these systems, often branded as "technical fixes" for structural problems, tend to amplify existing biases. By mandating strict accuracy, robustness, and cybersecurity requirements for these systems, the AI Act provides a mechanism for accountability that does not exist in the US or China.[8]
- **The Right to Explanation:** The Act enshrines transparency obligations that allow individuals to know when they are interacting with an AI (e.g., chatbots) and to receive explanations for automated decisions that affect their lives (e.g., loan denials or hiring decisions). This is seen as essential for preserving human agency in an increasingly automated world.[9]

3.2 The Strategic Value of the "Brussels Effect"

Supporters also argue that the AI Act is a strategic economic asset. By setting the first comprehensive rules, the EU aims to replicate the "Brussels Effect" seen with the GDPR, where multinational companies adopt EU standards globally to simplify their operations.

- **Trust as a Competitive Advantage:** The Commission posits that "Trustworthy AI" is a premium product. In a global market flooded with hallucinations, deepfakes, and biased algorithms, European AI—certified as safe, accurate, and rights-respecting—will command a higher value. This branding strategy aims to position Europe as the home of "responsible innovation".[6]
- **Legal Certainty:** Proponents argue that the alternative to the AI Act is not "no regulation," but a fragmented patchwork of 27 different national laws. By harmonizing the rules across the Single Market, the Act theoretically reduces barriers to cross-border trade, allowing a French AI startup to sell to a German hospital without navigating conflicting compliance regimes.[9]

3.3 Countering "Big Tech" Dominance

A significant strand of support for the Act comes from those who view it as a necessary check on the power of US-based technology giants. By imposing strict governance on "General-Purpose AI" models (mostly developed by US firms like OpenAI, Google, and Anthropic), the EU asserts its sovereignty and ensures that foreign entities cannot unilaterally dictate the terms of Europe’s digital infrastructure. The Act forces these companies to be transparent about their training data and to mitigate systemic risks, reasserting the primacy of democratic law over corporate terms of service.[10]

---

4. The Counter-Reformation: Arguments Against the AI Act

As 2026 progresses, the opposition to the AI Act has hardened. What began as industry grumbling has evolved into a full-throated critique from venture capitalists, tech executives, and increasingly, political leaders who fear Europe is committing economic suicide.

4.1 The Innovation Chill and "AI FOMO"

The most pervasive argument against the Act is that it imposes crushing compliance costs that stifle innovation and drive investment away from Europe. This critique has gained traction as the disparity between the booming AI sectors in the US and the stagnant European market becomes more evident.

- **The SME Burden:** While the Act claims to support SMEs, critics argue that the compliance reality is different. The cost of conformity assessments, establishing quality

management systems, and maintaining detailed technical documentation is estimated to be prohibitive for startups. A report by the Digital SME Alliance highlights that large incumbents can absorb these costs, but for a small European startup, they represent a "death by paperwork".[11]

- **Investment Flight:** There is a widespread perception that venture capital is fleeing Europe for jurisdictions with more "agile" regulations, such as the UK or the US. The uncertainty caused by the missed deadlines and the "Digital Omnibus" delays has only exacerbated this, as investors despise unpredictability. The "AI FOMO" narrative suggests that Europe has regulated the technology before it even managed to build it, effectively ceding the market to American and Chinese firms.[12]
- **The "Stop-the-Clock" Paradox:** Critics argue that the "stop-the-clock" mechanism in the Digital Omnibus is an admission of failure. By delaying enforcement because the regulators (CEN/CENELEC) could not keep up with the technology, the EU has created a "legal limbo" that punishes compliant companies while failing to stop bad actors.[7]

4.2 The "Digital Iron Curtain" Rhetoric

A more geopolitical strand of criticism characterizes the EU's regulatory framework (the AI Act combined with the Digital Services Act and GDPR) as a **"Digital Iron Curtain."** This rhetoric, often emanating from US Republicans and Silicon Valley libertarians, argues that Europe is isolating itself from the global internet.

- **Algorithmic Censorship:** Critics assert that the requirements to remove "disinformation" and "hate speech" under the DSA, backed by the AI Act's risk management rules, force platforms to implement aggressive, automated censorship filters. This is portrayed as an "authoritarian" control of information that mirrors the suppression of dissent in non-democratic regimes.[13]
- **The End of Encryption:** Proposals related to "Chat Control" (scanning encrypted messages for illegal content) are often conflated with the AI Act in this narrative. Critics argue that by mandating AI scanning of private communications, the EU is building a surveillance apparatus that creates a "backdoor" for state intrusion, effectively ending privacy in the name of protecting it.[13]
- **Technological Isolation:** The refusal of some US companies to launch their advanced models in the EU (e.g., Meta withholding multimodal models, Apple delaying Apple Intelligence features) is cited as evidence that the "Iron Curtain" is already descending. European consumers are denied access to the latest tools, creating a two-speed digital world where Europe is left behind.[10]

4.3 Regulatory Capture and Lobbying

Paradoxically, some critics from the left argue that the Act has been captured by the very companies it was meant to regulate. The intense lobbying by Big Tech (with spending reaching €151 million annually) has watered down the obligations for General-Purpose AI and introduced loopholes in the Digital Omnibus. These critics argue that the Act has become a

"compliance theater" that cements the dominance of incumbents while failing to protect citizens from the real harms of AI.[7]

---

5. Historical Parallel I: The Maltese Anomaly (1970s-1980s)

To contextualize the current debate over "digital sovereignty" and "protectionism," it is instructive to examine the technological policies of **Malta** during the 1970s and 1980s. Under the socialist administration of Prime Minister **Dom Mintoff**, Malta implemented a strict ban on the importation of personal computers. This policy serves as a potent case study in the unintended consequences of state attempts to centrally manage technological disruption.

5.1 The Political Economy of the Ban

Dom Mintoff's administration (1971-1984) was characterized by a philosophy of **autarky** (self-sufficiency) and non-alignment. Following Malta's independence and the closure of the British military base in 1979, the government faced the daunting task of transforming a fortress economy into a productive one. In this context, the personal computer was viewed not as a tool of liberation, but as a threat.

- **The "Job Protection" Rationale:** The official reasoning for the ban was the fear of **technological unemployment**. The government believed that widespread automation would lead to redundancies among the clerical and manual workforce, exacerbating the fragility of the post-colonial labor market.[15] This mirrored the "Luddite" anxiety that often accompanies technological shifts, but it was enshrined in state policy.
- **Import Substitution and Control:** The computer ban was part of a broader "bulk buying" and import substitution strategy. The government restricted imports of "luxury" goods (including color televisions and foreign chocolate) to protect foreign currency reserves and encourage local industry. Computers fell into the category of unnecessary foreign luxuries that drained national wealth.[17]

5.2 The Mechanics of Restriction: "Sole Agents" and Bureaucracy

The ban was enforced through a combination of strict import licensing and a **"sole agent"** system.

- **The Sole Agent Policy:** To prevent "wasteful competition," the government designated specific Maltese companies as the exclusive agents for particular technology brands. This created a non-competitive, oligopolistic market structure. A business could not simply order a computer; they had to go through the sanctioned agent, who in turn had to navigate "cumbersome paperwork" to justify the importation to the Department of Trade.[15]
- **Exclusion of Major Players:** The hostile regulatory environment led major international

players like **IBM** to refuse to operate directly in Malta. IBM strictly forbade its agents from selling equipment on the island, leaving the market to **ICL** (International Computers Limited), which was more willing to tolerate the government's conditions.[15]

5.3 The "Timesharing" Workaround: A Pre-Cloud Centralization

The restriction on personal hardware led to the emergence of a unique technological ecosystem based on **timesharing**. Since individual businesses (banks, hotels, parastatal entities) could not easily import their own computers, they purchased computing power from the few licensed providers like **Megabyte**, **Computime**, and **Panta Computers**.

- **Centralized Computing:** These service providers imported powerful mainframes and sold "time" on them to clients. Data processing was centralized in these hubs, with clients accessing the mainframes via dumb terminals or submitting batch jobs.
- **Unintended Innovation:** Ironically, this restriction forced Malta to adopt a model that prefigured modern **cloud computing**. While the rest of the West was moving toward decentralized personal computing (the PC revolution), Malta was building a centralized, service-based infrastructure born of scarcity.[15]

5.4 The Smuggling Economy and the "Desserta" Generation

The ban inevitably gave rise to a thriving black market. Just as Maltese citizens smuggled foreign chocolate (banned in favor of the local, waxy "Desserta" brand) and toothpaste from Sicily, they also smuggled technology.

- ** contraband Innovation:** The ZX Spectrum and Commodore 64 became prized contraband. Students and hobbyists would hide the devices in their luggage on flights from London or ferries from Catania. This created a generation of "bedroom coders" who learned to program in a clandestine environment, treating the computer as a subversive object.[17]
- **The End of the Ban:** The restrictions were eventually lifted in the late 1980s and early 1990s following the change in government. The removal of the "sole agent" regulation led to a collapse in prices and a flood of IBM-compatible clones, rapidly ending the era of timesharing dominance.[15]

---

6. Historical Parallel II: The Socialist Computer Dilemma

The Maltese experience was not unique; it was a microcosm of the broader **Eastern Bloc's** struggle with the information revolution during the 1980s. In the Soviet Union, Yugoslavia, and East Germany, the computer posed an existential dilemma: it was necessary for economic modernization but fatal for political control.

6.1 The Galaksija and the DIY Revolution in Yugoslavia

Socialist Yugoslavia faced severe economic constraints in the 1980s, leading to strict import restrictions. Citizens were banned from importing items worth more than 50 Deutschmarks, effectively outlawing all Western microcomputers (a Commodore 64 cost over 1,000 DM).[20]

- **The Galaksija Computer:** In response to this ban, inventor **Voja Antonić** designed the **Galaksija**, a build-it-yourself computer that used cheap, accessible components and a Z80 microprocessor. Antonić released the schematics in the magazine *Računari u vašoj kući* ("Computers in Your Home") in 1983.[21]
- **Radio Warez Distribution:** In a stunning example of decentralized innovation, the software for the Galaksija was distributed via **radio waves**. The radio show *Ventilator 202* would broadcast the screeching audio of the computer code. Listeners would record the broadcast onto cassette tapes, which they could then load into their homemade computers. This mechanism completely bypassed the state's physical import controls, creating a peer-to-peer software distribution network decades before the internet.[21]

6.2 The CoCom Embargo and Soviet Stagnation

While Yugoslavia had a vibrant DIY culture, the Soviet Union and its stricter satellites faced the **CoCom (Coordinating Committee for Multilateral Export Controls)** embargo. The US and its allies restricted the export of high-technology goods to the Eastern Bloc to maintain a military advantage.[22]

- **The Computer Arms Race:** The Soviet leadership, particularly the military, realized by the early 1980s that they were losing the "computer arms race." While the West was integrating computers into every facet of life and defense, the Soviets were relying on pirated IBM/360 designs (the Ryad series) which were often years behind.[23]
- **Information Control:** The regime's paranoia about information flow meant that even when computers were available, they were kept in guarded institutions. The concept of a *personal* computer was anathema to a state that registered typewriters. This control stifled the "hacker culture" that drove innovation in the West, leaving the Bloc with a "hardware-rich, software-poor" ecosystem that ultimately contributed to its economic collapse.[24]

---

7. Comparative Analysis: The Iron Curtain of Hardware vs. The Iron Curtain of Software

The juxtaposition of the 1980s hardware bans with the 2026 AI Act reveals a profound continuity in the logic of political control, even as the mechanisms have shifted from the physical to the regulatory.

7.1 Motivations: Protectionism then and Now

Table 2: Comparative Motivations for Technological Control

Era	1980s Malta / Eastern Bloc	2026 European Union
Primary Fear	**Unemployment & Instability.** Fear that automation would cause mass redundancy (Malta) or that information flow would undermine the regime (Bloc).	**Bias, Manipulation & Surveillance.** Fear that AI will undermine fundamental rights, democracy, and privacy (The "Human-Centric" defense).
Economic Logic	**Import Substitution.** Ban foreign goods to foster local industry (Desserta chocolate, local manufacturing).	**Regulatory Sovereignty.** Impose strict rules to force foreign tech to conform to EU values ("Brussels Effect") and foster "Trustworthy AI."
Official Rhetoric	"Protecting the Worker" / "Anti-Imperialism"	"Protecting the Citizen" / "Digital Sovereignty"

In both cases, the state frames the restriction as a protective measure against a chaotic external force. In the 1980s, Mintoff protected the Maltese worker from the "job-killing" computer; in 2026, the EU protects the European citizen from the "rights-violating" algorithm. However, critics argue that the *economic* effect is identical: insulation from the global technological frontier.

7.2 Mechanisms: From Customs Officers to Compliance Officers

The mechanism of control has evolved from physical borders to bureaucratic ones.

- **1980s (Hardware):** The control point was the **Customs Department**. Physical devices were seized, taxed, or banned. The "Sole Agent" was the gatekeeper.
- **2026 (Software):** The control point is the **Conformity Assessment**. Software is "seized" not at the border, but in the legal department. The "Notified Body" (the auditor) is the new Sole Agent. Just as IBM refused to deal with Mintoff's Malta, companies like Meta and Apple are refusing to release certain AI features in the EU due to regulatory friction.[10]

7.3 The "Workaround" Culture: Smuggling vs. VPNs

History demonstrates the futility of trying to strictly ban a desirable technology.

- **The Smugglers of 1984:** In Malta and Yugoslavia, the ban created a generation of smugglers. The desire for the Commodore 64 overrode the law. The distribution was decentralized (luggage, radio waves) and impossible to fully police.[17]
- **The VPN Users of 2026:** In the EU, the "Digital Iron Curtain" is being circumvented by **VPNs** and **open-source models**. If the EU bans a powerful US model for non-compliance, European developers simply access it via a VPN or download the weights of an open model (like Llama) to run locally, bypassing the safety filters and compliance checks. The "Digital Omnibus" delay is a recognition that the state cannot move fast enough to stop this flow.[7]

---

8. Conclusion

As of February 2026, the European Union stands on the precipice of a decision that will define its economic and social trajectory for decades. The **AI Act**, noble in its intent to preserve human dignity, threatens to replicate the stagnation of the 1980s protectionist regimes if its implementation continues to be marred by bureaucratic inertia and "stop-the-clock" delays.

The parallel with **Dom Mintoff's Malta** is stark. The Maltese government of the 1980s believed it could centrally manage the arrival of the computer to suit its own social and economic timeline. It failed. The result was not a protected workforce, but a lost decade of innovation, a thriving black market, and a painful game of catch-up in the 1990s.

Today, the "Digital Omnibus" represents a similar attempt to pause the clock. But technology does not pause. The risk for the EU is that while it perfects the regulations for "High-Risk AI," the rest of the world moves on to the next paradigm. The "Digital Iron Curtain" may be constructed of laws rather than barbed wire, but its capacity to isolate a population from the future remains just as potent. The lesson from the Galaksija and the Maltese smugglers is clear: the human desire to build, code, and innovate will eventually find a way around the state, no matter how high the wall is built.

Works cited

1. EU and Luxembourg Update on the European Harmonised Rules on Artificial Intelligence—Recent Developments - K&L Gates, accessed on February 10, 2026, https://www.klgates.com/EU-and-Luxembourg-Update-on-the-European-Harmonised-Rules-on-Artificial-IntelligenceRecent-Developments-1-20-2026
2. The First Requirements of the EU AI Act Come into Force in February 2025 | Littler, accessed on February 10, 2026, https://www.littler.com/news-analysis/asap/first-requirements-eu-ai-act-come-force-february-2025

3. Timeline for the Implementation of the EU AI Act | AI Act Service Desk, accessed on February 10, 2026, https://ai-act-service-desk.ec.europa.eu/en/ai-act/timeline/timeline-implementation-eu-ai-act
4. EU AI Act - Updates, Compliance, Training, accessed on February 10, 2026, https://www.artificial-intelligence-act.com/
5. European Commission misses deadline for AI Act guidance on high ..., accessed on February 10, 2026, https://iapp.org/news/a/european-commission-misses-deadline-for-ai-act-guidance-on-high-risk-systems
6. EU Unveils AI Omnibus: Sweeping Simplification of Digital Rules to ..., accessed on February 10, 2026, https://www.sgs.com/en-be/news/2026/01/eu-unveils-ai-omnibus-sweeping-simplification-of-digital-rules-to-boost-innovation-and-cut-costs
7. Article by article, how Big Tech shaped the EU's roll-back of digital ..., accessed on February 10, 2026, https://corporateeurope.org/en/2026/01/article-article-how-big-tech-shaped-eus-roll-back-digital-rights
8. EU: AI Act must ban dangerous, AI-powered technologies in historic law, accessed on February 10, 2026, https://www.amnesty.org/en/latest/news/2023/09/eu-ai-act-must-ban-dangerous-ai-powered-technologies-in-historic-law/
9. AI Act | Shaping Europe's digital future - European Union, accessed on February 10, 2026, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
10. The Geopolitics Of AI Regulation - The Yale Review Of International ..., accessed on February 10, 2026, https://yris.yira.org/global-issue/the-geopolitics-of-ai-regulation/
11. Why delaying AI Act enforcement is essential for European SMEs ..., accessed on February 10, 2026, https://www.digitalsme.eu/why-delaying-ai-act-enforcement-is-essential-for-european-smes/
12. European AI FOMO - Verfassungsblog, accessed on February 10, 2026, https://verfassungsblog.de/eu-digital-law-ai-fomo-omnibus/
13. Online Censorship and AI Mass Surveillance: How the EU Has ..., accessed on February 10, 2026, https://americarenewing.com/issues/online-censorship-and-ai-mass-surveillance-how-the-eu-has-captured-the-digital-era-and-why-america-must-challenge-it/
14. The digital iron curtain - North West Bylines, accessed on February 10, 2026, https://northwestbylines.co.uk/business/technology/the-digital-iron-curtain/
15. Computers in Malta (Business Industry) - Microcomputing Society, accessed on February 10, 2026, https://msmalta.org/computers-in-malta-business-industry/
16. How dose the older/younger generations view Dom Mintoff? How was he portrayed in school? Was he a great leader? Terrible leader? A good leader with

controversial aspects? How authoritarian would you say he was? : r/malta - Reddit, accessed on February 10, 2026, https://www.reddit.com/r/malta/comments/gtv910/how_dose_the_olderyounger_generations_view_dom/
17. Mintoff & The Chocolate Factory: Explaining Protectionism |... - Malta Daily, accessed on February 10, 2026, https://maltadaily.mt/articles/mintoff-the-chocolate-factory-explaining-protectionism-by-spunt-mt
18. The 1980s' bulk-buying system and public sector employment - The Malta Independent, accessed on February 10, 2026, https://www.independent.com.mt/articles/2024-07-07/local-news/The-1980s-bulk-buying-system-and-public-sector-employment-6736262535
19. Computers in 1980s Malta - Vassallo History - WordPress.com, accessed on February 10, 2026, https://vassallohistory.wordpress.com/computers-in-1980s-malta/
20. How one engineer beat restrictions on home computers in socialist Yugoslavia | Games, accessed on February 10, 2026, https://www.theguardian.com/games/2024/oct/24/how-one-engineer-beat-the-ban-on-home-computers-in-socialist-yugoslavia
21. The Lost History of Socialism's DIY Computer - Jacobin, accessed on February 10, 2026, https://jacobin.com/2020/08/computer-yugoslavia-galaksija-voja-antonic
22. An Overview of Export Controls on Transfer of Technology to the ..., accessed on February 10, 2026, https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1113&context=ncilj
23. Cold War Computer Arms Race - Marine Corps University, accessed on February 10, 2026, https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/MCU-Journal/JAMS-vol-14-no-2/Cold-War-Computer-Arms-Race/
24. PCs represented threat of potential revolution to Communists, recalls Czech IT expert, accessed on February 10, 2026, https://english.radio.cz/pcs-represented-threat-potential-revolution-communists-recalls-czech-it-expert-8616567
25. THE USSR CONFRONTS THE INFORMATION REVOLUTION - CIA, accessed on February 10, 2026, https://www.cia.gov/readingroom/docs/CIA-RDP89T00296R000200230004-9.pdf