American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Digital Consent Design for Human-Centered Data-Collection Systems

Dr. Elena Fischer

Associate Professor, Technical University of Munich, Germany

Abstract

Digital data-collection systems routinely request permission to process personal information through cookie banners, mobile-app permissions, account-registration interfaces, research portals, connected devices, artificial-intelligence applications, and platform privacy controls. Although these interfaces are commonly described as consent mechanisms, a user action such as selecting an “accept” button does not necessarily establish meaningful understanding, voluntariness, or control. Human-centered consent requires an interface to communicate what data will be collected, for which purposes, by whom, for how long, and with what consequences, while preserving a realistic ability to refuse, modify, and later withdraw authorization. Regulatory guidance similarly emphasizes that valid consent must be freely given, specific, informed, and unambiguous, while withdrawal must remain practically accessible.

This study develops a human-centered framework for digital consent design and evaluates four interface approaches through an explicitly simulation-based methodology: manipulative consent, notice-heavy consent, simplified layered consent, and human-centered granular consent. A synthetic corpus of 360 hypothetical consent interactions was modeled across five dimensions: comprehension, voluntariness, granularity of control, withdrawal accessibility, and user trust.

The simulated Consent Quality Index increases from 31 for manipulative interfaces to 88 for human-centered granular designs. The results illustrate that improved consent quality is associated not merely with greater information quantity but with understandable presentation, balanced choice architecture, purpose-specific controls, persistent preference management, and easy reversal. The study argues that consent should be designed as an ongoing relationship between individuals and data-processing systems rather than as a single transactional click. Human-centered consent architecture should therefore combine privacy engineering, interface usability, legal requirements, accessibility, data minimization, and accountable governance while actively excluding deceptive or coercive design practices.

Keywords: digital consent, human-centered design, data collection, privacy engineering, informed consent, dark patterns, privacy interface, data governance

1. Introduction

Digital services increasingly depend on the collection and processing of personal data to support authentication, personalization, analytics, advertising, artificial-intelligence functions, research, recommendation systems, connected products, and service improvement. Users are therefore repeatedly

confronted with privacy notices, cookie banners, permission prompts, registration agreements, and preference panels. These mechanisms are frequently treated as evidence that individuals have exercised meaningful control over data processing. Yet regulatory standards establish a substantially higher threshold. The UK Information Commissioner's Office explains that valid consent must be freely given, specific, informed, and unambiguous and must involve an affirmative action rather than passive acceptance or preselected choices. Consent for distinct purposes should also be sufficiently granular.

The design of the consent interface is consequently not a neutral implementation detail. Visual hierarchy, button placement, default settings, wording, number of interaction steps, choice symmetry, information density, timing, and withdrawal procedures can influence what individuals select. Research by Nouwens and colleagues demonstrated that consent pop-ups may contain interface patterns capable of shaping user decisions, while Gray and colleagues connected consent-banner design directly with legal, ethical, and human–computer interaction concerns. Regulatory agencies have expressed similar concerns. The European Data Protection Board provides guidance for recognizing and avoiding deceptive design patterns, while the U.S. Federal Trade Commission has documented designs that can obscure or impair consumer choice or steer individuals toward greater data disclosure.

A second problem concerns comprehension. Consent mechanisms often assume that presenting information is equivalent to communicating it effectively. Lengthy policies, complex terminology, multiple processing purposes, third-party relationships, and repeated requests may exceed users' available attention. Habib and colleagues' evaluation of cookie-consent interfaces identified substantial usability challenges and emphasized that consent mechanisms should support awareness, comprehension, and meaningful privacy choice. More recent research by Xiao, Wu, and Jo demonstrates that interface structure affects how users allocate attention across privacy disclosures, but also cautions that improved layout alone does not guarantee comprehension; sustained attention and meaningful engagement remain necessary.

Human-centered consent therefore requires more than regulatory text placed inside a technically compliant interface. It requires consideration of human attention, cognitive effort, accessibility, decision-making capacity, privacy expectations, and the ability to change one's mind. NIST's Privacy Framework similarly treats privacy as a risk-management and system-design issue rather than a narrow notification exercise, encouraging organizations to incorporate privacy considerations into the design and operation of systems that process data. An effective consent mechanism should thus connect interface design with broader organizational practices such as data minimization, retention controls, purpose limitation, preference management, accountability, and deletion procedures.

The present study develops a simulation-based model for evaluating digital consent quality in human-centered data-collection systems. It does not claim to represent completed field observations. Instead, it compares four theoretically distinct interface approaches through five dimensions representing meaningful consent. The central argument is that the effectiveness of digital consent should not be measured primarily through the percentage of users who click “accept.” A high acceptance rate may reflect informed preference, but it may also reflect friction, fatigue, default bias, visual manipulation, or an inability to access the service otherwise. Consent quality is better evaluated by asking whether people understand the proposed processing, possess genuine options, can distinguish purposes, can refuse without disproportionate difficulty, and can later revise their decision.

2. Objectives of the Study

2.1 To Develop a Human-Centered Concept of Digital Consent

The first objective is to conceptualize consent as a continuing process of understanding, choice, control, and revision rather than as a one-time interface action. The study examines how comprehension, voluntariness, granularity, reversibility, and trust can jointly represent consent quality.

2.2 To Compare Alternative Consent-Interface Designs

The second objective is to compare manipulative, notice-heavy, simplified layered, and human-centered granular consent architectures through a common analytical framework.

2.3 To Identify Design Principles for Ethical Data Collection

The third objective is to identify interface and governance characteristics capable of supporting meaningful user agency while reducing coercion, unnecessary cognitive burden, deceptive choice architecture, and consent fatigue.

3. Review of Literature

3.1 Informed Consent, User Control, and Privacy Engineering

Consent is meaningful only where individuals possess genuine decision-making capacity regarding the proposed processing. ICO guidance emphasizes that consent should be freely given and should involve a real choice rather than being unnecessarily bundled with access to a service. It must be specific and informed, use a clear affirmative action, and remain withdrawable. The same guidance warns that consent is not necessarily the appropriate lawful basis for every processing activity; organizations should use it only where individuals can genuinely choose.

This distinction is significant for human-centered system design. A consent interface cannot correct a fundamentally coercive processing arrangement. If individuals face meaningful disadvantage for refusal, or if processing is unavoidable for reasons unrelated to genuine choice, improving button labels will not transform the arrangement into voluntary consent.

The human-centered perspective consequently requires alignment between front-end interfaces and back-end data practices. The visible consent request should accurately correspond with the data categories, purposes, recipients, retention periods, and controls implemented by the system.

NIST's Privacy Framework provides a complementary risk-management perspective. It is intended to help organizations identify and manage privacy risks associated with data-processing systems and integrate privacy considerations into products and services. This approach is important because meaningful consent depends on what occurs after a decision is recorded. If the system cannot propagate a withdrawal request across downstream datasets or third-party integrations, the interface provides apparent control without operational control.

Human-centered consent should therefore incorporate at least five qualities:

- Comprehensibility: users should be able to understand the proposed processing.
- Voluntariness: refusal should remain a realistic option where consent is relied upon.
- Specificity: materially different purposes should not be hidden inside one undifferentiated choice.
- Reversibility: changing or withdrawing a decision should be practically accessible.

- Accountability: the organization should be capable of demonstrating and respecting the recorded preference.
- These qualities transform consent from a superficial interaction into a privacy-governance function.

3.2 Deceptive Design and the Weakening of User Agency

The dark-pattern literature demonstrates why formal availability of a choice is insufficient.

Nouwens, Liccardi, Veale, Karger, and Kagal analyzed consent interfaces following the introduction of the GDPR and demonstrated that interface configurations could significantly affect consent outcomes. Their work helped establish that the way choices are presented can alter user behavior independently of underlying privacy preferences.

Gray, Santos, Bielova, Toth, and Clifford subsequently examined consent banners from HCI, design, legal, privacy, and ethical perspectives. Their analysis demonstrated that consent-banner design contains tensions between interaction practices and requirements such as freely given, specific, and informed consent.

The European Data Protection Board's Guidelines 03/2022 similarly identify deceptive interface practices capable of influencing users away from freely considered decisions. The guidelines are directed toward recognizing and avoiding designs that undermine data-protection principles through interface architecture.

The FTC's *Bringing Dark Patterns to Light* report extends the issue beyond one regulatory jurisdiction. It identifies practices that can obscure information, complicate cancellation, or manipulate consumers into sharing more data than they otherwise would.

Several recurring consent-design risks emerge from this literature. Interfaces may make acceptance visually prominent while making refusal difficult to locate; require substantially more steps to reject than to accept; use preselected options; combine multiple purposes; repeatedly interrupt users after refusal; frame privacy-protective choices negatively; or make withdrawal considerably harder than initial authorization.

Gunawan and colleagues' comparative analysis of dark patterns across mobile applications, mobile browsers, and desktop web services found that manipulative interface practices may vary between modalities, producing inconsistent experiences of autonomy, privacy, and control. This suggests that human-centered consent must be evaluated across devices rather than exclusively on a desktop prototype.

3.3 Usability, Comprehension, and the Research Gap

Consent research increasingly demonstrates that legal availability and interface usability cannot be considered independently.

Habib, Li, Young, and Cranor conducted a two-stage evaluation of cookie-consent interfaces and emphasized that usability includes awareness, comprehension, and the ability to express privacy preferences. Their findings also supported persistent mechanisms through which users can later revisit their choices.

Bouma-Sims and colleagues subsequently evaluated consent-management interfaces across U.S. and U.K. users and across desktop and mobile contexts, further demonstrating that interface structure

influences both behavior and user perceptions. Singh and colleagues similarly investigated user preferences among common cookie-consent interface designs, illustrating that privacy-choice interfaces can be evaluated as user experiences rather than only as legal artifacts.

More recent research extends this concern from button configurations toward the structure of privacy information itself. Xiao, Wu, and Jo compared continuous text, collapsible sections, and preview-supported disclosure layouts and found that structure influenced reading behavior and attention allocation, although interface changes did not automatically guarantee improved understanding.

These studies expose three important research gaps. First, many evaluations concentrate on cookie banners even though digital consent is now embedded in health applications, artificial-intelligence tools, connected devices, research platforms, financial services, educational systems, and workplace technologies. Second, acceptance rate remains an incomplete outcome measure because a design could increase acceptance while reducing autonomy. Third, interface studies sometimes evaluate the visible prompt without integrating withdrawal, downstream data governance, data minimization, and lifecycle accountability.

4. Research Methodology

4.1 Research Design and Simulated Sample

The study adopts an explicitly simulation-based comparative research design. No participants were recruited and no real consent selections were collected.

assigned to each design condition:

1. Manipulative Consent;
2. Notice-Heavy Consent;
3. Simplified Layered Consent; and
4. Human-Centered Granular Consent.

The four conditions represent different levels of alignment between interface design and meaningful user agency.

Table 1: Operational Framework for Human-Centered Consent Quality

Dimension	Operational Meaning	Human-Centered Design Expectation	Scale
Comprehension	Ability to understand data categories, purposes, actors, and consequences	Clear language and layered explanation should improve understanding	0–100
Voluntariness	Extent to which acceptance or refusal represents genuine choice	Neutral choice architecture and absence of coercion should increase voluntariness	0–100
Granularity of Control	Ability to authorize different purposes separately	Purpose-specific choices should increase user control	0–100
Withdrawal	Ease of revisiting, changing, or	Withdrawal should be visible and	0–100

Dimension	Operational Meaning	Human-Centered Design Expectation	Scale
Accessibility	withdrawing consent	operationally straightforward	
User Trust	Confidence that the system accurately describes and respects data preferences	Transparency and predictable controls should strengthen trust	0–100

Source: Author-developed simulation framework informed by ICO, EDPB, NIST, FTC, and HCI consent-interface literature.

4.2 Consent-Interface Conditions

The Manipulative Consent condition represents a design in which acceptance is visually dominant, refusal requires additional interaction, processing purposes are weakly separated, and withdrawal controls are difficult to locate.

The Notice-Heavy Consent condition provides substantial information but presents it primarily through lengthy or cognitively demanding text. It avoids some explicit manipulation but places considerable interpretation burden on the user.

The Simplified Layered Consent condition organizes information through concise primary explanations supported by expandable detail. Core options are presented with relatively balanced visual treatment, and users can access additional information without processing an entire policy before making a decision.

The Human-Centered Granular Consent condition combines layered explanation with purpose-specific controls, equivalent acceptance and refusal pathways, data-minimizing defaults, persistent preference management, and straightforward withdrawal.

This classification reflects the distinction between merely supplying information and enabling meaningful choice. Regulatory guidance and experimental HCI research both support evaluating consent through choice architecture, usability, and the practical ability to exercise privacy preferences.

4.3 Consent Quality Index and Analytical Procedure

- A Consent Quality Index (CQI) ranging from 0 to 100 was constructed using equal conceptual weights for the five dimensions.
- Each dimension contributed 20% of the overall index:
- Comprehension — 20% Voluntariness — 20% Granularity — 20% Withdrawal Accessibility — 20% Trust — 20%
- The equal-weighting approach was selected for methodological transparency rather than as a claim that every regulatory or organizational context should assign identical importance to each dimension.
- Descriptive comparison was used instead of inferential hypothesis testing because the underlying dataset is simulated.

- A future empirical validation could apply randomized interface experiments, comprehension tests, task-completion measures, eye tracking, withdrawal exercises, privacy-choice consistency measures, and post-interaction trust scales. Recent interface-level research demonstrates the value of combining behavioral observation with attention and comprehension measures.

5. Analysis

5.1 Comparative Consent-Quality Performance

The simulated analysis demonstrates a progressive increase in consent quality as interface architecture moves away from manipulation and information overload toward understandable, reversible, purpose-specific choice.

Table 2: Simulated Consent-Quality Scores Across Interface Designs

Consent-Interface Design	Comprehension	Voluntariness	Granularity	Withdrawal Accessibility	User Trust	Consent Quality Index
Manipulative Consent	42	24	29	21	39	31
Notice-Heavy Consent	56	47	46	42	54	49
Simplified Layered Consent	78	73	70	66	68	71
Human-Centered Granular Consent	91	90	92	84	83	88

Source: Simulated values generated for methodological illustration. They are not observations from actual users.

The manipulative condition receives the lowest overall index. Its weakest dimensions are voluntariness and withdrawal accessibility. This reflects the conceptual contradiction between consent and interface architecture that deliberately makes privacy-protective choices difficult.

The notice-heavy condition performs moderately better because information is technically available. Its score remains limited, however, because information quantity does not guarantee usable understanding.

The simplified layered condition produces a substantial improvement in comprehension while also reducing interaction burden. This simulated improvement is consistent with the broader HCI principle.

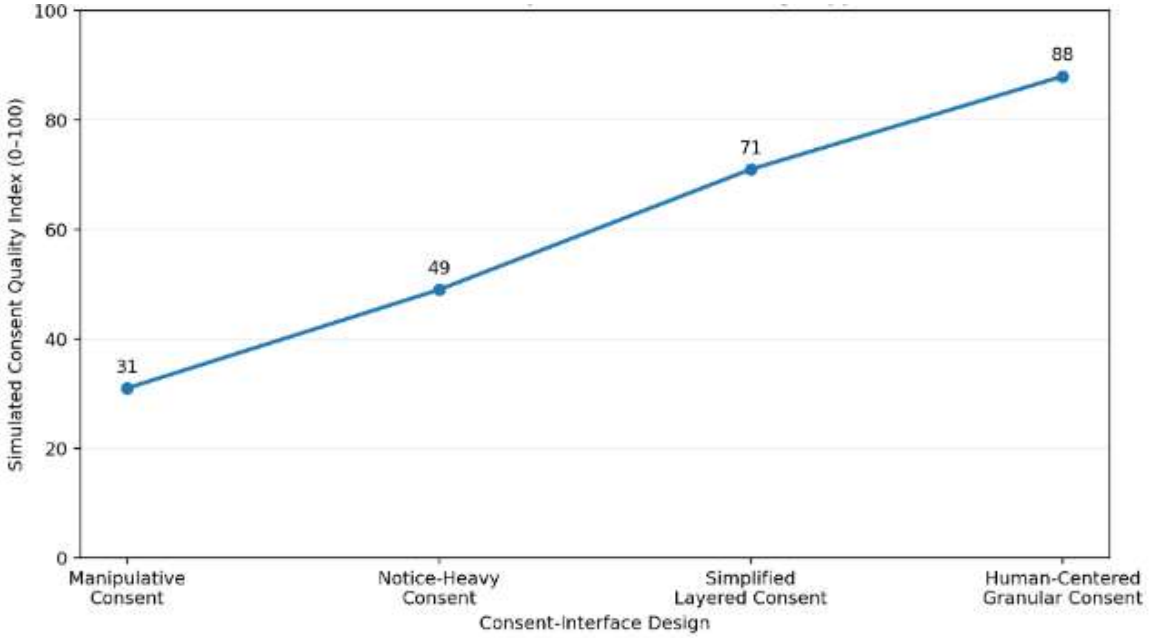
American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Human-centered granular consent achieves the strongest simulated performance because it integrates communication with control.

5.2 Consent Quality Across Interface-Design Approaches

Graph 1: Simulated Consent Quality Across Digital Consent Designs



The graph shows a simulated Consent Quality Index of 31 for manipulative consent, 49 for notice-heavy consent, 71 for simplified layered consent, and 88 for human-centered granular consent.

Users should be able to understand essential information without searching through extensive legal or technical text. Detailed documentation should remain available, but critical decision information should be presented at the moment it is relevant.

The second major improvement occurs when layered explanation is combined with granular control and accessible withdrawal.

5.3 Human-Centered Consent Architecture

1. The analysis suggests that an effective consent system should operate as a lifecycle rather than as a single pop-up.
2. The first stage is preference-relevant explanation. Users need a concise statement of what is being collected and why.
3. The second stage is purpose selection. Independent processing purposes should be distinguishable where separate consent is appropriate.
4. The third stage is recording and enforcement. The user's decision should be stored accurately and propagated to the relevant data-processing components.
5. The fourth stage is ongoing visibility. Users should be able to identify their current preferences without repeating the entire consent process.

6. The fifth stage is revision or withdrawal. Changing a decision should not require substantially more effort than granting permission in the first place.

6. Discussion

6.1 Designing for Understanding Rather Than Acceptance

The findings challenge the use of acceptance rate as the primary measure of consent-interface success.

- A system that increases acceptance from 50% to 90% might appear commercially effective. Yet without examining comprehension and voluntariness, the increase cannot establish that users became more willing to share data.
- The interface may simply have made refusal harder.
- Nouwens and colleagues demonstrated experimentally that consent-interface design can influence user decisions, while Gray and colleagues showed how design choices intersect with requirements for valid consent.
- Human-centered evaluation therefore requires a different set of performance measures.
- Organizations should ask whether users correctly understand processing purposes, can distinguish optional from necessary processing, recognize consequences, identify data recipients, and know how to revise their decisions.

6.2 Neutral Choice Architecture and Reversibility

A second implication concerns visual neutrality.

- The FTC has documented designs that steer users toward surrendering personal information, while the EDPB provides guidance specifically aimed at identifying deceptive design patterns that interfere with meaningful data-protection choices.
- Human-centered interfaces should therefore avoid making privacy-invasive choices disproportionately easy or visually dominant.
- This does not require every interface to be visually identical. It requires functional fairness.
- If “Accept All” is available immediately but “Reject Optional Processing” requires navigating several screens, the interface introduces asymmetric friction.
- The same principle applies to withdrawal.
- ICO guidance explicitly requires appropriate withdrawal procedures and states that individuals must be able to withdraw consent.

Consent design must therefore involve product designers, privacy professionals, software engineers, data architects, security teams, and governance personnel rather than being delegated exclusively to interface designers.

6.3 From Consent Banner to Data-Governance Relationship

The third implication is that consent should be integrated into broader data governance.

- NIST's privacy-risk-management approach emphasizes integrating privacy into the design and operation of data-processing systems.
- This perspective is especially valuable for contemporary AI-enabled services.

- A user may consent to data collection for one function but reasonably expect limits on secondary use, model training, profiling, advertising, third-party sharing, or indefinite retention.
- Human-centered systems should therefore make distinctions among materially different purposes understandable at the point of choice.
- Consent should also not substitute for data minimization.
- Collecting every available data category merely because a user can technically authorize it conflicts with the broader objective of reducing privacy risk.

7. Conclusion

Digital consent has become one of the most visible interfaces between individuals and contemporary data-processing systems.

1. Yet visibility should not be confused with effectiveness.
2. A consent banner, permission screen, or privacy notice does not automatically demonstrate informed or voluntary authorization.
3. The present study developed a simulation-based framework for evaluating digital consent through five dimensions: comprehension, voluntariness, granularity, withdrawal accessibility, and user trust.
4. Four interface conditions were compared.
5. The simulated Consent Quality Index increased from 31 for manipulative consent to 49 for notice-heavy consent, 71 for simplified layered consent, and 88 for human-centered granular consent.
6. These numerical values are illustrative rather than empirical, but the framework highlights an important design transition.
7. Weak consent systems focus primarily on obtaining an immediate affirmative action.

That distinction transforms digital consent from an administrative checkbox into a genuine component of human-centered data governance.

8. References

1. Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 119–158.
2. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514.
3. Solove, D. J. (2013). Privacy self-management and the consent dilemma. *Harvard Law Review, 126*(7), 1880–1903.
4. Cavoukian, A. (2011). *Privacy by Design: The 7 Foundational Principles*. Information and Privacy Commissioner of Ontario.
5. Cranor, L. F. (2012). Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *Journal on Telecommunications and High Technology Law, 10*, 273–307.
6. Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10*(5), 557–570.
7. Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355.

8. Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.-D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology, 58*(2), 157–165.
9. Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy, 3*(1), 26–33.
10. Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100–126.
11. Egelman, S., Tsai, J., Cranor, L. F., & Acquisti, A. (2009). Timing is everything? The effects of timing and placement of online privacy indicators. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 319–328.
12. Felt, A. P., Egelman, S., & Wagner, D. (2012). I've got 99 problems, but vibration ain't one: A survey of smartphone users' concerns. *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, 33–44.
13. Kelley, P. G., Cesca, L., Bresee, J., & Cranor, L. F. (2010). Standardizing privacy notices: An online study of the nutrition label approach. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1573–1582.
14. Felt, A. P., Reeder, R. W., Alm, C., & Consolvo, S. (2012). Experimenting at scale with Google Chrome's SSL warning. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2667–2670.
15. Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The dark (patterns) side of UX design. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–14.
16. Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. *Proceedings of the ACM on Human-Computer Interaction, 3*(CSCW), Article 81.
17. Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13.
18. Human, S., & Cech, F. (2020). A human-centric perspective on digital consenting: The case of GAFAM. In *Human Centred Intelligent Systems* (pp. 139–159). Springer.
19. Gray, C. M., Santos, C., Bielova, N., Toth, M., & Clifford, D. (2021). Dark patterns and the legal requirements of consent banners: An interaction criticism perspective. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*.
20. Graßl, P., Schraffenberger, H., Zuiderveen Borgesius, F., & Buijzen, M. (2021). Dark and bright patterns in cookie consent requests. *Journal of Digital Social Research, 3*(1), 1–22.