BİLGİ DÜNYASI
INFORMATION WORLD

Information World • 2026 • Volume 27 • Article 899 • 1-23
DOI: 10.15612/BD.2026.899

RESEARCH ARTICLE

Sensitivity review of public records: A thematic qualitative inquiry

Kamu belgelerinin hassasiyet değerlendirmesi: Tematik bir nitel inceleme

Hasan Öztürk[1], Fatih Rukancı[2]

[1]Bartın University, Bartın, Türkiye
[2]Ankara University, Ankara, Türkiye

Abstract

Sensitive information in public records is critically important for public security and individual privacy. For this reason, it is essential to examine in a comprehensive manner how records containing sensitive information are managed and appraised during their transfer to national archival institutions in accordance with records management and archival science principles. Research that approaches the sensitivity review process from a holistic perspective remains limited. This study aims to address this gap by examining the management and appraisal practices applied during the transfer of public records containing sensitive information to national archives. Within a qualitative research design, the views of archival specialists were collected through semi-structured interviews. Data were obtained from eight archival specialists, six from Türkiye and two from the United Kingdom, a leading country in the field of archives and records management. The findings reveal a comprehensive thematic structure consisting of five themes, eighteen categories and 101 codes. This structure demonstrates the challenges encountered in the sensitivity review process, the professional and technological approaches developed to address these challenges and the influence of institutional mechanisms on the process. Archival specialists insights provide new perspectives on the issues inherent in sensitivity review. The study concludes that sensitivity review is a context-dependent, multidimensional and ethically grounded area of professional practice that requires a systematic approach within archival agencies. It also offers original methodological and technological contributions to the literature by presenting Archival specialists evaluations on how AI-assisted review tools may transform sensitivity review processes.

Keywords: Privacy, sensitivity review, public records, archival appraisal, archival specialists' perspectives.

Öz

Kamu belgelerinde yer alan hassas bilgiler kamu güvenliği ve bireysel mahremiyet açısından kritik önem taşımaktadır. Bu nedenle hassas bilgi içeren belgelerin ulusal arşiv kurumlarına devir/transfer sürecinde belge yönetimi ve arşiv bilimi ilkeleri doğrultusunda nasıl yönetileceğinin ve değerlendirileceğinin kapsamlı biçimde incelenmesi gerekmektedir. Hassasiyet değerlendirmesi sürecini bütüncül bir yaklaşımla ele alan araştırmalar sınırlıdır. Bu çalışma söz konusu boşluğu karşılamak amacıyla hassas bilgi içeren kamu belgelerinin ulusal arşivlere devir sürecinde uygulanan yönetim ve değerlendirme pratiklerini incelemektedir. Çalışmada nitel

Cite as: Öztürk, H., & Rukancı, F. (2026). Sensitivity review of public records: A thematic qualitative inquiry. *Information World*, *27*, Article 899. https://doi.org/10.15612/BD.2026.899

Corresponding author: Hasan Öztürk • **Email:** hasanozturk258@gmail.com
Received: November 29, 2025 **Accepted:** September 12, 2026 **Published:** December 10, 2026

This study was derived from the PhD thesis of Hasan Öztürk, titled "Appraisal of public records containing sensitive information", conducted under the supervision of Fatih Rukancı at Ankara University, Institute of Social Sciences, in 2025.

Copyright © 2026 The Author(s). Published by University and Research Librarians Association. This is an open access article distributed under the Creative Commons Attribution License (CC BY), which permits unrestricted use, distribution, and reproduction in any medium or format, provided the original work is properly cited.

araştırma yöntemi kapsamında yarı yapılandırılmış görüşme tekniği ile arşiv uzmanlarının görüşlerine başvurulmuştur. Veriler, altısı Türkiye'den ikisi arşivcilik ve belge yönetimi alanında öncü bir ülke olan Birleşik Krallık'tan olmak üzere sekiz uzmandan toplanmıştır. Bulgular 5 tema 18 kategori ve 101 koddan oluşan kapsamlı bir tematik yapı sunmaktadır. Ortaya çıkan bu yapı hassasiyet değerlendirmesi sürecinde karşılaşılan zorlukları bunlara yönelik geliştirilen mesleki ve teknolojik yaklaşımları ve kurumsal yapıların süreç üzerindeki etkilerini ayrıntılı biçimde göstermektedir. Uzman görüşleri hassasiyet değerlendirmesi sürecindeki sorunlara yönelik yeni perspektifler sağlamaktadır. Ayrıca yapay zekâ destekli inceleme araçlarının hassasiyet değerlendirme süreçlerini nasıl dönüştürebileceğine ilişkin görüşler sunarak literatüre hem yöntemsel hem de teknolojik açıdan özgün bir katkı sunmaktadır.

Anahtar Kelimeler: Gizlilik, hassasiyet değerlendirmesi, kamu belgeleri, arşivsel değerlendirme, uzman görüşü.

Introduction

Archival appraisal constitutes one of the foundational functions of records management, encompassing the systematic evaluation of records according to their evidential and informational value. Among records subject to this process, those containing sensitive information occupy a critical position, as flawed appraisal decisions may produce consequences that are difficult to remedy. Sensitivity review has therefore emerged as a distinct component of appraisal, concerned with identifying and managing potential risks that certain records carry. Archives bear a fundamental responsibility to respect the privacy of those who create records or are represented in them, and the long-term preservation of public records aims to minimise adverse impacts on individuals and institutions. Without appropriate safeguards, disclosing sensitive information risks infringing upon individual and institutional rights, making careful appraisal a core archival function aimed at sustaining a balance between confidentiality, information security and the public interest (Association of Canadian Archivists, 2017).

Certain categories of information within public records carry a higher degree of sensitivity and, if disclosed, may result in greater harm, and are therefore governed by more stringent regulatory frameworks (Etzioni, 2014, p. 1277). Within data protection legislation, the concept of sensitive information is expressed through varying terminologies, all emphasising that particular data categories require stricter safeguards during processing (Al-Fedaghi, 2007, p. 165). However, there is no universally agreed understanding of what constitutes sensitive information. Data concerning trade union membership, for instance, may be regarded in some jurisdictions as a privacy risk, whereas in others it is sensitive only when associated with political or national security contexts. This variation demonstrates that sensitivity is inherently contextual, shaped by cultural norms, legal frameworks and professional practices.

Archival agencies must maintain a balance between protecting individual privacy and ensuring public access to information, in accordance with data protection legislation, intellectual property rights and confidentiality provisions. One of the most critical stages of records appraisal is sensitivity review, which constitutes an integral component of the risk-based approach (Sloyan, 2016, p. 31; McDonald, 2019, p. 52; Öztürk, 2024, p. 99). The appraisal process generally involves determining the archival value of records and, based on that assessment, deciding whether they should be retained, transferred, or disposed of (Rukancı et al., 2023, p. 42). Appraisal is traditionally defined as the primary professional responsibility involving the systematic review of records by a qualified appraiser (Cook, 2011, p. 174; Cox & Samuels, 1988, p. 29). This requires appraisers to promote the use of records while maintaining awareness of privacy and confidentiality requirements.

In the digital age, the exponential growth of data has made sensitivity review increasingly complex, both technically and ethically. Many national archival agencies have begun developing technology-assisted methods, including natural language processing, machine learning and text mining, to identify and classify sensitive information. Organisations such as The National Archives (UK) and The National Archives and Records Administration (NARA) have undertaken pilot projects in this evolving area (Marciano et al., 2018; National Archives and Records Administration, 2025; The National Archives, 2016; The National Archives, 2021; TOMES Project, n.d.). However, these tools cannot fully replace the contextual and ethical judgement required for sensitivity-related decision-making, and review is now often conducted through hybrid models combining human expertise with AI-assisted techniques.

This study extends beyond a single national context. The selection of Türkiye and the United Kingdom (UK) reflects a purposive rationale grounded in institutional contrast. The UK represents a mature archival system with extensively documented institutional practice, while Türkiye represents a developing archival tradition navigating its own regulatory transformation. Within the UK, The National Archives (TNA) served as the primary institutional reference point, given its systematic body of guidance in sensitivity review. Although countries such as the United States and France also possess well-established records management traditions, the UK was selected because TNA has produced the most comprehensive publicly accessible guidance specifically addressing sensitivity review. This provided a concrete reference framework against which the Turkish context could be examined. The two countries operate within distinct legislative environments. The UK functions within the framework of the Freedom of Information Act 2000, the UK GDPR and the Public Records Act 1958, while Türkiye operates under the Personal Data Protection Law (No. 6698, 2016), the Law on the Right to Information (No. 4982, 2003) and the Regulation on State Archival Services. Drawing on archival specialists' perspectives from both contexts, the study examines how professionals interpret legal frameworks and ethical principles, investigates the influence of record formats alongside emerging technologies, and considers the guiding role of advisory councils and professional guidelines within national archival systems.

Research Aim and Questions

The identification, processing and management of sensitive information in public records transferred to national archives is a complex undertaking. This study aims to examine how sensitivity review is conceptualised and practised during the transfer of such records, with particular attention to key issues emphasised or overlooked across different institutional contexts. Accordingly, the study addresses the following research questions:

- RQ1: How should the scope of sensitive information in public records be defined, how should such information be identified, and under what conditions should it be processed?
- RQ2: How should sensitivity review of public records be conducted, and does this process differ between physical/paper and digital media?
- RQ3: What challenges arise during the sensitivity review process, and how can these challenges be addressed?
- RQ4: What constitutes digital sensitivity review, and what are the functions of digital tools or software within this process? Should such tools be integrated into sensitivity review practices?
- RQ5: What should be the role and character of advisory/confidentiality councils and their institutional guidelines within the sensitivity review process?

The research questions were formulated to examine sensitivity review as a holistic professional practice rather than to compare national systems. The inclusion of participants from Türkiye and the UK was intended to capture diverse archival specialists' perspectives on the same phenomenon within different institutional settings, not to establish a cross-national comparative framework.

Literature Review

A wide range of studies has examined the multifaceted nature of sensitivity review. Evolving interpretations of what constitutes sensitive personal data and the absence of a universal consensus on its definition have been identified as key factors hindering the establishment of a coherent conceptual framework (Sillitoe, 1998, p. 12). The growing volume of information has accelerated research aimed at identifying sensitive elements within the content of records.

Studies on the identification of sensitive information (Sánchez et al., 2012; Whyte & Walsh, 2024) have increasingly shifted towards technology-assisted review approaches, encouraging engagement from technology-oriented disciplines. Digital analysis tools such as Bulk Extractor, Forensic Toolkit and EnCase Forensic have become widespread within appraisal processes. Recent research has centred on the use of AI and machine learning to automatically detect sensitive information

within the expanding volume of digital data (Berardi et al., 2015; Jaillant, 2022; Marciano et al., 2018; McDonald et al., 2014; McDonald et al., 2015; McDonald et al., 2018b; McDonald et al., 2019; McDonald et al., 2020; McKechnie & McDonald, 2024; Moss & Gollins, 2017; Narvala, 2024; Narvala et al., 2022a; Narvala et al., 2022b; Sánchez et al., 2012; The National Archives, 2016). These studies report high accuracy rates for the tools developed (McDonald et al., 2018b; McDonald, 2019; McDonald et al., 2020; Narvala et al., 2022b), although it remains difficult to demonstrate direct comparability between machine-based analyses and human performance, with error rates varying according to the evaluator's experience, perspective and institutional setting.

Algorithms, similar to human learning processes, can inherit societal biases and discriminatory patterns related to race, ethnicity, gender, nationality, income, sexual orientation, ability and political or religious belief (Jaillant & Rees, 2023; Wadsworth et al., 2018). These shortcomings are compounded by a further recognised limitation. Context-driven sensitivities are widely held to persist regardless of technological advancement (McDonald et al., 2015).

Alongside these technology-assisted approaches, several studies on sensitivity review (Johns, n.d.; Sloyan, 2016) have focused on the differences between paper-based and digital appraisal processes, particularly in response to the increasing volume of digitally created records. These studies have contributed to the development of approaches that identify both commonalities and distinctions between the two modes of appraisal.

The increasing volume of digital records and related information requests further complicates sensitivity review management (Branting et al., 2023). In 2022, over 928,000 FOIA requests were submitted in the United States, and processing delays led to lawsuits resulting in financial losses of 39 million dollars, significantly increasing interest in digital sensitivity review tools (US Department of Justice, 2023).

These developments in technology, digital records and information access provide a broader context for examining sensitivity review within national archival systems. The national contexts examined in this study, Türkiye and the UK, operate within distinct yet comparably complex frameworks governing sensitive information. In the UK, the Freedom of Information Act 2000 establishes public access rights to information held by public authorities while providing approximately twenty-five exemption grounds, including national security, defence, international relations, personal privacy and commercial confidentiality (McDonald, 2019; Moss & Gollins, 2017). The UK General Data Protection Regulation defines special categories of sensitive personal data with strict processing conditions, while the Public Records Act 1958 governs the statutory transfer of public records to TNA. TNA has operationalised this framework through a two-stage sensitivity review model, "think and find" followed by "check and do", in which records are first assessed against legislative grounds for closure or open transfer before final decisions are made in consultation with the Advisory Council (The National Archives, 2024). This institutionally embedded and systematically documented approach positions the United Kingdom as one of the most developed national contexts for sensitivity review practice.

In Türkiye, sensitive information is governed through a multi-layered but fragmented regulatory environment. Unlike the United Kingdom, Türkiye lacks a standalone archival law. Sensitivity-related practices are regulated through presidential decrees, regulations, standards and related legislation. The Personal Data Protection Law (No. 6698, 2016), broadly aligned with the European GDPR, defines special categories of sensitive personal data, including racial or ethnic origin, political opinion, religious belief, trade union membership, health data and biometric and genetic data, with strict processing conditions. The Law on the Right to Information (No. 4982, 2003) regulates public access, while the Regulation on State Archival Services (2019) governs the appraisal, retention and transfer of public records to the Presidency of State Archives (PSA). Confidentiality is assigned through three national classification levels, top secret, secret and for official use only, with "for official use only" being most directly associated with sensitive information in institutional workflows (Regulation on Classified Records, 2022). Declassification decisions are made by institutional appraisal commissions prior to transfer and by the Archive Records Confidentiality Appraisal Commission within PSA after transfer. However, Türkiye currently lacks dedicated guidance documents specifically addressing sensitivity review as a structured professional practice. Cengiz-Mater and Özdemir-Şahin (2026) found in a survey of 120 Turkish public bodies that 70.8% had not commenced sensitivity review of digital records and none used specialised software, underscoring that while legal foundations exist, their consistent translation into institutional practice remains underdeveloped.

Despite these structural differences, both countries share a common challenge. Existing legislative frameworks tend to define sensitive information through fixed categorical lists that struggle to accommodate the contextual, evolving and mosaic-like nature of sensitivity encountered in practice. This shared limitation provides an important context for interpreting the specialists perspectives gathered in this study.

Against this background, existing studies generally examine these challenges in a fragmented manner, focusing on isolated components. As a result, the field lacks an integrated understanding of how legal, organisational, contextual and technological factors interact within sensitivity review practices. This study contributes to addressing this gap by bringing together specialists insights from different institutional settings and examining these factors in relation to one another.

Methodology and Data Collection

This study adopted a qualitative research approach (Yıldırım & Şimşek, 2021, p. 37) and employed an explanatory embedded single-case study design (Yin, 1994, pp. 41–44). In this design, sensitivity review practice constitutes the single case, while Türkiye and the UK provide two distinct contextual settings for examining the phenomenon. Thus, the study does not treat Türkiye and the UK as separate cases but examines sensitivity review practice across these two contexts (Berg & Lune, 2019, p. 333).

The draft questions were reviewed by three academic experts for clarity, relevance and conceptual alignment. A pilot interview was conducted with a qualitative research specialist on 24 July 2024, and the feedback obtained was used to refine certain questions for greater clarity and conceptual coherence. Ethical approval was granted by the Ethics Committee of Ankara University on 5 July 2024, under Decision No. 16/187. A considerable number declined participation, reflecting the restricted nature of the subject matter and the access challenges inherent in sensitivity review research. The final study group comprised eight archival specialists, six from Türkiye and two from the UK, drawn from national archives, universities, ministries, press institutions and libraries. Maximum variation sampling was employed to ensure participant diversity (Creswell, 2013, p. 298). Case study research is not sampling research, and the typical criteria regarding sample size remain less relevant since the unit of inference is the case rather than the participant (Stake, 1995, pp. 4-6; Yin, 1994, p. 50). Sample adequacy was instead assessed through analytical saturation. From the sixth interview onward, no new codes emerged within the core categories, and across the final two interviews the coding framework of 5 themes, 18 categories and 101 codes remained structurally stable, indicating that thematic saturation had been reached in this homogeneous expert sample (Guest et al., 2006, p. 78). The depth of individual interviews, averaging sixty-seven minutes, further enhanced data richness, in line with the view that adequacy in qualitative research depends on depth rather than numerical size alone (Morse, 2000, pp. 4-5). The inclusion of eight archival specialists reflects the focused scope of the case and the institutional diversity attainable within the access conditions of sensitive-topic research, supporting an in-depth analytical engagement with each participant's account.

The interviews were conducted between 8 August and 19 October 2024, with an average duration of approximately sixty-seven minutes. Recordings were transcribed using Transgate (transgate.ai), an AI-assisted transcription tool. Audio files were permanently deleted following transcription, and all transcripts were manually verified before being imported into MAXQDA Analytics Pro (v.24.6.0).

Thematic content analysis (Braun & Clarke, 2019, p. 875) was applied through both deductive and inductive approaches concurrently (Patton, 2018, p. 453). The analysis followed three coding cycles. In the first cycle, transcripts were read line by line and initial descriptive codes were generated. In the second cycle, codes were compared across participants, merged where overlapping and grouped into candidate categories. In the third cycle, the categories were organised into overarching themes. All codes with analytical value were retained, including those mentioned by a single participant. Codes, categories and themes were documented in a structured codebook recording each code, its definition and representative quotations. The codebook was reviewed by an experienced expert, with differences resolved through discussion and consensus. The analysis yielded five themes, eighteen categories and one hundred and one codes. Credibility was ensured through prolonged engagement, pre-interview briefing and participant validation of transcriptions (Güler et al., 2015, p. 373; Yıldırım

& Şimşek, 2021, p. 289). Transferability was supported through detailed description of the data collection process and purposive sampling, dependability through audio recording, and confirmability through expert review (Altunışık et al., 2022, p. 487).

Direct quotations were reported in their original form, with statements that could reveal identities marked with an ellipsis. Participants were identified through anonymised codes (P1, P2, etc.). Representative quotations were selected where similar views emerged across participants, and recurrent codes were interpreted as evidence of emerging conceptual patterns.

Findings

The study was conducted with eight voluntary experts from seven institutions in Türkiye and the UK (See Table 1). "Expert" was defined as an individual with direct and sustained professional experience in the management, appraisal or governance of sensitive information within public records contexts. P2 and P6 were based in the UK; the remaining six represented the Turkish context. Their organisational affiliations included national archives, ministries, universities, press institutions and libraries. The majority held postgraduate degrees and had extensive professional experience. Demographic variables were considered indicators of sample diversity rather than independent variables.

Table 1. Demographic Information of the Participants[1]

Variable	Categories	n (8)
Country	Türkiye	6 (P1, P3, P4, P5, P7, P8)
	UK	2 (P2, P6)
Field of Graduation	Information and Records Management	2
	History	2
	Documentation and Information	1
	Theology	1
	Mathematics and Computer Science	1
	Business Administration	1
	Bachelor's Degree	1
Education Level	Master's Degree	6
	Doctorate	1
Years of Experience	6–10 years	1
	11–15 years	2
	More than 16 years	5

[1]Institution type and professional role were not included in Table 1 in order to protect participant confidentiality, given the small sample size and the restricted nature of the subject matter.

The analysis identified five themes and eighteen categories (See Table 3). The themes focused on the following areas: (1) Sensitive Information, (2) Sensitivity Review, (3) Review Challenges and Solutions, (4) Technology-Assisted Review and (5) Advisory Councils and Guides. Collectively, this structure addresses virtually all dimensions raised in the research questions, reflecting the complex and multi-layered nature of sensitivity review practices within public-sector archival environments.

Table 2. The Relationship Between Research and Interview Questions and the Themes

Research Questions (RQ)	Interview Questions (IQ)	Theme
RQ-1	IQ 1, 2	Theme-1
RQ-2	IQ 3,4	Theme-2
RQ-3	IQ 5,6,7,8,9	Theme-3
RQ-4	IQ 11,12,13,14	Theme-4
RQ-5	IQ 10, 15	Theme-5

The findings follow a structure that is directly aligned with the research questions. Each theme corresponds directly to a specific research question and its associated interview questions (See Appendix 1), demonstrating the structural alignment between the data collection instrument and the analytical framework (See Table 2). Participants' views are presented systematically under each category and the key insights that emerged regarding archival sensitivity review processes are examined in detail.

Table 3. Themes and Categories

Theme	Categories
Sensitive Information	Identification of Sensitive Information
	Scope of Sensitive Information
	Sensitive Information Legislation
Sensitivity Review	Review Approach
	Physical and Digital Review
Review Challenges and Solutions	Process Challenges
	Solutions for Ensuring Objectivity
	Time Oriented Solutions
	Solutions for Mosaic Structures
	Solutions for Access Provision
Technology-Assisted Review	Role of Supporting Tools
	AI
	Autonomous Review
	Freedom of Information (FOI) Requests
	Legal, Technical, and Ethical Issues
Advisory Councils and Guides	Structure of the Councils
	Qualifications of the Members
	Developing Guidelines

The findings are presented in a structured manner based on the categories within each theme (see Table 3). In addition, the category and code tables for each theme are used as supporting elements that enhance the traceability of the analysis.

While certain categories may appear conceptually proximate, such as "Scope of Sensitive Information" and "Identification of Sensitive Information" or "Role of Supporting Tools" "AI" and "Autonomous Review" each category was maintained as a distinct analytical unit on the grounds that participant responses, although thematically related, consistently converged around a specific and distinguishable focal point.

Findings Related to the Theme of Sensitive Information

The data derived from participants' statements were analysed under three categories within the theme of Sensitive Information (see Table 4).

Table 4. Categories and Codes under the Theme of Sensitive Information

Category	Codes	Participants
Identification of Sensitive Information	Format-Independent	*P1, P2, P3, P4, P5, P6, P7*
	Supporting Document	*P5, P6, P7*
	According to Procedures and Principles	*P5, P6*
	Definition-Based Identification	*P5*
	Context-dependent	*P2*
Scope of Sensitive Information	Institution-based classification	*P3, P5, P7, P8*
	Extensive	*P5, P6, P8*
	Subjective	*P2, P3, P6*
	Should allow for updates	*P4, P5, P7*
	Both public and personal	*P4*
	Process-based decision	*P3*
Sensitive Information Legislation	Non-Objective Classification	*P1, P3, P8*
	Off-List Sensitivity Formation	*P4, P6, P8*
	Subject-Based Classification	*P2*
	Legislative Requirement	*P1*
	Static	*P5*

Identification of Sensitive Information

Nearly all participants stated that sensitivity depends primarily on content rather than format (See Table 4). P4 emphasised that "*the sensitivity of a record depends on its content*," and P7 illustrated this with medical records, which "*remain sensitive whether physical or digital*". P2 added that "*a contextual understanding is needed to determine whether information is sensitive*".

Participants proposed two main approaches. The first is definition-based: P5 argued that defining the overall scope is preferable to listing individual elements such as religion, ethnicity or disciplinary records. The second is procedural: P6 stated that "*having procedures is extremely beneficial*", while P5 emphasised the need to specify how sensitive information is identified and what method should be applied. Supporting documents were also seen as essential, with P7 advocating an approach "*shaped by guidelines, policies and strategies" and P5 noting that "a guiding document would be more appropriate*".

Scope of Sensitive Information

Participants emphasised that the scope of sensitive information is broad, context-dependent and inherently subjective (See Table 4). P6 noted that "*the categories do not cover everything*", P3 that determination "*involves the subjective views of authorised individuals*", and P2 that "*different decision makers may reach different conclusions*". P4 added that "*definitions should be renewable and always open to updates*".

Regarding scope determination, P3 referenced the U.S. Department of Defense's six-step procedure as a systematic example. The most widely shared view, expressed by P3 and P7, is that institutions should develop their own regularly updated sensitivity inventories reflecting the information they create, process and store.

Sensitive Information Legislation

Most participants indicated that existing legislation provides only a partial framework for defining sensitive information (See Table 4). P3 stated that "*classification is carried out even though it does not include entirely objective criteria*", allowing new forms of sensitivity to emerge beyond formal definitions. P6, reflecting on the UK context, noted that "*there are many sensitivities beyond legislation and cultural sensitivity is a notable gap*". P4 argued that "*new sensitivities may emerge beyond the listed types*", whereas P2 considered the framework conceptually comprehensive as it "*offers legal reasons that explain why information cannot be disclosed and covers all expected subject areas*".

Most participants nevertheless criticised the static nature of current systems. P1 identified the absence of a standalone regulation specifically addressing sensitive information in the Turkish context as a significant structural gap. P5 argued that "*the types of sensitive information should always be determined dynamically*", warning that fixed lists may lead to systemic misclassification.

Findings on the Theme of Sensitivity Review

The findings indicate that participants approached sensitivity review from both an institutional policy and regulation based perspective and a technology supported risk management perspective (See Table 5).

Table 5. Categories and Codes under the Theme of Sensitivity Review

Category	Codes	Participants
Review Approach	Risk Based	*P2, P6, P7, P8*
	Collaboration with the Records-Creating Institution	*P1, P2, P4, P5*
	Two-Stage Review	*P1, P2, P4, P5*
	Institution-Based Management Policy	*P8*
	Legislation-Based	*P7*
Physical and Digital Review	Digital Information Carries Higher Risk	*P6, P7, P8*
	Management Differences by Format	*P4, P7*
	Similar Process Management	*P1*
	Method-Independent Risk	*P2*
	Paper Medium is Less Controlled	*P5*
	Digital Medium is Less Controlled	*P7*
	Large Volume of Digital Records	*P6*
	Difficult to Establish Relationships between Digital Records	*P7*

Review Approach

Participants strongly emphasised a risk-based approach (See Table 5). P6 stated that "*we apply a risk management approach by retaining detailed review for high risk records*", and P7 noted that sensitivity review "*should be based on a risk management approach*".

Collaboration with records-creating institutions was also central. P2 stressed that "*ideally, those who create the information should make such decisions based on their own risk context*". P5 reinforced this by noting that certain materials may have significance that is not recognized by archivists, making collaborative appraisal essential.

Participants also valued a two-stage review process: an initial appraisal at the moment of records creation, followed by a second review by archivists during transfer. P1 noted that records reach the national archives decades after creation,

necessitating reappraisal. P2 drew on Kahneman's Noise to provide a theoretical basis, stating that "*I would estimate that there is a considerable degree of noise in such highly subjective decision-making processes. This is also why it is important to have a reviewer above the person who makes the initial decision*".

P8 argued that permissions, access conditions and user roles should be clearly defined within each organisation, and P7 affirmed that "*the legislation of the country must be taken into account*". P2 further acknowledged that "*whether automated or manual, no process will be flawless*".

Physical and Digital Review

Participants expressed differing views on sensitivity review across paper and digital media (See Table 5). P7 noted that "*when information is shared in a digital media, it often spreads widely, and it is impossible to retract it. In contrast, in a physical media, a file can be closed or retrieved*". P6 pointed to additional challenges: "*digital records may encounter access problems because they are stored in obsolete or proprietary formats. Moreover, digital materials usually arrive in much larger quantities, making us more dependent on our risk management approach*".

P4 explained that "*reviewing a room full of paper records is not the same as reviewing a hard drive full of files. While physical records must be transported, digital ones can be examined interactively and simultaneously*". Despite these differences, P1 maintained that "*the review process for digital records and paper records should, in principle, be the same*".

Findings on the Theme of Review Challenges and Solutions

Participants presented multifaceted views on the challenges encountered in sensitivity review (See Table 6).

Table 6. Categories and Codes under the Theme of Review Challenges and Solutions

Category	Codes	Participants
Process Challenges	Context	*P1, P2, P3, P4, P6, P7, P8*
	Time	*P1, P2, P3, P5, P6, P7*
	Personal Perspective	*P1, P2, P3, P4, P7*
	Mosaic Structure	*P2, P3, P4, P6, P7*
	Undefined Level of Confidentiality	*P1, P8*
	Changing Level of Confidentiality	*P3*
	Hybrid Process Management	*P3*
	Legislative Changes	*P3*
	Corruption of Digital Records	*P6*
	Insufficient File and Retention Schedule	*P1*
	Lack of Awareness	*P8*
	Digital Transfer and Process Management	*P5*
	Repetitive Control Points	*P1*
Solutions to Ensure Objectivity	Legislation	*P2, P3, P4, P7, P8*
	Training and Awareness	*P1, P3, P8*
	Automation	*P2*
	Consultation	*P1*
	Defined Roles and Guidelines	*P1*

Table 6. Continued

Category	Codes	Participants
Time-Based Solutions	Access Restriction	*P2*
	Periodic Review	*P1*
	Process Management	*P3*
	Decision of the Records-Creating Institution	*P4*
Solutions for the Mosaic Structure	Establishing Relationships	*P1, P4, P8*
	Inter-institutional Coordination	*P4*
	Collaborative Review	*P6*
Solutions for Access Provision	Anonymisation	*P1, P5, P8*
	Redaction	*P2*
	Public Interest	*P2, P7, P8*
	Encrypted and Authorised Access	*P8*

Process Challenges

A central difficulty concerns context. From the Turkish perspective, P1 illustrated this with an archival example: "*when working on the Korean War, you expect to learn about the conflict itself (…) but you may encounter a record in which a regimental commander reports some inappropriate behaviour. It is not directly related to the war, yet the way it is written makes it difficult to separate it from the broader war narrative*". Similarly, in the Turkish institutional setting, P3 noted that "*a record created by the Ministry of Education might not receive a confidentiality designation, while the same type of records in intelligence or foreign affairs could be classified differently due to personnel-related sensitivities*". P7 added that context is shaped by "*political, cultural, social or religious factors*" and emphasised concern over "*how context changes once fragments of information are brought together*".

Time constitutes a second challenge. P5 observed that "*what is considered sensitive today may not be tomorrow, and what is not sensitive today may become sensitive in the future*". Drawing on the UK experience, P2 referenced atomic bomb records from the 1940s and 1950s, which "*are still incredibly sensitive… although the long-term trend is a decrease in sensitivity, contextual change can make previously non-sensitive material far more sensitive*". P7 pointed to shifting social norms: "*in the 1980s we removed details about extramarital relationships because they related to private life, but in the UK today, living together outside marriage is socially accepted*". In the Turkish context, P3 linked the issue to legal change: "*before the Personal Data Protection Law, certain personal information was not treated as sensitive; after the law came into effect, these records gained sensitivity*".

Personal judgement constitutes a further challenge. P7 stated that "*one's own views, political or cultural background, social life or personal values may make it harder to remain fully objective*", while P3 added that staff rotation creates inconsistencies, as "*five years later, a different official may interpret the same records differently*".

The mosaic structure of records presents another challenge. P2 noted that "*to hide something, you must know what other information exists and to what degree those pieces can reconstruct what you are trying to conceal*". P4 illustrated this concretely: "*a basic fuel procurement records may seem harmless, but when a researcher correlates it with operational flight records for the same year, it may gain a completely different meaning*".

Participants also raised structural concerns. P1 noted that some records lack confidentiality markings despite containing commercially sensitive content. P3 observed that confidentiality level changes create administrative problems when different sensitivity levels are managed on different platforms. P6 remarked that digital records in obsolete formats may suffer access problems, and P5 stressed the need to design systems governing the transfer, access and deletion of sensitive digital content.

Solutions to Ensure Objectivity

Most participants stated that ensuring objectivity requires a clearly defined regulatory framework supported by institutional policies (See Table 6). P4 advocated "*an implementation order or an institutional regulation that sets the standard, with provisions allowing for updates and amendments*". P3 argued that "*objective measures should be defined through institutional policies grounded in legislation*", and P1 linked objectivity to job descriptions and procedural instructions.

Training was also considered essential. P3 noted that "*organisation-wide training and awareness activities should be provided, because this is how subjectivity can be turned into objectivity*". P1 underscored internal consultation mechanisms, explaining that doubtful cases are referred to the commission for collective assessment. P2 highlighted the potential of automation in "*making some procedures more systematic and less dependent on individual interpretation*".

Time-Based Solutions

Participants highlighted the limitations of existing time-based practices (See Table 6). P2 acknowledged: "*we have solutions such as withdrawal from access; we release something and then remove it from access (...) but perhaps we need other solutions*".

P4 suggested that "*the records-creating authority could set timeframes for each record individually; this may provide a solution*". P1 emphasised institutionalised reappraisal cycles: "*if we can note that certain materials will be re-evaluated at specific intervals, we might be able to overcome this issue over time*". P3 argued that "*process-based objective criteria would resolve this problem*".

Solutions for the Mosaic Structure

Most participants emphasised that mosaic-related challenges arise when individual records appear harmless but gain sensitivity once linked (See Table 6). P1 underscored that "*we need to conduct the review by establishing connections with records from other departments within the institution*". P8 argued that "*data should be grouped into relational clusters and identified within a shared analytical pool*", and P6 noted that "*frequent discussions about the content being examined are extremely important; this provides numerous opportunities to collectively identify mosaic sensitivities*".

P4 suggested that "*coordination with the records-owning institution is necessary when considering potential measures*". P1 explained that their institution is developing "*a new cataloguing approach that evaluates the relationships between records rather than relying solely on traditional descriptive fields*".

Solutions for Access Provision

Participants identified anonymisation, redaction and controlled-access mechanisms as principal strategies for enabling access to sensitive records (See Table 6). P5 proposed that "*techniques could be developed to render the information anonymised*", and P1 added that "*within a 400-page records, there may be just a single sentence that could be considered offensive, and if we could redact that line, there would be no objection to disclosing the remaining records to the public*".

Redaction was also presented as a procedural tool within FOI contexts. Reflecting on UK practice P2 explained that "*when a request is made under the FOI, you can respond by heavily redacting the sensitive parts before disclosure, or perform the redaction prior to transferring the records to the archive*". P8 noted that sensitive digital records should be "*encrypted and accessed through authorisation controls*".

Participants also highlighted cases where public interest provides a legitimate basis for disclosure. P7 cited the income of a Member of Parliament as a matter citizens have a right to know, while P2 added that even politically sensitive records, such as pandemic decision-making materials, may be disclosed if a legally mandated public inquiry requests them.

Findings on the Theme of Technology-Assisted Review

Participants' views on technology-assisted sensitivity review highlighted the potential of AI-supported tools to accelerate the process and enhance consistency, while emphasising their limitations in perceiving contextual nuances and observing ethical boundaries (See Table 7).

Table 7. Categories and Codes under the Theme of Technology-Assisted Review

Category	Codes	Participants
The Role of Supporting Tools	Keyword-Based Capture	*P4, P6*
	Speed	*P1, P2, P8*
	Consistency	*P2*
	Volume	*P2*
	Automated Classification	*P8*
	Time–Cost Efficiency	*P8*
	Lower Reliability	*P1*
	Struggles with Synonyms	*P4, P6*
	Changing Terminology	*P7*
AI	Context Detection	*P5, P8*
	Time-Sensitive	*P4, P7, P8*
	Objectivity	*P1, P5*
	Autonomous Processes	*P2, P5*
	Should Be Learnable	*P5*
Autonomous Review	Human-Dependent	*P1, P2, P3 P4, P5, P7, P8*
	Centralised Rule Based	*P5*
	Experience, Intuition, and Empathy	*P2, P3*
	Verification Required	*P4*
FOI Request	Necessity	*P2, P8*
	Process Acceleration	*P1, P4, P5, P7 P8*
	After Manual Tagging	*P3*
Legal, Technical, and Ethical Issues	Institutional Responsibility	*P1*
	Rule Based Framework	*P5*
	Unclear Legal Responsibility	*P3*
	Contract Based	*P4, P5, P6*
	Domestic Software	*P8*

The Role of Supporting Tools

Participants expressed both positive and negative views on supporting tools (See Table 7). P4 observed that "*sensitivities can be detected through specific keywords*". P8 noted efficiency benefits: "*automated tools reduce manual or physical procedures, enabling more effective and efficient use of time and resources*". P2 stressed scalability: "*massive volumes of digital information, digital piles, that are now impossible to review manually. Therefore, to scale such processes, automation has become essential*".

Despite these advantages, P1 argued that "*the human element remains more important and reliable*". P6 pointed out that "*words have multiple meanings, and many false positives can occur*". P4 illustrated this through the term bomb, which can

denote an explosive device, a compliment or a local dessert. P7 highlighted evolving terminology: "*terminology surrounding sexual offences has changed considerably, and failure to update tools may lead to serious ethical and legal issues*".

AI

Participants expressed both positive and negative views on AI-assisted systems (See Table 7). P8 stated that "*sensitive records should be regularly reviewed through AI systems*", and P7 emphasised that "*when using technology-assisted AI sensitivity review tools, the time factor must be integrated into the software*". On context-aware appraisal, P5 explained that "*you need to feed the completed work into the AI system and train it. AI learns from that structured data, establishes its own model, and later evaluates new records according to your defined perspective*".

P5 also stated that "*through AI-based analysis, the sensitivity can be assessed fully objectively*", and P1 observed that "*software applications can contribute significantly by reducing personal or subjective judgements*".

Despite these advantages, P5 warned that "*when you train an AI model and then freeze it, the rules valid at the time of training remain fixed*", arguing that adaptive learning systems are necessary. P5 summarised: "*AI may ease 80-90% of the work, but it does not become 100% autonomous*".

Autonomous Review

Participants consistently emphasised that fully autonomous decision-making is neither feasible nor desirable (See Table 7). P5 stated that "*the rules are defined by humans and entered into the system, which then operates within those parameters. Therefore, it is not possible to speak of full autonomy*". P3 added that "*since evaluation tools lack human experience and intuition, the sensitivity review process should not be left entirely to such systems*".

P2 argued that "*in any decision-making process that affects the lives of individuals and communities, the presence of humans in the loop should remain a legal requirement*", stressing that "*the greatest strength of humans lies in our lived experience and capacity for empathy, the ability to understand how a decision might affect another person*".

P5 proposed "*a central system in which rules are defined*" that could analyse records and assign a sensitivity score, while P4 cautioned that "*verification is always necessary*".

FOI Request

Participants noted that supporting tools improve consistency and accelerate FOI request processing (See Table 7). P1 stated that "*by using automated tools, both the volume and frequency of FOI requests could be reduced*", and P7 described them as "*a great solution for FOI requests... because evaluating these requests and locating information is very time-consuming*". P4 illustrated this: "*when a citizen requests historical data on wheat export rates from the Ministry of Agriculture, a staff member would normally have to manually search archival records. However, through software and specific algorithms, such requests could be processed much more efficiently*".

P3 explained that "*the identification and labelling of information within records should be performed through human interpretation and intuition. Once labelled, the system can automatically respond to requests, and marking the locations of sensitive information would increase and accelerate the response rate*".

Legal, Technical, and Ethical Issues

Participants identified several legal, technical and ethical risks (See Table 7). On legal responsibility, P5 stated that "*responsibility is entirely determined by contractual arrangements*". P1 took the opposite view: "*you cannot place responsibility on software developers. Ultimately, the institution itself will be accountable*". P3 pointed to persistent uncertainty "*in cases of incorrect evaluation*".

P5 highlighted that "*because rule sets are written by humans, the system can only be as ethical and lawful as the rules embedded within it*". P8 raised national data security concerns: "*a nationally developed system would be better because cross-border data flows could grant access to other countries and create serious risks for national data integrity*".

Findings on the Theme of Advisory Councils and Guides

Participants' views indicate that decision-making mechanisms should be supported by independent, interdisciplinary and expertise-based advisory structures providing guidance across ethical, legal and technical dimensions (See Table 8).

Table 8. Categories and Codes under the Theme of Advisory Councils and Guides

Category	Codes	Participants
Structure of the Councils	Independent	*P1, P4, P7, P8*
	Both Dependent and Independent	*P3*
	Supervisory	*P7*
	Advisory Board	*P1, P4*
	Risk Control System	*P5*
	Non-archival Higher Authority	*P1*
	Should Formulate Policy	*P3*
Qualifications of the Members	Archival Expertise	*P4, P8*
	Should Consist of Managers from Diverse Disciplines and Institutions	*P1, P3, P4, P8*
	Next-generation Technology Competence	*P4*
	Should Be Civilian	*P7*
	Empirical and Mathematical Approach	*P2*
Developing a Guideline	Inter-institutional Collaboration	*P3, P7, P8*
	Based on Knowledge and Experience	*P2*
	General and Institution-Specific	*P4, P5, P8*
	Accelerates Problem Solving	*P8*
	Systematic and Efficient Operation	*P8*

Structure of the Councils

P1 stated that the advisory council "*should be located within the national archival agencies but operate independently*", functioning "*as a higher-level body rather than being composed of regular archival staff*".

P2 explained that such councils "*are primarily advisory in nature, yet they should also assume a supervisory role when necessary*", overseeing institutional decisions about transferring sensitive records "*within the principles of public interest, accountability and transparency*". P4 added that the council should operate "*as a consultative mechanism guiding records-creating bodies and facilitating dialogue regarding sensitivity-related decisions*".

P3 emphasised the council's policy role: "*the council should be policy-oriented (...) it ought to have the authority and competence to develop and regulate policies concerning the management, oversight, training and handling of complaints related to sensitive records*".

Qualifications of the Members

Participants expressed their views on the qualifications of council members (See Table 8). P4 noted that "*the council should consist of individuals with proven expertise in their respective fields, preferably representatives from major public institutions*". P3 proposed a council composed of "*experts in information and records management, law, information technologies and software, information security, and data analysis*".

P4 emphasised that members should be "*proficient in utilising AI and other emerging technologies efficiently",* while P2 called for a "*more scientific, more empirical and more mathematical perspective*".

P7 underscored independence: "*members of such councils are usually senior and civilian figures (...) often retired governors or journalists" and "should definitely not consist of current public officers or active civil servants*".

Developing a Guideline

Participants shared their views on developing guidelines (See Table 8). P8 stated that guidelines "*would help accelerate the sensitivity review process and serve as a problem-solving reference*". P2 underlined the importance of codifying practice: "*if we take the time to codify what we know or what we have learned by creating guidelines and manuals, we will progress collectively in the fastest way (...) we must constantly revise and adapt our approaches*".

P3 noted that "*guidelines should be developed through communication and collaboration between institutions*". P5 stressed combining a shared national framework with institutional flexibility: "*a central guideline outlining the general framework would be highly beneficial. Institutions and departments could then adapt it to their own context and conduct their evaluations within this general procedural framework*".

Discussion

This study identified multidimensional findings related to sensitivity review. One of the most consistent findings across both national contexts is that sensitivity is determined by content rather than format; format instead shapes how sensitive information is identified and managed in practice. This finding extends the existing literature, which has largely treated format differences as a technical rather than a conceptual challenge, and repositions sensitivity review as a content-driven intellectual process. At the same time, the increasing volume of digital information makes detection more difficult, and the reliance of legislation on fixed patterns and keywords to define sensitivity limits institutional flexibility in both countries examined. Accordingly, participants suggested that legislative frameworks should adopt broader definitions, that institutional regulations should allow the updating of supplementary documents, and that institution-specific sensitivity frameworks should be developed.

The legislative frameworks of the two countries illustrate this shared limitation through different institutional trajectories. In the UK, the Freedom of Information Act 2000 provides an extensive exemption framework, which TNA has operationalised through a substantial body of guidance covering categories of personal information and closure periods (The National Archives, 2019), access exemptions addressing national security, defence and trade secrets (The National Archives, 2015), and a two-stage review model (The National Archives, 2024). Despite this institutional maturity, UK participants noted that cultural sensitivities and contextual variability remain inadequately captured. In Türkiye, the absence of a standalone archival law and the relatively recent enactment of the Personal Data Protection Law (No. 6698, 2016) mean that sensitivity-

related practices are governed through dispersed regulations without a unifying procedural framework. Turkish participants consistently identified the static nature of legislation and the absence of institution-specific guidance as structural gaps. This is consistent with Cengiz-Mater and Özdemir-Şahin (2026), who found that 70.8% of Turkish public bodies had not commenced the sensitivity review of digital records and none used specialised software. These findings suggest that legislative maturity does not resolve the challenge of contextual sensitivity but determines the degree of institutional support available to practitioners.

Risk management is central to sensitivity review (Sloyan, 2016). Participants differed on whether paper or digital media carry greater risk, but agreed that the risk assessment process itself does not depend on the medium. The volume, fragmented structure and uncontrolled circulation of digital information complicate review (McDonald et al., 2014; The National Archives, 2016; Whyte & Walsh, 2024). A finding that diverges from the literature is participants' emphasis on format-based management differences, pointing to the need for privacy-level-driven process management as a distinct operational requirement. Collaboration with the originating institution and a two-phase review approach form the basis of hybrid practices applicable in both national contexts, albeit at different stages of institutional development.

The challenges relate to context (Gollins et al., 2014; McDonald et al., 2018a; Sloyan, 2016), time (McDonald, 2019; Moss & Gollins, 2017; Peterson, 2007; Sillitoe, 1998; The National Archives, 2015), personal perspective (Dressler & Kearns, 2023; Rukancı et al., 2021; Thompson & Kaarst-Brown, 2005) and mosaic structure (Belen-Sağlam et al., 2022; McDonald, 2019; Photopoulos, 2011). The country-specific dimensions are noteworthy. In the UK context, time-based challenges are illustrated by evolving social norms, where practices that were once considered standard are now reconsidered in light of changed societal values. In the Turkish context, legal change constitutes the primary driver, with the Personal Data Protection Law retroactively redefining the sensitivity status of existing records. These parallel but distinct manifestations demonstrate that sensitivity review must be understood as a context-responsive practice shaped by national regulatory and cultural dynamics. The lack of clearly defined confidentiality levels and limited institutional awareness further complicate the process, requiring not only regulatory revision but also structured internal frameworks guiding practitioners through the appraisal of sensitive content.

The literature widely emphasises the need for new technologies to support sensitivity review of digital public records (McDonald et al., 2017; McDonald, 2019; Narvala et al., 2022b; Sánchez et al., 2012). Although AI and technology-assisted tools contribute to context awareness (Jaillant, 2022), temporal reappraisal and objectivity, they cannot fully replace human intervention (Gollins et al., 2014; McDonald et al., 2020; The National Archives, 2016; Tough, 2018). This study contributes a nuanced position: participants framed automation as a decision-support mechanism rather than a decision-making one. This distinction is theoretically significant because it reframes the human-AI relationship as complementary rather than substitutive. Whereas Jaillant (2022) argues that automatic tagging can be performed through AI, participants stated that assessments, particularly within FOI contexts, need to be carried out manually. Human intuition, experience and empathy remain ethically and legally indispensable. Participants underlined that legal responsibility should be shared between software developers and institutions, and cautioned against risks associated with foreign-developed technologies. Recent AI-related regulation[1] in the European Union underscores the importance of a robust legal framework in this area.

Advisory councils should consist of independent, multidisciplinary and experienced experts (McDonald et al., 2018a; Narvala, 2024; Whyte & Walsh, 2024), functioning not only as supervisory bodies but also as active entities developing policies and strategies. In the UK, the Advisory Council operates as an established mechanism with a defined role in sensitivity decisions at the point of transfer. In Türkiye, no equivalent body currently exists, and participant perspectives suggest that establishing such a body, adapted to the Turkish institutional environment, would constitute a meaningful step towards more systematic and accountable sensitivity review practice. Participants further recommended that council members possess advanced technological competencies enabling them to evaluate and integrate AI-assisted tools within the process. Institutional

[1] In June 2024, the European Parliament adopted and enacted the world's first comprehensive artificial intelligence legislation, the Artificial Intelligence Act. The Act requires AI applications to be classified according to their risk level and introduces strict oversight mechanisms for high risk Technologies. See European Parliament & Council of the European Union. (2024).

cooperation (Mathers, 2000) and participant feedback will facilitate the creation of comprehensive guidelines[2], within which each institution can develop its own sensitivity policies (Keskin, 2012).

Conclusion and Suggestions

Sensitivity review is a high-risk and multidimensional process bringing together legal, ethical, institutional and technological considerations. The findings demonstrate that it cannot be reduced to a simple examination of content. Contextual interpretation, changes in sensitivity levels over time and institutional risk cultures shape the process, requiring a holistic approach that integrates explicit rules with professional judgement, expertise and risk management.

This study makes several contributions to the existing literature. First, it empirically establishes that sensitivity is content-driven rather than format-driven, offering a conceptual clarification with direct implications for how sensitivity review is structured in practice. Second, by drawing on archival specialists' perspectives from two distinct national contexts, it demonstrates that while the core challenges of sensitivity review are universal, their manifestations and the institutional resources available to address them differ substantially between the UK and Türkiye. Third, it advances the debate on AI-assisted review by establishing a theoretically grounded distinction between automation as a decision-support mechanism and automation as a decision-making one.

The findings also reveal that many institutions, particularly in the Turkish context, lack a systematic framework for sensitivity review and that practices are often shaped by individual expertise rather than institutional procedure. Challenges including contextual interpretation, evolving sensitivity, the mosaic effect, the tension between transparency and confidentiality and the pressure of digital information growth represent central problem areas across both national contexts examined.

Several practice-oriented conclusions emerge. Sensitivity review should be structured as a process with clearly defined steps, with criteria for identifying sensitive information, decision pathways and the rationale behind restriction or disclosure decisions documented systematically. Institutions should rely on interdisciplinary teams combining archival expertise, legal knowledge, information security and data governance. Clear guidelines, checklists, decision-tree models and sample scenarios are essential for translating abstract principles into concrete, records-based practices. These recommendations reflect both the institutional maturity observed in the UK context and the developmental needs identified in the Turkish context.

AI and machine learning applications offer important opportunities for pattern detection, prioritisation and consistency, but should function as decision-support systems rather than autonomous decision-makers. Human oversight, transparency, explainability and ethical awareness remain indispensable. Emerging technologies such as blockchain and distributed ledger systems also warrant attention as potential mechanisms for transparent documentation of sensitivity decisions, though they must be critically assessed in terms of scalability, interoperability and data protection before adoption.

The findings offer insights applicable beyond the specific national contexts examined. However, the geographical and contextual boundaries of the study should be taken into account when interpreting the results. The findings reflect the perspectives of archival specialists operating within the specific legislative, institutional and cultural frameworks of Türkiye and the UK and may not be directly transferable to countries with fundamentally different archival traditions or administrative structures. Future research involving additional national contexts would contribute to a more comprehensive understanding of the phenomenon.

In conclusion, sensitivity review is a critical domain at the intersection of archival theory, information governance and digital transformation. Strengthening this process requires integrating explicit normative frameworks, institutionally resilient practices and carefully designed technological tools, thereby safeguarding individuals while supporting meaningful access to public records and reinforcing democratic accountability.

[2] See Sillitoe (1998), "ACA guidelines"; Sloyan (2016), "CLIR guidelines".

The following suggestions are proposed to ensure the effective management of public records containing sensitive information:

- Legislative frameworks should establish definition-based approaches that allow sensitivity to be determined in a context-dependent manner and updated as institutional and societal conditions evolve, rather than relying on fixed categorical lists.
- Institutions should identify potentially sensitive records within routine workflows and develop institution-based sensitivity inventories that reflect the types of sensitive information they create, process and store.
- Technology-assisted review tools should be designed around central, rule-based frameworks with mechanisms for feedback and periodic updates, and should be capable of supporting FOI-related procedures with speed and consistency while remaining subject to human validation.
- Sensitivity review committees and advisory councils should coordinate at both institutional and national levels, with online catalogues used to gather user feedback and support early detection of potential errors.
- Reviewers should be supported with informative prompts and identification checklists tailored to the characteristics of each record type.
- In-service training programmes addressing the appraisal, archiving and transfer of records containing sensitive information should be delivered in accordance with policies and guidelines prepared by national archival authorities and integrated into institutional workflows across all public institutions.

Author contributions

Conception: H.Ö., F.R.; Design: H.Ö., F.R.; Data acquisition: H.Ö.; Data analysis: H.Ö.; Data interpretation: H.Ö., F.R.; Drafting of the manuscript: H.Ö.; Critical revision of the manuscript: H.Ö., F.R. All authors reviewed the results, approved the final version of the manuscript, and agreed to be accountable for all aspects of this study.

Ethical approval

This study was approved by the Ethics Committee of Ankara University (Date: 5 July 2024, Decision No: 16/187).

Data availability statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Conflict of interest

The authors declare that this study was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Funding

The authors declare that this study received no funding.

Generative AI statement

The authors declare that no generative AI or AI-assisted technologies were used in the writing or preparation of this study.

References

Al-Fedaghi, S. (2007). How sensitive is your personal information? In *Proceedings of the 2007 ACM Symposium on Applied Computing* (pp. 165–169). Association for Computing Machinery. https://dl.acm.org/doi/10.1145/1244002.1244046

Altunışık, R., Boz, H., Gegez, E., Koç, E., Sığrı, Ü., Yıldız, E., & Yüksel, A. (2022). *Sosyal bilimlerde araştırma yöntemleri: Yeni perspektifler* (1st ed.) [Research methods in social sciences: New perspectives]. Seçkin Yayıncılık.

Association of Canadian Archivists. (2017). *Association of Canadian Archivists Code of Ethics and Professional Conduct*. https://www.archivists.ca/Policies-and-Codes

Belen-Sağlam, R. B., Nurse, J. R., & Hodges, D. (2022). Personal information: Perceptions, types and evolution. *Journal of Information Security and Applications, 66*, 103163. https://doi.org/10.1016/j.jisa.2022.103163

Berardi, G., Esuli, A., Macdonald, C., Ounis, I., & Sebastiani, F. (2015). Semi-automated text classification for sensitivity identification. In *Proceedings of the 24th ACM International Conference on Information and Knowledge Management* (pp. 1711–1714). Association for Computing Machinery. https://doi.org/10.1145/2806416.2806597

Berg, B. L., & Lune, H. (2019). *Qualitative research methods for the social sciences* (A. Arı, Trans.; 4th Turkish ed.). Eğitim Yayınevi.

Bilgi Edinme Hakkı Kanunu. (2003, October 24). [Law on the Right to Information], No. 4982. *Official Gazette of the Republic of Türkiye* (Issue No. 25269).

Branting, K., Brown, B., Giannella, C., Guilder, J. V., Harrold, J., Howell, S., & Baron, J. R. (2023). Decision support for detecting sensitive text in government records. *Artificial Intelligence and Law*, 1–27. https://doi.org/10.1007/s10506-023-09383-6

Braun, V., & Clarke, V. (2019). Psikolojide tematik analizin kullanımı [Using thematic analysis in psychology]. *Eğitimde Nitel Araştırmalar Dergisi – Journal of Qualitative Research in Education, 7*(2), 873–898. https://doi.org/10.14689/issn.2148-2624.1.7c.2s.17m

Cengiz-Mater, E., & Özdemir-Şahin, L. (2026). An examination of the challenges and awareness presented by the transfer of born-digital records in the public sector: A case study of Türkiye. *Information Development*, *42*(1), 251-266. https://doi.org/10.1177/02666669231214529

Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches* (M. Bütün & S. B. Demir, Eds. & Trans.; 3rd Turkish ed.). Siyasal Kitabevi.

Cox, R. J., & Samuels, H. W. (1988). The archivist's first responsibility: A research agenda to improve the identification and retention of records of enduring value. *American Archivist*, *51*(1-2), 28–42. https://www.jstor.org/stable/40293193

Cook, T. (2011). We are what we keep; we keep what we are: Archival appraisal past, present and future. *Journal of the Society of Archivists*, *32*(2), 173–189. https://doi.org/10.1080/00379816.2011.619688

Devlet Arşiv Hizmetleri Hakkında Yönetmelik. (2019, October 18). [Regulation on State Archival Services]. *Official Gazette of the Republic of Türkiye* (Issue No. 30922).

Dressler, V., & Kearns, J. (2023). Probing archivists' perceptions and practices in privacy. *Archives and Records, 44*(2), 175–201. https://doi.org/10.1080/23257962.2022.2073207

Etzioni, A. (2014). A cyber-age privacy doctrine: More coherent, less subjective, and operational. *Brooklyn Law Review, 80*(4), 1263–1308. https://ssrn.com/abstract=2506313

European Parliament & Council of the European Union. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik. (2022, April 26). [Regulation on Classified Records]. *Official Gazette of the Republic of Türkiye* (Issue No. 31821).

Gollins, T., McDonald, G., Macdonald, C., & Ounis, I. (2014). On using information retrieval for the selection and sensitivity review of digital public records. In *Proceedings of the 1st International Workshop on Privacy-Preserving IR* (pp. 39–40). http://ceur-ws.org/Vol-1225/pir2014_submission_9.pdf

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field Methods, 18*(1), 59–82. https://doi.org/10.1177/1525822X05279903

Güler, A., Halıcıoğlu, M. B., & Taşğın, S. (2015). *Sosyal bilimlerde nitel araştırma* [Qualitative research in social sciences] (2nd ed.). Seçkin Yayıncılık.

Jaillant, L. (2022). More data, less process: A user-centered approach to email and born-digital archives. *The American Archivist, 85*(2), 533–555. https://hdl.handle.net/2134/16560135

Jaillant, L., & Rees, A. (2023). Applying AI to digital archives: Trust, collaboration and shared professional ethics. *Digital Scholarship in the Humanities, 38*(2), 571–585. https://doi.org/10.1093/llc/fqad019

Johns, R. (n.d.). *Appraisal and disposal*. https://silo.tips/embed/04-appraisal-and-disposal.html

Keskin, İ. (2012). Türkiye için bir arşiv kanunu yazmak: Bir model önerisi [Writing an archival law for Türkiye: A model proposal]. *Arşiv Dünyası, 13*, 5–19.

Kişisel Verilerin Korunması Kanunu. (2016, April 7). [Personal Data Protection Law]. No. 6698. (2016). *Official Gazette of the Republic of Türkiye* (Issue No. 29677).

Marciano, R., Underwood, W., Hanaee, M., Mullane, C., Singh, A., & Tethong, Z. (2018). *Automating the detection of personally identifiable information (PII) in Japanese-American WWII incarceration camp records*. University of Maryland, Digital Curation Innovation Center. https://doi.org/10.1109/BigData.2018.8622634

Mathers, J. (2000). Providing access to sensitive records: The Personal History Index (PHIND). *Archives and Manuscripts, 28*(2), 58–70. https://publications.archivists.org.au/index.php/asa/article/view/8855

McDonald, G. (2019). *A framework for technology-assisted sensitivity review: Using sensitivity classification to prioritise documents for review* [Doctoral dissertation, University of Glasgow]. https://theses.gla.ac.uk/41076/1/2019mcdonaldphd.pdf

McDonald, G., García-Pedrajas, N., MacDonald, C., & Ounis, I. (2017). A study of SVM kernel functions for sensitivity classification ensembles with POS sequences. In *Proceedings of the 40th International ACM SIGIR Conference on Research and Development in Information Retrieval* (pp. 1097–1100). ACM. https://doi.org/10.1145/3077136.3080731

McDonald, G., Macdonald, C., & Ounis, I. (2014). Towards a classifier for digital sensitivity review. In *Advances in Information Retrieval: 36th European Conference on IR Research* (pp. 500–506). Springer. https://doi.org/10.1007/978-3-319-06028-6_52

McDonald, G., Macdonald, C., & Ounis, I. (2015). Using part-of-speech n-grams for sensitive text classification. In *Proceedings of the 2015 International Conference on the Theory of Information Retrieval* (pp. 381–384). https://doi.org/10.1145/2808194.2809493

McDonald, G., Macdonald, C., & Ounis, I. (2018a). Active learning strategies for technology-assisted sensitivity review. In *European Conference on Information Retrieval* (pp. 439–453). Springer. https://doi.org/10.1007/978-3-319-76941-7_32

McDonald, G., Macdonald, C., & Ounis, I. (2018b). Towards maximising openness in digital sensitivity review using reviewing time predictions. In *European Conference on Information Retrieval* (pp. 699–706). Springer. https://doi.org/10.1007/978-3-319-76941-7_47

McDonald, G., Macdonald, C., & Ounis, I. (2020). How sensitivity classification effectiveness impacts reviewers in technology-assisted sensitivity review. *ACM Transactions on Information Systems, 39*(1), 1–34. https://doi.org/10.1145/3295750.3298962

McKechnie, J. & McDonald, G. (2024). SARA: A collection of sensitivity-aware relevance assessments. arXiv. https://doi.org/10.48550/arXiv.2401.05144

Morse, J. M. (2000). Determining sample size. *Qualitative Health Research, 10*(1), 3–5. https://doi.org/10.1177/104973200129118183

Moss, M. S. & Gollins, T. J. (2017). Our digital legacy: An archival perspective. *Journal of Contemporary Archival Studies*, *4*(2), 3. https://elischolar.library.yale.edu/jcas/vol4/iss2/3

Narvala, H., McDonald, G., & Ounis, I. (2022a). Sensitivity review of large collections by identifying and prioritising coherent document groups. In *Proceedings of the 31st ACM International Conference on Information and Knowledge Management* (pp. 4931–4935). https://doi.org/10.1145/3511808.3557182

Narvala, H., McDonald, G., & Ounis, I. (2022b, March 14). The role of latent semantic categories and clustering in enhancing the efficiency of human sensitivity review. In *Proceedings of the 2022 Conference on Human Information Interaction and Retrieval* (pp. 56–66). https://doi.org/10.1145/3498366.3505824

Narvala, H. (2024). *Identifying latent relationship information in documents for efficient and effective sensitivity review* [PhD thesis]. University of Glasgow.

National Archives and Records Administration. (2025). *AI Use Cases – Inventory of AI Applications in NARA*. https://www.archives.gov/ai

Öztürk, H. (2024). Kamu belgelerinin hassasiyet değerlendirmesi: Kuram, süreç ve zorluklar [Sensitivity review of public records: Theory, process and challenges]. *Hazine-i Evrak Arşiv ve Tarih Araştırmaları Dergisi, 6*(6), 91–126. https://doi.org/10.59054/hed.1497456

Patton, M. Q. (2018). *Nitel araştırma ve değerlendirme yöntemleri* [Qualitative research and evaluation methods] (3rd ed.). Pegem Akademi.

Peterson, T. H. (2007). Attitudes and access in the United States of America. In *Proceedings of the Japan–US Friendship Association Seminar* (pp. 1–8). https://www2.archivists.org/sites/all/files/11_Trudy_PETERSON.pdf

Photopoulos, C. (2011). *Managing catastrophic loss of sensitive data: A guide for IT and security professionals*. Elsevier.

Rukancı, F., Anameriç, H., & Başar, A. (2021). *Arşiv ve arşivcilik: Kuram, strateji ve uygulamalar* [Archives and archiving: Theory, strategy and practices]. T.C. Cumhurbaşkanlığı Devlet Arşivleri Yayınları.

Rukancı, F., Anameriç, H., & Başar, A. (2023). *Arşiv Terimleri* [Archival terms]. Devlet Arşivleri Başkanlığı Yayınları.

Sánchez, D., Batet, M., & Viejo, A. (2012). Detecting sensitive information from textual documents: An information-theoretic approach. In *Modeling Decisions for Artificial Intelligence: 9th International Conference Proceedings* (pp. 173–184). Springer. https://doi.org/10.1007/978-3-642-34620-0_17

Sillitoe, P. J. (1998). Privacy in a public place: Managing public access to personal information controlled by archives services. *Journal of the Society of Archivists, 19*(1), 5–15. https://doi.org/10.1080/00379819809514418

Sloyan, V. (2016). Born-digital archives at the Wellcome Library: Appraisal and sensitivity review of two hard drives. *Archives and Records, 37*(1), 20–36. https://doi.org/10.1080/23257962.2016.1144504

Stake, R. E. (1995). *The art of case study research.* Sage.

The National Archives. (December, 2015). *Access to public records.* Erişim adresi: https://cdn.nationalarchives.gov.uk/documents/information-management/access-to-public-records.pdf

The National Archives. (February, 2016). *The application of technology-assisted review to born-digital records transfer, inquiries and beyond*. https://cdn.nationalarchives.gov.uk/documents/technology-assisted-review-to-born-digital-records-transfer.pdf

The National Archives. (March, 2019). *Personal information: a guide for justification wording.* https://cdn.nationalarchives.gov.uk/documents/information-management/personal-information-justification.pdf

The National Archives. (July, 2021). *Access at transfer – Sensitivity Review Overview.* https://cdn.nationalarchives.gov.uk/documents/information-management/access-at-transfer-sensitivity-review-overview.pdf

The National Archives. (2024). *Step 3: Sensitivity review records*. https://www.nationalarchives.gov.uk/information-management/manage-information/digital-records-transfer/digital-transfer-steps/step-3-sensitivity-review/

Thompson, E. D., & Kaarst-Brown, M. L. (2005). Sensitive information: A review and research agenda. *Journal of the American Society for Information Science and Technology, 56*(3), 245–257. https://doi.org/10.1002/asi.20121

TOMES Project. (n.d.). *Transforming online mail with embedded semantics*. https://www.dncr.nc.gov/tomes/20181127-tomessoftwareoverview/download

Tough, A. G. (2018). The scope and appetite for technology-assisted sensitivity reviewing of born-digital records in a resource-poor environment: A case study from Malawi. In P. Ngulube (Ed.), *Handbook of Research on Heritage Management and Preservation* (pp. 175–182). IGI Global. https://doi.org/10.4018/978-1-5225-3137-1.ch009

US Department of Justice. (2023). *Summary of Annual FOIA Reports for Fiscal Year 2022.* https://www.justice.gov/oip/page/file/1581856/dl?inline=

Wadsworth, C., Vera, F. & Piech, C. (2018, June 30). *Achieving fairness through adversarial learning: an application to recidivism prediction*. arXiv. https://doi.org/10.48550/arXiv.1807.00199

Whyte, J., & Walsh, T. (2024). Carefully and cautiously: How Canadian cultural memory workers review digital materials for private and sensitive information. *The Canadian Journal of Library and Information Practice and Research, 19*(1), 1–26. https://doi.org/10.21083/partnership.v19i1.7180

Yıldırım, A., & Şimşek, H. (2021). *Sosyal bilimlerde nitel araştırma yöntemleri* [Qualitative research methods in social sciences] (12th ed.). Seçkin Yayıncılık.

Yin, R. K. (1994). *Case study research: Design and methods* (2nd ed.). Sage Publications.

Appendix-1

Interview Form

Demographic Questions	
1	What is your name and surname?
2	What is your educational status and field/profession (please indicate if there is a continuing education in addition to the education you have completed)?
3	Which institution and unit do you work (how many years have you been working in this institution)?
4	How many years have you completed in your professional life?
Interview Questions	
1	Do you think that the catego ries of sensitive information in information legislation are sufficient? Please expand. Are there categories/context of sensitivity that exist outside the specified categories in legislation?
2	Which approach should be taken for the identification and scope of sensitive information? Please give examples.
3	What approach should be implemented regarding public records containing sensitive information and the sensitivity review process? Please give examples.
4	How is the evaluation process for sensitive information contained in paper and digital records carried out? If there are differences, in which aspects? Please give examples.
5	What difficulties may be experienced during the sensitivity review process? Please give examples. Are these challenges similar for paper and digital records?
6	How can sensitivity review be conducted objectively, independent of personal perspective and experience? Please give examples.
7	Can records lose or gain sensitivity over time? What kind of solution can be implemented to tackle the above issue? Please give examples.
8	What is the role of "context" within the sensitivity process? Please give examples.
9	What are your views on mosaic sensitivities? What measures can be taken in this regard? Please give examples.
10	What factors should be taken into consideration when national archives form advisory committees on national records and archives that have a remit to advise on topics such as sensitivity records? What role can these advisory committees play in the sensitivity review process? Should these advisory committees be independent bodies?
11	What are your views on technology-assisted sensitivity review in general?
12	What are your views on technology-assisted sensitivity review for digital records?
13	Can ethical and legal issues arise when using technology-assisted tools for the sensitivity review process? Please give examples
14	What are your views on the use of technology-assisted tools to aid the processing of FOIA requests for sensitive records? Please give examples.
15	What do you think about the use of auxiliary resources such as manuals and guides in the process of sensitivity review in the public sector?