计算机工程与应用
Computer Engineering and Applications
ISSN 1002-8331,CN 11-2127/TP

《计算机工程与应用》网络首发论文

题目： App 合规性检测综述
作者： 刘晓建，彭玉坤
网络首发日期： 2022-09-30
引用格式： 刘晓建，彭玉坤．App 合规性检测综述[J/OL]．计算机工程与应用．
https://kns.cnki.net/kcms/detail/11.2127.TP.20220929.1427.004.html

App 合规性检测综述

刘晓建，彭玉坤

西安科技大学 计算机科学与技术学院，西安 710054

摘　要：随着 App 使用者数量迅速增长，个人信息主体隐私泄露问题也日渐严重。为此，近年来我国相继出台了有关 App 个人隐私信息安全的相关法律文件，有关部门也相继开展了 App 整治工作，旨在对 App 个人信息的采集、存储和处理等方面进行规范。综述了 App 合规性问题：首先，揭示出我国 App 安全面临的挑战性问题，列举了我国各层次部门颁布的 App 相关法规和政策，并介绍了国家在 App 治理方面推出的相关措施；然后，综述了 App 合规性检测方法，将国内外 App 合规性检测分成 App 隐私政策的完整性检测、一致性检测和可读性检测三类，并从不同维度和切入点对这三类检测方法进行了分析和总结；第三，对国内 App 合规性检测平台及其相应功能进行了整理和分析；最后，提出了 App 合规性检测仍存在的挑战性问题，并展望了未来的发展方向。

关键词：App 合规性检测；隐私政策；完整性；一致性；可读性
文献标志码: A　　**中图分类号**:TP393.08　　DOI：10.3778/j.issn.1002-8331.2206-0453

Review of App compliance detection

LIU Xiaojian, PENG Yukun

College of Computer Science and Technology, Xi’an University of Science and Technology, Xi’an 710054, China

Abstract: With the rapid growth of the number of App users, the privacy disclosure of personal information subjects has become increasingly serious. Therefore, in recent years, China has successively issued relevant legal documents on App personal privacy information security, and relevant departments have also carried out App rectification work to regulate the collection, storage and processing of App personal information. This paper summarizes the compliance problems of App. Firstly, it reveals the challenging problems of App security in China, lists the relevant regulations and policies of App issued by various levels of departments in China, and introduces the relevant measures launched by the state in App governance. Then, the App compliance detection methods are summarized, and the App compliance detection at home and abroad is divided into three categories : integrity detection, consistency detection and readability detection of App privacy policies. The three detection methods are analyzed and summarized from different dimensions and entry points. Third, sorting out the domestic App compliance detecting platform and corresponding functions. Finally, the challenges that still exist in App compliance detecting are proposed, and the future development direction is prospected.

Key words: App compliance detection; privacy policy; integrity; consistency; readability

基金项目：国家自然科学基金(61702408)；陕西省自然科学基金(2017JM6105)；教育部产学协同育人项目(西安四叶草信息安全有限公司“软件安全课程建设和教学资源开发”)；教育部产学协同育人项目(华为技术有限公司“基于 openEuler 的操作系统课程资源开发”)。

作者简介：刘晓建(1971－),男,博士后,副教授,研究方向为 Android App 安全漏洞检测和计算机软件及计算机应用,E-mail: 780209965@qq.com;**彭玉坤**(1998－),男,硕士研究生, CCF 会员，研究方向为 Android App 安全漏洞检测、自然语言处理。

目前我国现存 App 总数已超过 200 万款，App 在为人们带来便利的同时，也带来了诸多安全性问题，特别是 App 强制授权、过度索权、超范围收集个人信息等现象普遍存在。隐私泄露事件频发，泄露规模愈演愈烈[1]。国际上，欧盟为全面增强对个人隐私信息的保护，推出了《通用数据保护条例》（GDPR）[2]，并于 2018 年 5 月被强制执行；美国联邦贸易委员会提出了公平信息实践五原则（FIPP，Fair Information Practice Principles）[3][4]，即“告知”（Notice）、“选择”（Choice）、“可访问性”（Access）、“安全”（Security）和“实施”（Enforcement）。近年来我国也出台了一系列法规政策，旨在规范个人信息控制者在收集、存储、使用、共享、转让、公开披露等信息处理环节中的相关行为，来遏制个人信息非法收集、滥用、泄漏等乱象，最大程度地保障个人的合法权益和社会公共利益[5]。

为保护个人信息权益、规范个人信息处理活动，一系列的法律法规和行业规范相继出台[6]。这些法规政策也为监管机构提供了合规性监管依据。目前，我国的 App 监管单位主要包括中华人民共和国工业和信息化部（简称工信部）、中华人民共和国国家互联网信息办公室（简称网信办）、国家市场监督管理总局（简称市监局）以及中华人民共和国公安部（简称公安部），这些部门有权通告、下架违法违规的 App。我国 App 数量也由 2018 年的 421 万款下降到 2021 年的 252 万款，可以看出国家对 App 违规行为采取零容忍态度[7]。

隐私政策是附加在一个 App 中的、关于该 App 如何收集、管理、使用、披露个人信息主体数据的声明[8]，它是个人信息安全保护的“第一道防线”，必须满足法规政策中对 App 隐私政策的相关要求。一个 App 的隐私政策应单独成文、易于阅读、易于访问、并对敏感信息应给出显著标识[9]。然而，App 隐私政策往往规范化程度较低、侵权风险高，App 隐私政策的完整性问题、一致性问题和可读性问题仍是 App 合规的主要挑战性问题。

为了更全面地认识 App 合规性检测问题，为 App 监管部门提供技术和工具支撑，本文对 App 合规性相关研究展开综述。首先介绍了 App 法规政策和技术文献的来源；其次在法律层面和 App 市场治理层面，分析了法规政策间的引用关系、各层次部门间的隶属关系和法规政策对 App 的合规要求；然后在技术层面，将 App 合规性检测方法分成隐私政策的完整性检测、一致性检测和可读性检测三类，对每类的主要检测思路和方法进行分析和总结，按照“性质-维度-切入点”的层次关系提炼出 App 合规性检测方法的体系结构，并以此展开更详细的分析；然后在工具层面，整理出 7 个国内主要的 App 合规性检测平台，包括其网址和检测重点。最后总结了 App 合规性检测仍存在的挑战性问题，并展望了未来 App 合规性研究的发展方向。

1 资料来源

App 相关法规政策的资料来源主要为工信部、网信办、市监局、中国信通院等官方网站，如表 1 所示。通过“App”、“应用程序”、“应用软件”、“隐私政策”、“合规”等关键词，筛选出 60 余部内容与 App 合规相关的法规政策。

表 1 法规政策来源

Table 1 Sources of regulations and policies

名称	网址
中华人民共和国国家互联网信息办公室	http://www.cac.gov.cn
中国信息通信研究院	http://www.caict.ac.cn
中华人民共和国工业和信息化部	https://www.miit.gov.cn
国家市场监督管理总局	https://www.samr.gov.cn
中华人民共和国公安部	https://www.mps.gov.cn
全国信息安全标准化技术委员会	https://www.tc260.org.cn
中国网络安全审查技术与认证中心	https://www.isccc.gov.cn
App 专项治理工作组	https://www.pipchina.cn

在近 5 年的国内外文献中，查找到 App 隐私政策完整性检测相关文献 19 篇（关键词：“完整性”、“integrity”等）；App 隐私政策的一致性检测相关文献 18 篇（关键词：“一致性”、“fidelity”等）；App 隐私政策的可读性检测相关文献 16 篇（关键词：“可读性”、“readability”等），文献来源分布如表 2 所示。

表 2 文献来源

Table 2 Literature resources

地区	来源	数量（篇）
国内	北大核心、CSSCI、CSCD	11
	其他核心（如通信技术等）	4
	学位论文（如北京邮电大学等）	5
国外	IEEE	13
	SCI	5
	顶级会议	5
	其他期刊、会议（如 SAGE 期刊、IFIP 会议）	5

2 我国颁布的 App 合规性相关法规政策

为保护个人隐私安全，规范个人信息控制者在收集、存储、使用、共享等信息处理环节中的相关行为，国家陆续出台相关法规政策，统筹发展和安全，推动数据安全建设，加强个人信息保护[10]。列举了我国近 5 年来各层次部门颁布的主要法规政策，如表 3 所示。

表 3 颁布的 App 相关法规政策

Table 3 Regulations and policies promulgated for Apps

颁布时间	颁布政策
2018 年	电信和互联网用户个人信息保护白皮书
2019 年	App 安全认证工作的公告、互联网个人信息安全保护指南、App 违法违规收集使用个人信息自评估指南、App 收集个人信息基本规范（草案）、数据安全管理办法（征）、工信厅网安 42 号、国信办秘字 191 号、中央网信办公告 2019 年第 1 号、工信部信管函 337 号、软件开发包（SDK）安全与合规白皮书、CNCA-App-001
2020 年	软件开发包（SDK）安全与合规报告、工信部信管函 164 号、个人信息告知同意指南（征）、GB/T 35273-2020、CNCA-20-18、TC260-PG 系列（20202A-20205A）、T/TAF 077 系列（077.1-077.8）、T/TAF 078 系列（078.1-078.10）
2021 年	软件开发包（SDK）安全研究报告、网络数据安全管理条例（征）、App 个人信息保护治理白皮书、国信办秘字 14 号、工信部信管函 292 号、TTAF 077 系列（077.9-077.17）、GB/T 40652-2021
2022 年	互联网信息服务深度合成管理规定（征）、移动互联网应用程序信息服务管理规定、信安秘字 112 号、网信办第 18 号公告、关于进一步规范移动智能终端应用软件预置行为的通告（征）、移动互联网应用程序个人信息保护管理暂行规定（征）、GB/T 41391-2022

注：1.收集截止时间为 2022 年 6 月 15 日；2.“征”代表征求意见稿

2021 年之前我国 App 安全相关的政策体系是以《网络安全法》为核心，其他规章政策紧紧围绕而形成的。2021 年后我国陆续颁布了《数据安全法》和《个人信息保护法》，逐渐形成了以《个人信息保护法》为核心的 App 安全政策新体系。本文归纳出部分法规政策之间的引用关系，如图 1 所示。

图 1 法规政策引用关系

Fig.1 Regulations and policies reference relationship

国家近年来对个人信息保护进行了前瞻性战略部署，开展了系统性的顶层设计。我国发布法规政策的执法机构具有层次关系，已形成较成熟的管理结构[11]。本文整理出颁布 App 相关法规政策所属部门的主要层次结构，如图 2 所示。全国人大及其常委会制定法律，其效力最高（如《网络安全法》、《数据安全法》等）。国务院制定的行政法规，是为落实法律要求而提出的规范性要求。国务院下的工信部、网信办等部门、机构及下属的机构、单位、组织根据行政法规，提出指导性要求与结合实际的指导意见等。

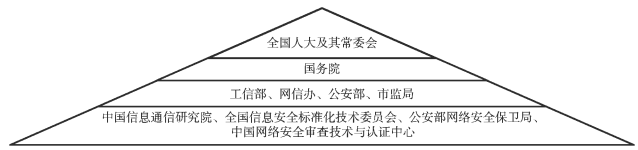

图 2 颁布 App 相关政策的部门层次结构

Fig.2 The departmental structure of promulgated App policies

本文在收集的法规政策中通过查找“合规”、“合法”、“违规”、“违法”等关键词，对法规政策进行筛选，并总结出 App 合规的主要要点，如图 3 所示。

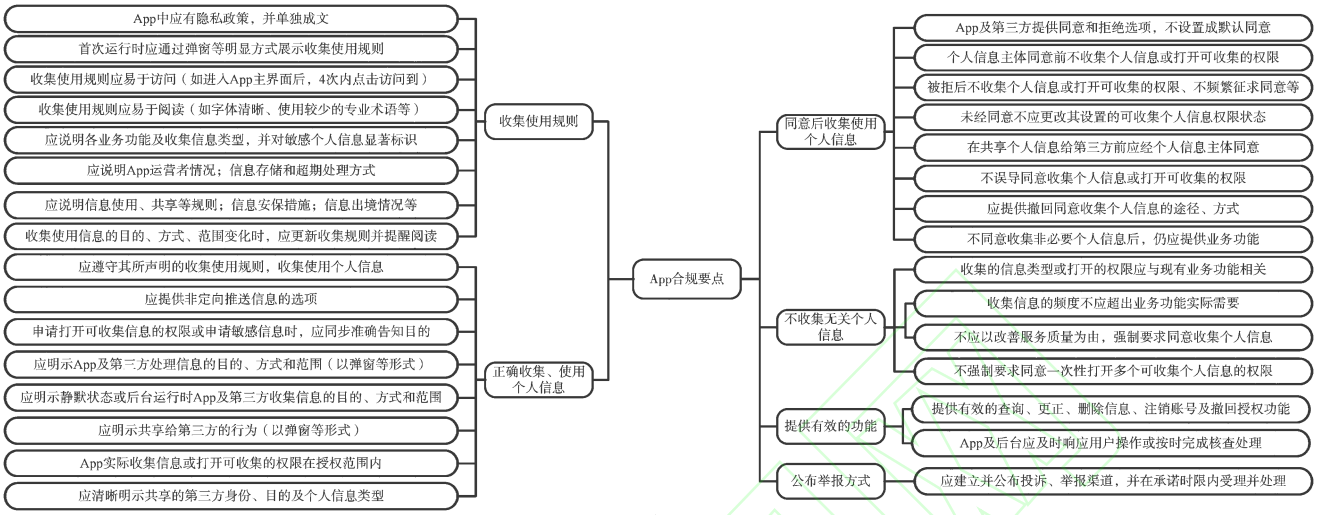

图 3 App 合规主要要点

Fig.3 Main points of App compliance

3 从技术角度检测 App 合规性问题

通过阅读国内外有关 App 合规性检测的文献，将 App 合规性检测方法划分成了三个类别，即 App 隐私政策的完整性检测、一致性检测和可读性检测。到目前为止，隐私政策的完整性检测和隐私政策的一致性检测还没有公认的定义，不同文献中有不同的理解和侧重点，本文采用集合论尝试给出完整性和一致性的数学定义，并辅以例子来诠释完整性和一致性内涵，如图 4 所示。

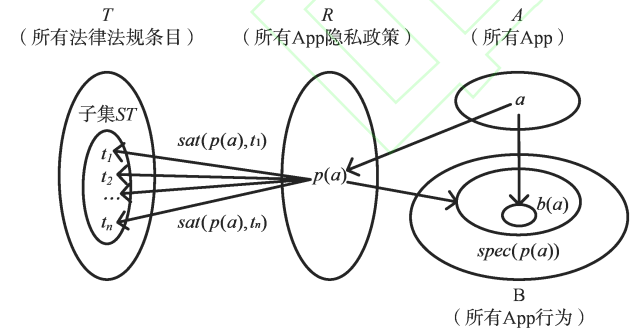

图 4 完整性检测和一致性检测

Fig.4 Integrity detection and consistency detection

设 T 表示一个法律法规文件或国标文件，其中定义了若干 App 隐私政策应满足的条目。因此，可以把 T 定义为如下有限集，即

$$T=\{t_1,t_2,\cdots,t_n\}$$

其中 $t_i(1\le i\le n)$ 为用自然语言描述的、App 隐私政策应满足的条目。

便于讨论起见，定义如下四个域：

T：所有法律法规文件中规定的条目的集合；

A：所有 App 的有限集；

R：所有 App 隐私政策的有限集；

B：所有 App 行为的有限集，其中的一个元素表示一个 App 的行为集合。

设 $a:A\to R$ 和 $b:A\to B$ 为两个函数，它们分别把一个 App $a\in A$ 映射到其隐私政策和行为集合，即 $p(a)\in R$，$b(a)\in B$。

通常讨论一个 App 的完整性时，总是针对一个具体的条件集合。为此，令 $ST\subseteq T$ 是 T 的一个子集，其中的元素（即条件）必须是逻辑相容的，即相互不矛盾的。

定义 1（完整性）一个 App $a\in A$ 如果满足如下条件，则称 a 关于一组条目 ST 是“完整的”：

$$\forall t\in ST.sat(p(a),t),$$

其中，$sat(p(a),t)$ 是一个谓词，表示 a 的隐私政策满足条目 $t\in ST$ 所指示的要求。

由于 $p(a)$ 是用自然语言描述的隐私政策，t 也是用自然语言描述的条目，因此判断谓词 $sat(p(a),t)$ 是否为真，需要借助自然语言分析技术。

定义 2（一致性）一个 App $a\in A$ 如果满足如下条件，则称其隐私政策与其行为是一致的：

$$b(a)\subseteq spec(p(a)),$$

其中，$spec(p(a))$ 表示 a 的隐私策 $p(a)$ 所约定的 a 的行为空间。

简单来说，$b(a)\subseteq spec(p(a))$ 表示“a 的实际行为不应超过 a 的隐私政策 $p(a)$ 所约定的行为范围”，即 a 的实际行为是隐私政策规约的“精化”（Refinement）。但是在实际检测中，如何定义 App

的“行为”和隐私政策所约定的“行为”却是一个开放的问题。如果从程序的形式语义角度来理解“行为”，程序行为通常被定义为从程序初始状态开始的由状态迁移构成的序列的集合，然而 App 的隐私政策是文字描述，因此无法对二者直接进行比较。因此，要检测 App 的一致性问题，需要对“行为”做出明确的解释，并采用特定的方法从程序和隐私政策中抽象出二者的行为，才能进行比较和判断。不同研究工作所采取的具体方法见后面 3.2 节所述。

下面以一个具体例子来说明上述定义。令 T 代表《信息安全技术 个人信息安全规范》（以下简称《规范》），其中规定了若干隐私政策应满足的条目。假如 t_1 代表其中的一个条目，即“业务功能需要依赖部分信息才得以运行，我们需要收集的必要信息包括：…”；某 App 对应隐私政策 $p(a)$ 内容包括“如果您注册成为我们的会员，您需要提供手机号或我们支持的第三方账号进行登录，便于我们为您提供服务”。通过自然语言处理等技术，判断出谓词 $sat(p(a),t_1)$ 为真，即该 App 的隐私政策满足条目 $t_1 \in ST$ 所指示的要求；当满足子集 ST 的 n 个要求后，称该 App 关于一组法律法规的条目 ST 是“完整的”。

再如，某 App 对应隐私政策 $p(a)$ 内容包括“我们不会收集您的个人信息，如地理位置信息、…”；通过对 a 的程序行为进行分析，发现其程序中存在“android.location.LocationManagergetLastknownLocation()”即获取位置信息，显然 App 的实际行为 $b(a)$ 不再是隐私政策声明的行为空间 $spec(p(a))$ 的子集，也就是超出了该 App 的隐私政策所约定的行为范围。因此可以判定该 App 的隐私政策与行为是不一致的。

某 App 的隐私政策（如 $p(a)$）易于阅读和易于理解的程度，通常被称为 App 隐私政策的可读性[12]。本文对这三类研究方法进行了总结，如表 4 所示。同时本文仅关注移动设备端 App 的合规要点，暂不考虑 App 后端服务处理个人信息的行为。

表 4　App 合规性检测的三个类别

Table 4　Three categories of App compliance detection

划分类别	App 隐私政策的完整性检测	App 隐私政策的一致性检测	App 隐私政策的可读性检测
涉及文献	文献[12-28]	文献[29-48]	文献[49-75]
解决方法	通常用机器学习、自然语言处理、文本分析、内容分析等方式提炼出法规政策条目的要点后，与 App 隐私政策做对比，完成完整性检测	通常用静态检测、动态检测等技术得到 App 的实际行为后，与隐私政策对应声明内容进行一致性对比	衡量 App 隐私政策的可读性通常会用到公式法（中文可读性公式、英文可读性公式）

通过对相关文献的通读，按照“性质-检测维度-主要切入点”的层次结构，本文提炼出 App 合规性的检测体系，如图 5 所示。App 隐私政策的完整性检测通常依据法规政策的要点分类和要点框架，来检测 App 隐私政策的具体条目是否符合对应要点；App 隐私政策的一致性检测通常把 App 实际行为（数据流、API、权限）和 App 隐私政策放在同一个域中，检查 App 实际行为是否为 App 隐私政策的一个子集，从而实现一致性检测；App 隐私政策的可读性检测通常利用公式计算出的可读分数，来评估 App 隐私政策的可读性，本文将按照英文可读性公式和中文可读性公式展开阐述。

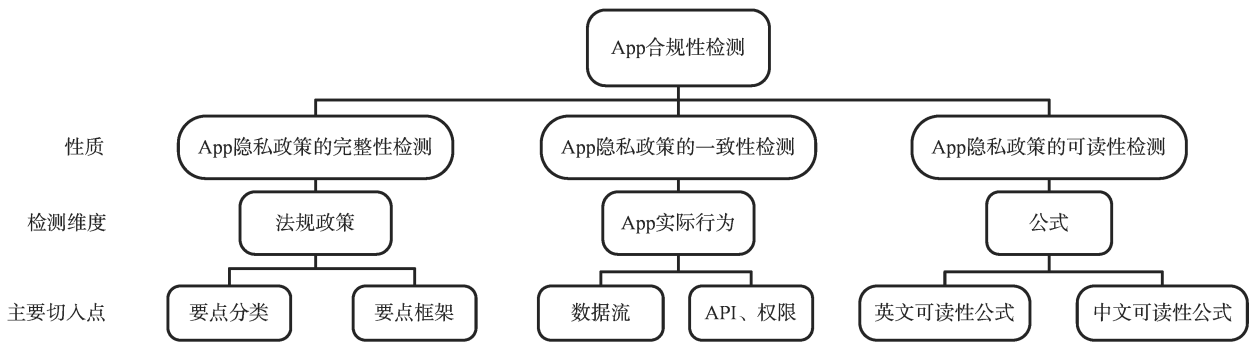

图 5　App 合规性检测体系

Fig.5　App compliance detection system

3.1 App 隐私政策的完整性检测

完整性检测方法主要采用文本分析法、内容分析法、问卷调查法来分析 App 的隐私政策[13]，也常用机器学习等方式对 App 的隐私政策文本进行分类。在 19 篇 App 隐私政策的完整性检测文献中，6 篇利用机器学习，4 篇使用文本分析，3 篇采用问卷调查，2 篇计算要点权重，2 篇使用内容分析法，2 篇使用其他方法。完整性检测文献分布如图 6 所示。App 隐私政策的完整性所对比的国外标准法规政策通常为 GDPR，或早期美国联邦贸易委员会提出的 FIPP；对比的国内法规政策通常为《规范》。

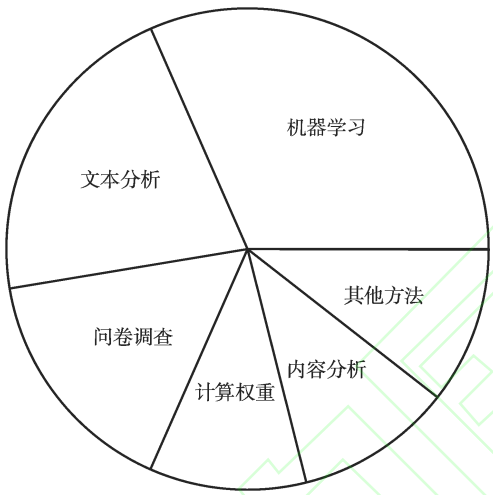

图 6 完整性检测文献分布

Fig.6 Literature distribution of integrity detecting

同时给出 App 隐私政策完整性检测的衡量指标，如表 5 所示，可以看出大部分文献仍以应有要点（法律法规条目的抽象）作为衡量指标，部分文献的直接衡量指标不是应有要点，但都是以要点为基础，通过一系列操作，得到的更加直观的衡量指标。

表 5 完整性检测的衡量指标

Table 5 Measurement index of integrity detection

文献	衡量指标
张艳丰等[13]	灰色加权关联度
Torre 等[14][15]	识别元数据的精确度（precision）、召回率（recall）
M ü ller 等[16]	合规率（compliance ratios）
Fan 等[17]	标签数
朱璋颖等[18]	隐私政策评分 E
朱侯等、赵波等[20]	CR 值（克隆巴赫 Alpha 系数）
姚胜译等[22]	内容可读性得分
张艳丰等、苗慧等、Verderame 等、Sun 等、徐磊等[23]、杜永欣等[24]、唐远清等[25]、马骋宇等[26]、何培育等[27]、姜盼盼等[28]	应有要点

3.1.1 要点分类

通过机器学习等技术，将具体条目抽象出几个要点并分类，根据分类结果检测 App 隐私政策的完整性，本文将这种检测依据统称为要点分类。Torre 等[14][15]利用机器学习等技术识别隐私政策要点。该方法共分五步：前两步对隐私政策文本进行预处理、概括并把句子转换为向量表示；步骤 3-5 使用三种方法对句子分类，将隐私政策的句子分类成一种或多种要点类型；再基于分类结果对隐私政策的句子进行要点类型预测；最后通过给定句子的上下文要点类型，完成后期处理。整个步骤如图 7 所示。将得到的隐私政策要点与 GDPR 要点进行对比，实现 App 隐私政策的完整性检测。

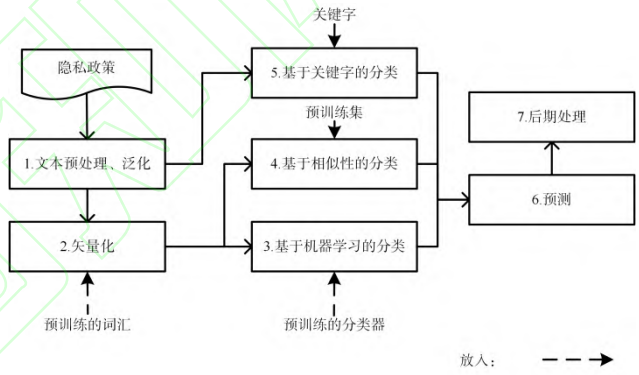

图 7 隐私政策要点识别

Fig.7 Key points identification of privacy policy

利用分类器对 App 隐私政策应有要点进行分类之后，可以根据分类结果检测 App 隐私政策的完整性。M ü ller 等[16]和 Fan 等[17]根据 GDPR 利用分类器训练出 App 隐私政策应包含的类别，并与 GDPR 进行对比以检测 App 隐私政策的完整性。朱璋颖等[18]根据《规范》建立了基于机器学习算法的层次多标签分类模型，能够根据分类结果完成 App 隐私政策的完整性检测。其完整性检测的准确率较高，检测结果显示，App 普遍存在隐私政策不完整的情况，其中缺少个人信息超期处理方式的情况尤为严重。

在进行 App 隐私政策完整性检测时，对比的法律法规文件并非只有 GDPR 和《规范》，如 Verderame 等[19]通过 3PDroid 工具对 App 隐私政策进行完整性检测时，对比的标准是 Google Play 隐私准则。3PDroid 可检测页面是否包括 App 隐私政策，涉及的部分代码如表 6 所示。3PDroid 还可判断 App 隐私政策是否包含所有敏感信息的声明条例，进而验证 App 隐私政策是否满足 Google Play 对敏感信息的声明要求。

表 6 隐私政策的页面检测

Table 6 Page detection of privacy policy

```
textContent ← extractFromXML (xmlContent);//从页面的 xml 中提取文本内容
preprText ← dataPreprocessing (textContent);//删除非 ASCII 字符
detected ← MLPClassifier.isPolicyPage (preprText);//检测文本是否为隐私政策
```

3.1.2 要点框架

在进行 App 隐私政策的完整性检测时，将具体条目抽象、提炼成几个一级要点及更详细的二级要点，并以这样的框架（体系）作为完整性的检测依据。本文将这种类似框架（体系）的检测依据称为要点框架（体系），使用完整的要点框架能更全面地检测 App 隐私政策的完整性。根据《规范》，赵波等[20]建立的 App 个人信息安全量化评估模型，和张艳丰等为要点框架里的具体要点赋予了权重，可通过计算权重得知 App 隐私政策的完整程度。

Sun 等[21]和姚胜译等[22]参考了 GDPR，并使用问卷调查的方式建立 App 隐私政策完整体系，姚胜译还根据《规范》来检测 App 隐私政策是否公开发布且易于访问。朱侯等参考的是 FIPP，通过问卷调查的方式构建了 App 隐私政策要点体系，并以此检测 App 隐私政策的完整情况。

在 App 隐私政策的完整性检测中，通常使用文本分析方法。苗慧等根据《规范》等政策对中外 App 隐私政策进行文本分析并建立了 App 隐私政策要点框架。基于《规范》，徐磊等[23]利用文本分析的方式，对不同的 App 分析出各自隐私政策框架；杜永欣等[24]基于文本分析出 App 隐私政策应有的 11 个要求，从而建立完整性框架以供检测。App 隐私政策的完整体系应具有层次关系，以唐远清等[25]依据《网络安全法》和 GDPR 建立的 App 隐私政策框架为例，其体系结构如图 8 所示。

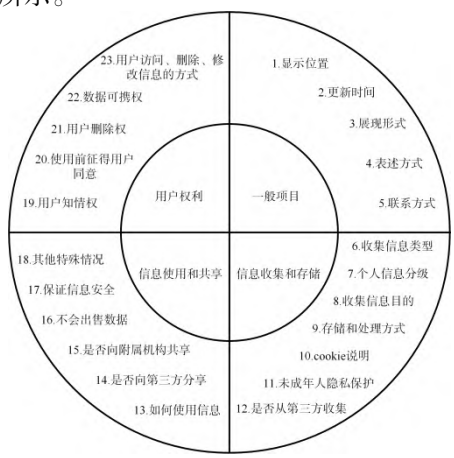

图 8 隐私政策的完整组成部分

Fig.8 The complete part of privacy policy

基于《规范》，张艳丰等利用内容分析法检测 App 隐私政策在各个指标的符合程度，马骋宇等[26]利用内容分析法构建出基于数据生命周期的 App 隐私政策评价体系完成完整性检测。此外还有其他方法可用于 App 隐私政策的完整性检测。基于《规范》，何培育等[27]利用实证考察法对比 App 隐私政策各方面完整性，并给出优化隐私政策条款设计、加强合法性监督和落实隐私政策违法行为的责任等建议；姜盼盼等[28]从便于个人信息主体的角度出发，给出包含 8 个要点的隐私政策框架。

本文归纳出检测 App 隐私政策完整性时有针对性的部分文献，如表 7 所示。

表 7 完整性检测针对的类别

Table 7 Integrity detection for categories

文献	检测类别
张艳丰等[13]	移动阅读类 App 隐私政策
Fan 等[17]	移动健康类 App 隐私政策
徐磊等[23]	图书类 App 隐私政策
杜永欣等[24]	网站类隐私政策
朱侯等、唐远清等[25]	社交媒体类 App 隐私政策
马骋宇等[26]	移动健康类 App 隐私政策
何培育等[27]	Web 浏览器类隐私政策
姜盼盼等[28]	图书馆类隐私政策

3.2 App 隐私政策的一致性检测

App 隐私政策的一致性检测通常会分别对隐私政策和 APK 文件进行分析，通过 NLP、机器学习等文本分析技术提取出隐私政策中对行为功能的描述，并利用静、动态等分析技术得到 App（及 SDK）的实际行为（数据的流向、调用的 API、申请及使用的权限等），最后对比二者来完成 App 隐私政策的一致性对比，如图 9 所示。

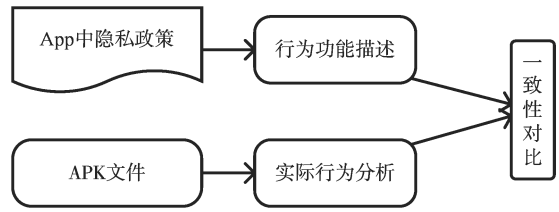

图 9 App 隐私政策的一致性检测

Fig.9 Consistency detection of App privacy policy

不同的工作在分析 App 实际行为时的侧重点不同，部分工作侧重于数据流的一致性检测，还有部分工作侧重于 API、权限的一致性检测。因此在进行 App 隐私政策的一致性时，需要将对比的两个本体放入同一个域中进行比较，也就是检测 App 的实际行为是否为 App 隐私政策声明行为的子集。本文归纳出文献对

应的 App 实际行为检测重点及检测范围，如表 8 所示，后文将详细阐述各文献的检测重点。通常用检测重点为基础的隐私政策或 App 不一致数量（或百分比），作为 App 隐私政策的一致性的衡量指标。

表 8 一致性的检测重点

Table 8 Focus of consistency detection

文献	实际行为的检测重点（范围）
Verderame 等[19]	API（第一方、第三方）、权限（第一方）
Andow 等[32]	数据流（第一方、第三方）
Fan 等、Yu 等[33]	数据流（第一方）
Kununka[34]	数据流（第三方）
Olukoya 等[35]、Yu 等[36][37]、Feng 等、Wang 等[38]	权限（第一方）
Slavin 等、贺雪乔[39]	API（第一方、第三方）
胡杰克等[41]	API（第一方）、权限（第一方、第三方）
王靖瑜等[42][43]	权限（第一方、第三方）
Zhang 等[44]、杜代忠[47]	API（第三方）

3.2.1 分析数据流

在进行 App 隐私政策一致性对比时，将对比的域放在数据流上，通过检查 App 实际的数据流是否为 App 隐私政策声明对应的数据流的子集，从而完成一致性检测。本文将这种把对比的域放在数据流上的检测方式称为分析数据流。

常用 FlowDroid[29]和 VulHunter[30]等基于静态分析的数据流分析工具，通过数据的流向来得知 App 如何操纵数据，进而可得知 App 隐私政策所声明的内容与 App 实际收集、使用的数据是否吻合。Fan 等利用 word2vec[31]将 App 隐私政策内的名词短语转换为可计算形式，并计算余弦相似度筛选出收集、使用数据的语句。同时利用 FlowDroid 和 VulHunter 等工具对 App 内的数据流进行分析，得到实际收集、使用的数据，对比 App 隐私政策筛选出的语句完成一致性检测。

Andow 等[32]提出了一个高精度的一致性分析模型 POLICHECK，用于比较 App 数据流和 App 隐私政策声明内容，并区分了第一方和第三方的数据流，来确定 App 是否正确地披露其隐私敏感行为；Yu 等[33]开发的 PPchecker 用于检测数据的收集、存储、使用；Kununka[34]等检测传输给第三方的数据，都是基于数据流检测，进而与 App 隐私政策做一致性对比。

3.2.2 分析 API、权限

在进行 App 隐私政策一致性对比时，将对比的域放在 API、权限上，通过检查 App 实际的 API、权限是否为 App 隐私政策声明对应 API、权限的子集，进而完成一致性检测。本文将这种把对比的域放在 API、权限上的检测方式称为分析 API、权限。

Olukoya 等[35]利用静态分析获取 App 实际请求的权限，并利用 NLP 技术将其转换成文本形式与对应的描述进行对比；Yu 等[36][37]开发出基于静态分析的 TAPVerifier 框架，利用 App 的隐私政策和其字节码，逐步加强了描述和权限的一致性检测效果；Wang 等[38]开发了 SmartPI 框架，从个人信息主体评论中推出 App 使用的权限，进而和对应描述做对比，这些一致性对比的域都是 App 的权限。贺雪乔[39]结合动静结合的检测方法，将 App 实际调用的敏感 API 和 App 隐私政策对比，完成一致性检测，对比的域是 API。

App 中往往集成了不少的第三方 SDK，因此 SDK 实际的行为功能（权限、API 等）是否符合 App 隐私政策的要求，同样是 App 隐私政策一致性检测的要素。之前研究工作通常使用白名单方法来检测第三方库，然而白名单方法覆盖率不全，现在通常会用第三方库分析工具，如 LibRadar[40]等。第三方库分析工具是为了得到第三方库使用的 API、权限等信息，进而将对比的域放在第三方库的 API、权限上，实现 App 隐私政策的一致性检测。如胡杰克等[41]和王靖瑜等[42][43]利用 LibRadar 工具分析出第三方 SDK 使到的权限，一致性检测对比的域为第三方 SDK 的权限；Zhang 等[44]利用 LibRadar 检测出第三方 SDK 用到的 API，对比的域为第三方 SDK 的 API，进而实现 App 隐私政策的一致性检测。Verderame 等在 3PDoird 中能够检测 App 及其第三方库的 API 使用是否符合 App 隐私政策的要求，对比的域为 App 和第三方库的 API。

App 行为（如调用的 API、申请的权限等）与文本（如 App 隐私政策对应的描述、短语等）的映射关系，也常被用来检测 App 隐私政策的一致性。Feng 等[45]和 Yu 等[46]利用描述和对应权限的映射关系，得到描述对应的权限后，与 App 分析出的权限做一致性对比，对比的域是 App 的权限，胡杰克和杜代忠[47]将对比的域放在了第三方 SDK 的权限上；Slavin 等[48]把 API 作为对比的域，整理出 API 和 App 隐私政策短语，并建立好 API 和对应 App 隐私政策短语的映射关系，并以此检测 App 隐私政策的一致性。

3.3 App 隐私政策的可读性检测

影响 App 隐私政策可读性的因素不仅包括自身的特征（文本长度、复杂词汇的数量、排版风格、字体大小等），还包括个人信息主体看到和阅读到隐私政策的机会、阅读能力、阅读需求。公式法是目前最常用来衡量 App 隐私政策可读性的方式，可读性公式计算出的分数通常作为 App 隐私政策可读性的衡量指

标。如 *FKGL*[49]公式是 *FRES*[50]公式的改良，利用单词、音节和句子的数量来确定文本的复杂性，分值越高则文本越易于阅读；*GFI*[51]公式使用文本中的单词数和复杂单词来确定文本的难易程度，分值越低则文本越容易阅读；*SMOG*[52]公式通过多音节单词的数量来确定文本的阅读难度[53]，分值越低则文本越容易阅读。不少学者利用 *FRES* 公式、*FKGL* 公式、*GFI* 公式、陈世敏公式[54]等较成熟的公式来评估 App 隐私政策可读性，大部分 App 隐私政策也被证实其可读性不强[55]。本文整理出 16 篇文献依据的隐私政策可读性评估指标，如表 9 所示。可以看出绝大部分工作是以可读性公式作为衡量 App 隐私政策可读性的评估指标，朱侯等把可读性特征作为衡量可读性的指标。

表 9 可读性评估指标

Table 9 Readability assessment indicators

文献	评估指标
朱侯等[4]	字体、行距、小标题数等 10 个指标
苗慧等[12]	陈世敏公式、*FKGL*
Farooq 等[53]	*FRES*、*FKGL*、*SMOG*、*GFI*、*RGL*、词数
Das 等[55]	*RGL*
Yu 等、Redmiles 等[56]	*FRES*
Powell 等[57]	*FRES*、*FKGL* 等 15 项指标
Fowler 等[58]	*FKGL*
秦克飞等[59]	陈世敏公式
王英等[61]	*FKGL*、*FRES*
Robillard 等[62]	*FKGL*、*SMOG*、*GFI*
Javed 等[63]	*FRES*、*FKGL*、词数
Zhang 等[64]	*FRES*、*FKGL*、*GFI*、*SMOG*
Basch 等[65]	*FRES*、*FKGL*、*SMOG*、*GFI*、*CLI*
Krumay 等[66]	*FKGL*、*SMOG* 等 7 项可读性公式
Fabian 等[67]	*SMOG*、*RIX*、*LIX* 等 10 项可读性公式

3.3.1 英文可读性公式

英文类 App 隐私政策可读性的影响因素包括单词和句子长度、词缀数量、音节数等，每个句子的平均单词数和被动语态百分比等。本文整理出 9 个常用的英文可读性公式的计算方式（*FRES*、*LIX*[68]、*NDC*、*FKGL*、*RIX*[68]、*SMOG*、*CLI*[69]、*GFI*、*ARI*[70]），如表 10 所示。

表 10 英文可读性公式

Table 10 English readability formulas

名称	公式
FRES	$FRES = 206.835 - 1.015 \times ASL - 84.6 \times ASW$
LIX	$LIX = ASL + 100 \times LW/words$
NDC	$NDC = 0.1579 \times PDW + 0.0496 \times ASL + 3.6365$
FKGL	$FKGL = 0.39 \times ASL + 11.8 \times ASW - 15.59$
RIX	$RIX = LW/words$
SMOG	$SMOG = 3 + sqrt(CW)$
CLI	$CLI = 5.89 \times characters/words - 30 \times sentences/words - 15.8$
CFI	$CFI = 0.4 \times (ASL + HW)$
ARI	$ARI = 0.5 \times ASL + 4.71 \times ALW - 21.43$

注：*ASL* 为平均句子长度；*ASW* 为每个单词的平均音节数；*LW* 为超过 6 个字符的单词数；*PDW* 为不在 Dale Chall 常用 3000 词列表的词的百分比；*CW* 为含 3 个及以上音节的单词数；*HW* 为文本中难词的比例；*ALW* 为每个词的平均字母数

3.3.2 中文可读性公式

国内也有不少学者开发了中文可读性公式，其中所使用的影响可读性的因素涉及平均笔画数、难字或完全对称字率、特殊词或难词率、句均字或词数等。整理出 6 个中文可读性公式（陈世敏公式、王蕾公式[71]、左虹公式[72]、杨金余公式[73]、郭望皓公式[74]、孙汉银公式[75]），如表 11 所示。

表 11 中文可读性公式

Table 11 Chinese readability formulas

名称	公式
陈世敏	$Y = 0.81 \times A + B$
王蕾	$Y = 72.749 - 0.462 \times C + 0.802 \times D - 7.515 \times E + 2.464 \times F$
左虹	$Y = 23.646 + 0.485 \times G - 125.931 \times H - 0.647 \times E$
杨金余	$Y = 0.95 \times I + 0.975(I + J) + K + L$
郭望皓	$Y = -11.946 + 0.123 \times K + 0.198 \times M + 0.811 \times N$
孙汉银	$Y = -7.00685 + 14.34587 \times O - 2.13791 \times H - 3.38799 \times A + 4.00371 \times P$

注：*Y* 为中文可读性分数；*A* 为每句平均字数；*B* 为难字百分比；*C* 为总词数；*D* 为简单词数；*E* 为虚词数；*F* 为分句数；*G* 为甲级字数；*H* 为难词比；*I* 为平均每百字丙级、丁级、超纲字数；*J* 为平均每百字固定词组数；*K* 为平均句长；*L* 为平均每百字丙级以上语法项目数；*M* 为汉字难度；*N* 为词汇难度；*O* 为平均笔画数；*P* 为句均词数

4 App 合规性检测平台

为了更便利、更全面地从多个角度对 App 进行合规性检测，本文收集和整理了 App 合规性检测平台网址和对应的功能，如表 12 所示。这些 App 合规检测平台主要根据国家颁布的各种法规政策，来检测 App 的隐私政策是否符合对应要点的要求，也就是检测 App 隐私政策的完整性。其中存在个别平台还可以检测 App 实际行为和 App 隐私政策声明内容是否一致，

即检测 App 隐私政策的一致性，如阿里云 App 合规监　　测平台。

表 12　App 合规性检测平台及功能

Table 12　App compliance detecting platforms and functions

App 合规性检测平台（网址）	功能
史宾格安全及隐私合规平台 https://mtc.baidu.com/privacy	根据工信部信管函 164 号等法规政策，可检测 App 隐私政策的完整性
爱加密 https://www.ijiami.cn/personalinformation	根据 GB/T 35273-2020 等检测标准，可检测 App 隐私政策的完整性
娜迦科技 http://www.nagain.com	根据 GB/T 35273-2020 等检测标准，可检测 App 隐私政策的完整性
三六零天御 https://jiagu.360.cn/#/global/details/privacy	根据《App 违法违规收集使用个人信息行为认定方法》等规定，可检测 App 隐私政策的完整性
T-Sec 应用合规平台 https://cloud.tencent.com/product/acp	根据法律法规、国家标准等，可检测 App 隐私政策的完整性
盘古 Janeus https://www.Appscan.io	根据国信办秘字 191 号等法规政策，可检测 App 隐私政策的完整性
阿里云 https://www.aliyun.com/activity/security/app_privacy	根据国家相关法律法规及行业规范，可检测 App 隐私政策的完整性和一致性

5　结束语

在安装 App 时，App 往往会要求用户授权，个人信息主体往往不愿意泄露敏感信息，从而存在严重的个人隐私泄漏隐患[76]。因此从管控和技术两部分出发，对国家施行的 App 治理防护措施和 App 合规检测方法进行了归纳总结。对该领域的研究成果进行了回顾，App 合规性检测虽取得了一定的进展，但很多方面需要进一步探索，尤其是国内以“App 合规性检测”为主题的文献寥寥无几。因此针对 App 的合规性检测仍存在以下几个挑战性问题值得广大学者继续研究：

（1）如何加强对法规政策中合规要点的提取。目前国内尚未出台包含 App 及 App 隐私政策应具有的完整合规要点的法规政策，但在不同法规政策中陆续出现对不同类别 App 的合规要求。因此需要按照不同类别，在法规政策中提取对应的合规要点。未来的研究者仍需要继续探索基于机器学习的文本提取、文本分类、文本一致性对比等技术。

（2）如何构建全面的语料库。分类建立与法规政策中要点语义相同的语料库，可通过要点匹配的方式检测 App 隐私政策是否完整。因此如何建立语义更全面的词库，实现更高的检测精度，将会是未来的发展方向。

（3）如何结合多种检测方法对 App 进行检测。恶意 App 的检测包括静态检测快速初检、动态检测运行时监测、基于网络数据检测云端检测。当前动静结合的检测方法已取得一定成功，这种检测方式仍是未来普遍认同的发展方向。

（4）如何多样化度量 App 隐私政策的可读性。App 隐私政策可读性往往使用公式法，或利用语言表层要素进行评估。未来会更多地运用到机器学习、深度学习、增强学习、眼动仪等实验法对文本的可读性进行评定。

参考文献：

[1] 魏立斐,李梦思,张蕾,陈聪聪,陈玉娇,王勤.基于安全两方计算的隐私保护线性回归算法[J].计算机工程与应用,2021,57(22):139-146.

WEI L F, LI M S, ZHANG L, CHEN C C, CHEN Y J, WANG Q. Privacy-Preserving linear regression algorithm based on secure Two-Party computation[J]. Computer Engineering and Applications, 2021, 57(22): 139-146.

[2] VOIGT P, VON DEM BUSSCHE A. The eu general data protection regulation (gdpr)[J]. A Practical Guide, 1st Ed., Cham: Springer International Publishing, 2017, 10(3152676): 10.5555.

[3] 市场化个人征信行业个人信息保护问题分析[EB/OL].[2022].https://www.creditchina.gov.cn/home/lfyj/202107/t20210714_239446.html.

Analysis of personal information protection in marketized personal credit reference industry[EB/OL]. [2022]. https://www.creditchina.gov.cn/home/lfyj/202107/t20210714_239446.html.

[4] 朱侯,张明鑫,路永和.社交媒体用户隐私政策阅读意愿实证研究[J].情报学报,2018,37(04):362-371.

ZHU H, ZHANG M X, LU Y H. An empirical study on privacy policy reading intention of social media users[J]. Journal of the China Society for Scientific and Technical Information, 2018, 37(04): 362-371.

[5] 信息安全技术个人信息安全规范[EB/OL]. [2022]. https://ansafe.xust.edu.cn/DownLoad/2020SafeInstruction.pdf.

Personal information security specification[EB/OL]. [2022]. https://ansafe.xust.edu.cn/DownLoad/2020SafeInstruction.pdf.

[6] 中华人民共和国个人信息保护法[EB/OL]. [2022]. http://fsga.foshan.gov.cn/attachment/0/224/224359/5099735.pdf.
Personal information protection law of the People's Republic of China full translation[EB/OL]. [2022]. http://fsga.foshan.gov.cn/attachment/0/224/224359/5099735.pdf.
[7] 灵鲲 App 隐私合规产品白皮书[R/OL].[2022].https://max.book118.com/html/2021/1015/5244022313004031.shtm.
Lingkun App privacy compliance product white paper[R/OL]. [2022]. https://max.book118.com/html/2021/1015/5244022313004031.shtm.
[8] 张艳丰,邱怡.硬规则下我国移动阅读 App 隐私政策合规性研究[J].现代情报,2022,42(01):167-176.
ZHANG Y F, QIU Y. Research on compliance of privacy policy of mobile reading App in China under hard rules[J]. Journal of Modern Information, 2022, 42(01): 167-176.
[9] 移动互联网应用程序(App)收集使用个人信息自评估南[EB/OL].[2022].https://www.tc260.org.cn/front/postDetail.html?id=20200722134829.
Mobile Internet application(App)collection and use of personal information self-assessment guide[EB/OL]. [2022]. https://www.tc260.org.cn/front/postDetail.html? id=20200722134829.
[10] 中华人民共和国数据安全法[EB/OL].[2022].https://gkml.samr.gov.cn/nsjg/bgt/202111/t20211105_336461.html.
Data security law of the People's Republic of China[EB/ OL]. [2022].https://gkml.samr.gov.cn/nsjg/bgt/202111/t20211105_336461.html.
[11] 我国 197 项数据安全政策回顾汇总[EB/OL]. [2022]. http://www.ciphergateway.com/product/40738.html.
Summary of 197 data security policies in China[EB/OL]. [2022].http://www.ciphergateway.com/product/40738.html.
[12] 苗慧.中外移动 App 的个人信息保护研究[D].北京:北京邮电大学,2021.
MIAO H. Research on personal information protection of Chinese and foreign mobile Apps[D]. Beijing: Beijing University of Posts and Telecommunications, 2021.
[13] 张艳丰,邱怡.我国移动阅读应用个人信息保护政策合规性测度研究[J].图书情报工作,2021,65(22):9.
ZHANG Y F, QIU Y. Research on compliance measurement of personal information protection policy for mobile reading application in China[J]. Library and Information Service, 2021,65(22):9.
[14] TORRE D, ABUALHAIJA S, SABETZADEH M, et al. An AI-assisted approach for checking the completeness of privacy policies against GDPR[C]//2020 IEEE 28th International Requirements Engineering Conference(RE). IEEE, 2020.
[15] AMARAL O, ABUALHAIJA S, TORRE D, et al. AIenabled automation for completeness checking of privacy policies[J]. arXiv preprint ar-Xiv:2106.05688, 2021.
[16] MÜLLER N M, KOWATSCH D, DEBUS P, et al. On GDPR compliance of companies'privacy policies[C]// International Conference on Text, Speech, and Dialogue. Springer, Cham, 2019: 151-159.
[17] FAN M, YU L, CHEN S, et al. An empirical evaluation of GDPR compliance violations in Android mHealth Apps[C]// 2020 IEEE 31st International Symposium on Software Reliability Engineer-ing(ISSRE). IEEE, 2020: 253-264.
[18] 朱璋颖,陆亦恬,唐祝寿,张燕.基于隐私政策条款和机器学习的应用分类[J].通信技术,2020,53(11):2749-2757.
ZHU Z Y, LU Y T, TANG Z S, ZHANG Y. Application classification based on privacy policy terms and machine learning[J]. Communications Technology, 2020, 53(11): 2749-2757.
[19] VERDERAME L, CAPUTO D, ROMDHANA A, et al. On the (un) reliability of privacy policies in android Apps[C]// 2020 International Joint Conference on Neural Networks (IJCNN). IEEE, 2020: 1-9.
[20] 赵波,刘贤刚,刘行,胡影.Android 应用程序个人信息安全量化评估模型研究[J].通信技术, 2020, 53(08):201 9-2026.
ZHAO B, LIU X G, LIU X, HU Y. Quantitative evaluation model of personal information security for android applications[J]. Communications Technology, 2020, 53(08): 2019-2026.
[21] SUN R, XUE M. Quality assessment of online automated privacy policy generators: an empirical study[M]//Proceedings of the Evaluation and Assessment in Software Engineering. 2020: 270-275.
[22] 姚胜译,吴丹. App 隐私政策用户友好度评价研究[J].信息资源管理学报, 2021, 11(1): 30-39.
YAO S Y, WU D. Assessment research to App privacy policy user-frendliness[J]. Journal of Information Resources Management, 2021, 11(1): 30-39.
[23] 徐磊,郭旭.大数据时代读者个人信息保护的实践逻辑与规范路径——以图书类 App 隐私政策文本为视角[J]. 图书馆建设, 2021,1:74-83.
XU L, GUO X. Practice logic and normative path of protecting readers' personal information in the age of big data--From the perspective of privacy policy of book Apps[J]. Library Development, 2021, 1: 74-83.
[24] 杜永欣,周茂君.我国网站个人信息保护的合规性考察——基于九家网站隐私政策的文本分析[J].重庆邮电大学学报(社会科学版),2021,33(04):62-72.
DU Y X, ZHOU M J. Study on the compliance of website personal information protection in China--Text analysis based on privacy policy of nine websites[J]. Journal of Chongqing University of Posts and Telecommunications (Social Science Edition), 2021, 33(04): 62-72.
[25] 唐远清,赖星星.社交媒体隐私政策文本研究——基于 Facebook 与微信的对比分析[J].新闻与写作,2018 (08):31-37.
TANG Y Q, LAI X X. Social media privacy policy text research--Comparative analysis based on Facebook and WeChat[J]. News and Writing, 2018 (08): 31-37.
[26] 马骋宇,刘乾坤.移动健康应用程序的隐私政策评价及实证研究[J].图书情报工作,2020,64(07):46-55.
MA C Y, LIU Q K. Research on the privacy policy's evaluation and empirical study of mobile health applications[J]. Library and Information Service, 2020, 64(07): 46-55.
[27] 何培育,马雅鑫,涂萌.Web 浏览器用户隐私安全政策问

题与对策研究[J].图书馆,2019(02):19-26.
HE P Y, MA Y X, TU M. A study on problems and countermeasures of web browser user privacy security policy[J]. Library, 2019(02): 19-26.
[28] 姜盼盼.图书馆隐私政策合规性的依据与标准[J].图书馆建设,2019,4:79-86.
JIANG P P. Compliance basis and standards of library privacy policy[J]. Library Development, 2019, 4: 79-86.
[29] ARZT S, RASTHOFER S, FRITZ C, et al. Flowdroid: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android Apps[J]. Acm Sigplan Notices, 2014, 49(6): 259-269.
[30] QIAN C, LUO X, LE Y, et al. Vulhunter: toward discovering vulnerabilities in android applications[J]. IEEE Micro, 2015, 35(1): 44-53.
[31] CHURCH K W. Word2Vec[J]. Natural Language Engineering, 2017, 23(1): 155-162.
[32] ANDOW B, MAHMUD S Y, WHITAKER J, et al. Actions speak louder than words: entity-sensitive privacy policy and data flow analysis with policheck[C]//29th USENIX Security Sympo-sium(USENIX Security 20). 2020: 985-1002.
[33] YU L, LUO X, LIU X, et al. Can we trust the privacy policies of android Apps?[C]//2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). IEEE, 2016: 538-549.
[34] KUNUNKA S, MEHANDJIEV N, SAMPAIO P. A comparative study of Android and iOS mobile applications' data handling practices versus compliance to privacy policy[C]// IFIP International Summer School on Privacy and Identity Manage-ment. Springer, Cham, 2017: 301-313.
[35] OLUKOYA O, MACKENZIE L, OMORONYIA I. Security-oriented view of App behaviour using textual descriptions and user-granted permission requests[J]. Computers & Security, 2020, 89: 101685.
[36] YU L, LUO X, QIAN C, et al. Enhancing the description-to-behavior fidelity in android Apps with privacy policy[J]. IEEE Transactions on Software Engineering, 2017, 44(9): 834-854.
[37] YU L, LUO X, QIAN C, et al. Revisiting the description-to-behavior fidelity in android applications[C]//2016 IEEE 23rd International Conference on Software Analysis, Evolution, and Reengineering (SANER). IEEE, 2016, 1:415-426.
[38] WANG R, WANG Z, TANG B, et al. Smartpi: Understanding permission implications of android Apps from user reviews[J]. IEEE Transactions on Mobile Computing, 2019, 19(12): 2933-2945.
[39] 贺雪乔.iOS 应用隐私条例与敏感行为一致性检测系统的设计与实现[D].北京:北京邮电大学,2020.
HE X Q. Design and implemention of consistency detection and generation technology for privacy policy of IOS Apps[D]. Beijing: Beijing University of Posts and Telecommunications, 2020.
[40] MA Z, WANG H, GUO Y, et al. Libradar: fast and accurate detection of third-party libraries in android Apps[C]//Proceedings of the 38th International Conference on Software Engineering Companion. 2016: 653-656.
[41] 胡杰克.基于敏感数据流的 Android 恶意程序及隐私泄露检测方法研究[D].深圳:哈尔滨工业大学,2021.
HU J K. Research on android malware and privacy leak detection method based on sensitive data flow[D]. Shenzhen: Harbin Institute of Technology, 2021.
[42] 王靖瑜. Android 应用隐私条例一致性检测及其生成技术的研究与实现[D].北京:北京邮电大学,2018.
WANG J Y. Research and implementation of consistency detection and generation technology for privacy policy of android Apps[D]. Beijing: Beijing University of Posts and Telecommunications, 2018.
[43] 王靖瑜,徐明昆,王浩宇,徐国爱.Android 应用隐私条例与敏感行为一致性检测[J].计算机科学与探索,2019,13(01):56-69.
WANG J Y, XU M K, WANG H Y, XU A G. Auto-mated Detection of Consistence Between App Beha-vior and Privacy Policy of Android Apps[J]. Journal of Frontiers of Computer Science and Technology, 2019, 13(01): 56-69.
[44] ZHANG C, WANG H, WANG R, et al. Re-checking App behavior against App description in the context of third-party libraries[C]//SEKE. 2018: 665-664.
[45] FENG Y, CHEN L, ZHENG A, et al. Ac-net: Assessing the consistency of description and per-mission in android Apps[J]. IEEE Access, 2019, 7: 57829-57842.
[46] YU L, LUO X, CHEN J, et al. PPchecker: Towards accessing the trustworthiness of android Apps' privacy policies[J]. IEEE Transactions on Software Engineering, 2018, 47(2): 221-242.
[47] 杜代忠. Android 应用隐私政策与权限使用的一致性分析引擎的研究与实现[D].北京:北京邮电大学,2021.
DU D Z. Research and implementation of consistency analysis engine for android application privacy policy and permission usage[D]. Beijing: Beijing University of Posts and Telecommunications, 2021.
[48] SLAVIN R, WANG X, HOSSEINI M B, et al. Toward a framework for detecting privacy policy violations in android application code[C]//Proceedings of the 38th International Conference on Software Engineering. 2016: 25-36.
[49] SOLNYSHKINA M I, ZAMALETDINOV R R, GORODETSKAYA L A, et al. Evaluating text complexity and Flesch-Kincaid grade level[J]. Journal of Social Studies Education Research, 2017(3).
[50] FARR J N, JENKINS J J, PATERSON D G. Simplification of Flesch reading ease formula[J]. Journal of Applied Psychology, 1951, 35(5): 333.
[51] GUNNING R. The fog index after twenty years[J]. Journal of Business Communication, 1969, 6(2): 3-13.
[52] MC LAUGHLIN G H. SMOG grading-a new readability formula[J]. Journal of reading, 1969, 12(8): 639-646.
[53] FAROOQ E, GHANI MANUI, NASEER Z, et al. Privacy policies' readability analysis of contemporary free healthcare Apps[C]//2020 14th International Conference on Open Source Systems and Technologies (ICOSST). IEEE, 2020: 1-7.
[54] 陈世敏.中文可读性公式试拟[J].新闻学研究,1971(8):181-225.

CHEN S M. Chinese Readability Formula[J]. Mass communication Research, 1971(8): 181-225.
[55] DAS G, CHEUNG C, NEBEKER C, et al. Privacy policies for Apps targeted toward youth: descriptive analysis of readability[J]. JMIR mHealth and uHealth, 2018, 6(1): e7626.
[56] REDMILES E M, MORALES M, MASZKIEWICZ L, et al. First steps toward mea-suring the readability of security advice[C]//The 2018 IEEE Security & Privacy Workshop on Technology and Consumer Protection (ConPro). 2018.
[57] POWELL A, SINGH P, TOROUS J. The complexity of mental health App privacy policies: a potential barrier to privacy[J]. JMIR mHealth and uHealth, 2018, 6(7): e9871.
[58] FOWLER L R, GILLARD C, MORAIN S R. Readability and accessibility of terms of service and privacy policies for menstruation-tracking smart-phone applications[J]. Health Promotion Practice, 2020, 21(5): 679-683.
[59] 秦克飞.手机 App 隐私政策的可读性研究[J].情报探索,2019(01):18-23.
QIN K F. Research on readability of mobile App privacy policies[J]. Information Research, 2019(01): 18-23.
[60] SUNYAEV A, DEHLING T, TAYLOR P L, et al. Availability and quality of mobile health App privacy policies[J]. Journal of the American Medical Informatics Association, 2015, 22(e1): e28-e33.
[61] 王英.若干国家或地区图书馆协会隐私政策的纵向分析[J]. 图书馆理论与实践,2020 (4):28-34.
WANG Y. A longitudinal analysis on privacy policies of several national or regional library associations[J]. Library Theory and Practice, 2020 (4): 28-34.
[62] ROBILLARD J M, FENG T L, SPORN A B, et al. Availability, readability, and content of privacy policies and terms of agreements of mental health Apps[J]. Internet Interventions, 2019, 17: 100243.
[63] JAVED Y, AL QAHTANI E, SHEHAB M. Privacy policy analysis of banks and mobile money services in the middle east[J]. Future Internet, 2021, 13(1): 10.
[64] ZHANG M, CHOW A, SMITH H. COVID-19 contact-tracing Apps: analysis of the readability of privacy policies[J]. Journal of Medical Internet Research, 2020, 22(12): e21572.
[65] BASCH C H, MOHLMAN J, HILLYER G C, et al. Public health communication in time of crisis: Readability of on-line COVID-19 information[J]. Disaster medicine and public health preparedness, 2020, 14(5): 635-637.
[66] KRUMAY B, KLAR J. Readability of privacy policies[C]// IFIP Annual Conference on Data and Applications Security and Privacy. Springer, Cham, 2020: 388-399.
[67] FABIAN B, ERMAKOVA T, LENTZ T. Large-scale readability analysis of privacy policies[C]//Proceedings of the international conference on web intelligence. 2017: 18-25.
[68] ANDERSON J. Lix and rix: Variations on a little-known readability index[J]. Journal of Reading, 1983, 26(6): 490-496.
[69] COLEMAN M, LIAU T L. A computer readability formula designed for machine scoring[J]. Journal of Applied Psychology, 1975, 60(2): 283.
[70] SENTER R J, SMITH E A. Automated readability index[R]. Cincinnati Univ OH, 1967.
[71] 王蕾.初中级日韩留学生文本可读性公式初探[D].北京:北京语言大学, 2005.
WANG L. Research on Chinese Readability formula of texts for elementary and intermediate Korean and Japanese students[D]. Beijing: Beijing Language and Culture University, 2005.
[72] 左虹,朱勇.中级欧美留学生汉语文本可读性公式研究[J].世界汉语教学,2014,28(2):14.
ZUO H, ZHU Y. Research on Chinese readability formula of texts for intermediate level European and America students[J]. Chinese Teaching in the World, 2014, 28(2):14.
[73] 杨金余.高级汉语精读教材语言难度测定研究[D].北京:北京大学,2008.
YANG J Y. The study on measurement of language difficulty of advanced Chinese intensive reading textbooks[D]. Beijing: Peking University, 2008.
[74] 郭望皓.对外汉语文本易读性公式研究[D].上海:上海交通大学, 2010.
GUO W H. Research on readability formula of Chinese text for foreign students[D]. Shanghai: Shanghai Jiao Tong University, 2010.
[75] 孙汉银.中文易读性公式[D].北京：北京师范大学,1992.
SUN H Y. Chinese readability formula[D]. Beijinig: Beijing Normal University, 1992.
[76] 侯尧,陶洋,杨理,熊炼.基于差分隐私的个人轨迹信息保护机制[J].计算机工程与应用, 2020,56(9):106-110.
HOU Y, TAO Y, YANG L, XIONG L. Personal Trajectory Information Protection Based on Differential Privacy Mechanism[J]. Computer Engineering and Applications, 2020, 56(9): 106-110.