112 年委託研究報告

網際網路傳播社會調查委託研究採購案

期末報告

計畫委託機關：國家通訊傳播委員會

中華民國 113 年 3 月

112 年委託研究報告

GRB 系統編號：PG11204-0128

網際網路傳播社會調查委託研究採購案

期末報告

受委託單位

財團法人電信技術中心

計畫主持人

王牧寰

共同主持人

林俞君

協同主持人

吳秦雯、林家暘

計畫顧問

江耀國、柯舜智

研究人員

林永翰、楊儷綺、蕭亦庭、陳聖薇

本報告不必然代表國家通訊傳播委員會意見

中華民國 113 年 3 月

目次

目次.....I

表次.....IX

圖次.....XVII

提要.....XX

一、研究緣起.....XX

二、研究方法及過程.....XX

三、重要發現.....XXI

四、建議事項.....XXII

Abstract.....XXIV

第一章　緒論.....1

第一節　研究緣起與背景.....1

第二節　研究之分析架構.....2

一、研究動機與目的.....2

二、研究架構.....3

第三節　研究方法與執行進度說明.....5

一、研究方法.....5

二、執行進度說明.....7

第二章　國際間網際網路社會問題及處理模式研析.....10

第一節　歐盟.....11

一、監理脈絡.....11
二、政府機關法制政策作為.....12
三、第三方監督或產業自律機制.....30
四、小結.....36
第二節　德國.....37
一、監理脈絡.....37
二、政府機關法制政策作為.....41
三、第三方監督或產業自律機制.....52
四、小結.....58
第三節　法國.....60
一、監理脈絡.....60
二、政府機關法制政策作為.....64
三、第三方監督或產業自律機制.....83
四、小結.....86
第四節 英國.....87
一、監理脈絡.....87
二、政府機關法制政策作為.....91
三、第三方監督或產業自律機制.....114
四、小結.....119

第五節　美國.....121
一、監理脈絡.....121
二、政府機關法制政策作為.....122
三、第三方監督或產業自律機制.....132
四、小結.....135
第六節　加拿大.....136
一、監理脈絡.....136
二、政府機關法制政策作為.....137
三、第三方監督或產業自律機制.....143
四、小結.....149
第七節　澳洲.....150
一、監理脈絡.....150
二、政府機關法制政策作為.....153
三、第三方監督或產業自律機制.....175
四、小結.....182
第八節　紐西蘭.....183
一、監理脈絡.....183
二、政府機關法制政策作為.....185
三、第三方監督或產業自律機制.....188

四、小結.....201
第九節　日本.....202
一、監理脈絡.....202
二、政府機關法制政策作為.....212
三、第三方監督或產業自律機制.....228
四、小結.....235
第十節　韓國.....236
一、監理脈絡.....236
二、政府機關法制政策作為.....240
三、第三方監督或產業自律機制.....254
四、小結.....262
第十一節　新加坡.....263
一、監理脈絡.....263
二、政府機關法制政策作為.....265
三、第三方監督或產業自律機制.....291
四、小結.....292
第十二節　綜合歸納與比較.....294
一、違法內容處理之象限圖與電訪概要模式說明.....294
二、共通性議題之處理模式比較研析.....297

第三章　我國網際網路傳播社會問題盤點.....308

第一節　我國網際網路相關服務之使用情形.....308

一、網際網路之使用比例及頻率.....308

二、使用網際網路之主要目的.....309

三、最常造訪網站.....312

四、最常搜尋關鍵字.....313

第二節　我國網際網路相關服務之主要問題盤點.....314

一、網際網路社會問題過去相關研究分析.....316

二、現有網路社會問題協力機制.....319

三、現有網路社會問題研究缺口與待解決問題.....326

第四章　我國網際網路傳播社會問題調查之設計及調查結果.....329

第一節　社會問題調查研究方法.....329

一、一般大眾電話訪問.....330

二、公民團體面訪.....344

三、網際網路傳播相關服務業者面訪.....346

四、焦點團體座談.....348

第二節　一般大眾電話訪問調查結果.....354

一、日常網路行為：網路行為與使用平臺.....355

二、衍生之個人及社會問題，以及其風險與危害之認知..364

三、網路及電視交互作用影響下之效果 376

四、民眾偏好的網路問題處理方式.....379

五、各利害關係人角色分析.....401

第三節 綜合觀察.....423

一、電話訪問.....423

二、公民團體及業者面訪.....424

三、焦點團體座談.....425

四、「協力模式」作為最大公約數.....427

第五章 國內主要網際網路傳播相關服務公共問責模式研析.....428

第一節 一般大眾網路問卷調查 428

一、網路調查摘要.....428

二、問卷設計暨背景說明.....429

第二節 一般大眾網路問卷調查結果 436

一、日常行為：網路行為與使用平臺調查 436

二、使用者對於平臺各項措施之滿意度 447

三、民眾對違法內容移除機制之偏好.....452

四、第三方協力治理模型.....457

五、線上串流影音服務擴充題.....469

六、綜合分析.....472

第三節　諮詢座談會辦理成果 475

一、網路調查問卷之解讀結果探討.....477

二、協力治理模型之調整建議.....478

三、跨部會法規制度之整合建議.....482

四、自律框架之設定建議.....483

第四節　問責模式研析.....485

一、關於問責模式的主要發現.....485

二、協力治理模式.....489

第六章　綜合觀察與政策建議 497

第一節　本研究研析重點回顧暨政策評估檢討 497

一、國際平臺問責法制持續演進.....497

二、數位中介服務法草案倡議中止後之立法行動 500

三、未來可能的立法嘗試之挑戰.....501

四、本研究民眾意見調查與政策建議之關係 502

五、本研究專家諮詢座談會與政策建議之關係 503

第二節　法制政策建議.....504

一、短期建議：揉合行政體系能量，適切對應分散式立法 506

二、中長期建議：仍有必要走向集中式立法，建構穩定法制 509

參考資料.....515

一、書籍.....515

二、期刊.....516

三、其他.....517

附錄一 一般民眾電話訪問調查問卷.....533

附錄二 網路調查問卷.....549

表次

表 1：近年美國關於 CDA 第 230 條修正及平臺問責之討論.....128

表 2：加拿大「數位公民倡議：對抗網路假訊息及其他有害內容」架構.....148

表 3：《線上安全法》之網路內容監理與處置程序.....165

表 4：「澳洲數位平臺錯誤訊息與新聞品質準則」規劃方向.....175

表 5：不實與錯誤訊息行為準則目標與對應作法.....178

表 6：《準則》承諾之減少線上有害內容傳散措施.....194

表 7：《紐西蘭線上安全及危害行為準則》促進使用者知悉權之承諾.....198

表 8：《紐西蘭線上安全及危害行為準則》對於提高透明度之承諾.....199

表 9：《紐西蘭線上安全及危害行為準則》支持獨立研究與評估之承諾.....200

表 10：《仇恨言論消除法》與《部落歧視消除推動法》條文比較227

表 11：LINE 群組（グループ）與社群（オープンチャット）功能差異.....232

表 12：研究國別就政治不實訊息之處理模式.....297

表 13：研究國別就兒少網路安全之處理模式.....299

表 14：研究國別就網路交易安全之處理模式.....302

表 15：研究國別就網路霸凌之處理模式 304

表 16：研究國別就使用者權益之處理模式 306

表 17：iWIN 申訴機制 323

表 18：一般民眾調查樣本檢定結果 337

表 19：調查樣本分佈檢定結果（依縣市） 338

表 20：住宅電話調查訪問接觸結果 339

表 21：住宅電話調查訪問接觸結果（續） 340

表 22：手機電話調查訪問接觸結果 341

表 23：手機電話調查訪問接觸結果（續） 342

表 24：本研究公民團體面訪名單 344

表 25：本研究網際網路傳播相關服務業者面訪名單 346

表 26：一般民眾場次（8/2）出席民眾名單 349

表 27：一般民眾場次（8/4）出席民眾名單 349

表 28：一般民眾場次（8/10）出席民眾名單 350

表 29：公民團體場及學者場次（8/11）出席名單 350

表 30：網際網路傳播相關服務業者場次（8/14）出席名單 351

表 31：一般民眾場次討論題綱 351

表 32：公民團體場及學者、網際網路傳播相關服務業者場次討論提綱 353

表 33：民眾使用社群媒體平臺的頻率 355

表 34：民眾使用通訊媒體平臺的頻率 356

表 35：民眾使用網路新聞媒體平臺的頻率 357

表 36：民眾使用拍賣、購物平臺的頻率 358

表 37：民眾使用串流影音服務的頻率 359

表 38：民眾使用傳統電視的頻率 360

表 39：網路、傳統電視使用與使用者年齡之交叉分析 361

表 40：社群媒體平臺與年齡交叉分析 362

表 41：通訊軟體與年齡交叉分析 362

表 42：網路新聞平臺與年齡交叉分析 363

表 43：網路購物平臺與年齡交叉分析 363

表 44：民眾針對政治不實訊息的經驗、風險與危害認知 365

表 45：（續）民眾針對政治不實訊息的經驗、風險與危害認知 366

表 46：民眾針對兒少網路安全的經驗、風險與危害認知 368

表 47：民眾針對網路交易安全的經驗、風險與危害認知 370

表 48：民眾針對網路霸凌的經驗、風險與危害認知 372

表 49：民眾針對使用者權益的經驗、風險與危害認知 374

表 50：問題強度分析 375

表 51：網際網路平臺使用模式（只使用網路、只使用傳統電視，或

兩者都用）.....376
表 52：網際網路傳播社會問題「認知」之變異數分析（ANOVA）.....377
表 53：網際網路社會問題「經驗」之 t 檢定.....377
表 54：面對政治不實訊息，民眾認為應出面負責者.....380
表 55：民眾認為網路使用者面對「政治不實訊息」的應有作為..380
表 56：民眾認為網路平臺管理員面對「政治不實訊息」的應有作為.....381
表 57：民眾認為網路平臺面對「政治不實訊息」的應有作為.....381
表 58：民眾認為政府面對「政治不實訊息」的應有作為.....382
表 59：民眾認為民間組織面對「政治不實訊息」的應有作為.....382
表 60：面對兒少網路安全，民眾認為應出面負責者.....383
表 61：民眾認為網路使用者面對「兒少網路安全」問題的應有作為.....384
表 62：民眾認為粉專管理員面對「兒少網路安全」問題的應有作為.....384
表 63：民眾認為網路平臺面對「兒少網路安全」問題的應有作為.....385
表 64：民眾認為政府面對「兒少網路安全」問題的應有作為.....385
表 65：民眾認為民間組織面對「兒少網路安全」問題的應有作為.....386
表 66：面對網路交易安全，民眾認為應出面負責者.....387

表 67：民眾認為網路使用者面對「網路交易安全」問題的應有作為 388
表 68：民眾認為粉專管理員面對「網路交易安全」問題的應有作為 388
表 69：民眾認為網路平臺面對「網路交易安全」問題的應有作為 389
表 70：民眾認為政府面對「網路交易安全」問題的應有作為.....389
表 71：民眾認為民間組織面對「兒少網路安全」問題的應有作為 390
表 72：面對網路霸凌，民眾認為應出面負責者.....391
表 73：民眾認為網路使用者面對「網路霸凌」問題的應有作為..392
表 74：民眾認為網路平臺粉專管理員面對「網路交易安全」問題的應有作為.....392
表 75：民眾認為網路平臺面對「網路霸凌」問題的應有作為.....393
表 76：民眾認為政府面對「網路霸凌」問題的應有作為.....393
表 77：民眾認為民間組織面對「網路霸凌」問題的應有作為.....394
表 78：在使用者權益上，民眾認為可維護權利的方式.....395
表 79：民眾使用串流影音服務時之消費爭議經驗.....397
表 80：曾有串流影音服務消費爭議經驗之民眾認為最需解決之爭議類型.....397
表 81：民眾認為政府面對流影音服務消費爭議最需要採取之措施

.....397
表 82：網路問題強度分析 429
表 83：網路調查民眾認為在各類網路危害中應負最大責任者之主體 430
表 84：近一個月內有使用社群平臺的民眾與使用時間 436
表 85：近一個月內有使用影音分享平臺之民眾與使用時間 437
表 86：近一個月內有使用網路論壇的民眾與使用時間 438
表 87：近一個月內有使用通訊軟體的民眾與使用時間 439
表 88：近一個月內有使用網路新聞平臺的民眾與使用時間 440
表 89：近一個月內有使用拍賣、購物平臺的民眾與使用時間 441
表 90：近一個月內有使用傳統電視的民眾與使用時間 442
表 91：民眾閱讀平臺服務與使用者條款分布 444
表 92：對「政治不實訊息」所訂定的使用者條款之滿意度 447
表 93：對「兒少網路安全」所訂定的刪除機制之滿意度 448
表 94：對「網路交易安全」所訂定的防詐機制之滿意度 449
表 95：對「網路霸凌」所訂定的防護機制之滿意度 450
表 96：對「個人權益」所訂定的使用者申訴與審查機制之滿意度 451
表 97：民眾對於網路上違法資訊或內容的移除強度分布 452
表 98：民眾對於網路上違法資訊或內容的移除範圍分布 453
表 99：民眾認為行政機關與司法機關對於違法資訊或內容處理機

制之權限分布 454
表 100：移除機制範圍與法官保留強度結構象限表 456
表 101：除機制範圍與移除機制強度結構象限表 457
表 102：民眾對協力治理模型之認同度 459
表 103：民眾對協力治理模型之認同度（續） 459
表 104：民眾對協力治理模型之認同度（續） 460
表 105：民眾認為應被賦予更多責任的角色可做的事情 462
表 106：民眾偏好的第三方機構組成結構 464
表 107：民眾對於第三方機構與政府之互動關係的看法 465
表 108：民眾對於第三方機構與網路平臺之互動關係的看法 466
表 109：民眾對於第三方機構與使用者之互動關係的看法 468
表 110：民眾使用串流影音平臺之統計 469
表 111：民眾使用串流影音平臺的平均時間.....470
表 112：民眾使用串流影音平臺時所曾遭遇的消費爭議 470
表 113：民眾認為消費爭議中最需要被解決的問題 471
表 114：民眾認為政府面對「串流影音服務的消費爭議」最需要採取的措施.....471
表 115：「網際網路傳播社會調查暨法制政策架構」諮詢座談會出席名單.....475

表 116：「網際網路傳播社會調查暨法制政策架構」諮詢座談會討論題綱.....476

圖次

圖 1：Ofcom 執法與制定實踐準則之階段性規劃示意圖 105

圖 2：澳洲電子專員辦公室組織架構圖 154

圖 3：eSafety 執行策略 155

圖 4：第一類與第二類內容分級制度 158

圖 5：《線上安全法》之申訴處理機制 159

圖 6：違法與受限制內容之處置通知 163

圖 7：eSafety 業界規範立場文件之線上安全規範 174

圖 8：《澳洲不實與錯誤訊息行為準則》之治理委員會 176

圖 9：打擊錯誤訊息和虛假訊息之 ACMA 權力行使 181

圖 10：紐西蘭數位安全小組工作綜覽 184

圖 11：《紐西蘭線上安全及危害行為準則》之權力與責任分布架構圖 192

圖 12：日本 65 歲以上民眾之網路使用率變化 203

圖 13：違法、有害資訊諮詢中心處理諮詢案件數變化（單位：件） 205

圖 14：假資訊對策的未來政策方向建議 206

圖 15：研究會提出的自律框架及執行程序 207

圖 16：《青少年網際網路環境整備法》修正條文賦予之義務 213

圖 17：日本服務提供者責任限制法「通知及取下條款」運作流程圖

.....219
圖 18：修法前之發訊人資訊揭露程序（第三階段並非資訊揭露程序）
.....220
圖 19：修法後之發訊人資訊揭露程序（訴訟程序並非資訊揭露程序）
.....222
圖 20：日本《霸凌防止對策推動法》規範內容.....224
圖 21：韓國民眾週平均網路使用時間歷年變化.....239
圖 22：《線上刑事犯罪危害法》之命令運作說明.....290
圖 23：世界各國網際網路傳播社會問題之處理模式象限圖（一）
.....294
圖 24：世界各國網際網路傳播社會問題之處理模式象限圖（二）
.....296
圖 25：我國 16 歲以上民眾最近 3 個月內使用網路所從事之活動前十名.....309
圖 26：我國民眾使用網路之主要目的.....310
圖 27：我國民眾使用網路應用服務情形.....311
圖 28：我國民眾使用網路的顧慮前十名.....314
圖 29：我國民眾使用即時通訊軟體時接觸不同意見之情況.....315
圖 30：一般大眾電訪問卷設計架構.....330
圖 31：一般大眾網路問卷設計架構.....431
圖 32：民眾對與使用者條款之了解程度.....446
圖 33：移除強度與法官保留象限分析.....455

圖 34：移除強度與移除範圍象限分析 456

圖 35：第三方協力治理模型架構圖 458

圖 36：本研究提出之協力治理模式架構圖 489

圖 37：英國 OSA 與我國《數位中介服務法》草案課與義務比較圖(1) 498

圖 38：英國 OSA 與我國《數位中介服務法》草案課與義務比較圖(2) 499

圖 39：網際網路社會治理協作模式 505

提要

關鍵詞：數位平臺、平臺問責、數位中介服務法

一、研究緣起

自網際網路開放商用以來，其自由、開放與多元之特性促進了各類創新應用的蓬勃發展。隨著整體產業與公民社會的溝通模式出現重大轉變，人們日常生活與網際網路形成密不可分的關係，產業、使用者及政府亦有必要正視網際網路跨境、即時傳播之特性，積極回應數位時代下的新興傳播議題，透過多方利害關係人參與、自律、他律之機制，共同維繫良好而安全的網際網路環境。

隨著網際網路傳播政策於 111 年政府組織改造後，成為國家通訊傳播委員會（NCC）之業務執掌，委託單位擬透過本研究之推動，掌握我國公民社會就網際網路傳播議題之意向及重要公共議題，結合次級資料之研蒐，輔以質性及量化調查，以期回應數位時代社會所需，作為研議推動網際網路傳播政策與相關治理機制之重要參考。

二、研究方法及過程

本研究依據各委託辦理工作項目，採用文獻分析法、個案研究法及比較分析法，量化問卷調查暨統計分析、檢定方法，並舉辦焦點訪談座談會。本研究「我國網際網路傳播社會問題調查」之電訪調查及「我國主要網際網路傳播相關服務公共問責模式研析」之網路調查，將採用量化問卷進行統計分析。

其中，「我國網際網路傳播社會問題調查」係委託趨勢民調股份有限公司進行，調查對象涵蓋一般民眾、公民團體及網際網路傳播相關服務業者。一般民眾之樣本數達 1,301 份（信心水準至少 95%，抽樣誤差不超過±3%）;「我國主要網際網路傳播相關服務公共問責模式研析」之網路調查則係委託典通股份有限公司，以其獨家開發之 EZChoice 行動 APP 為執行平臺，有效樣本數達 300 份，且調查對象在社群平臺、影音分享平臺、網路論壇、通訊軟體、拍賣及購物平臺五種類型中，至少為其中三種之註冊會員，且在近一個月內有使用。

三、重要發現

（一）瞭解世界各國因應網際網路傳播社會問題之法制概況

隨著網路中介服務逐漸普及，世界各國也開始注意到其在當代所引發的各種社會問題。包括政治不實訊息、兒少網路安全、網路交易安全、網路霸凌、使用者權益等，皆係世界主要國家所關切之重要議題。尤其在遏止線上違法內容傳散的議題上，各國對於違法內容之定義範圍、資訊限制令是否採法官保留原則等具體設計之方向雖有所差異，但多可觀察到「平臺問責」概念興起之趨勢。

透過「禁制違法內容廣泛／有限」、「高密度／低密度網際網路內容執法措施」、「有法官保留／無法官保留」等共通性指標，本研究將歐盟、德國、法國、英國、美國、加拿大、澳洲、紐西蘭、日本、韓國、新加坡等研究國別之法制整備概況進行分類，除作為後續執行社會調查時向一般民眾說明之基礎，亦有助於委託單位瞭解當前相關議題之國際法制趨勢。

（二）瞭解我國網際網路相關服務之主要問題及民眾使用習慣

透過電話訪問調查及網路問卷調查之執行，本研究對於我國民眾使用網際網路之習慣、風險認知、對於平臺服務及使用者條款之瞭解程度等面向皆有所掌握，並觀察到民眾認為網路社會問題需有明確負責對象的意向。其中，政治不實訊息、兒少網路安全、網路霸凌屬於問題強度較高的類型，民眾希望政府有所做為；網路交易安全問題、使用者權益保障問題則屬於問題強度較低的類型，但民眾也希望由網路平臺以主動巡視的方式解決此類問題。

另一方面，本研究也藉由網路及電視交互作用之分析發現：同時使用傳統電視和網際網路並不會加深、加重民眾對於網際網路傳播社會問題的感知；但相反地，完全不使用網際網路平臺的民眾更容易認為網際網路平臺存在嚴重的社會問題。

四、建議事項

（一）立即可行建議

有鑑於當前我國就網際網路社會問題採取「分散式立法」模式之現狀，相關法規散落於各部會、各地方政府主管機關，為避免業者法遵成本增加及困難，導致秩序難以形成，政府機關應首先對內進行法規之盤點與資源整合，並建立行政院層級之跨部會會報，以透過網路治理業務之協調落實跨域治理，最終形成網際網路的框架性規範。

另一方面，在此跨部會協調機制中，具有獨立機關與合議制特性之 NCC 雖不適合擔任主責協調之部會，仍應依新修《國家通訊傳播委員會組織法》第 3 條第 1 款所明訂之執掌，持續觀察各部會法制政策及執法的發展，並以此基礎視其可能性及需要性，研議包括處理非法內容之共通機制等可行的集中式立法策略。

除此之外，政府部門也應瞭解：網際網路所衍生之社會問題並非僅靠由上而下的管制即可解決，關鍵在於使利害關係人創建彼此共同之目的與相互信任。是故，政府機關必須做為創建共識的協力者，與業者、公民團體維持對話，同時對民眾持續進行教育，除了打造良好的對話環境、給予充分的資源、也應持續資訊共享，才能使網際網路的協力模式發揮完整的治理功能。

（二）中長期建議

為求國際市場之管制對接，避免大型數位中介服務提供者因法遵成本等問題而退出臺灣市場之風險，中長期而言，政府機關仍須借鏡《數位中介服務法》草案之推動經驗，持續考量集中式立法之可能性。亦即，透過「定礎與加建」之策略，建立一套適用於各種數位中介服務之普通法，再針對特殊種類之平臺或違法資訊類型，另以部門硬法作為特別法，予以追加或排除規範，且應在違法資訊的移除或限制接取程序上，將法官保留作為設計原則，以維護使用者之言論自由。

具體而言，此一「普通法」課予數位平臺之義務，或可先從「建立並揭露通知及行動機制」、「制訂並揭露內容調控之處理標準」、「建

立並揭露完善之內容調控制度與人員」、「儘速告知通知人及被通知人處理結果」、「透明性報告」等五項國際趨勢下較無爭議之類型出發，以降低業者法遵成本。

另一方面，為求網際網路秩序之穩定，也應汲取 iWIN 之經驗，由政府委託一具有社會公信力的協會組織作為發起人，邀請平臺業者、民眾、公民團體、政府主管機關等，共同創建網際網路協力治理之聯盟。此一聯盟之功用在於提供各界對話平臺以促進共識形成，是故應透過立法授權保障其組織之獨立性，且政府機關之代表也須最小化，以帶回意見整合資源為其主要任務，盡可能地保障其財務暨人事獨立性，後續則完全交由業界或民間自治，此才能徹底得到業界及民眾的信賴。

Abstract

Keywords: Digital Platform, Platform Accountability, Digital Intermediary Services Act

I. Origin of this Study

Since the Internet was opened for commercial use, its characteristics of freedom, openness and diversity have promoted the vigorous development of various innovative applications. As the communication model between the overall industry and civil society has undergone major changes, people's daily life and the Internet have formed an inseparable relationship. It is also necessary for industry, users and governments to face up to the cross-border and real-time communication characteristics of the Internet and actively respond to it. Emerging communication issues in the digital era jointly maintain a good and safe Internet environment through the participation of multiple stakeholders, self-discipline, and heteronomy mechanisms.

As the Internet communication policy has become the business responsibility of the National Communications Commission (NCC) after the government organizational restructuring in 2022, the commissioning unit intends to use the promotion of this study to understand our civil society on Internet communication issues. Important public issues are combined with the research and search of secondary data, supplemented by qualitative and quantitative surveys, in order to respond to the needs of society in the digital era and serve as an important reference for discussing and promoting Internet communication policies and related governance mechanisms.

II. Research Methodology and Process

Based on each entrusted work project, this study adopts literature analysis, case study and comparative analysis methods, quantitative questionnaire survey and statistical analysis and verification methods, and plans to hold focus interviews and symposiums. The survey on social issues in Internet communication, and the online survey will use quantitative questionnaires for statistical analysis.

Among them, the survey on social issues in Internet communication was commissioned by Trend Polls. The survey targets include the general public, citizen groups and Internet communication-related service providers. The number of samples from the general public reached 1,301 (the confidence level is at least 95%, and the sampling error does not exceed ±3%); the online survey was commissioned by DSIGroup, with its exclusively EZChoice as the execution platform, the number of valid samples reached 300, and the survey subjects need to have regisrerd and used three of thee following five types of platforms: social platforms, video sharing platforms, online forums, communication software, auctions and shopping platforms.

III. Preliminary Findings

(1) Understanding the legal system in response to social issues spread through the Internet around the world

As Internet intermediary services become more and more popular, countries around the world have begun to pay attention to the various social problems it has caused in contemporary times. Including political misinformation, children's online safety, online transaction safety, online bullying, user rights, etc., are all important issues of concern to major

countries in the world. Especially on the issue of curbing the spread of illegal content online, although countries have different definitions of illegal content and whether the information restriction order adopts the principle of judge reservation, the concept of "platform accountability" can be observed in many countries. Rising trend.

Through common indicators such as "extensive/limited ban on illegal content", "high-density/low-density Internet content enforcement measures", "judge reservation/no judge reservation", this study combines countries like EU, Germany, France, the United Kingdom, the United States, Canada, Australia, New Zealand, Japan, South Korea, Singapore, to serve as the basis for explaining to the general public when conducting subsequent social surveys, and to help the commissioning unit understand current relevant issues and international legal trends.

(2) Understanding the main issues and public habits of Internet-related services in Taiwan

Through the implementation of telephone interviews and online questionnaires, this study has a better understanding of Taiwan's Internet usage habits, risk perceptions, understanding of platform services and user terms, etc., and has observed that people believe that social problems on the Internet require clear intentions of those responsible. Among them, political misinformation, children's online safety, and cyberbullying are issues with higher intensity, and people hope that the government will do something; issues with online transaction security and user rights protection are issues with lower intensity. type, but people also hope that the online platform will solve such problems through proactive inspections.

On the other hand, this study also found through the analysis of the interaction between the Internet and television: using traditional television and the Internet at the same time will not deepen or aggravate the public's perception of social problems spread by the Internet; but on the contrary, people who don't use Internet platforms at all are more likely to think that Internet platforms have serious social problems.

IV. Preliminary Recommendations

(1) Immediately feasible suggestions

In view of the current situation in which the government adopts a "decentralized legislation" model on social issues related to the Internet, relevant laws and regulations are scattered among various ministries and local government agencies. In order to avoid increased compliance costs and difficulties for businesses, which would make it difficult to form order, government agencies should first conduct an internal inventory of regulations and integrate resources, and establish an inter-ministerial meeting at the Executive Yuan level to implement cross-domain governance through the coordination of network governance operations, and ultimately form a framework specification for the Internet.

On the other hand, in this inter-ministerial coordination mechanism, although the NCC, which has the characteristics of an independent agency with collegial system, may not be suitable to serve as the coordinator, it should still follow Article 3, paragraph 1, of the newly revised National Communications Commission Organization Act. The commission should continue to observe the development of legal policies and law enforcement of various ministries, and consider the possibility and necessity to study feasible centralized legislative

strategies, including common mechanisms for dealing with illegal content.

In addition, government departments should also understand that social problems arising from the Internet cannot be solved by top-down regulation alone. The key lies in establishing common purposes and mutual trust among stakeholders. Therefore, government agencies must act as collaborators in building consensus, maintain dialogue with industries and citizen groups, and at the same time continue to educate the public. In addition to creating a good dialogue environment, providing sufficient resources, and continuing to share information, only in this way can the Internet collaborative model exerts complete governance functions.

(2) Medium and long-term suggestions

In order to seek regulatory alignment with the international market and avoid the risk of large digital intermediary service providers withdrawing from the Taiwan market due to compliance costs and other issues, in the long term, government agencies must still learn from the experience of promoting the draft "Digital Intermediary Services Act" and continue to consider the possibility of centralized legislation. That is to say, through the strategy of " cornerstone-and-addition ", we should establish a set of common laws applicable to various digital intermediary services, and then use departmental hard laws as special laws to target special types of platforms or types of illegal information, and retain judges reservation as a design principle in the removal or restriction of access to illegal information to safeguard users' freedom of speech.

Specifically, this "common law" obligation imposed on digital platforms may start with relatively uncontroversial types under

international trends, such as "establishing and disclosing notice and action mechanisms", "formulating and disclosing handling standards for content moderation", "establishing and disclosing comprehensive content moderation ", "inform the notifier and the notified party of the processing results as soon as possible", to reduce industry compliance costs.

On the other hand, to ensure the stability of the Internet order, the experience of iWIN should also be learned. The government should entrust an association with social credibility as the initiator, and invite platform operators, the public, citizen groups, government authorities, etc. to jointly create an alliance for collaborative Internet governance. The function of this alliance is to provide a dialogue platform for all stakeholders to promote the formation of consensus. Therefore, the independence of its organization should be protected through legislative authorization, and the representatives of government agencies must also be minimized, with the main task of bringing back opinions and integrating resources. The alliance’s financial and personnel independence must be protected as much as possible, and leave the follow-up completely to the industry or private autonomy. Only in this way can we fully gain the trust of the industry and the public.

第一章　緒論

第一節　研究緣起與背景

自網際網路開放商用以來，其自由、開放與多元之特性促進了各類創新應用的蓬勃發展。隨著整體產業與公民社會的溝通模式出現重大轉變，人們日常生活與網際網路形成密不可分的關係，產業、使用者及政府亦有必要正視網際網路跨境、即時傳播之特性，積極回應數位時代下的新興傳播議題，透過多方利害關係人參與、自律、他律之機制，共同維繫良好而安全的網際網路環境。

隨著網際網路傳播政策於 111 年政府組織改造後，成為國家通訊傳播委員會（NCC）之業務執掌，委託單位擬透過本研究之推動，掌握我國公民社會就網際網路傳播議題之意向及重要公共議題，結合次級資料之研蒐，輔以質性及量化調查，以期回應數位時代社會所需，作為研議推動網際網路傳播政策與相關治理機制之重要參考。

綜上所述，本研究之主要工作項目如下：

（一）透過國內外既有文獻及次級資料之蒐集，配合以基底（bottom-up）思維發展之社會調查問卷，盤點及分析我國網際網路傳播相關服務之使用情形及主要問題。

（二）以一般大眾、公民團體及網際網路傳播相關服務業者為對象，針對我國網際網路傳播之社會問題進行問卷調查與分析。調查面涵蓋日常網路使用行為、衍生之個人及社會問題、訊息經由網路及電視交互作用下之傳播效果或相關社會影響、風險與危害認知、對現行各種網路問題處理成效及處理方式之看法與建議等。

（三）針對社會調查所彙整之網際網路傳播社會問題，綜整分析國際間（包含歐盟、德國、法國、英國、美國、加拿大、澳洲、紐西蘭、日本、韓國、新加坡等國家）相應之最新作法及優劣比較分析，包括政府機關政策法制作為、第三方監督及產業組織自律作法等。

（四）就我國提供服務之主要網際網路傳播相關服務公共問責模式之運作方式進行蒐集研析，探求公眾或第三方介入協助強化其問責之可行性，並執行網路調查。

（五）彙整前述之調查結果及研析資料，提出適合我國情境之議題相應政策及法制建議。

（六）於履約期間，提供委託單位與本案相關之業務諮詢、資料蒐集、議題分析、法規研究建議及相關資料。且每月至少 1 次向委託單位說明研究進度或進行議題研討。

第二節　研究之分析架構

一、研究動機與目的

隨著數位匯流帶動科技應用的多元發展，網際網路已成為當代生活所不可或缺之重要媒介，並推動了社會溝通模式的巨大轉變。有鑑於網際網路具有跨境、即時傳播之特性，網路言論自由、使用者隱私保護、消費者權益、違法內容及不實訊息處理、數位平臺服務提供者責任規範等也成為了數位時代下受到各界正視的新興傳播議題。

為建立涵蓋多方利害關係人參與、自律、他律之機制，建構良好而安全的網路使用環境，實有必要掌握我國公民社會就網際網路傳播議題之意向及重要公共議題，據以探求適宜我國之網際網路傳播政策與治理機制。

因此，本研究之研究目的，係瞭解我國網際網路相關服務之使用情形及主要問題，並耙梳各研究國別之具體法制或政策措施、公私協力機制，及促進產業自律之作為等通傳匯流法制整備、行政與司法經驗，以為委託單位提供法制革新建議。

本研究將試圖回答以下問題：

（一）我國民眾使用網際網路相關服務之情形為何？因此衍生哪些個人與社會問題？使用者對於網路傳播之社會影響與風險危害有何種程度之認知？對於各種網路問題之處理成效與處理方式又有何看法？

（二）針對我國網際網路傳播環境中具有重要性之社會問題，國際間所採取之應對手段為何？研究國別具體而言採取了哪些政策法制作為、第三方監督及產業組織自律手段？

（三）目前我國提供服務之主要網際網路傳播相關服務，其公共問責模式之運作方式為何？有無公眾或第三方介入協助強化其問責之可行性？

（四）針對我國網際網路之整體使用情形、重要議題與相關服務之公共問責模式，適宜之政策與法制建議為何？

二、研究架構

本研究可概分為「國際資料研析」及「我國資料研析與調查」兩大部分，詳細說明如下。

第一部分，「國際資料研析」將以歐盟、德國、法國、英國、美國、加拿大、澳洲、紐西蘭、日本、韓國、新加坡等國家或地區為對象，就世界主要國家所面臨之網際網路傳播社會問題進行盤點，進而對其採用之相應作法進行綜合整理及比較。此部分之研究結果除將作為我國網際網路傳播社會調查及網路調查問卷之設計基礎，亦將提供研擬我國網際網路政策建議之思考。

第二部分，就「我國資料研析與調查」則再細分為以下三大階段進行：第一階段「網際網路傳播社會問題盤點」係透過既有文獻資料之蒐集，勾勒我國民眾接觸使用網際網路傳播相關服務之情形及常見問題，並配合國際資料研析，作為後續執行網際網路社會調查之基礎。第二階段「網際網路傳播社會調查」則以我國一般大眾、公民團體及

網際網路傳播相關服務業者為對象，分別執行電話訪問及個別面訪，進而透過焦點團體座談進行綜合分析，提出調修我國法制政策之思考方向。第三階段「我國主要網際網路傳播相關服務公共問責模式研析」在於蒐集並研析於我國提供服務之主要網際網路傳播相關服務公共問責模式之運作方式、分析其模式之優缺點，探求公眾或第三方介入協助強化其問責之可行性，並辦理諮詢座談會及執行網路調查，蒐集網路使用者對於社會調查結果及網際網路傳播相關服務問責模式之相關意見。

礙於本研究所囊括之資料眾多，且各階段皆涉及國內外資料之交互研析，在研究結果的最終呈現上，報告將採用先行聚焦國際資料及法制政策之方式，再依序呈現網際網路社會調查、網際網路傳播相關服務公共問責模式研析等階段之研究成果，最終收斂至「綜合觀察與政策建議」，透過完整調查結果及研析資料之彙整，提出適合我國情境之議題相應政策及法制建議，以便委託單位參考。

第三節　研究方法與執行進度說明

一、研究方法

本研究依據各委託辦理工作項目，採用文獻分析法、個案研究法及比較分析法，量化問卷調查暨統計分析、檢定方法，並規劃舉辦焦點訪談座談會，最終整合各研究方法與工作項目的產出，提出數位通訊傳播匯流法制革新之具體研析建議及相關法律條文。相關研究方法分述如下：

（一）文獻分析法

文獻分析法（document analysis）是指根據一定的研究目的或課題，透過蒐集有關市場資訊、調查報告、產業動態等文獻資料，從而全面而精準地掌握所要研究問題的一種方法。蒐集內容儘量要求豐富及廣博，再將所蒐集來的資料，經過分析後歸納統整，再分析事件淵源、原因、背景、影響及其意義等。文獻資料可以是政府部門的報告、工商業界的研究、文件記錄資料庫、企業組織資料、圖書館中的書籍、論文與期刊、報章新聞等等。其分析步驟有四，即閱覽與整理（reading and organizing）、描述（description）、分類（classfying）及詮釋（interpretation）。

針對本研究所涉及之議題，研究團隊將蒐集研究國別之通傳匯流法制整備、規管趨勢與相關作為等有關資訊的最新進展，以掌握研究議題，並提出具體建議。

（二）個案研究法及比較分析法

個案研究是為了決定導致個人、團體或機構之狀態或行為的因素或諸因素之間的關係，做深入縝密的研究，廣泛地蒐集個案資料，了解接受研究的單位，進行深入探究與分析，以解釋現狀，或描述探索足以影響變遷及成長諸因素的互動情形，並確定問題癥結，進而提出矯正的建議。

研究團隊就所蒐集到的學研界、產業界及平臺業者等各界意見、與國際資訊等，進行比較法研究與比較政策分析，找出意見與資訊間之關聯性，並歸納異同，從中尋找可資參考之重點，並研析可供我國數位通訊傳播匯流法制革新等政策調修參酌之依據。

其次，本研究再就前述所得之分析歸納結果，與我國現行法制、以及調修中或曾提出草案之法制架構進行綜合分析，並考量我國數位通訊傳播現況與基礎環境，擬定我國未來匯流環境下，所需之法規調和與法制革新之建議。

（三）辦理焦點訪談座談會

本研究規劃舉辦至少 5 場焦點訪談座談會，邀請與會對象包括一般民眾、公民團體、學者專家及網際網路相關服務業者。

具體而言，研究團隊將以電訪調查、國際資料研析等研究所得為基礎，設計切合本研究計畫之相關議題，並於會議中提供與會者進行討論，以了解焦點團體對於本研究所提策略規劃之想法與建議，進而完善本研究計畫之相關工作項目。

（四）量化問卷調查暨統計分析、檢定方法

本研究「我國網際網路傳播社會問題調查」之電訪調查及「我國主要網際網路傳播相關服務公共問責模式研析」之網路調查，將採用量化問卷進行統計分析。

其中，「我國網際網路傳播社會問題調查」係委託趨勢民調股份有限公司進行，調查對象涵蓋一般民眾、公民團體及網際網路傳播相關服務業者。一般民眾之樣本數至少達 1,100 份（信心水準至少 95％），採用電腦輔助電話訪問系統（Computer Assisted Telephone Interview System, CATI）進行電話訪問，公民團體及網際網路傳播相關服務業者則採面對面訪談之方式。調查所得之原始資料將以 SPSS 進行檢誤，並透過 Pearson 卡方檢定分析法，以「基本資料」對「各項議題」進行交叉分析，瞭解不同背景的民眾對各議題之看法是否具有所差異。

而「我國主要網際網路傳播相關服務公共問責模式研析」之網路調查則係委託典通股份有限公司，以其獨家開發之 EZChoice 行動 APP 為執行平臺。EZChoice 之會員人數達 10 萬餘人，具有實名登入、手機帳戶認證、基本資料反覆驗證等避免多重填卷之機制，且會員係依照我國行動族結構分布進行招募，母體為「居住於臺灣 22 縣市之普通住戶內年滿 12 歲之本國籍人口」，具有母體代表性，且其母體結構的涵蓋率已經達 75％以上。此部分之調查預計完成至少 300 份有效樣本數。

二、執行進度說明

本研究於契約生效次工作日起 270 日內提出之期末報告初稿，以下應包含之項目皆如期完成。

（一）我國網際網路傳播相關服務使用情形及主要問題盤點分析：

1. 透過廣泛蒐集國際及國內既有文獻及次級資料（包含政府機關、民間團體、學者發布之相關研究或調查報告），勾勒我國民眾接觸使用網際網路傳播相關服務之情形及常見問題。
2. 由民眾、公民團體、網際網路傳播相關服務業者等需求及問題角度出發，以基底（bottom-up）思維發展社會調查問卷，調查內容應以不重複，且能與既有文獻資料互補為原則。

（二）我國網際網路傳播社會問題調查與分析：

1. 就現行國際處理網際網路傳播社會議題之範圍及方式（包含但不限於歐盟、德國、法國、英國、美國、加拿大、澳洲、紐西蘭、日本、韓國、新加坡等國家）就處理議題、範圍與方法分類統整成概略性模式，作為本調查對受訪者之背景說明。
2. 就已蒐集之國際及國內文獻或次級資料，盤點出對一般大眾、公民團體及網際網路傳播相關服務業者調查之議題面向。
3. 問卷設計前置作業：辦理學者專家諮詢會議（至少 3 人），審

查問卷面向設計與關切議題重點，並作成紀錄。依諮詢建議完成問卷設計，經委託單位審核確認後定稿。

4. 針對一般大眾進行問卷調查，並針對公民團體、網際網路傳播相關服務業者進行面訪調查。

5. 針對一般大眾（至少 3 場，每場至少 8 人）、公民團體與專家學者（至少 8 人）、網際網路傳播相關服務業者（至少 5 人）辦理焦點團體訪談，就前述問卷與面訪之調查結果，交叉分析深入探討原因及因應之道。

（三）完整國際資料蒐集研析：

1. 針對社會調查彙整之網際網路傳播社會問題，綜整分析國際間（包含但不限於歐盟、德國、法國、英國、美國、加拿大、澳洲、紐西蘭、日本、韓國、新加坡等國家）最新相應作法及優劣比較分析。

2. 前項國際間作法應包含政府機關政策法制作為、第三方監督及產業組織自律作法等。

（四）國內主要網際網路傳播相關服務公共問責模式研析：

1. 蒐集並研析於我國提供服務之主要網際網路傳播相關服務公共問責模式之運作方式、分析其模式之優缺點，並探求公眾或第三方介入協助強化其問責之可行性。

2. 辦理諮詢座談會：針對社會調查結果、網際網路傳播相關服務公共問責模式、國際作法等相關研析資料，邀請業者及學者專家（至少 8 人）辦理諮詢座談。

3. 執行至少 300 份網路調查（來源至少取自 3 種不同服務類型的平臺），蒐集網路使用者對於社會調查結果及網際網路傳播相關服務問責模式之相關意見。

（五）綜合觀察與政策建議：

1. 彙整前述調查結果及研析資料，提出適合我國情境之議題相

應政策及法制建議。

2. 針對委託單位在網際網路傳播政策扮演之角色提出相關政策及法制建議。

第二章　國際間網際網路社會問題及處理模式研析

本章節將透過廣泛之資料蒐集，從「政府機關法制政策作為」及「第三方監督或產業自律機制」兩大面向切入，分別研析歐盟、德國、法國、英國、美國、加拿大、澳洲、紐西蘭、日本、韓國及新加坡所關注之網際網路社會問題及其處理模式。

如前所述，國際資料研析之作用在於提供比較與借鏡之基礎，除將作為本研究前期規劃網際網路傳播社會調查、網路調查問卷設計之基底，也將為後期我國網際網路社會問題之解決、法制政策建議之撰擬提供參考，對於本研究所有階段之規劃與進行皆具有高度之重要性。但考量本研究資料眾多，若報告之編排如實依循各階段國內外資料交互比較之思路，恐不利閱讀。因此，在報告之資料呈現上，研究團隊擬以本章率先聚焦國際資料之完整研析，再依序展示網際網路社會調查、網際網路傳播相關服務公共問責模式研析等研究成果，以利委託單位參考。

第一節　歐盟

一、監理脈絡

作為一多會員國組成之組織，歐盟對於網際網路相關服務之責任框架已有多年之討論及實務經驗，亦致力於各會員國規範之協調，其於 2000 年制定之《電子商務指令》（Directive on electronic commerce, 2000/31/EC, ECD）[1]即為最具代表性之規範框架。

然而，隨著網際網路進入更加去中心化的「web 3.0」時代，違法內容對社會造成影響之事件層出不窮，歐盟執委會（European Commission）也於 2020 年 12 月 15 日提出「數位服務法」包裹立法（The Digital Services Act Package），意圖改革過往《電子商務指令》之不足，力求在新時代下確立網路中介者之獨立義務。

具體而言，「數位服務法」包裹立法包含《單一市場數位服務暨修正電子商務指令之規章》[2]及《數位部門競爭性與公平性市場之規章》[3]兩部草案，分別簡稱《數位服務法》（Digital Services Act, DSA）及《數位市場法》（Digital Markets Act, DMA）草案。經過近兩年的立法討論，《數位市場法》已在 2022 年 7 月 18 日正式通過，並於 11 月 1 日開始生效，2023 年 5 月 2 日施行[4]；《數位服務法》則於 10 月 4 日正式通過，11 月 16 日生效，而除了部分條文先行施行外，本法原則上於 2024 年 2 月 17 日開始施行[5]。

---

[1] Council Directive 2000/31, of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce), 2000 O.J. (L 178) 1 [hereinafter ECD].

[2] Commission Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825 final (Dec. 15, 2020) [hereinafter DSA].

[3] Commission Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) COM(2020) 842 final (Dec. 15, 2020) [hereinafter DMA].

[4] DMA, Art. 54.

[5] DSA, Art. 93.

二、政府機關法制政策作為

（一）《數位服務法》

《數位服務法》之前身係歐盟於 2000 年通過之《電子商務指令》。該指令除以「資訊社會服務」（information society service）之概念廣泛涵蓋電商零售、通訊服務、網路搜尋引擎等網際網路上多樣化之經濟活動，亦確立了網路中介服務提供者（providers of intermediary service）的基本責任。《電子商務指令》之目標在於促進歐盟電子商務的發展，透過建構共同法律框架拉齊各會員國法律，進而確保會員國間資訊社會服務之自由流動與消費者對線上電子商務之信心[6]，但隨著網際網路相關服務之態樣日益創新，跨境網路中介服務提供者日漸興起，帶來法律遵循之不確定性，歐盟執委會遂於 2020 年提出「數位服務法」包裹立法，試圖建立新時代的網路中介服務提供者秩序。

就規範內容與責任體系而言，《數位服務法》乃過往《電子商務指令》之延伸與強化；但在立法形式的選擇上，相較於《電子商務指令》採用之指令（directive）形式係自歐盟層級制定共同目標，具體執行手段則留待各會員國以內國法規劃，《數位服務法》採用的「規章」（regulation）具有更高的強度，本身即具有歐盟全境一體適用之性質，無待各會員國另訂內國法即可落實[7]。究其原因，乃網際網路上之服務具有「無國界」之跨境提供性質，過往單純以國家層級進行之立法除不利歐盟單一市場之服務流通與利用，亦無法有效保護歐盟民眾與企業之網路安全及權利。面對不斷推陳出新之跨境數位服務，歐盟層級的一致化立法模式除可提供規範之可預見性及法律明確性，更可確保網路中介服務提供者應對任何網路違法內容時皆採取一致之行動，為所有歐盟民眾提供平等的保障。

在具體規範之擘劃上，《數位服務法》最大的特色在於承襲《電子商務指令》對於網路中介服務之定義，並自過往「連線服務」（mere

---

[6] *See* DIRECTORATE-GENERAL FOR THE INFORMATION SOCIETY AND MEDIA (EUROPEAN COMMISSION), EU STUDY ON THE LEGAL ANALYSIS OF A SINGLE MARKET FOR THE INFORMATION SOCIETY: NEW RULES FOR A NEW AGE? (2014).

[7] European Union, *Types of legislation*, https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en (last visited Aug. 11, 2023).

conduit）、「快速存取服務」（caching）及「資訊儲存服務」（hosting）三大基本服務態樣中，進一步延伸出「線上平臺」（online platform）、「非常大型線上平臺」（very large online platform, VLOP）與「非常大型線上搜尋引擎」（very large online search engine, VLOSE），視不同服務型態逐級課予相應之累加義務，且設立以服務提供者年收入或營業額計算之高額罰鍰，作為落實相關義務之手段。

經過兩年左右之審議，《數位服務法》已於 2022 年 10 月 4 日正式通過，並於 11 月 16 日生效。至於其施行日期，原則上定於 2024 年 2 月 17 日，但其中第 24 條關於線上平臺透明度報告之部分規範、第 33 條、第 37 條、第 40 條及第 43 條涉及執委會對非常大型線上平臺與非常大型線上搜尋引擎之職權規範，以及第 4 章罰則涉及非常大型線上平臺與非常大型線上搜尋引擎之第 4 節至第 6 節部分，則自 11 月 16 日生效日起同步施行[8]。

此外，執委會在 2024 年 2 月 17 日前，亦得依第 33 條第 4 項規定，先行指定非常大型線上平臺與非常大型線上搜尋引擎，使其在受指定 4 個月後先行適用相應之義務規範[9]。

1. 規範對象與定義

《數位服務法》之規範對象為以下數種類型之服務提供者：

（1）連線服務

連線服務為網路中介服務三種子類型之一。承襲《電子商務指令》之定義，係指提供通訊網路之接取，或在通訊網路中傳輸服務接收者所提供資訊之服務[10]。針對使用者透過連線服務所傳輸之資訊，若連線服務提供者並未主動發動該資訊之傳輸、並未篩選該資訊之接收者，且未就該資訊為任何篩選或修改，即無須就該資訊負責[11]。

[8] DSA, Art. 93.
[9] DSA, Art. 92.
[10] DSA, Art. 3(g)(i).
[11] DSA, Art. 4.

（2）快速存取服務

快速存取服務為網路中介服務三種子類型之一。承襲《電子商務指令》之定義，係指提供在通訊網路中傳輸服務接收者所提供之資訊時，基於促使或確保資訊傳輸更有效率之單一目的，而對資訊所為之自動的、中間的與暫行的儲存行為之服務[12]。

針對使用者透過快速存取服務所傳輸之資訊，若快速存取服務提供者並未改變存取之資訊、依服務使用條款接取資訊、依產業廣泛認可及普遍使用之方式更新資訊、並未透過干涉產業普遍使用之合法技術取得資訊使用資料，且於知悉儲存之原始傳輸來源被移除或限制接取，或經法院裁判或行政機關依法律所為行政處分要求移除或限制接取時，立即移除所儲存之資訊或限制其接取，即無須就該資訊負責[13]。

（3）資訊儲存服務

資訊儲存服務為網路中介服務三種子類型之一。承襲《電子商務指令》之定義，係指依使用者要求，而儲存該使用者所提供之資訊之服務[14]。針對使用者透過資訊儲存服務所傳輸之資訊，若資訊儲存服務提供者對涉嫌違法之內容不知悉，且於他人請求損害賠償時，依顯示之事實，亦不能察覺該內容為明顯違法；或知悉涉違法內容後，立即移除該資訊或限制其接取，即無須就該資訊負責[15]。

（4）線上平臺

線上平臺係《數位服務法》基於資訊儲存服務而延伸之新服務類型，指依使用者要求，將資訊儲存並向公眾傳散之資訊儲存服務提供者[16]。

其中，為因應線上平臺大量媒合使用者進行交易之現況，《數位服務法》亦於第 3 章第 4 節針對允許使用者締結通訊交易契約（distance contract）之線上平臺訂有特殊規範，要求此一類型之平臺

[12] DSA, Art. 2(g)(ii).
[13] DSA, Art. 5.
[14] DSA, Art. 3(g)(iii).
[15] DSA, Art. 6.
[16] DSA, Art. 3(i)

需遵守賣家溯源、使用介面設計要求、使用者之知悉權等義務，以提昇使用者之權益保障。至於「通訊交易契約」之定義，則須參照《消費者權利指令》（Consumer Rights Directive, Directive 2011/83/EU）第 2 條第 7 項之規定[17]，係指[18]：賣家與消費者在組織化的遠距銷售或服務提供方案下未有任何實體接觸，直至締結契約當下（也包括締結契約當下）僅透過一個或多個遠距通訊工具締結之契約。

（5）非常大型線上平臺

非常大型線上平臺係指歐盟境內月平均實際服務接收者達 4,500 萬人，且歐盟執委會經諮詢該服務所設立之會員國、或評估相關資料後指定之線上平臺。執委會也應對符合非常大型線上平臺要件之服務提供者進行造冊，並應視情況隨時更新名冊[19]。

在計算上，無論使用者與該線上平臺之互動方式係要求其儲存資訊，或接觸其儲存並透過線上介面傳輸之資訊，皆會被視為該線上平臺之「實際服務接收者」[20]。

按歐盟執委會 2023 年 4 月 25 日之公告[21]，首批被指定為非常大型線上平臺之服務提供者包括：Alibaba AliExpress、Amazon Store、Apple AppStore、Booking.com、Facebook、Google Play、Google Maps、Google Shopping、Instagram、LinkedIn、Pinterest、Snapchat、TikTok、Twitter、Wikipedia、YouTube，以及 Zalando；同年 12 月 23 日公告[22]指定之第二批非常大型線上平臺則有：Pornhub、Stripchat，以及 XVideos。

按《數位服務法》第 92 條之規定，前述之 17 家服務提供者需在受指定 4 個月後先行適用相應之義務規範，然以線上販售時尚服飾與

---

[17] DSA, Art. 3(l).
[18] Directive 2011/83/EU, Art. 2(7).
[19] DSA, Art. 33.
[20] DSA, Art. 3(p).
[21] European Commission, *Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines*, Press corner (2023/04/25), https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413 (last visited Aug. 12, 2023).
[22] European Commission, *Commission designates second set of Very Large Online Platforms under the Digital Services Act*, Press corner (2023/12/23), https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6763 (last visited Dec. 25, 2023).

美妝產品為主要業務、總部設立於德國的 Zalando 於 6 月 27 日向歐盟法院（Court of Justice of the European Union, CJEU）正式提起訴訟，主張其以零售為主之商業模式並不會帶來第三方散布有害或違法內容之系統性風險，並強調執委會採用之認定方法並未清楚一致，導致認定結果有失公平[23]。無獨有偶地，以線上零售為主要業務的 Amazon 也透過發言人在 7 月提出類似的主張，進而提起訴訟。Amazon 表示，《數位服務法》所欲處理之系統性風險應係來自提供言論及資訊傳遞服務、以廣告為主要收入來源之非常大型線上大型平臺，但此與 Amazon 之服務性質並不相同同，且 Amazon 本身甚至不是歐盟境內規模最大的零售商，執委會之指定有失公平[24]。

目前兩起案件皆由歐盟法院審理中，其結果有待後續追蹤。

（6）線上搜尋引擎

線上搜尋引擎係允許使用者以關鍵字、語音請求、詞組或其他形式輸入查詢一切主題，搜尋原則上所有或使用特定語言之網站，並以所查獲內容相關資訊之一定格式呈現搜尋結果之網路中介服務[25]。就此，《數位服務法》與 2019 年 6 月通過之《線上中介服務規章》（Regulation (EU) 2019/1150, P2B Regulation）[26]及《數位市場法》採用相同之定義。

值得注意的是，《數位服務法》雖將線上搜尋引擎定位為「網路中介服務」之一種，然其條文本身及立法說明皆未明言其究竟係屬連線服務、快速存取服務或資訊儲存服務，亦未如前述三種網路中介服務子類型般，針對線上搜尋引擎服務明訂相應之「安全港」規範，因而在解釋上，線上搜尋引擎能否適用資訊儲存服務之免責規定仍容有

---

[23] Zalando, *Zalando files legal action against the European Commission to contest its designation as a "Very Large Online Platform" as defined by the Digital Services Act* (2023/06/27), https://corporate.zalando.com/en/company/zalando-files-legal-action-against-european-commission-contest-its-designation-very-large (last visited Aug. 12, 2023).

[24] EURACTIV, *Amazon joins Zalando in challenging very large online platform designation* (2023/07/11), https://www.euractiv.com/section/platforms/news/amazon-joins-zalando-in-challenging-very-large-online-platform-designation/ (last visited Aug. 12, 2023).

[25] DSA, Art. 3(j).

[26] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, Art.2(5).

爭議。

（7）非常大型線上搜尋引擎

非常大型線上搜尋引擎與非常大型線上平臺相同，皆是以歐盟境內月平均實際服務接收者達 4,500 萬人作為門檻，且需由歐盟執委會經諮詢該服務所設立之會員國、或評估相關資料後進行指定[27]。而在計算上，透過請求該搜尋引擎，進而於其線上介面接觸其所排序及呈現內容之使用者，即屬該線上搜尋引擎之「實際服務接收者」[28]。

根據歐盟執委會 2023 年 4 月 25 日之公告[29]，首批被指定為非常大型線上搜尋引擎之服務提供者為 Bing 及 Google Search。按《數位服務法》第 92 條之規定，兩家服務提供者皆須在受指定 4 個月後先行適用相應之義務規範。

2. 累加義務設計

如前所述，《數位服務法》最大之特色在於，其係按網路中介服務提供者之服務性質及規模進行分類，逐級課予相應之義務，以確保其服務不致遭違法活動所濫用。此一設計係基於比例原則之考量，是故部分實質性義務僅課予擁有龐大使用者數量、就公共事務討論及經濟活動皆舉足輕重之非常大型線上平臺及非常大型線上搜尋引擎；相對而言，微小規模之企業則可豁免於部分義務之適用[30]。

《數位服務法》針對不同服務提供者類型所課予之層級化義務分述如下：

（1）所有網路中介服務提供者之義務

A. 配合內國法院或行政機關之命令

網路中介服務提供者應配合相關司法機關或行政機關之命令，採取打擊違法內容及使用者資訊開示之義務[31]。此規範之目的在於建立

[27] DSA, Art. 33.
[28] DSA, Art. 3(q).
[29] European Commission, *supra* note 21.
[30] DSA, Art. 19.
[31] DSA, Art. 9-10.

協力執法之平臺，只要個案涉及各會員國，網路中介服務提供者即應遵守該會員國之司法或行政機關依法所為之資料調取、移除或阻斷接取等命令；此外，本法也建立前揭命令之記載之事項，諸如事由、涉犯法條、必要性及救濟管道等，並應落實「透明政府」理念。

B. 指定聯絡窗口

網路中介服務提供者應設立單一聯絡窗口，以作為與內國主管機關、歐盟執委會與歐洲數位服務委員會之直接溝通管道[32]。此外，網路中介服務提供者亦應提供使用者之單一聯絡窗口，令使用者得以友善、迅速之電子方式與其直接聯繫[33]。

C. 指定法律代表

歐盟境外之網路中介服務提供者，若於歐盟境內提供資訊服務，應指定一位法律代表[34]。

D. 揭露服務使用條款

網路中介服務提供者應於服務使用條款中揭露其服務可能對使用者帶來之任何限制，包括其政策、程序、措施或用於內容調控（content moderation）之工具，包括以演算法進行之決策工具、人工審核機制及內部申訴審核系統等，且相關資訊皆應以清楚、明確、可理解、對使用者友善且無語言歧異之方式公開[35]。

此外，服務使用條款有任何顯著異動時，皆應通知其使用者。以未成年人為主要使用對象之服務提供者，亦應以其可理解之方式解釋服務使用條款之內容，以保障其權益[36]。

---

[32] DSA, Art. 11.
[33] DSA, Art. 12.
[34] DSA, Art. 13.
[35] DSA, Art. 14(1).
[36] DSA, Art. 14(2), (3).

E. 定期公布透明度報告

網路中介服務提供者應至少每年公布一次，以機器可讀之格式及易於接取之方式公布透明度報告[37]。線上平臺之透明度報告內容應額外包含訴外爭端解決機制及濫用機制防止措施之處理件數、時間與結果，以及揭露平臺使用之自動化措施等[38]；非常大型線上平臺應再額外揭露其投入內容調控之人力資源、人員能力審核、訓練與後勤狀況等，且應將法遵審查之查核報告及時交予數位服務協調官（digital services coordinators）與歐盟執委會，並在三個月內將報告公開[39]。

值得注意的是，《數位服務法》針對非常大型線上平臺及非常大型線上搜尋引擎之義務規範先行適用後，由 Facebook、Google Search、AliExpress 等受指定業者提出的第一波透明度報告仍有數據格式缺乏標準化、各家業者因對法條文字理解不同而有揭露範圍落差等問題，導致難以進行橫向之比較研析[40]，此一問題未來可能仍須透過執委會制定之指引解決。

（2）資訊儲存服務提供者之累加義務

A. 建立「通知即行動」機制

資訊儲存服務提供者應建立「通知即行動」機制。倘決定移除或阻斷他人接取系爭資訊，也應通知資訊提供者並清楚敘明其理由[41]。

B. 犯罪嫌疑通報

資訊儲存服務提供者若獲知可能發生、正在發生或即將發生涉及生命、人身安全危害之重大刑事犯罪或有此嫌疑之情事時，應迅速告知執法單位並提供相關資訊[42]。

---

[37] DSA, Art. 15.
[38] DSA, Art. 24.
[39] DSA, Art. 42.
[40] Gabby Miller, *First Transparency Reports Under Digital Services Act Are Difficult to Compare*, TechPolicy.Press (2023/11/23), https://www.techpolicy.press/first-transparency-reports-under-digital-services-act-are-difficult-to-compare/ (last visited Dec. 21, 2023).
[41] DSA, Art. 16-17.
[42] DSA, Art. 18.

（3）一般線上平臺服務提供者之累加義務

A. 建立內部與外部之權利救濟機制並防止其濫用

為減緩過度移除之疑慮，線上平臺應建立內部異議機制，當其決定移除或阻斷接取違法資訊、暫停或終止提供全部或一部服務或使用者帳號時，應提供不服該決定之當事人易於近用且友善之表達意見機制，使其可依循傳統民事訴訟程序外之內部申訴管道[43]。此外，線上平臺亦應擇定一外部單位或組織，協助其處理爭議，包含平臺透過內部申覆機制仍無法有效處理之紛爭[44]，而此訴外爭端解決機制並不妨礙當事人之訴訟權利。

相對地，線上平臺亦應採取必要措施以確保其「通知即行動」機制與內部異議機制不被濫用，必要時得暫停該使用者使用此功能[45]。

B. 建立認證舉報者機制

為提升「通知即行動」之「通知」品質，加速線上平臺處理違法內容，線上平臺應採取適當技術措施及組織規劃，確保其得以立即且優先處理「認證舉報者」（trusted flaggers）舉報事項之機制，而任何具有偵測、辨識及舉報違法內容之專業能力，且代表集體利益和獨立於線上平臺之外，並可秉持客觀、盡職之原則及時提出通知之實體（entity）[46]，即可由所在地之會員國之數位服務協調官加以認定，授予認證舉報者之資格。

若線上平臺知有認證舉報者提出大量不明確或不適當通知之情事時，應將必要之解釋理由及相關事證送交數位服務協調官。若數位服務協調官認定有啟動調查之相當理由，則該認證舉報者之資格應於調查期間暫停。數位服務協調官經調查認定該認證舉報者已不符資格規定時，亦應廢止該認證舉報者之認可[47]。

---

[43] DSA, Art. 20.
[44] DSA, Art. 21.
[45] DSA, Art. 23.
[46] 所謂實體，即係指個人無法擔任認證舉報者；同時實體並不妨為公法人等行政部門。 DSA, Rec. 61.
[47] DSA, Art. 19.

換言之，認證舉報者仍係「通知即行動」機制之一環，只是《數位服務法》建立了一條特殊通道，供線上平臺迅速採納其通知。

C. 線上介面

線上平臺之界面設計或編排，不得欺瞞、操縱，或扭曲、削減使用者自由決定之能力，例如：要求使用者進行選擇時賦予特定選項較高之顯著性、利用彈出式視窗等干擾使用體驗之方式重複要求使用者做成已做成之決定、刻意將終止服務所需之程序設計得較訂閱服務繁瑣等[48]。

由於數位時代的營利模式係以個人資料之分析與廣告精準投放作為基礎，使用者在平臺的停留時間與互動等數據皆可能被轉化為數位資本，平臺的使用者介面設計及使用者經驗皆可能形成某種「助推」（nudge），在自願性、非自願性，甚至潛意識影響的情況下左右使用者的意願與選擇，進而為平臺帶來「注意力經濟」之效益。透過此類「暗黑模式」（dark pattern）的誘導，使用者的意識認知與行為自主皆可能受到影響，導致其在無法完整同意或撤回同意、也無從保護個人資料及隱私的情況下受到平臺之服務使用條款拘束。

為防止線上平臺惡意透過「暗黑模式」對使用者之意思決定能力帶來危害，正式通過版之《數位服務法》特別新增此一要求，以應對服務提供者影響使用者選擇之情況[49]。

D. 線上廣告透明性

線上平臺負有線上廣告之揭露義務。展示廣告時，必須同時於使用者介面即時、清楚地向使用者展示該資訊為廣告、廣告主，及決定廣告投放對象之主要參數有用資訊[50]。至於非常大型線上平臺則更有特別義務，其應額外將所有投放之廣告彙集和儲存於資料庫，並向公

[48] DSA, Rec. 67.
[49] DSA, Art. 25.
[50] DSA, Art. 26.

眾揭露，且應自該廣告最後一次播放後保存一年[51]。

E. 資訊推薦系統之透明性

使用推薦系統之線上平臺應於其服務使用條款揭露主要參數，以及可供使用者調整或影響該主要參數之功能[52]。

F. 未成年人保障

線上平臺應於其服務為未成年人提供高規格之隱私、安全保障及防護措施，且不得展示基於未成年人個人剖析（profiling）之廣告，亦不得為遵循本法第 28 條所定之義務而進行額外之個人資料處理，以判定使用者是否具有未成年身分[53]。

（4）允許使用者與賣家締結通訊交易契約之線上平臺服務提供者之累加義務

A. 賣家溯源

站在為消費者確保更安全、更透明的網路環境的總體目標下，《數位服務法》特別強調「賣家溯源」（traceability of traders）之重要性，並據此明訂，允許使用者與賣家締結通訊交易契約之線上平臺有義務接收、儲存、部分驗證和發布使用其服務之賣家資訊。

若線上平臺允許其消費者與賣家締結通訊交易契約，則應負擔解決假冒和危險產品等之責任，意謂著服務平臺應在允許貿易商使用服務而進行交易前，確保取得並審查身分等相關必要資訊，即所謂賣家溯源。若該資訊有錯誤，線上平臺也應依歐盟或內國法規所定期限要求貿易商更正；對於不從者，則應暫停對其提供服務，直至其達到資訊完備為止[54]。

應注意者係，為求消費者保障之周延[55]微小企業不得豁免於本條

[51] DSA, Art. 39.
[52] DSA, Art. 27.
[53] DSA, Art. 28
[54] DSA, Art. 30.
[55] DSA, Rec.57.

義務之要求[56]。

B. 使用介面設計要求

若線上平臺允許其消費者與賣家締結通訊交易契約，其線上使用介面之設計與編排，應使賣家得以遵循其賣家溯源等義務，並使其可向消費者提供清楚之產品標示、商標展示等[57]。同樣地，微小企業亦不得豁免於本條義務之要求。

C. 使用者之知悉權

若線上平臺允許其消費者與賣家締結通訊交易契約，且得知有賣家利用其服務流通違法商品或違法服務時，應自知悉有此情事起，聯繫過去 6 個月內曾購買該商品或服務之使用者，告知該商品或服務之違法性、賣家身分等資訊[58]。同樣地，微小企業亦不得豁免於本條義務之要求。

（5）非常大型線上平臺及非常大型線上搜尋引擎之累加義務

A. 風險管理

雖然《電子商務指令》實施後，歐盟關於消費者保護、契約法或誤導性廣告等問題已經由相關法律之補充有所應對，但在當代網際網路生態的快速變遷下，演算法決策、線上廣告系統等新發展仍衍生出新的資訊不對稱。例如在某些情況下，平臺雖提供不同的服務，然其核心商業模式仍為廣告銷售，且與其他商業模式間具有相互依存之關係[59]，民眾、小型企業用戶或組織等卻無從監督這類龐雜且具有影響力之系統[60]，因而衍生出四類風險[61]：

---

[56] DSA, Art. 29.
[57] DSA, Art. 31.
[58] DSA, Art. 32.
[59] European Commission, COMMISSION STAFF WORKING DOCUMENT, IMPACT ASSESSMENT REPORT, ACCOMPANYING THE DOCUMENT: PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON A SINGLE MARKET FOR DIGITAL SERVICES (DIGITAL SERVICES ACT) AND AMENDING DIRECTIVE 2000/31/EC, SWD/2020/348 FINAL, Annex 5, at 110-111.
[60] *Id.* Annex 5, at 96.
[61] DSA, Rec. 80-84.

（a）濫用服務而傳散違法內容之風險：一為本身即屬違法之內容，諸如傳播兒童性暴力資訊或違法仇恨性言論等；二為與違法內容有關之違法活動，亦即提供歐盟或各會員國法律所禁止之產品或服務，例如銷售仿冒產品等。

（b）損害《基本權利憲章》所保護的基本權利之風險：包含表現與資訊自由、隱私權、反歧視之權利及未成年子女之權利等。該等權利可能因為非常大型平臺所設計的演算法系統、或有心人士藉由惡意濫用服務，或其他壓制言論或妨礙競爭等情事，進而引發受有損害之風險。

（c）對民主程序、公眾知悉、選舉程序，及公共安全之實際或可見之負面影響。

（d）故意、甚至經常性地操縱平臺服務，對健康和未成年人保護造成可預見影響之風險：例如透過創建假帳號、使用機器人或其他（部分）自動化措施，從而快速、廣泛的傳散違法內容或與違反線上平臺服務使用條款之資訊。

因此，非常大型平臺及非常大型線上搜尋引擎應建置必要的措施，致力降低風險評估中所發現的系統風險，應考慮以下措施：諸如加強或以其他方式調整其內容調控、演算法系統及線上介面等之設計與功能，以利阻止或限制違法內容的傳散、調整決策過程，或調整其服務使用條款[62]。

《數位服務法》規定非常大型線上平臺及非常大型線上搜尋引擎應至少每年一次進行風險評估，包括違法內容傳散、特定基本權之負面效果，或具負面效果之故意服務操縱；並應採取合理必要之措施減輕風險[63]。本條規範即在回應前開因「最佳化選擇系統」而服務可能遭資訊操縱等濫用情事。

[62] DSA, Rec. 87.
[63] DSA, Art. 34-35.

B. 危機處理機制

若影響公共安全或健康之重大危機發生時，執委會得依數位服務委員會之建議，要求非常大型線上平臺、非常大型線上搜尋引擎採取相應之特別措施[64]。所謂之危機可能肇因於武裝衝突、恐怖行動、地震或颶風等天災，以及疫情大流行等影響公共健康之跨境威脅[65]。

C. 外部風險稽核

非常大型線上平臺及非常大型線上搜尋引擎應至少每年 1 次，委託第三方組織進行獨立之法遵審查（independent audit），評估其是否符合本法規範之所有義務，並由該組織出具查核報告，倘查核結果非正面者，非常大型線上平臺則應於收受該查核結果起 1 個月內實施報告建議之改善措施，或應敘明其不採納報告建議之理由[66]。

D. 資訊推薦系統之透明性

除了線上平臺應遵守之資訊系統透明性要求外，非常大型線上平臺及非常大型線上搜尋引擎亦需提供使用者至少一種非基於個人剖析之主要參數調整選項[67]。

E. 線上廣告之特別透明性

非常大型線上平臺及非常大型線上搜尋引擎應額外將所有投放之廣告彙集和儲存於資料庫，並向公眾揭露，且應自該廣告最後一次播放後保存 1 年[68]。

F. 分享資料予主管機關

非常大型線上平臺及非常大型線上搜尋引擎應向數位服務協調官或歐盟執委會，以及研究者提供和分享必要資訊，以協助其監管與

---

[64] DSA, Art. 36.
[65] DSA, Rec. 91.
[66] DSA, Art. 37.
[67] DSA, Art. 38.
[68] DSA, Art. 39.

評估是否符合本法之規定。相對地，數位服務協調官或執委會僅能將該資訊用於《數位服務法》監管及法律遵循評估之目的，且應遵循個人資料保護等規範，以維護服務提供者之權益[69]。

此外，非常大型線上平臺及非常大型線上搜尋引擎，應依設立國之數位服務協調官或歐盟執委會之要求，向其說明自身演算法系統（包括內容推薦系統）之設計、運作及測試情形[70]。

G. 設置法遵單位

非常大型線上平臺及非常大型線上搜尋引擎應設置獨立於營運團隊之法遵單位（compliance function），並賦予其充分之監督權限與資源[71]。

H. 監管費

執委會每年得向非常大型線上平臺及非常大型線上搜尋引擎課徵監管費[72]。監管費之課徵目的在於支應執委會因執行《數位服務法》所生之監管成本，包括第 33 條針對非常大型線上平臺及非常大型線上搜尋引擎之指定與監理、第 24 條第 5 項共同資料庫之維持與運作、第 85 條協助執委會、數位服務委員會及數位服務協調官相互聯繫之資訊共享系統等支出。

3. 違法內容之處理

針對違法內容之處理，《數位服務法》第 3 條第 h 款將「違法內容」定義為「本身違反歐盟法或符合歐盟法之內國法之資訊，或與違反歐盟法或符合歐盟法之資訊相關之產品、服務等活動」。換句話說，違法內容可藉由各會員國之內國法加以定義。

除了「通知即行動」等機制外，《數位服務法》亦設有啟動要件相當嚴格之暫時資訊限制令作為阻斷違法內容之最後手段。按本法第

[69] DSA, Art. 40(1)-(2).
[70] DSA, Art. 40(3).
[71] DSA, Art. 41.
[72] DSA, Art. 43

51 條第 3 項規定，針對所有違反本規章之行為，若本規章可採取之處罰手段已用盡，但違反規章之行為仍在持續而造成嚴重傷害，且其他公權力之行使無從遏止時，若各會員國之數位服務協調官認定內國行政作為手段無效，且已涉及對個人生命或安全危害之刑事犯罪，即可在給予利害關係人至少 14 天書面說明之機會後，向內國法院聲請暫時限制接取該違法內容；若技術不可行時，則暫時限制接取該線上中介服務提供者之線上介面[73]。

針對非常大型線上平臺與非常大型搜尋引擎，《數位服務法》第 82 條則另行賦予執委會要求各國數位服務協調官啟動資訊限制令之權力，且該條規定並未以「內國行政作為手段無效，且涉及對個人生命或安全危害之刑事犯罪」作為前提要件，更要求內國法院准予暫時限制接取後，不得做出歧異之裁判[74]。

4. 罰則

針對違反本法所定義務之網路中介服務提供者，最高得處以年收入或營業額之 6%之罰鍰；資料申報不實或未能更正者，最高得處以年收入或營業額之 1%之罰鍰[75]。

而本法特別針對非常大型平臺設立罰則，針對違反本法所定義務或未遵循執委會之命令等情事，最高得處前一個會計年度總營業額之 6%之罰鍰；而若有未遵守依申報資料命令、更正不實訊息或提供完整資訊，未提供現場查檢等情事，最高得處前一個會計年度總營業額 1%之罰鍰，並自裁決日起算，每日最高得處前一會計年度之日平均營業額 5%之連續處罰[76]。

[73] DSA, Art. 51(3).
[74] DSA, Art. 82.
[75] DSA, Art. 52.
[76] DSA, art. 74-76.

5. 主管機關及監理機制

（1）數位服務協調官及歐洲數位服務委員會

為擔負《數位服務法》相關事務之實施與執行，本法新設「歐洲數位服務委員會」，委員會由數位服務協調官所組成，而數位服務協調官則是由各會員國指派一個或數個主管機關任之。數位服務協調官之主要功能為以獨立、公正、透明且妥速之方式負責該國境內有關《數位服務法》之一切事務，並確保國家層級間之協調，並向執委會與數位服務協調官提供本法規範事項之建議。

而為實行該法所訂任務之必要，亦賦予數位服務協調官擁有對網路中介服務提供者之調查權、對其採取臨時措施、接受其承諾、暫時限制用戶接取網路中介服務之權利等[77]。

另一方面，為適當監督非常大型線上平臺是否遵循本法，數位服務協調官可以要求其提交或報告特定數據，包含評估非常大型線上平臺所可能引發之系統風險和危害之相關數據，諸如內容篩檢、演算法系統、資訊推薦系統或廣告系統之準確度、運作及檢測。

（2）歐盟執委會

歐盟執委會亦屬監理單位之一環，除擔任歐洲數位服務委員會之主席[78]外，尚應協助發展與實施自願性之產業標準；且於必要時，得依職權邀請相關之非常大型線上平臺、非常大型線上搜尋引擎、線上平臺、線上搜尋引擎、網路中介服務提供者或公民團體組織與相關當事人，共同訂定行為準則或危機處置合作[79]。

特別是執委會應有權存取及調查任何相關文件、數據和資訊，並藉以監督有無遵守本法之相關義務，至於相關文件、數據和資訊之所有者為何或實際儲存之形式、位置，則在所不問。執委會可以向各會員國內之政府機關、公共機構，或任何自然人或法人索取與本法相關之資訊。執委會有權在獲得相關人員同意後，要求其說明相關數據資

[77] DSA, Art. 67-70.
[78] DSA, Art. 62(2).
[79] DSA, Art. 48.

料及演算法，並記錄其陳述。執委會亦被賦予實施與本法規定所必須之調查權限。

執委會得針對監督非常大型線上平臺是否有遵守與實施本法所定之義務而採取必要措施，亦得命其提供與說明相關數據和演算法[80]。甚可得至現場稽查（inspections），由執委會及其選任之查核人員或專家要求非常大型線上平臺或第 52 條第 1 項所指之其他人，對其組織、運作、IT 系統、演算法、數據收集及商業行為進行說明[81]。

（二）因應特殊違法內容之規範

如前所述，《數位服務法》之目的在於強化《電子商務指令》之不足，並透過規章形式建立歐盟全境一體適用、包含一般性違法內容處理之平臺問責規範。然而網際網路上之服務型態千變萬化，違法或有害內容對社會形成之風險程度亦高低有別，例如：可供使用者自行上傳影音內容之視訊分享平臺（video sharing platforms, VSP）即具有不同於一般社群網站之特殊性與影響力；涉及恐怖主義之違法內容則對實體社會之重大生命安全帶來危害，其處理往往具有更高之迫切性，故歐盟近年亦有針對此類較為特殊之違法內容議題制定相應措施，待《數位服務法》施行後，仍可作為其在網路違法內容處理之特別規範或補充。

舉例而言，2018 年通過之《修正視聽媒體服務指令》（Directive (EU) 2018/1808, “Revised AVMSD”）便將使用者可自行上傳內容之視訊分享平臺納入規管範疇[82]，視訊分享平臺服務有義務提供適當具體措施，以避免涉及暴力與仇恨性言論、影響兒少身心，或煽惑恐怖攻擊犯罪等之不當視聽商業通訊的內容傳播，包括親子鎖、內容分級、不當內容標記、採取兒少個資保護措施等義務。並保護無障礙之近用權益、彰顯公共利益、保護內容編輯責任者之權益、促進歐洲視聽媒體服務作品彰顯及其內容產製，且應促進共管架構與自律機制，增進媒體素養，且確保視聽媒體服務監理機關的獨立性，以具體維護歐盟

[80] DSA, Art. 67.
[81] DSA, Art. 69.
[82] Revised AVMSD, Art. 1(1)(aa).

視聽服務環境之健全發展[83]。

另一方面，2021 年 4 月 29 日通過、2022 年 6 月 7 日開始施行之《打擊線上恐怖主義內容規章》（Regulation (EU) 2021/784），則將規範對象定為提供儲存並應用戶要求而向公眾傳播資訊或資料之服務提供者，相當於《數位服務法》之線上平臺，課予其迅速刪除恐怖主義內容之義務。服務提供者原則上應配合主管機關要求移除或阻斷接取恐怖主義內容之命令，且須附理由說明何以移除或阻斷接取該內容。如未履行，則可能面臨其全球營業額 4%之高額罰鍰[84]。

三、第三方監督或產業自律機制

（一）與事實查核組織合作

隨著近年世界各國密切關注不實訊息對民主社會公共議題討論所造成之危害，歐盟在 2022 年 1 月 1 日也正式宣布啟動「歐洲事實查核準則計畫」（European Fact-checking Standards Project），將委託六家歐洲的獨立事實查核組織及不實訊息調查機構，草擬適用歐洲查核組織之《職業操守準則》（Code of Professional Integrity）[85]。該準則有望成為繼國際事實查核聯盟（International Fact-Checking Network, IFCN）2016 年公布之《事實查核準則》（Code of Principles）後，第二部可供國際依循之事實查核標準。

按「歐洲事實查核準則計畫」之規劃，歐盟執委會將向法國「法新社」（L'Agence France-Presse, AFP）、德國「Correctiv」、波蘭「Demagog」、義大利「Pagella Politica」、「Facta」，以及位於比利時的「歐盟不實訊息實驗室」（EU DisinfoLab）挹注總計 90 萬歐元之資金，預計在未來兩年內與歐洲相關之組織及研究團隊展開合作，以制定針對歐洲事實查核及公開來源資訊（Open Source INTelligence, OSINT）調查組織之《職業操守準則》，並為其他組織提供符合該準則

[83] Revised AVMSD, Art. 28b.
[84] Regulation (EU) 2021/784, Art. 2, 18; Rec. 17-18, 45.
[85] European Fact-checking Standards Project, https://www.disinfo.eu/projects/european-fact-checking-standards-project/ (last visited June 21, 2023).

之教育訓練。

按執委會之要求，「歐洲事實查核準則計畫」所催生之《職業操守準則》必須在歐洲的媒體生態下，制定出得以適用於不同規模及工作場域（包括政治查核、資訊查證、公開來源資訊調查）之準則，除了要求獨立性、中立性及道德標準，也須明定相關組織所需具備之主要技能、資格與能力，例如：數位技能、商業永續性與網路安全等。除此之外，也需將該組織與網路平臺、媒體、公民團體等有關單位之合作納入考量。另外，按「歐洲事實查核準則計畫」之初步規劃，查核社群擬成立一可代表歐洲事實查核社群之治理主體，負責執行相關之工作，以及各組織是否遵循《職業操守準則》之獨立評鑑。

（二）因應不實訊息之相關實踐準則

按照歐盟執委會之定義，「不實訊息」（disinformation）係指「可辨識為錯誤或誤導性之訊息」（verifiably false or misleading information），其目的在於達成特定經濟目的或意圖欺騙公眾。不實訊息之製作、提出與散布可能造成公眾損害，威脅民主政治與政策制定程序之公共利益，亦可能傷害歐盟公民之健康與環境安全[86]。

有鑑於此，歐盟執委會遂於 2015 年起採取一系列打擊線上不實訊息之措施，包括：成立「假新聞高階專家工作小組」（High Level Expert Group, HLEG）、公布「假新聞高階專家工作小組報告」（Final report of the High Level Expert Group on Fake News and Online Disinformation），以及於 2018 年 9 月公布《因應不實訊息實踐準則》（EU Code of Practice on Disinformation）[87]。

根據《因應不實訊息實踐準則》之定義，不實訊息本身並不包含誤導性廣告、錯誤報導、嘲諷性言論，或是明顯具有政黨色彩之新聞與評論。至於準則內容之落實則非屬強制性，可由業者自行決定是否簽署加入並履行相關規範。相應地，歐盟也會在每一年度評估簽署方

[86] European Commission, *Tackling online disinformation*, https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation (last visited Aug. 11, 2023).

[87] European Commission, *Code of Practice on Disinformation*, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation (last visited Sep. 14, 2023).

是否確實履行其義務，也會定期以會議檢討其執行進度與落實方式，藉此與數位平臺達成自律共識，使業者主動採取防止不實訊息之因應措施。

為追蹤《因應不實訊息實踐準則》之落實情況，歐盟委由其轄下組織「歐洲視聽媒體服務管制組織」（European Regulators Group for Audiovisual Media Services, ERGA）評估簽署業者之執行成效，而其主要評估依據有二，一為業者提出之自我評估報告（Self-Assessment Report, SAR），二為業者委託第三方機構審查其自我評估報告後所出具之意見報告。ERGA 並會從五大面向針對簽署業者所承諾之事項進行評估，據而提出改善準則之建議與配套措施[88]。

2021 年 5 月，歐盟執委會提出《執委會就強化因應不實訊息實踐準則之指引》（Commission Guidance on Strengthening the Code of Practice on Disinformation），提出加強實踐《因應不實訊息實踐準則》之具體建議，除呼籲簽署業者於 2021 年秋季提交相關承諾初稿予執委會[89]，也號召更多利害關係人共同參與[90]。而隨著 Meta、Google、Twitter、TikTok 等 34 個簽署平臺陸續加入，歐盟執委會更在 2022 年 6 月 16 日進一步發布新版《強化因應不實訊息實踐準則》（Strengthened Code of Practice on Disinformation）。新版準則之重點內容包括[91]：

- 增加參與者：除有大型平臺業者等陸續加入對抗不實訊息傳播之工作，亦歡迎更多的簽署成員加入。
- 確保散布不實訊息者無法透過廣告獲益，以此減少散布不實

[88] ERGA, *Report of the activities carried out to assist the European Commission in the intermediate monitoring of the Code of practice on disinformation (ERGA Report)*(June 2019), https://erga-online.eu/wp-content/uploads/2019/06/ERGA-2019-06_Report-intermediate-monitoring-Code-of-Practice-on-disinformation.pdf (last visited Sep. 15, 2022).

[89] *See* European Commission, *Commission presents guidance to strengthen the Code of Practice on Disinformation*, Press Release (2021/05/26), https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2585 (last visited Aug. 28, 2023).

[90] *See* European Commission, *The 2022 Code of Practice on Disinformation*, Shaping Europe's digital future, https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation (last visited Aug. 28, 2023).

[91] European Commisiion, *Disinformation: Commission welcomes the new stronger and more comprehensive Code of Practice on disinformation*, Press Release (2022/06/16), https://ec.europa.eu/commission/presscorner/detail/en/ip_22_3664 (last visited Aug. 28, 2023).

訊息之經濟動機。

- 納入新型態的資訊操縱行為，包括透過假帳號散布不實訊息、機器人帳號、或惡意的深偽（Deep Fake）等。
- 提供更完善的工具，為使用者對不實訊息之辨識、認知及示警進行培力；將事實查核機制擴張至所有歐盟國家及所有歐盟國家使用之語言，並確保事實查核工作可獲得公平之報酬。
- 透過更妥善之標示，及有關贊助者、經費、投放期間之更完善資訊，令使用者可更輕易地分辨出政治廣告，以確保政治廣告之透明化；為研究者提供更便利的平臺資料獲取管道，以強化對研究者的支持；透過強化的監督框架與平臺定期報告評估平臺對承諾之落實與成效。
- 建立透明化中心與任務小組，藉由簡化與透明之方式審查行為準則之落實狀況。

值得注意者係，《數位服務法》正式通過後，前述針對不實訊息的各種準則與指引也成為了歐盟新法制框架下的共同監管工具。

《數位服務法》在其前言便指出:歐盟執委會及歐洲數位服務委員會應鼓勵自願性行為準則之起草與相關規範之落實，以協助本法實施[92]，尤應注意特定違法內容之風險減輕措施需透過自律或合意共管方式推動，也應注意特定系統性風險對社會及民主體制可能帶來的負面影響，例如不實訊息，或具有操縱性、虐待性等戕害未成年人之行為等。

針對不實訊息等領域之系統性風險，非常大型線上平臺或非常大型線上搜尋引擎之服務提供者若有參與、落實既有行為準則之事實，雖無法作為推定其確實遵守本法義務之唯一依據，但若服務提供者確實堅守及遵循既有之行為準則，將有可能被視為已採取妥適之風險減輕措施。相對地，若服務提供者在缺乏正當理由的情況下拒絕加入此

[92] DSA, Rec. 103.

類行為準則，此一情事亦有可能會在判斷其是否違反《數位服務法》所課予之義務時一併被納為審酌因素[93]。

另一方面，《數位服務法》也在其前言特別指出：本法所有關於行為準則之條文皆可為歐盟層級之既有自律規範提供基礎，例如執委會已發布、作為「歐洲民主行動計畫」（European Democracy Action Plan）[94]一環之新版《強化因應不實訊息實踐準則》即為一例[95]。

換言之，在不實訊息的應對上，具有規章性質的《數位服務法》與《因應不實訊息實踐準則》、《強化因應不實訊息實踐準則》等自願性質之準則實可共同發揮相輔相成、環環相扣之作用。在此框架下，《數位服務法》提供的誘因將有助於提昇業者加入簽署相關行為準則之意願，簽署相關行為準則亦有助於業者對《數位服務法》之法律遵循。而相對地，執委會針對前述準則發布之《執委會就強化因應不實訊息實踐準則之指引》，對於簽署業者而言便會因此具有相當於解釋性行政規則之地位，對於業者之法律遵循亦至關重要。

隨著《強化因應不實訊息實踐準則》的各簽署平臺陸續提出第一次報告[96]，歐盟執委會價值與透明性副主席（Vice-President for Values and Transparency）Věra Jourová 也在 2023 年 6 月時指出：面對來自俄羅斯之戰爭宣傳與資訊操縱等關鍵議題，該行為準則之成效仍嫌緩慢，且近來更有歐盟 2024 年大選、AI 生成內容之濫用等議題需要面對，呼籲各平臺無論語言、規模，皆須共同提昇打擊不實訊息之努力。執委會內部市場委員（Commissioner for Internal Market）Thierry Breton 則表示：各大簽署平臺提出之報告雖然提供了非常有價值的資料，但

---

93 DSA, Rec. 104.

94 「歐洲民主行動計畫」之內涵可分為四大面向，包括「公正選舉」、「杜絕不實訊息」、「媒體自由」，以及作為核心之「公民與公共社會培力」，其重點措施包括：透過《數位服務法》及不實訊息相關實踐準則課予線上平臺責任、針對外國勢力之資訊操縱與選舉干預強化反制工具、制定促進媒體編輯獨立性、廣告透明化與禁止針對媒體使用間諜軟體之《歐洲媒體自由法》（European Media Freedom Act）等。*See* European Commisiion, *Protecting democracy*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy_en (last visited Dec. 14, 2023); European Commisiion, *Defence of Democracy – Commission proposes to shed light on covert foreign influence*, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6453 (last visited Dec. 23, 2023).

95 DSA, Rec. 106.

96 Transparency Centre, *Reports Archive*, https://disinfocode.eu/reports-archive/?years=2023 (last visited Dec. 8, 2023).

也顯示事實查核量能、歐盟境內之內容調控、對研究單位之資料開放等面向仍有許多努力空間，未來《強化因應不實訊息實踐準則》甚至有可能被執委會採納為法規命令，成為非常大型線上平臺按《數位服務法》系統性採取風險緩解措施應依循之標準[97]。

（三）打擊線上仇恨言論行為準則

歐洲因近年接受大量難民，引發難民與極端主義份子間之衝突，歐盟對於仇恨性言論之容忍度有日漸降低之趨勢，遂於 2016 年與 Facebook、Google 與 Twitter 等社群平臺業者共同簽署《打擊線上仇恨言論行為準則》（Code of Conduct on Countering Illegal Hate Speech Online）[98]，嗣後於 2018 年至 2021 年間，亦加入 Instagram、Google+、Dailymotion、Snapchat、Jeuxvideo.com、TikTok 和 LinkedIn 等其他社群平臺，意即涵蓋歐盟市場 96%之社群平臺皆同意參與仇恨言論打擊之行列。

此行為準則要求平臺業者制定禁止仇恨言論的規則和社群標準，並建立系統和團隊來審查違反此類標準的內容；應於 24 小時內審查經標記之內容，並在必要時刪除或禁止訪問仇恨言論內容；針對仇恨言論的內容對員工進行培訓；與其他機構建立合作夥伴關係並開展培訓活動，以擴大其與認證舉報者之網路合作；設置負責應對聯繫國家主管機關之主責窗口；增強平臺對於使用者與公眾之透明度等。

《打擊線上仇恨言論行為準則》施行後，歐盟自 2016 年至 2021 年間已進行過 6 次施行成效評估，其評估方式乃透過民間機構與會員國官方組織之協力，針對簽署業者發送關於仇恨性言論之通報進行測試，以評析其對於此類訊息的處理成效及速度。

---

[97] European Commisiion, *Strengthened Code of Practice on Disinformation: Signatories to identify ways to step up work one year after launch* (2023/6/2), https://digital-strategy.ec.europa.eu/en/news/strengthened-code-practice-disinformation-signatories-identify-ways-step-work-one-year-after-launch (last visited Dec. 8, 2023)

[98] Council of European Union, Progress on combating hate speech online through the EU Code of conduct, https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/assessment_of_the_code_of_conduct_on_hate_speech_on_line_-_state_of_play__0.pdf (last visited Aug. 18, 2023).

四、小結

近年來，歐盟已深刻認知到跨國數位平臺對其單一市場所帶來之競爭與系統性風險，故其係以效力強於《電子商務指令》之《數位服務法》為全境一體適用之法規基底，明確課予服務提供者更高的責任，並配合其他特殊違法內容之補充性處理機制，共同構成網路違法內容之處理體系。

《數位服務法》採累加義務模式，著重於處理線上違法內容、強化平臺之透明度，並因應網際網路之跨境特性而設立數位服務協調官、歐洲數位服務委員會等，透過更高強度、全境適用且設有高額罰鍰之規章，建構安全而具問責機制之網路空間，進而達到保障數位服務消費者之目的，其監理數位平臺之態度已明顯走向積極、事先干預之路徑。但另一方面，歐盟也並未停止業者自律、公私協力機制之推動，近期仍持續強化其因應不實訊息實踐準則、推動歐洲事實查核準則計畫等，以因應不實訊息流竄對社會形成之危害。《數位服務法》本身也提供業者加入自願性實踐準則之誘因，在不實訊息等風險之應對與減輕上發揮相輔相成之效果

作為世界舉足輕重、可透過強大市場力量使其制度外溢之龐大經濟體，歐盟近年來的政策也展現了「布魯塞爾效應」(Brussels effect)，使世界各國逐漸興起平臺問責之相應立法倡議。就國際數位匯流之發展與監理趨勢而言，歐盟《數位服務法》之推行成效無疑是值得持續且密切關注的關鍵指標。

第二節　德國

一、監理脈絡

德國的媒體監理，乃各邦之治理權限，非屬中央職權。為了統一全國媒體監理密度，各邦媒體管理局共同組成「邦媒體管理局協會」（Die Medienanstalten），就達全國性質之媒體事務進行觀察。

針對去年德國國民的數位媒體使用情況，邦媒體管理局協會公布兩份文件，分別為「影音趨勢 2022」（Viedo Trends 2022）[99]以及「邦媒體管理局協會 2022 年多元性報告」（Vielfaltsbericht 2022 der Medienanstalten）[100]，是相當合適的參考資料。以下分別就「影音趨勢 2022」之數據、「邦媒體管理局協會 2022 年多元性報告」中所彰顯之各方面訊息來論述，尤其是民眾使用社群網站的重要意義，以及因年齡階層呈現出不同的網路使用習慣。

（一）德國國民影音收視方式逐漸移轉到線上

「影音趨勢 2022」主要針對德國國民的收視方式進行調查。直至 2022 年，能夠連接網際網路收看網路影音的設備，已經達到 92%[101]。2022 年德國國民使用網路影音之內容，估計已經達到 84.6%的民眾有收看過網路影音，而幾乎每天都會收視者，已將近 50%[102]。這已顯示網路影音越來越受到國民喜愛。

雖然國民仍花近半數收視時間在收看傳統電視，然而不容否定的是，民眾留給收看直播串流（Livestream）與隨選隨看視訊（Video On Demand, VOD）的時間比率持續在增加，從 2016 年的 20%一路翻倍成長到 43.5%[103]。再對網路影音內容類型進一步分析，發現影音分享

[99] Die Medienanstalten, *Viedo Trends 2022*, abrufbar unter: https://www.die-medienanstalten.de/fileadmin/user_upload/die_medienanstalten/Publikationen/Digibericht_Video/2022_Video_Trends/Video_Trends_2022.pdf (letzter Abruf Juli 20, 2023).

[100] Die Medienanstalten, *Vielfaltsbericht 2022 der Medienanstalten*, abrufbar unter: https://www.die-medienanstalten.de/fileadmin/user_upload/die_medienanstalten/Publikationen/Vielfaltsbericht/Vielfaltsbericht_2022_DMA_final_WEB.pdf (letzter Abruf Juli 20, 2023).

[101] Die Medienanstalten, a.a.O. (Fn. 1), S. 3

[102] Die Medienanstalten, a.a.O. (Fn. 1), S. 3

[103] Die Medienanstalten, a.a.O. (Fn. 1), S. 4.

服務的使用情況是最為普遍的，約有總人口的 62.8%一個月內至少使用一次，每日使用人口則占其中使用人口四分之一，為 27.9%；有趣的是，透過社群網站所傳送之影音收看者最少，約總人口 37.4%，但是每日使用者的比例卻很高，占使用人口的 46.6%[104]。這或許能反映出網路各種影音型態的服務特性，例如影音分享服務可能具有較高的多元性，產生較為多數的用戶需求，但由於觀眾的收視目的性較為強烈，也就導致收看黏著度較低。

（二）社群網站作為民眾使用網路的重要資訊來源

另一方面，「邦媒體管理局協會 2022 年多元性報告」也揭露了許多德國民眾網路使用習性的重要內容。首先，該報告指出，對於德國民眾而言，傳統電視仍為最重要的獲得資訊途徑，每日媒體觸及率仍達 55.5%，但與 2020 年下半年相比已有些微下滑；反之，網際網路則呈現微小但持續性的成長，來到 53%，已接近傳統電視；其餘者，廣播重要性持續微幅下滑，佔據 47.7%，傳統報紙持平，始終維持在 3 成線附近，雜誌則有些微上升的趨勢，到達 10.1%[105]。不過，問起民眾心中看法，卻認為網路才是最重要的資訊來源，其次才是電視與報紙，這樣的觀念在近幾年並無太大變動[106]。

就此趨勢，該報告特別針對社群網站對民眾接收資訊的重要性進行調查。首先，與 2017 年相比，14 歲以上之社群網站使用人口，從原本的 1,510 萬人，大幅提升到 2,350 萬人，且這種現象廣泛出現在各年齡層[107]。換言之，已幾乎是三分之一德國人口會透過社群網站接收資訊。至於民眾對社群網站與傳統媒體（傳統電視、廣播、報紙、雜誌、周刊、新聞雜誌等與以上媒體透過網頁、App、電子紙所呈現之數位化版本）之間的每日觸及率關係，會隨著年齡階層而有差異。以 14 歲以上人口總括來看，僅使用傳統媒體者仍較主流，占據 52.2%，同使使用社群網站與傳統媒體吸收資訊者，占據 29.3%，僅使用社群網站者，占據 4.1%，不使用傳統媒體與社群網站而僅使用其他

[104] Die Medienanstalten, a.a.O. (Fn. 1), S. 5.
[105] Die Medienanstalten, a.a.O. (Fn. 2), S. 10.
[106] Die Medienanstalten, a.a.O. (Fn. 2), S. 10.
[107] Die Medienanstalten, a.a.O. (Fn. 2), S. 34.

網路資源者，只有 2.5%，其餘為不接觸資訊者；這項數據隨著年齡層越低，而導致只使用傳統媒體者的比例大幅下降，例如，50 歲以上族群有 74.3%僅使用傳統媒體，而只有 13.8%亦使用社群網站，然而在 14 歲到 29 歲這一族群，前者僅有 15.7%，後者則有 53%[108]。

從社群網站茁壯為主流資訊來源的情況來看，可以推測德國民眾接收資訊之習慣漸漸往網路靠攏，且隨著年齡層越低，這種情況愈加明顯。如果將視野放大至整個網路媒體服務之範疇，社群網站作為資訊來源的地位也是顯著的。

「邦媒體管理局協會 2022 年多元性報告」調查社群網站與其他具有網路中介者性質服務之間被當作資訊來源的重要性關係，像是即時通訊軟體、影音分享平臺、搜尋引擎，從中發現了一些有趣現象。網路中介者總體而言，對於 14 歲以上德國國民，有 67.4%的人會將各種網路中介者視為資訊來源，其中最常使用者為即時通訊，有 6,240 萬人，但是將其視為資訊來源者僅有當中 5.6%，次常使用者為搜尋引擎，有將近 6,100 萬人，其中將搜尋引擎視為資訊來源則有其中 51.1%，接著為社群網站的 4,390 萬人，當中卻有高達 57.6%的人將其視為資訊來源，最後則是影音分享平臺的 3,850 萬人，僅有 36.1%視為資訊來源[109]。由此可見，社群網站對於當今公共意見形成活動而言，占有重要地位。

（三）年輕族群之網路使用習慣有顯著差異

除了對於社群網站作為主要的資訊來源，「邦媒體管理局協會 2022 年多元性報告」特別關切青少年與青年族群相較於整體國民的網路使用習慣差異，正如前開所說，網路作為資訊來源情況，越年輕族群是越顯著的。調查年輕族群與其他族群的網站使用習慣，恰可作為德國當前產業調查的指引。該研究將各種線上服務作為分類，分別觀察不同年齡族群的資訊接收習慣是否有顯著差異。答案應該是肯定的，因為 14 歲到 29 歲世代，相較於整個德國使用網路族群，顯然容

[108] Die Medienanstalten, a.a.O. (Fn. 2), S. 40.
[109] Die Medienanstalten, a.a.O. (Fn. 2), S. 28.

易接受傳統電視電台與報紙、雜誌等新聞出版事業所提供的各項電子化影音服務，除此之外使用 Wiki 百科、其他類似 Wiki 的百科全書資料庫與部落格的比例也都高於一般國民[110]。

從最常被使用的網路中介者前五名來觀察，分別為 Instagram（社群網站類型，總體國民之每日媒體觸及率 24.6%，年輕族群 65.3%）、Facebook（社群網站類型，總體國民之每日媒體觸及率 23.2%，年輕族群 25.2%）、WhatsApp（即時通訊軟體類型，總體國民之每日媒體觸及率 60.7%，年輕族群 88.3%）、YouTube（影音分享平臺類型，總體國民之每日媒體觸及率 36.7%，年輕族群 71.1%）與 Google（搜尋引擎類型，總體國民之每日媒體觸及率 58.4%，年輕族群 81%）[111]。

至於在是否特別將網路中介者視為資訊來源的調查中，本報告列出了 5 個社群網站類型事業，分別為 Instagram、Tiktok、Facebook、Twitter、Snapchat，其中最受年輕族群青睞者為 Instagram，相較於總體國民的每日媒體觸及率 9.7%，來到 29%，可謂差距甚大。另一差距較大者為 Tiktok，3.6%對上 14.1%，其餘網站則較無顯著差異。而就即時通訊軟體方面，WhatsApp 與 Telegram 對於年輕族群的每日媒體觸及率亦較高一點，不過由於後者數量太少，在此不贅述；至於影音分享平臺類型，僅有調查 YouTube，13.4%對上 29.4%；搜尋引擎列出 Google 與 Bing，明顯是 Google 具有壓倒性的使用者，且頗受年輕族群青睞，每日媒體觸及率高達 42.4%，高於一般國民的 29.5%[112]。

值得一提的事，該報告也對德國新聞整合平臺的使用習慣進行了首次調查。以 14 歲以上國民來看，最高為 Google News 的 7.6%，其次為 Google Discover 的 5.7%，再者 Upday for Samsung 的 4.9%，接續為 Apple News Widget 的 4.3%，接下來為 Facebook News 的 2.9%，接續為 msn 的 2.2%，最後兩名為 Huawei Assistant Today 的 0.6%與 yahoo 的 0.5%；反觀年輕族群，有相當高的比例集中在 Google News、Google Discover 與 Apple News Widget，都超過 10%，其餘不同業者

[110] Die Medienanstalten, a.a.O. (Fn. 2), S. 13.
[111] Die Medienanstalten, a.a.O. (Fn. 2), S. 16.
[112] Die Medienanstalten, a.a.O. (Fn. 2), S. 17.

所提供的服務則與 14 歲以上國民相差不大[113]。

二、政府機關法制政策作為

（一）NetzDG 之適用爭議與法院裁定

近年來，德國針對網路中介服務最重要之立法當屬 2017 年制定之《強化社群網站法律執行法》（Netzwerkdurchsetzungsgesetz, NetzDG）。

為因應社群網站上持續增長之仇恨性言論等種類多樣之違法內容，避免其對自由、開放與民主的共同生活形成威脅，NetzDG 課予社群網站服務提供者建立違法內容申訴及處置程序之義務。按該法第 3 條之規定，服務提供者在接獲申訴後，應立即檢查被申訴之內容是否確有違法之情事，除非服務提供者與擁有管轄權之刑事調查機構約定較長之移除或封鎖時限，否則應於接獲申訴後之 24 小時內執行移除或者封鎖明顯違法之內容。至於非屬明顯違法之內容，則原則上應於接獲申訴後之 7 日內執行刪除或封鎖。

不過，NetDG 也設有兩種不受 7 日移除限制之例外[114]。其一，當被申訴內容之違法性取決於事實陳述之真實性或可得而知應以其他事實狀態為依據時，服務提供者應給予當事人陳述意見之機會；其二，服務提供者接獲申訴後，於七日內將該案移轉給「受認可的受管制之自我管制機構」（anerkannte Einrichtung der Regulierten Selbstregulierung），以該機構之決定作成最終決定。

由於 NetzDG 自施行以來便遭遇諸多批評，論者指出該法對於使用者發言權利之保障明顯不足，恐形成「過度封鎖」（overblocking）之危險[115]，2021 年的《修改 NetzDG 法案》遂透過新增第 3b 條異議程序與第 3c 條調解機制進行使用者權益之補強。但另一方面，NetzDG

[113] Die Medienanstalten, a.a.O. (Fn. 2), S. 31.

[114] Liesching, in: Paschke/Berlit/Meyer/Kröner (Hrsg.), Hamburger Kommentar Gesamtes Medienrecht, 4. Aufl., 2021, 71. Abschnitt, Rn. 24.

[115] *E.g.* Eifert/v. Landenberg-Roberg/Theβ/Wienfort, a. a. O. (Fn. 217), S. 187 f; Hong, a. a. O. (Fn. 201), S. 82 f.

也面臨了違反歐盟指令爭議之批評。

1. 爭議緣起與第一次裁定

按照 NetzDG 第 1 條第 1 項與第 2 項之意旨，凡於德國境內提供服務之非小型社群網站，均受有本法所制定之相關義務。換言之，本法採取所謂市場地原則[116]。然而，自 NetzDG 生效以來，認為其違反歐盟層級法規之爭議，始終不斷。因為，對於歐盟境內之電子媒體制定基礎規制框架之《電子商務指令》（E-Commerce-RL）中的第 3 條，即有關內國法適用範圍規定，顯然採取所謂來源國原則，也就是電子媒體原則上僅受到其營業處所在地之歐盟國法律拘束，不受歐盟其他國家之法律限制[117]。基於轉換前開指令要求而制定之德國《電子媒體法》（Telemdiengesetz）第 3 條，亦不可避免地採取來源國原則。即便德國國會對此爭議有所意識，在 2021 年亦進行相當程度修法，同樣不能避免違法性質疑；復加上德國立法者於 2020 年也基於其他歐盟指令之故，而就《電子媒體法》（Telemdiengesetz）新增影音分享平臺之規定，進而產生出極為複雜的適用關係[118]。

何以 NetzDG 自立法起就遭遇到違反歐盟法之質疑，按照 Liesching 教授的看法，德國在制定 NetzDG 時，恐怕並未就《電子商務指令》之來源國原則規定進行足夠縝密的審酌。最核心的關鍵，在於《電子商務指令》第 3 條第 4 項規定，各會員國僅得於個案情況下實施規避會員國原則之具體保護措施，不過德國卻以制定法律之方式實施對於境外社群網站之管制；既然 NetzDG 為具有一般、抽象性質的「法律」，那麼，其規制作用實非僅針對個案而已[119]。況且，這些規避來源國原則措施之實施，依據同條第 6 項，必須立即向歐盟執委會進行通報，並由歐盟執委會判斷合法性，然而德國並無踐行合法的通

---

[116] 王牧寰、林家暘、陳譽文等，數位科技應用發展暨我國匯流法制革新規劃研究，國家通訊傳播委員會委託研究成果報告，頁 182（2021）。

[117] 陳志宇、林家暘、吳秦雯、江耀國、王牧寰等，因應國際數位匯流發展趨勢之法制研究，國家通訊傳播委員會委託研究成果報告，頁 108 以下（2022）。

[118] 同上註，頁 102 以下。

[119] Liesching, *Gilt das NetzDG für Facebook, YouTube und Twitter?*, abrufbar unter: https://community.beck.de/2020/02/11/gilt-das-netzdg-fuer-facebook-youtube-und-twitter (letzter Abruf Juli 20, 2023). Dazu auch vgl. Grünwald/Nüßing, Vom NetzDG zum DSA: Wachablösung beim Kampf gegen Hate Speech, MMR 2021, 283, S. 284.

報歐盟執委會程序[120]。

這項爭議，隨著 YouTube 與 Meta 向德國科隆行政法院（Verwaltungsgericht Köln，以下稱 VG Köln）聲請暫時凍結 NetzDG 數項規定，法院同意原告部分請求，凍結 NetzDG 第 3a 條之犯罪嫌疑通報聯邦刑事局（Bundeskriminalamt）義務條款，更顯激烈。

VG Köln 認為，NetzDG 第 3a 條（發現違法內容即時通報聯邦刑事局義務）明顯牴觸了《電子商務指令》第 3 條第 2 項之來源國原則，主要理由在於 NetzDG 之制定過程並無踐行該指令第 3 條第 4 項第 b 款以及第 5 項所規定之通知程序，以前規定而言，德國並未先行敦請其他會員國執行相關措施或者有其他會員國實行相關措施無成效或有所不足之情形，亦無告知其他會員國以及歐盟執委會將執行相關措施之意圖，以後規定而言，德國亦無儘速告知歐盟執委會於其他會員國執行特定措施之情形，並附上存有緊急情況之理由[121]。

至於前開 Liesching 教授所質疑的「把法律當成措施」事項，VG Köln 仍持開放立場，不表示法律見解[122]。不過，VG Köln 卻駁回原告所主張亦應凍結 NetzDG 第 3b 條（建構對於社群網站違法內容與否決定之異議申訴程序之義務）效力之聲請[123]。法院的理由在於，此項義務規定仍合於《電子商務指令》第 14 條第 3 項，換言之，既然該指令同意，各會員國法院或行政官署得對資訊儲存服務提供者要求停止、阻止違法狀態，以及允許各會員國制定移除或封鎖該資訊接取途徑之程序，那麼各會員國無論如何應能依此建構有關違法內容之處置程序[124]。

---

[120] Liesching, a.a.O.(Fn. 19).
[121] VG Köln, Beschl. V. 01.03.2022 – 6L 1277/21, Rn. 221 ff.
[122] VG Köln, Beschl. V. 01.03.2022 – 6L 1277/21, Rn. 214 f.
[123] VG Köln, Beschl. V. 01.03.2022 – 6L 1277/21, Rn. 150 ff.
[124] VG Köln, Beschl. V. 01.03.2022 – 6L 1277/21, Rn. 240 ff. 另參見陳志宇、林家暘、吳秦雯、江耀國、王牧寰等，前揭註 116，頁 110。

2. 終局裁定結果

原告不服 VG Köln 之部分裁定，其認為，法院一方面同意暫時凍結第 3a 條與第 4a 條之效力，另一方面卻又讓第 3b 條繼續適用，這種區別待遇並無理由，因此對第 3b 條部分提出抗告。本案由北萊茵·西伐利亞高等行政法院（Oberverwaltungsgericht Nordrhein-Westfalen，以下稱 OVG NRW）於 2023 年 3 月 21 日作成裁定，其變更 VG Köln 之原裁定，並同意原告多數主張，確認原告於主要程序判決確定前，暫不受有 NetzDG 第 3b 條之義務[125]。因此，OVG NRW 與 VG Köln 的見解最大差異處，可說是對《電子商務指令》第 14 條第 3 項適用範圍之理解。整體而言，高等行政法院的見解可以區分成三個分面來談，以下分別論之。

首先、也是最為重要的關鍵點，在於 OVG NRW 認為，雖然《電子商務指令》第 14 條第 3 項同意各會員國得建構移除或封鎖該資訊接取途徑之程序，然而此條具有內在效力界限，正是同指令第 3 條第 2 項之會員國原則，易言之，第 14 條第 3 項之規範內容並不能構成會員國原則的例外或特別規定[126]。法院特別強調，《電子商務指令》第 12 到第 15 條之所以確立起各種電子商務服務提供者之規範，主要目的仍在於創造各會員國的法律狀態之一致性，這些規範作為一種於部分領域生效之特別規定，使各會員國各自獲得實施一定程度相關措施之權能，而仍不被視為違反共同市場之精神[127]。故第 14 條的作用，在於使歐盟境內的資訊儲存服務提供者獲得一致性的「責任豁免特權（Haftungsprivilegierung）」，更具體言之，使其在滿足一定條件下（尤其是吾人所熟知的「知悉即行動」）毋庸回應他方主張停止作為或除去作為之請求權，其中同條第 3 項之目的，實為《電子商務指令》容許各會員國對此豁免特權設定僅適用於各國之特殊限制，從而不能遽而論定，此條款可作為會員國原則之例外規定，使得會員國可以直接對境外之資訊儲存服務提供者實施限制措施或制定限制性之法律[128]。

[125] OVG NRW, Beschl. V. 21.03.2023 – 13B 381/22.
[126] OVG NRW, Beschl. V. 21.03.2023 – 13B 381/22, Rn. 33.
[127] OVG NRW, Beschl. V. 21.03.2023 – 13B 381/22, Rn. 32.
[128] OVG NRW, Beschl. V. 21.03.2023 – 13B 381/22, Rn. 48.

其次，OVG NRW 重申 NetzDG 第 3b 條之制定過程與實體規定，不符合《電子商務指令》第 3 條第 4 項合法規避來源國原則之前提要件。《電子商務指令》第 3 條第 4 項規定，各會員國在滿足一定條件下，得針對特定資訊社會服務實施相關措施（Maßnahme），總而言之，該項措施必須符合比例原則的要求。

然而，NetzDG 框架中所制定之各種義務，可能無法稱得上是一種「措施」，換言之，措施理論上是一種針對特定服務提供者所施行之個案性措施（Einzelfallmaßnahme），故 NetzDG 第 3b 條作為一種抽象的、針對某一特定描述性範疇服務提供者的規定，得否視為此指令所言之措施，非無疑問[129]。

VG Köln 不願就此表達法律見解，而 OVG NRW 則同意被告（聯邦司法局，Bundesamt für Justiz）的主張：在自由的服務交易秩序下，系爭抽象規定所課予之義務具有正當理由時，亦可適用於其他會員國之之服務提供者，否則創造自由交易之共同市場宗旨將會落空[130]。言下之意，OVG NRW 認為，《電子商務指令》第 3 條第 4 項意義下的措施，非必然指涉僅針對單一事件所為之行政作為。

最後，第三個重點，則表現在：既然 OVG NRW 不認為內國法以法律形式執行規避會員國原則之措施必然違反《電子商務指令》第 3 條第 4 項規定，那麼 NetzDG 第 3b 條為何仍違反會員國原則？理由實際上與 VG Köln 認定 NetzDG 第 3a 條違反會員國原則雷同，也就是德國並未踐行《電子商務指令》第 3 條第 5 項之程序。故 OVG NRW 亦就本案是否滿足法定程序一事作出判斷。

《電子商務指令》第 3 條第 5 項規定，在緊急情況下（dringlicher Fall），會員國得規避第 3 條第 4 項第 b 款之要件，但必須儘速告知歐盟執委會於其他會員國執行特定措施之情形，並附上存有緊急情況之理由。OVG NRW 認為，《電子商務指令》第 3 條第 5 項規定必然涉及到一種無法事前預見而有及時處置之急迫必要情形，導致難以按照第 3 條第 4 項第 b 款遂行法定程序，但是經一般國家立法程序所制定

[129] OVG NRW, Beschl. V. 21.03.2023 – 13B 381/22, Rn. 114 f.
[130] OVG NRW, Beschl. V. 21.03.2023 – 13B 381/22, Rn. 120 ff.

之法律，顯然無法滿足此一要求[131]。

此外，如果會員國欲規避《電子商務指令》第 3 條第 4 項第 b 款而主張第 5 項之緊急情況，那也必須以擬採行之措施乃針對具體、實際之危險狀態當作前提，以確保《電子商務指令》第 3 條第 4 項第 b 款之保護法益免受重大危脅[132]。但是 NetzDG 第 3b 條對於社群網站服務提供者所課予之建構異議程序義務，無法明確看出其乃面臨前開所述之具體、實際之危險情形[133]。

基於上開理由，OVG NRW 將 NetzDG 第 3b 條之效力亦暫時凍結，原告暫時不需要建構起異議申訴之義務。以下這段話或可作為法院作出此等判斷的最佳註解：「對於營業處在其他會員國的社群網站服務提供者適用本國規定，恐怕是違反歐盟法之重要根據，因此等作為違反《電子媒體法》第 3 條第 2 項連結《電子商務指令》第 3 條第 2 項所揭示的來源國原則[…]於會員國之間運用來源國原則之目的，在於使自由交易能夠常態性地跨越國界，進而確保共同市場內之『資訊社會服務』，其中各會員國一方面對於自己國內之服務提供者按照自己的法律進行規制，另一方面使得受到相同程度規制之服務提供者能夠完全按照其會員國法提供服務與營運[134]」。

最終仍須提醒，前開兩項裁定僅為暫時處分裁定，有關 NetzDG 之違反歐盟法爭議，仍有待後續主要程序判決出爐後，方能塵埃落定。

[131] OVG NRW, Beschl. V. 21.03.2023 – 13B 381/22, Rn. 137.
[132] OVG NRW, Beschl. V. 21.03.2023 – 13B 381/22, Rn. 140.
[133] OVG NRW, Beschl. V. 21.03.2023 – 13B 381/22, Rn. 142.
[134] OVG NRW, Beschl. V. 21.03.2023 – 13B 381/22, Rn. 17, 22.

（二）《數位服務法》與 NetzDG 之競合

2022 年 11 月 16 日，歐盟正式完成《數位服務法》之立法程序，原則上於 2024 年 2 月 17 日正式施行。這部作為於各歐盟會員國境內直接生效之規章（Verordnung）象徵著歐盟網路治理之典範移轉。相較於以往將網際網路視為創新與經濟成長驅動力的《電子商務指令》，其給予網路相關服務提供者較大的責任豁免特權，本規章則是強調，在不過度妨礙網路發展的前提下，引進適當的網路管控機制，以應付資訊社會活動所帶來的社會與經濟危機，尤其是大型的網路中介者所提供的網路服務已具備干涉公民法律生活、影響公共意見形成的能力，有鑒於此，網路空間的安全性應予特別重視[135]。

在上述前提下，《電子商務指令》對於網路中介者所採取的分類方式，即分成網際網路連結服務提供者、快取服務提供者與資訊儲存服務提供者，即有調整必要，故《數位服務法》主要再針對資訊儲存服務提供者進行更細緻化的分類，期望能夠更精確地界定各種類型資訊儲存服務提供者之權利與賦予不同程度的注意與照料義務[136]。

按照《數位服務法》第 18 條規定，資訊儲存服務提供者於知悉有對生命或人身安全造成危險之犯罪嫌疑時，有立即通報官署之義務。這項規定之內容恰好與 2022 年被 VG Köln 裁定暫時凍結效力之 NetzDG 第 3a 條相同，這也是德國政壇與學界開始討論《數位服務法》與 NetzDG 規範競合問題的起點。

有鑑於《數位服務法》通過立法對德國所造成的衝擊，在野黨團對執政黨團提出相關疑問，德國政府所給予的答覆，看起來立場頗為一貫。其表示由於《數位服務法》之規章性質具有統一全歐盟規範效果之作用，因此未來《數位服務法》可能會逐漸取代 NetzDG 的地位，但無論具體而言應如何進行規範銜接、又或者是後續可能引發之效應，皆有待進一步評估，政府目前仍未有答案；另外，NetzDG 目前的主管機關為聯邦司法部（Bundesministerium für Justiz），至於《數位服務

[135] Kraul/Schmidt, Plattformregulierung 2.0 – Digital Services Act und Digital Markets Act als Herausforderung für die Compliance-Organisation, CCZ 2023, 177, S. 177 f.
[136] Ebenda, S. 179 f.

法》之主管機關，政府目前也尚未決定[137]。值得留意的是，德國政府在面對在野黨團提到 NetzDG 第 3a 條遭法院凍結效力如何因應時，回答在 2024 年《數位服務法》生效之後，社群網站又會承擔類似的通報義務，應證了前開所述《數位服務法》可能會逐漸取代 NetzDG 的地位觀點[138]。

德國政府進一步認為，NetzDG 與《數位服務法》雖然立法目的與規範內容相似，但是使用的規範技術並不相同，例如民眾發現違法內容之申報機制，兩法皆要求服務提供者應建構友善的通報機制，但是兩者所定義之違法內容本質上並不相同，相較於 NetzDG 直接列舉犯罪類型規定，《數位服務法》則是未自行確定，而是轉由國家法律與歐盟特別法規決定，不過《數位服務法》之違法內容又僅只限於對於生命或人身安全造成危險之行為，可能意味著比 NetzDG 範圍更小的犯罪類型[139]。

另外，不同於 NetzDG 賦予社群網站法定時限內之違法內容處理義務，《數位服務法》本身並無類似的期限規定，僅有在立法理由第 87 點提到 2016 年的歐盟執委會《對抗網路中違法仇恨性訊息行為準則》（Verhaltenskodex für die Bekämpfung rechtswidriger Hassreden im Internet）應於 24 小時內刪除[140]。未來是否確有相關處理時間限制要求，仍未明朗。

目前有關兩部法律的競合問題，在學界討論中仍不甚完整。有論者已經提到《數位服務法》之施行將會使之前被法院凍結效力的 NetzDG 數項條文實際上「復活」[141]。關於 NetzDG 之未來，有論者談到，《數位服務法》之施行，將會使規制範圍相同的內國法走入歷史，因為統一歐盟領域內的網路治理秩序正是該法的主要目標[142]。亦

---

[137] BT-Drs. 20/1937, S. 2.
[138] BT-Drs. 20/1937, S. 3.
[139] BT-Drs. 20/2308, S. 4 f..
[140] BT-Drs. 20/2308, S. 3 f.
[141] Kraul/Schmidt, a.a.O. (Fn. 35), S. 181; Netzpolitik, *Meta muss keine Widerspruchsmöglichkeit anbieten*, abrufbar unter: https://netzpolitik.org/2023/netzdg-reform-ungueltig-meta-muss-keine-widerspruchsmoeglichkeit-anbieten (letzter Abruf Juli 20, 2023).
[142] Holznagel, *Das DSA ist fertig – Neunummerierung, Inkrafttreten, Behördezuständigkeit und Zukunft des NetzDG & Co.*, abrufbar unter: https://www.cr-online.de/blog/2022/11/04/der-dsa-ist-fertig-neunummerierung-inkrafttreten-behoerdenzustaendigkeit-und-zukunft-des-netzdg-co (letzter

有論者認為，即便《數位服務法》的規制內容與 NetzDG 多有重疊，但是後者恐怕仍有繼續存在的必要性，像是第 5 條課予社群網站服務提供者應於德國境內設置全權代理人義務，仍屬有必要且未為《數位服務法》所規範[143]。

特別值得注意的是，有部分論者認為兩部法律有不同的立法目的，實不能斷言新法必然會完全取代舊法。持此見解者最主要的理由，在於按照 NetzDG 第 1 條第 3 項，該法之立法目的在於確保公共安全，乃典型危險防禦之概念，然而《數位服務法》則是追尋更多種目標，像是經濟性目標，或者是著重在意見自由與仇恨性言論之間的平衡點等等，以至於其適用範圍比 NetzDG 要來得廣泛許多[144]。倘若吾人遵循這種看法，那麼會傾向作出以下結論：NetzDG 毋庸因《數位服務法》而廢止，僅有修正之需要。

總而言之，有關 NetzDG 與《數位服務法》之間究竟是互補還是競合關係，仍有待未來持續討論。

Abruf Juli 20, 2023).

[143] Kahl/Lippert, *Warum nan das NetzDG doch noch braucht*, abrufbar unter: https://www.lto.de/recht/hintergruende/h/netzdg-das-zustellungsbevollmaechtigter-inland-rechtsschutz-internetnutzer-plattformhaftung (letzter Abruf Juli 20, 2023).

[144] Tschorr, *Meldepflicht von illegalen Inhalten an staatlichen Stellen – Digital Services Act versus Netzwerkdurchsetzungsgesetz, MMR 2022, 1053, S. 1056 f.; Schleif/Kettmann, Komplementär oder konkurrierende: NetzDG und DSA*, abrufbar unter: https://www.hans-bredow-institut.de/de/blog/komplementaer-oder-konkurrierend-netzdg-und-dsa (letzter Abruf Juli 20, 2023).

（三）《數位服務法執行法草案》

2023 年 8 月，德國數位與交通部（Bundesministerium für Digitales und Verkehr）公布了一份簡稱為《數位服務法執行法案草案》[145]（為求精簡，本研究以下以 D-DSA- RefE 稱之）之包裹立法文件。

該法案之目的，係為德國應建立起一套整合性的法律規範，以因應歐盟 DSA 於 2024 年 2 月正式生效[146]。由於德國現行的網路治理法律體系中的各部法律，乃基於不同時期的需求而制定，顯得複雜、分歧，開始產生法律適用上的困難，因此德國數位與交通部認為，藉由 D-DSA- RefE 的提出，得以將諸多規範定於一尊。而這也意味著，當本法案通過後，不只能為本身具有直接適用於歐盟各會員國效力之 DSA 提供必要性補充，更會一併廢止現行 NetzDG 與《電子媒體法》，兩者之實質規範內容將匯入 D-DSA- RefE 第 1 條所編寫之全新法典—《數位服務法》（Digitale-Dienste-Gesetz, DDG）[147]。

另外，為求法律用語一致性，D-DSA- RefE 也會同時針對其他法律進行相應之修改，例如涉及國家安全之《聯邦憲法保護法》（Bundesverfassungsschutzgesetz）、《不正競爭防制法》（Gesetz gegen den unlauteren Wettbewerb, UWG）、《電信與電子媒體資料保護法》（Telekommunikation-Telemedien-Datenschutz-Gesetz, TTDSG）等[148]。

職是之故，D-DSA- RefE 之重點將會是第 1 條有關《數位服務法》草案（DDG-RefE）之內容。以下做重點介紹。

首先，按照 DDG-RefE 第 1 條第 1、第 2 項規定，本法將適用於所有數位服務提供者，至於對於以提供內容為核心服務項目的數位服

---

[145] 法案原文全銜為：Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG sowie zur Durchführung der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten und zur Änderung weiterer Gesetze. 該份法案全文可由下開連結下載：https://bmdv.bund.de/SharedDocs/DE/Anlage/Gesetze/Gesetze-20/gesetz-durchfuehrung-verordnung-binnenmarkt-digitale-dienste.html （最後瀏覽日：2023 年 12 月 20 日）。

[146] D-DSA- RefE, S. 1.

[147] D-DSA- RefE 第 37 條即規定兩法應於本法案生效後同時廢止。參見：D-DSA- RefE, S. 47.

[148] D-DSA- RefE, S. 29 f.

務，有特別的法定要求，則受各邦的媒體法拘束。DDG-RefE 第 3 條重申《電子媒體法》的來源國原則。DDG-RefE 第 4 條規定數位服務提供者毋庸向德國主管機關進行登記或許可，亦與《電子媒體法》相同。DDG-RefE 第 5 條以下，規定電子服務提供者自身與商業通訊（kommerzielle Kommunikationen，或者可以以廣告理解之）之公開義務，此部分也與《電子媒體法》第 5 條與第 6 條雷同。

原本《電子媒體法》第 7 條以下有關各類型電子媒體法律責任豁免特權規定，因為歐盟 DSA 已制定直接有效的新規範，因此 DDG-RefE 僅就《電子媒體法》中有所規定而 DSA 未規範到的部分予以保留，其餘則不再作特別規定。至於前開仍保留舊法而構成例外之部分，乃原本《電子媒體法》第 7 條第 4 項以及第 8 條第 4 項之規定，分別成為 DDG-RefE 第 7 條與第 8 條。DDG-RefE 第 7 條乃授予網路使用者於其著作權受到侵害時請求服務提供者為封鎖之權利；第 8 條則是針對無線區域網路服務提供者給予特別義務免除規定[149]。

至於 DDG-RefE 其他部分之規定，圍繞在執行 DSA 之組織性、細節性事項，包含法規主管機關、主管機關與歐盟之協調機構合作、年度報告、各會員國主管機關之合作、主管機關與邦媒體管理局協會合作、罰則等等。

DDG 之法規主管機關，按照 DDG-RefE 第 12 條第 1 項，為聯邦網路管制局（Bundesnetzagentur），按照第 14 條，其亦為 DSA 之執行以及監理機關，同時作為 DSA 第 49 條意義下的協調事務處（Koordinierungsstelle）。

此外，就特殊之事務領域，亦有其他機關為法規主管機關。依據 DDG-RefE 第 12 條第 2 項規定，聯邦兒少保護中心（Die Bundeszentrale für Kinder- und Jugendmedienschutz）為 DSA 第 14 條第 3 項與第 28 條第 1 項之主管機關，以執行數位服務中的兒少保護任務。依據 DDG-RefE 第 12 條第 3 項規定，聯邦資料保護與資訊自由受託機構（Der oder die Bundesbeauftragte für den Datenschutz und die

[149] 詳參王牧寰、林家暘、陳譽文等，前揭註 116，頁 168 以下。

Informationsfreiheit）則為 DSA 第 26 條第 3 項與第 28 條第 2 項之主管機關。最後，依據 DDG-RefE 第 13 條，聯邦犯罪防制署（Bundeskriminalamt）為 DSA 第 18 條第 1 項之主管機關。

D-DSA- RefE 已於 2023 年 12 月 22 日送至聯邦參議院審議[150]，其立法動態有待進一步追蹤。

三、第三方監督或產業自律機制

（一）NetzDG 建構之共管機制簡介

NetzDG 第 3 條第 2 項第 3 款規定，社群網站服務提供者對於非屬明顯違法之內容，得自行作成處置與否之決定，或者於接受申訴後七日內移轉給所謂「受認可的受管制之自我管制機構」（anerkannte Einrichtung der Regulierten Selbstregulierung）審理。這種由法規主管機關以公權力認可特定機構，並委由該機構執行法定任務之行政控管模式，稱為共管（Co-Regulierung）[151]。

截至目前，社團法人多媒體服務提供者自願性自我管制機構（Freiwillige Selbstkontrolle Multimedia-Dienstanbieter e. V.，以下稱 FSM）仍是掌管 NetzDG 事務之聯邦司法局（Bundesamt für Justiz, BfJ）唯一承認之社會自我管制機構。FSM 為承擔此項任務，完成修正《FSM 規章》（FSM-Satzung）與制定《NetzDG 程序規則》（NetzDG-Verfahrensordnung），就相關事務之作業予以規範框架。一旦案件轉至「受認可的受管制之自我管制機構」，原受有 NetzDG 法定義務之服務提供者將免除審查之義務與責任，而該機構將指定一 NetzDG 審查委員會進行審理，並且依據前開之程序規則，完成審查委員會之組成以及執行正規審查程序，與後續對審查決定不服時所展開的異議申訴程序[152]。

---

[150] Deutscher Bundestag, BR-Drucksache 676/23, https://dip.bundestag.de/vorgang/entwurf-eines-gesetzes-zur-durchf%C3%BChrung-der-verordnung-eu-2022-2065-des/307296 (letzter Abruf Dez. 26, 2023).

[151] 陳志宇、林家暘、吳秦雯、江耀國、王牧寰等，前揭註 117，頁 78 以下。

[152] 同上註，頁 112 以下。

（二）社會自我管制機構之業務概況

FSM 自 2020 年 3 月承擔此項共管任務以來，每年均會公開一份年度報告，供讀者了解其年度活動概況。最新的年度報告，統整了自 2022 年 3 月至 2023 年 3 月的業務活動[153]。在這一年當中，FSM 總共受理了 102 項案件，其中有 41 案中之被申訴內容被判斷為違法，也就是大約佔總數 40%左右[154]。被申訴之嫌疑內容，最大宗為使用者以自己名義所發布之貼文，有 46 件，其餘則是影片 26 件、使用者留言評論 22 件，圖片或圖表最少，計有 8 件[155]。

有關涉及違法類型部分，最大宗者為《刑法》第 185 條（公然侮辱罪），將近 45 件；次高為《刑法》第 130 條（煽動族群仇恨罪），將近 28 件；其次為《刑法》第 186 條（誹謗罪），近 26 件；再者為《刑法》第 86 條（散發違憲組織宣傳品罪）與第 86a 條（使用違憲組織符號罪），共計有約 24 件；再者為《刑法》第 187 條（造謠汙衊罪），近 17 件；其餘除了第 140 條（讚揚與鼓勵犯罪罪）外，其餘案件數量未達 10 件[156]。至於被判定構成違法內容之類型排序，與申訴案件違法類型數量大致上亦呈正相關，仍以《刑法》第 185 條為最大宗，有 11 件，其次為第 186 條，9 件，接著是第 130 條，8 件，再者為第 86 條與第 86a 條，6 件，其餘僅在 5 件以下。

與 2022 年相比，2023 年的案件量有微幅成長，由 93 件躍升破百件，惟在 2023 年度中，涉及違法內容之著作型態，以貼文與影片為大宗，而與過去留言評論多於影片的情況不同。至於違法內容之類型，雖大致上相同，但是涉及《刑法》第 86 條與第 86a 條之案件數量卻相比去年有顯著成長，上一年度甚至沒有涉及本兩條所作成之案件紀錄。這是由於上一年度實際上並無相關申訴出現，或者僅為未轉由 FSM 審理而已，欠缺進一步之資料可資推論。至於被判定構成違法內容之類型，與 2022 年有顯著不同，2023 年的違法類型，相較於

---

153 FSM, *Tätigkeitsbericht 03/2022 - 03/2023*, abrufbar unter: https://www.fsm.de/files/2023/05/20230517_fsm-taetigkeitsbericht-netzdg-selbstregulierung.pdf (letzter Abruf Juli 20, 2023).

154 Ebenda, S. 4.

155 Ebenda, S. 5.

156 Ebenda, S. 6.

去年近半數集中在第 185 條，說得上是更為多元，確認違反第 185 條、第 186 條與第 130 條之案件數旗鼓相當，或許這反映出，FSM 的 NetzDG 審查委員會已較嫻熟案件之分析方法，而能作出更為全面的審酌與判斷。

（三）社會自我管制機構執法範例

按照 NetzDG 及章程之規定，FSM 必須受理與審查受當事人所申訴之案件。因此，就受理案件中之系爭網路內容，給予違法或不違法之裁決，屬於 FSM 在 NetzDG 內的核心任務。FSM 在其官方網站中，會以當事人資訊去識別化以及不過度彰顯爭議網路內容之方式，公開其裁決書之重點內容，以讓外界能夠了解 FSM 如何就系爭個案進行判斷與論證工作。

以下茲舉兩個由 FSM 之 NetzDG 審查委員會於 2023 年所作成之決定，結果分別為判定申訴內容違法或不違法，以供參考。

1. 性聯想與掀起族群仇恨影片案

在檔案編號「NetzDG0442023」決定書[157]中，可以看見決定書的體例與法院判決頗為類似。換言之，先寫出主文「系爭內容（不）具有 NetzDG 第 1 條第 3 項意義下的違法性」，接著陳述案件事實，最後則是就系爭內容進行法律上之判斷與論證。

本案涉及到一名影片上傳者，其剪接一個枕頭廣告影片並命名為「一整個就很粗俗的片子」（Dauerderbe Sendung），亦即在特定段落嵌入自己所製作的內容，使得原本的廣告意涵完全改變。像是一開頭播放正常版本的廣告影片，然後重複某個段落，但改變其中字句表達，植入讓人產生不雅性聯想與汙穢性的字句。不僅如此，亦將片中的男人唇上添加黑色四方形，以影射希特勒的形象，並將原枕頭廣告影片中的女人畫面上加上「家庭主婦與母親」（Hausfrau und Mutter）、「工作使人自由」（Arbeit macht frei）等字句，意圖使人喚起德意志第三帝國之標語記憶。檢舉人認為，這個影片的改造與公開傳輸是名譽侮辱

[157] FSM, *Entscheidung v. 23.05.2023 - NetzDG 0442023*, abrufbar unter: https://www.fsm.de/files/2023/06/netzdg0442023_voe.pdf (letzter Abruf Juli 20, 2023).

與使人受傷的，且使人有不當的性聯想。

NetzDG 審查委員會就此事實分別就《刑法》第 186 條與第 187 條（意圖誹謗罪）、《刑法》第 185 條（公然侮辱罪）、《刑法》第 86a 條（使用違憲組織符號罪）以及《刑法》第 130 條（煽動族群仇恨罪）進行討論，最終其認定系爭內容皆不該當以上所提之條文所示之構成要件。

就意圖誹謗罪而言，NetzDG 審查委員會認為不會有明顯嫌疑，因為內容並未涉及到不正確的真實陳述。至於公然侮辱方面，審查委員會作了較為縝密的討論。審查委員會先行闡述有潛力形成公然侮辱之言論為何，也就是針對特定權利主體從整體脈絡而言有意加以貶低社會評價之表述。此外，公然侮辱也能透過對於個人之倫理或社會價值加以蔑視或者不予注意之方式完成。系爭影片內容是否出現具有對於特定人進行貶低社會評價或者蔑視個人之倫理或社會價值之表述，審查委員會認為皆無法排除。但是，審查委員會一致認為，這支影片至多僅能作為一種諷刺劇來看待，從而受到憲法上藝術自由的保障，非能認定為一種公然侮辱之表述。

最主要的原因有二，其一為觀眾在看到影片標題時，應該就要知道不能過於嚴肅看待這支影片；其二在於，這支影片並未超出作為人們面對諷刺劇所應容忍之界限，此界限在於：當其對於人性弱點之浮誇描述並未包含對被描述者之認真羞辱（ernstliche Herabwürdigung）。申言之，這支影片僅有借用枕頭廣告的片段，進行無意義的性聯想與汙穢字眼創作，並無對描述者進行認真羞辱之情況。

就使用違憲組織符號罪而言，片中雖使用希特勒鬍子，但這並非直接使用違憲之國家社會主義德意志勞工黨（NSDAP）相關標誌，至多只是該黨領導人標誌，不能滿足《刑法》第 86a 條要件。

最後，片中出現「工作使人自由」，或許會使人認為觸犯煽動族群仇恨罪，因為這句出現在奧許維茲集中與滅絕營大門上之標語，具有一種象徵性意義，使人聯想到強調種族主義之納粹暴政。不過，NetzDG 審查委員會認為，「工作使人自由」本身僅為一中性字句，與

使用納粹十字架或者納粹禮（Sieg Heil，意即勝利萬歲）有別。就片中內容而言，作者無意藉此羞辱與蔑視納粹黨政下的犧牲者。NetzDG 審查委員會並強調，法律要避免的是讚頌納粹，而非無格調的戲謔或愚蠢的胡鬧。

2. 掀起族群仇恨之社群網站貼文案

與前案決定作成時點相近的另一份檔案編「NetzDG0432023」決定書，則認為某社群網站中之一個貼文違法[158]。本案事實較前案單純，某一社群網站帳號於 2023 年 3 月 12 日張貼一個附有圖檔的貼文，圖檔顯現出被橡樹枝環包圍著的帝國鷹（按：此為納粹領導階層使用之標誌），中間鑲有暗喻綠黨的向日葵標誌，並著文：「現代納粹不是棕色的（按：指德國極右翼政黨「祖國」（Die Heimat），前身為德國國家民主黨 NPD），而是彩色的。綠色帝國（按：指德國綠黨），其所執行的大屠殺為謀殺自己的民族與消滅所有國籍」。

審查委員會就此事實，認定其符合《刑法》第 130 條第 2 項第 1 款第 a 目與第 b 目所描述之情況，進而確認此乃 NetzDG 意義下的違法內容。《刑法》第 130 條第 2 項第 1 款禁止對公眾散布或對個人提供、移交或使其得以近用符合第 a 目到第 c 目情形之內容。第 a 目描述該內容能夠激發對特定族群之仇恨，第 c 目則是對該特定族群之人性尊嚴，以咒罵、惡意藐視、加以汙衊等方式進行攻擊。

審查委員會先行確認該則貼文符合《刑法》第 11 條第 3 項所定義之「內容」[159]。其次，該貼文可視為一種對特定族群的攻擊，因為該貼文所使用的文字與圖像皆明顯針對綠黨，而綠黨本身既屬本國多數人政治意志所形成之團體，具備獨立而有別於其他民族一部分之特徵，例如政治與世界觀，因此可視為本國之特定族群。

在上開前提下，審查委員會進而對該貼文之內容進行違法性審查。就此而言，審查委員會先行確認此等貼文已經構成第 a 目之情形。因

[158] FSM, *Entscheidung v. 11.05.2023 - NetzDG 0442023*, abrufbar unter: https://www.fsm.de/files/2023/06/netzdg0432023_voe.pdf (letzter Abruf Juli 20, 2023).

[159] 德國《刑法》第 11 條第 3 項規定：「本法意義下之內容，指以文字、聲音或圖片載體、資料記憶體、圖像或其他有形物所包含者，不取決於其經由何種資訊或通訊之傳遞所產生的儲存方式」。

為在該貼文的脈絡中，作者有意將綠黨與納粹政權作等同連結，包含「現代納粹」、將納粹的象徵帝國鷹與綠黨的象徵向日葵結合在一起、「綠色帝國」有意使人聯想到第三帝國、以大屠殺形容綠黨的政治理念等等。這些作法試圖激起看到貼文者的憤怒以及相對於執政黨之無力感情緒等等。再者，系爭貼文也構成第 c 目的情況，因為這則貼文已經透過將其與納粹等同看待以及連結到大屠殺方式，對於綠黨作了客觀意義上特別嚴重之無價值判斷，何況綠黨作為反映一部分德國利益以及代表部分選舉人意志之政黨，發文者之攻擊並不適當且難以令人接受。

審查委員會仍按照德國刑事實務就《刑法》第 130 條所持之見解，仍就該貼文所可能彰顯之意見自由復行考量，方能最終斷定內容之違法性。對此，審查委員會必須就保護法益（公共秩序安寧）與意見自由所能實現的利益之間，作個案性權衡。審查委員會基於該發文所使用的措辭過於激烈，以及疫情時代的網路輿論氛圍日益激化，火上加油情況應予遏止，故不認為意見自由具備特別優先的意義。

最終，審查委員會也不認為本案符合《刑法》第 130 條第 8 項之社會衡平（Sozialadäquanz）排除條款，即如屬國家公民之啟蒙行為、防禦違憲之努力作為、藝術或知識性行為、研究或學術性行為、對於時代或歷史現象之報導或出於類似目的之行為時，不罰。因此，本案之貼文內容被判定為違法內容，受有 NetzDG 義務之服務提供者應對該內容予以移除或者封鎖。

四、小結

隨著德國民眾對於網際網路各種中介服務之資訊依賴漸深，社群網站等中介服務提供者應被賦予更重責任，已成為共識。在歐盟制定《數位服務法》制定後，德國又將如何加以因應，以及對於當前有效之 NetzDG 將產生何種影響，應觀察《數位服務法執行法案草案》的立法進程與調修狀況。無論如何，當前 NetzDG 架構下的共管機制，已經有效且順利運轉，受有審查任務之 FSM 所承辦的案件越來越多，且其審查結果與所持理由均為公開，已展現出頗為成熟的判斷能力，就此點而言，值得我國效仿之。

總體而言，在德國內國法層級之《數位服務法》出爐前，NetzDG 延續《電子媒體法》的精神，承擔起釐清網路言論責任歸屬與課予社群網站等電子媒體一定的打擊違法言論內容任務。

NetzDG 之「法遵制度」帶來兩項啟示。其一，由於整部法律的設計著重在要求社群網站等電子媒體應積極建構出保障使用者免於受網路違法內容危害之機制，故這項包含電子媒體應建立起申訴窗口、處理違法內容、異議機制與送 FSM 外審等等的程序安排，即為保障「使用者權益」能夠落實之方法。

其二，由於 NetzDG 有意識地將違法內容定義為特定之刑法犯罪行為類型，故只要觀察這些犯罪類型，就能輕易得知該部法律的關注課題，也就是仇恨性言論與假訊息（新聞）的具體內涵。被視為是違法內容者，尤其是德國《刑法》（下同）第 89a 條（預備危害國家暴力行為罪）、第 100a 條（外患謠言罪）、第 126 條（恐嚇公眾罪）、第 130 條（煽動族群仇恨罪）、第 166 條（汙衊宗教與宗教團體罪），可視為對於散布「政治不實訊息」而影響公共秩序安寧的反應。至於第 184b 條（散布、販賣與持有兒童色情刊物罪），則明顯針對「兒少網路安全」。

再者，傳統妨礙名譽罪名，像是第 185 條（公然侮辱罪）、第 187 條（意圖誹謗罪），以及揭露他人隱私秘密之罪，像是第 201a 條（妨礙隱私秘密罪），均有防範或降低「網路霸凌」危險之旨意。

擔任社會自我管制之 FSM，乃作為社群網站等電子媒體之外的案件審理機構，也是依據前開 NetzDG 的違法內容當作職權範圍。由於 NetzDG 主要針對仇恨性言論與假訊息（新聞）而設，故有關「網路交易安全」部分，例如在網路架設以假亂真之購物網站或者交易平臺進行網路詐騙（Internet-Betrug），即非規制範圍內。

第三節　法國

一、監理脈絡

法國最早在《1986 年 9 月 30 日第 86-1067 號通訊自由法》（*Loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication*，法國一般簡稱為《Léotard 法》，以下則簡稱為《1986 年通訊自由法》）就從電信（*télécommunication*）的角度，開始處理網際網路通訊自由的議題，一方面改制原本的視聽通訊署（*la Haute Autorité de la communication audiovisuelle*）成為新的獨立機關[160]：國家通訊與自由委員會（*Commission nationale de la communication et des libertés*, CNCL）[161]；二方面在一定的安全條件下，確立電信業的建立、使用與服務之自由，主要涉及無線電視頻道、有線電視網路與手機之私有化管理[162]，同時也保障接收使用相關電信服務者的資料應符合保密原則[163]。

接著，從 1998 年開始，在時任總理 Lionel Jospin 的主導下，推動一系列的資訊社會政府規劃（*le programme d'action gouvernemental concernant la société de l'information*），並以法律、文化、社會挑戰為中心，提出不同的計畫方向[164]。1999 年 8 月 26 日以「所有人共享資訊的社會」（*Une société de l'information pour tous*）為主軸，提出國家願景[165]，並設立三大目標：確立每個人的權利與責任，以確保網路通

---

[160] LAROUSSE, *Commission nationale de la communication et des libertés (C.N.C.L.)*, https://www.larousse.fr/encyclopedie/divers/Commission_nationale_de_la_communication_et_des_libert%C3%A9s/114251 (consultée le Nov. 22, 2023).

[161] *Loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication (Loi Léotard)*, https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006068930/ (consultée le nov. 22, 2023).

[162] Lextenso, *Journée mondiale de la télévision : focus sur la loi du 30 septembre 1986*, https://www.lextenso-etudiant.fr/culture-juridique/journ%C3%A9e-mondiale-de-la-t%C3%A9l%C3%A9vision-focus-sur-la-loi-du-30-septembre-1986 (consultée le Nov. 22, 2023).

[163] Arcom, L'Arcom rend hommage à François Léotard, ancien ministre de la Culture et père de la loi du 30 septembre 1986, Communiqué de Presse (2023/04/25), https://www.arcom.fr/presse/larcom-rend-hommage-francois-leotard-ancien-ministre-de-la-culture-et-pere-de-la-loi-du-30-septembre-1986 (consultée le Nov. 22, 2023).

[164] 總理於 1999 年 1 月 9 日之宣誓：Lionel Jospin, Déclaration de M. Lionel Jospin, Premier ministre, sur le programme d'action gouvernemental concernant la société de l'information, notamment sur les enjeux juridiques, culturels et sociaux des nouvelles technologies de l'information, Paris le 19 janvier 1999, Vie-publique.fr (1999/01/09), https://www.vie-publique.fr/discours/158963-declaration-de-m-lionel-jospin-premier-ministre-sur-le-programme-dac （最後瀏覽日：2023 年 11 月 22 日）。

[165] Olivier, Frédérique, et Stephane Senacq, « La société de l'information et le droit », LEGICOM, Vol.

訊自由；促進更多大眾接近資訊網路；確保網路交易的安全與公平，並提出《資訊社會法》草案（*projet de loi sur la société de l'information*）[166]，交付全國公共辯論[167]。儘管歷經多次折衝，最終於 2004 年 6 月 21 日完成立法，制定公布《2004 年數位經濟信任法》（*Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*，下稱《LCEN 法》）。而之後二十餘年迄今，更是陸續制定規管密度越高越廣的各種相關立法，由此可見，法國政府很早就對網路服務使用高度密切並在多元面向上進行關注。

依據法國之相關研究文獻可知，該國迄今之規管監理脈絡，主要因為政府部門，觀察到資訊服務業（*services de la société de l'information*）快速發展以來，因為這些服務允許大量的服務使用者，彼此之間進行資訊分享，一方面變動了以往的資訊取得、傳播與交換的方式，對人民如何凝聚形成公意與民主運作帶來新風險[168]。例如明顯帶有違法性內容的資訊被不經查證地廣泛傳播、錯誤訊息的誤導、某些特定情況下的虛假訊息而影響人們對資訊空間的信賴。

另一方面，經濟活動的運作模式也因此受到了影響。因為經濟生活中的生產者與消費者，透過資訊服務的提供與分享，彼此相互連結，形成一個又合作又競爭的「共同競爭」（*coopétition*）模式，甚至共同摸索新的經濟型態，加上資訊服務產業的跨國性，業者、消費者、公權力機關此一傳統的三面關係變得更為複雜[169]。

除此之外，資訊社會下快速而無邊界的資訊互相分享方式，改變了接近與取得資訊的方式，擴大人們獲取知識與資源的可能性與方便

21-22, no. 1-2, 2000, pp. 1.

[166] 可謂為資訊社會政府規劃的第二階段，可參考 Projet de loi: société de l'information (LSI). Synthèse du document d'orientation deuxième étape de l'action gouvernementale pour la société de l'information août 1999, LEGICOM, 2000/1-2 (N° 21-22), p. 169, URL: https://www.cairn.info/revue-legicom-2000-1-page-169.htm (consultée le Nov. 22, 2023).

[167] Début de la consultation sur la « loi sur la société de l'information », https://www.lemoniteur.fr/article/debut-de-la-consultation-sur-la-loi-sur-la-societe-de-l-information.207429 (consultée le Nov. 22, 2023).

[168] Bilan et perspectives de la lutte contre la diffusion de contenus haineux en ligne, https://www.arcom.fr/nos-ressources/etudes-et-donnees/mediatheque/lutte-contre-la-diffusion-de-contenus-haineux-en-ligne-bilan-des-moyens-mis-en-oeuvre-par-les-plateformes-en-ligne-en-2022-et-perspectives (consultée le Nov. 22, 2023).

[169] Christian de Boissieu, Introduction, Nicolas Curien et Pierre-Alain Muet, La société de l'information, rapport Conseil d'Analyse Économique, p. 7 (2004).

性，也因而打亂了長期以來的生產、分配與服務模式。這些問題並非從無前例，但網路服務的便捷性也使其相形惡化，例如言論自由、智慧財產權所面臨的新衝擊，因為網路的言論會依據其於不同網域上發布，而受不同地域法令管制，突破以往國家以地域進行規管的傳統。加上網路的使用，造成以往保護人身自由和隱私權的相關法令難以有效管制，因爲利用網路更容易擴大人口販運、進行各種詐欺以及作為色情和色情內容的工具。當全球的網路建置不以國界、邊境為限制，無須考慮領土地域的差異性時，規管的法框架並非無法建立，而是必須因應新的網路社會進行調整[170]。

關於法國對於網際網路相關服務之法制發展，從 1998 年的討論、立法、修法迄今，儘管其中經過國內外不同的衝擊與變化，但仍與一開始設定的主軸息息相關，也因此以下將簡要說明當時設定的三大目標內容[171]。

（一）確立每個人的權利與責任，以確保網路通訊自由

首先定調網路上的通訊應該是免費的，且通訊自由是網路的基礎，政府期待促進網路上的通訊自由並簡化網站的創建，降低人們使用網路的障礙；也對於網際網路域名進行明確的管理，避免域名混淆。其次，給予方便的同時，也要將相關網路資訊參與者的職責，包括編輯、技術中介者（*intermédiaires techniques*）予以釐清。

同時，也期待進行合理的內容監管，預計透過成立組織，以公私協力之方式，進行協商並遵守應有的道德規範。成立之公私協力組織將特別負責根據自我監管的原則，確保網路上傳播的內容符合道德規範。而在智慧財產權方面，也因應網際網路服務的特性，進行相關權利設計的法制調整。

[170] Dominique Delaplace, « Donner un cadre juridique à la société de l'information », Bulletin des bibliothèques de France (BBF), 2000, n° 5, p. 130, https://bbf.enssib.fr/consulter/bbf-2000-05-0130-005 (consultée le Nov. 22, 2023).

[171] 以下內容主要整理自 1999 年提出的《資訊社會法》草案，參考前註 166。

（二）促進更多大眾接近資訊社會

為了促進網路彼此之間的串接，法國首先大力採取降低價格、引進新的接取技術並發展競爭，將其視為公共服務的一環，與歐洲合作夥伴一起推展讓學校都能順利進行網路連結，以改善網路品質。同時為了提供各地區普遍的公共服務，持續發展高速網路存取，以減少地區之間的不平等。技術上則是排除各種網路連結的障礙、發展新數位載具的技術，並在保留法國政府管理權限的情況下，促進衛星系統的發展。

為了達到人人有網路的資訊社會，法國也調整電信服務監理框架、加速轉換歐洲相關電信網路的指令、協調有線網路和電信網路的法律制度，以便將有線與電信網路進行統一監管，於促進競爭的同時，兼顧公共領域良好管理的必要性。而與此相關的法律規定，都必須再與相關業者進行公眾諮詢後再提出，以確保盡可能多的人獲得真正多樣化的內容。

（三）確保網路交易的安全與公平

為了保護此一目標中最為關鍵的消費者，國家的立法在轉換歐盟指令時，必須明確規範跨國電子商務的法律適用問題，以同時確保內部市場的發展和消費者的保護。而且，必須確保網路透明度。因為，不論使用網路與否，所有的交易都必須以能夠正確識別交易各方，並且確定資訊交換的透明度，才能夠讓交易公平進行並發展。在此基礎上，自然必須透過修法，以承認透過電子方式傳輸的文件與電子簽名的法律效力。

技術上，關於加密技術（*moyens de cryptologie*）的使用必須免費使用，但必須配合法官有權存取未加密的原始文件，同時強化政府部門的安全監管。當然，因應網路使用而產生的新型態犯罪、智慧財產的侵權行為，必須透過跨國警察合作與相關法令的修訂，以確保正當法律程序與因應新型態的違法行為。最後，由國防部規劃並確定國家重要的通訊基礎設施和資訊服務，以保護國家重要網路，避免可能的風險。

此一法律草案所建立的三大主軸與內容，歷經公共辯論程序，形成並引領法國相關網際網路傳播規管之方向，這也是為何法國的相關立法著重於言論自由、營業自由之兼顧、並同時強調文化保障；規管主體也向來以政府為主，產業自律與第三方協助基本上也是政府機關主導，產業配合制定相應法令與第三方協助為輔。

以下將接續說明，在 1999 年設定之大框架下，二十多年來法國政府機關之法制政策作為，以及產業自律與第三方之角色。

二、政府機關法制政策作為

法國目前因應網際網路產業與服務的快速與大量發展，可從兩方面進行分析，首先是在組織面進行規管機關的組織調整，其次則是全面性的法令修訂。

（一）組織調整

如前所述，《1986 年通訊自由法》創設了法國第一個主管傳播通訊的獨立機關：國家通訊與自由委員會（CNCL）。

1989 年 CNCL 歷經組織調整，改為「最高視聽委員會」（*le Conseil supérieur de l'audiovisuel*，以下簡稱為 CSA）；直到 2021 年時，法國又透過《2021 年 10 月第 2021-1382 號數位時代近用文化作品之管制與保護法》（*LOI n° 2021-1382 du 25 octobre 2021 relative à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique*，以下簡稱為《2021 文化作品法》），將 CSA 及網路作品散佈與權利保護高等署（*Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet*，以下簡稱為 HADOPI）合併，成立新的網路監管行政機關：視聽與數位通訊管制署（*Autorité de régulation de la communication audiovisuelle et numérique*，以下簡稱為 ARCOM）。

由於本研究著重在法國如何因應歐盟制定公布之《數位服務法》，因此不再特別說明以往的電信傳播業管制機關，僅以最新成立之機關，即 2022 年元旦開始運作之 ARCOM 為介紹對象。

ARCOM 之設立，主要在調整並整合兩個因應資訊社會而成立的行政機關。其一是運作已超過 20 年，因為成立以來各種具有爭議性的決定、組織成員被批評未必具備專業性加上行政人員可能的慣性，又有外在政治力的介入，而逐漸失去人民信任的 CSA[172]；其二則是考量到網路上智慧財產權保護，已經因為網路使用的特性而受到挑戰，也有整合加以管理的必要的機關 Hadopi。

儘管 Hadopi 乃是 2009 年為了強化網際網路相關智慧財產之管理獨立性、公正性與靈活性，才將 2007 年成立的智慧財產權管理獨立機關：科技技術管制署（*L'Autorité de régulation des mesures techniques*，簡稱為 ARMT）改制而成[173]，在此仍須注意：關於電子通訊、郵務和新聞播送，亦即法國網路，以及固定、行動和電信交換網路、郵政服務技術面的權限機關並非 ARCOM，而是隸屬於另一個獨立行政機關：電子通訊、郵務與新聞播送管制署（*Autorité de régulation des communications électroniques, des postes et de la distribution de la presse*，簡稱為 Arcep）。

ARCOM 主要是視聽及數位通訊的監管機構，以保障通訊自由並確保視聽創作的財政經濟和權利保護為主。不過礙於兩機關的權限有部分容易混淆之處，現在兩機關已透過職務協助的方式簽訂協議互相合作。此外，早在 ARCOM 仍為 CSA 之時期，兩機關自 2020 年 3 月開始就會以「保護未成年人對抗線上色情」為主題，每月進行固定的聯席會議[174]。

---

[172] 陳志宇、林家暘、吳秦雯、江耀國、王牧寰等，前揭註 117，頁 152。

[173] 可參考上議會之法案研究報告：Michel THIOLLIÈRE, Projet de loi favorisant la diffusion et la protection de la création sur Internet, Rapports Législatifs (2008/10/22), https://www.senat.fr/rap/l08-053/l08-053.html （最後瀏覽日：2023 年 11 月 23 日）。

[174] CSA, Coopération entre régulateurs: L'Arcep et le CSA développent de nouvelles collaborations au sein d'un pôle commun, Communiqué de presse (2020/03/20), https://www.csa.fr/Informer/Espace-presse/Communiques-de-presse/Cooperation-entre-regulateurs-L-Arcep-et-le-CSA-developpent-de-nouvelles-collaborations-au-sein-d-un-pole-commun (consultée le Nov. 23, 2023).

以下將分別自組織及職權兩方面，針對 ARCOM 進行說明：

1. ARCOM 之組織

ARCOM 乃是 2017 年法國立法[175]調整獨立機關數量與組織類型後，新成立的「獨立公權力機關」(autorité publique indépendante, API）類型，乃是被授予公法人法律地位的行政機關，主要職責為保護人民之重要權利，因而，此類機關通常被授予確定權、法令制定權或裁罰權[176]。

包含主席在內，目前 ARCOM 共有 9 位委員，其任期 6 年，不得連任。其中，一名委員由總統提名並任主席，該任命必須得到上下議院常設委員會五分之三以上同意；其次，上議院議長及下議院議長分別任命 3 名委員，皆需由各該議院負責文化事務的常設委員會，以五分之三多數票通過無記名投票同意之，議院任命之代表每兩年更換三分之一，且必須有一男一女的不同性別配置。最後，1 名委員由中央行政法院（*Conseil d'Etat*）首長即副院長任命現任法官擔任之，一名則由最高法院（*Cour de cassation*）首席法官（*premier président*）選任現職法官為之。

ARCOM 的所有會議皆須有至少 6 名委員的出席，出席委員過半數的同意方得作成決議。儘管委員任期內不因為年齡限制問題而去職，但提名或任命時不得超過 65 歲。

ARCOM 下設 8 個常設工作小組，以個案議題為主進行分組，由小組進行審議後提出初步解決方案或決議：保護公眾與法國社會多元；媒體教育、生態轉型與公共衛生；視聽、電影和音樂之創作和生產；資訊和節目的多元化與倫理；網路平臺之監督；數位廣播與影音；電視服務與串流影音服務之出版與發行；網路之權利保護。每一位委員擔任一個工作小組的主席，並兼任另一個工作小組的副主席[177]。如

---

[175] *LOI n° 2017-55 du 20 janvier 2017 portant statut général des autorités administratives indépendantes et des autorités publiques indépendantes*.

[176] Petit, Étienne. « Chapitre 3. Les autorités administratives et publiques indépendantes », Les institutions administratives en tableaux, sous la direction de Petit Étienne, Ellipses, pp. 84-89 (2021).

[177] 以上組織相關內容來自 ARCOM 官網：https://www.arcom.fr/nous-connaitre/notre-institution/gouvernance （最後瀏覽日：2023 年 11 月 23 日）。

有必要時，也會臨時組成特定主題的專案工作小組。

ARCOM 總共有 370 名人員，在行政組織上分設 10 個組，包括：

- **創作組：**主要確保視聽媒體服務遵守有關創作作品的財務與發行義務，採取有效措施保護非物質化內容免於非法使用，並促進其在網路上的合法傳播。
- **公共、多元化和社會凝聚力組：**透過制定多元化主義的法令與協定，要求遵守權利與自由，並保護兒童、公眾與社會凝聚力。
- **電視和視訊串流組：**實施與視聽媒體服務市場准許有關的規則和程序。負責規劃數位電視（*la télévision numérique terrestre*, TNT）播送的頻率，監督 TNT 授權的所有程序，從公告招標到實際頻道播送。也對於傳播服務產業發展進行追蹤、研究等。
- **廣播和數位音訊組：**負責監管廣播業者並監控線上音訊內容的發展。確保數位（DAB+）和類比（FM）模式下無線電廣播所用頻率的規劃，廣播授權程序之確定，同時也監督公共和私人廣播服務遵守歌曲和音樂放送的義務。
- **線上平臺組**（*La Direction des plateformes en ligne*）：負責對線上平臺（特別是社交網路和搜尋引擎）營運商的違法、有害內容進行系統性監管。其任務包括制定評估線上平臺營運商，是否一方面能夠遵守自己內控規則實施手段的方法，同時也符合 ARCOM 設定的規範。
- **法務組：**確保 ARCOM 所有活動的法律安全。主要負責進行法律解釋和 ARCOM 所做決定、意見所必需的法律研究，也負責準備 ARCOM 在爭議案件中的辯護與爭議解決程序。
- **研究、經濟和前瞻組：**進行視聽和數位通訊監管所需的研究和分析，特別是在創新和數位技術方面。歐洲和國際事務組，負責提出並實施 ARCOM 的歐洲和國際行動。

- **傳播組**：負責所有監管機構的形象宣傳。行政、財務和資訊系統組負責預算和財務事務、人力資源、社會對話、一般資源和資訊系統。
- 其他：一個會計出納單位、一個秘書處協助相關庶務、一個地區秘書處，負責協調和領導 ARCOM 區域分支機構，並確保接收、保護和控制頻譜，同時與視聽技術官員一起管理分配給 ARCOM 管理之頻段內之接收並進行頻譜控制。

2. ARCOM 之職權

為了達成確保言論、通訊自由，促進網路通訊產業之營業自由，同時保障新傳播模式下的文化權之立法目的，《2021 年文化作品法》，在創設 ARCOM 的同時，也授予其較以往更多的程序權力及監管手段，尤其是透過調解程序之進行及調查權之行使，配合裁罰，以便能夠有效地對抗盜版行為、保護未成年人、打擊虛假與仇恨性言論[178]。以下分別說明調解程序、調查權之行使方式、以及透過公私協力進行之監控權：

（1）調解程序

本程序主要針對文化作品之智慧財產權保護與爭議解決，分為兩方面。首先是軟體發行商、技術系統製造商與服務營運商，認為有任何人或行為，影響自己對於文化作品之傳輸權利時，得向 ARCOM 提出調解申請；另一方面是針對重製作品的豁免主張，任何人重製作品係為了身心障礙者之接近使用，有權主張豁免相關限制法令之適用。

ARCOM 接受有權當事人調解請求後提交委員會，要求爭議雙方當事人提出所有相關資料進行調查，兩個月內提出調解方案，如未能達成調解，依據《智慧財產法典》法律第 331-32 條規定，ARCOM 可以為駁回請求之決定，或發布禁制令，或為具體改善之措施[179]。

---

[178] *Loi du 25 octobre 2021 relative à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique*, Vie-publique.fr (2021/10/26), https://www.vie-publique.fr/loi/279380-loi-lutte-contre-le-piratage-audiovisuel (consultée le Nov. 22, 2023).

[179] Hadopi, *Saisir L'Arcom: Intéropérabilité et Bénéfice des Exceptions*, https://www.hadopi.fr/outils-usages/saisir-larcom (consultée le Nov. 22, 2023).

（2）調查權之行使

首先，ARCOM 被賦予向所有行政機關與相關受管制對象調閱資料之權力，以便其能出具必要之意見、報告和建議。行政機關方面，除因《憲法》第 4 條規定之政黨和團體自由開展活動而產生的限制，均應提供所有資訊。

其他對象包括以下[180]：

- 視聽和電影作品的製作者、《1986 年通訊自由法》第 95 條所列舉者[181]、視聽通訊服務的出版商（*éditeur*）和分銷商、提供視聽通訊服務的公司以及影片共享平臺。
- 衛星網路運營商，要求其提供，所有為確定所承載的點播、訂製之電視和視聽媒體服務，其發佈者和負責會員國之必要資訊。
- 任何直接或間接持有出版或發行，以促進政治和一般資訊流通的廣電服務公司，10%以上股份或表決權的自然人或法人，如該人或由該人控制的公司在過去 24 個月內已投標，可要求其提供所有關於公共採購（*marchés publics*）和公共服務特許（*délégations de service public*）的資訊。

其次，除了要求以上所述對象提出資料外，為了確保其提出資料的完整性與真實性，ARCOM 也對視聽通訊服務的出版商和分銷商、衛星網路運營商、提供視聽通訊服務的公司和影片共享平臺，進行必要的調查，以確保上開主體遵守其義務。

依據《2021 年文化作品法》第 331-14-I 條之規定，後來納入《1986 年通訊自由法》第 19 條，調查權的行使由 ARCOM 授權之公務員進行，並且須遵守中央行政法院以政令發布之宣誓與程序規定。在進行調查期間，公務員得於不遵守受調查者營業秘密之情況下，得取得所有調查所需之專業文件與資訊協助，包括資訊用戶或發布訊息者之身

[180] 陳志宇、林家暘、吳秦雯、江耀國、王牧寰等，前揭註 117，頁 153。

[181] 電視或廣播服務的經銷商或出版商、接收系統的營運商、允許透過數位訊號接收電視或廣播服務技術系統之全部或部分的相關智慧財產權持有者。

分、郵政地址、電子地址以及電話聯絡方式；得進行聽證（*audition*）程序，亦得透過雙方當事人皆出席且得相互詰問的之對審形式（*façon contradictoire*）後，製作書面報告（*procès-verbal*）。報告的副本應於作成後的五天內送達有關人員；蒐集調查所需的資訊與證據。

同條亦規定，在調查進行中，授予獲得授權之公務員可以在豁免刑事責任的情況下，以假名參與可能違反受調查活動所適用之規定有關的電子通訊交流；或使用以這種方式提取、獲得或保存關於這些服務的證據，以便確定事實。

這些行為不得導致煽動他人犯罪的效果，否則其所獲得之證據無效（*à peine de nullité*）。根據本條規定收集的資訊，只得為本法目的之利用，不得用於完成本法賦予的任務以外的目的。上開資訊應嚴守保密原則，洩漏以上資料都是被禁止的。

（3）監控權及相關公私協力機制

由以上的組織與職權介紹可知，ARCOM 確實能夠透過組織、分工與職權行使，達到其所宣示之職責目標：「監管線上平臺，包括：社交網路、搜尋引擎、影片分享平臺等，特別是監督線上平臺，以打擊資訊操縱以及避免仇恨、違法和有害內容而得採取有效必要之手段」[182]。

由於法律授權將 ARCOM 指定為許多線上平臺監管之主管機關，因此在政治不實訊息、兒少網路安全、網路交易安全、網路霸凌及使用者權益，其都有相應的管制作為，並建立公私協力機制，包括：

A. 設立網路仇恨觀察站

早在 2022 年 ARCOM 正式上路前，CSA 就已依據《2020 年對抗網路仇恨內容法》（*loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet*，一般簡稱為《Avia 法》）第 16 條，配合《LCEN 法》第 6-4 條第 1 項所確認的內容，在 2020 年 7 月成立「網路仇恨觀察站」（*Un observatoire de la haine en ligne*）以確保兒

[182] Arcom, Découvrir l'institution, https://www.arcom.fr/nous-connaitre/decouvrir-linstitution (consultée le Nov. 25, 2023).

少網路安全、減少網路霸凌、確保網路交易安全與使用者權益。

網路仇恨觀察站之主要任務在於分析及量化網路上的仇恨現象，以增進對其原因及動態的了解，並鼓勵利害關係人之間分享資訊和回饋經驗。組成者匯集所有可能關注打擊和預防這些犯罪行為的經營者、協會團體、行政部門和研究人員，並考慮到公眾，特別是未成年人的多樣性。

目前組成網路仇恨觀察站的成員包括[183]：

- 協會團體：公民實驗室（Civic Fab）、法國猶太機構代表委員會（CRIF）、網路兒童（e-Enfance）、法國網路命名合作協會（AFNIC）、數位世代（*Génération numérique*）、InterLGBT、La Quadrature du Net、人權聯盟、國際反對種族主義和反猶太主義聯盟（*Ligue Internationale contre le racisme et l'antisémitisme*, LICRA）、陰謀觀察站、接觸點（*Point de contact*）、數位復興（Renaissance numérique）、尊重區（Respect Zone）、SOS 恐同症、SOS 種族主義、停止恐同症、策略對話研究所（Institute for Strategic Dialogue）。
- 行政機關：國家身心障礙者諮詢委員會、國家人權諮詢委員會（*Commission nationale consultative des droits de l'homme*, CNCDH）、國家數位委員會、反對種族主義、反猶太主義和反 LGBT 仇恨部際代表、人權監察使、最高性別平等委員會、文化部、數位事務部、教育、青年與體育部、歐洲和外國事務部（數位大使）、內政部之「PHAROS」平臺[184]、法務部之刑事事務與赦免司（DACG），以及被授權負責男女平等、多元化和機會的部會。
- 任職於高等教育機構從事相關研究的研究者，共 7 名。

[183] Arcom, *Observatoire de la haine en ligne : analyser pour mieux luter*, https://www.arcom.fr/nous-connaitre-nos-missions/superviser-les-plateformes-en-ligne-et-les-reseaux-sociaux/observatoire-de-la-haine-en-ligne-analyser-pour-mieux-lutter (consultée le Nov. 25, 2023).

[184] 警示的協調、分析、交叉檢查與引導平臺（*Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements*, PHAROS），法國政府設立於 2009 年，專門收受網路上違法內容訊息之舉報。

B. 確保選舉期間網路平臺遵守對抗虛假訊息之義務

以《2018 年反資訊操縱法》(*Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information*）為其主要法規依據，ARCOM 在 CSA 時期即於 2019 年 5 月 15 日發布建議路徑：CSA 對網路營運平臺對抗虛假訊息傳播之合作義務建議（*Recommandation n° 2019-03 du 15 mai 2019 du Conseil supérieur de l'audiovisuel aux opérateurs de plateforme en ligne dans le cadre du devoir de coopération en matière de lutte contre la diffusion de fausses informations*)，要求符合《消費法典》法律第 111-7 條規定條件之網路營運平臺，即依據前一年度之資料每月平均使用者流量超過 500 萬者，都必須符合指引內的合作義務，共同對抗有可能侵擾公共秩序或對選舉真實性的產生警示的虛假訊息，並回應主管機關所進行之調查。

不過，ARCOM 並未被法律賦予強制網路營運平臺遵守此些義務之權力，因此只是一個行政指導的性質。主要的合作義務簡述如下：

- **建立可接近及可見的通報規範**(*La mise en place d'un dispositif de signalement accessible et visible*)

ARCOM 建議平臺可進行以下措施：建立的通報規範使用清楚的文字加以顯示；將通報規範設置在靠近可能被檢舉的內容或帳號的位置；平臺可以提供一些共通性的違規內容或可疑網址，方便使用者辨識；設置使用者可以互相交流以確認虛假訊息或傳送方式的機制；設計簡單且合乎邏輯的報通報流程，用戶應該能夠透過最多三個超連結來完成報告程序，所有舉報原因（如仇恨內容、虛假資訊等）應顯示在一個對話方塊中；允許使用者追蹤其通報後的處理情況，以便了解進展情況，並儘快告知他們針對通報內容採取的行動。

- **演算方式的透明**

使用者必須能夠以知情的方式對線上平臺提供的內容進行批判性思考。讓使用者能夠存取訊息、了解和理解控制該內容的組織、選擇和排序演算法的操作原理。為此，ARCOM 鼓勵平臺讓每一位用戶可以追蹤其所接收到的受推薦或具有優先順序的資訊，不論該資訊是

否由平臺故意提供或搜集；提供使用者清晰、足夠精確且易於搜尋的演算法標準；關於參考和推薦演算法的主要變化及其影響的資訊；提供用戶聯絡演算操作員的簡單聯絡方式，並為使用者提供獲得有關演算法操作的個人化和精確資訊的可能性。

- **標示由公司、新聞機構或是視聽通訊服務業者提供的內容**

委員會建議線上平臺營運商：提供使用者清晰可見的指標來辨識公司、新聞機構和視聽通訊服務業者的內容來源。鼓勵線上平臺業者採納標籤程序；設置技術手段，讓用戶能夠看得出資訊的來源，尤其是透過搜尋引擎查得之結果、新聞提要和其他透過自動分類操作播送管道中所謂的「事實核查」的內容。

- **打擊加速和放大虛假訊息的帳號傳播**

委員會鼓勵線上平臺營運商實施確保偵測到大量散播假訊息的帳戶的適當程序；阻礙這些帳戶行動的適當程序，像是採取：警告、刪除、隔離、限制使用者權利或其分發內容的範圍等方式，以符合言論和通訊自由；進行並設置偵測和處理這些帳戶相關的公共監控和統計系統；提供一個易於存取的資訊欄，以清晰、準確的方式告知使用者可能導致平臺進行干預的做法，像是使用者異常地建立大量帳戶、異常頻率共享內容、使用虛假、被盜或誤導性資訊等。

- **向使用者提供有關內容的性質、來源、傳播方式以及為傳播資訊內容而支付報酬者之身份的相關資訊**

平臺應建立適當的系統，讓使用者了解內容傳播的性質、來源和方法，建議措施：明確區分贊助內容和其他內容，鼓勵平臺開發工具，使用戶能夠識別平臺向他們提供此類內容的原因與標準；平臺應呼籲用戶對被檢舉的內容保持警覺；明確標識播放內容的來源並以明顯方式顯示；明確說明推播內容的傳播方式，盡可能說明其刊載的條件，例如是否有提供金援、傳播程度（如觀看次數、目標人群類型等）以及是否以自動方式產生；也可以採取措施，告知使用者內容傳播者之自然人身分或公司名稱、註冊辦事處以及向其支付報酬的法人實體的企業宗旨。

- **鼓勵推動媒體與資訊教育**

鼓勵網路平臺幫助用戶識別可靠的資訊來源和不可靠的資訊來源。鼓勵業者讓使用者意識到自己內容的影響力，幫助培養使用者的批判意識，尤其是兒少族群。鼓勵線上平臺營運商開發適當的工具來分析資訊來源的可靠性，例如視訊模組和指南。建議線上平臺營運商支持專案並建立有助於媒體教育、資訊和數位工具的合作夥伴關係。鼓勵線上平臺支持記者和研究人員的獨立倡議，以便達到更好地理解和衡量虛假資訊現象。也建議線上平臺轉發媒體和資訊教育領域參與者的宣傳活動。

- **提供主管機關資訊**

首先，網路平臺每年都要提送經營年報，在與其活動相關的財政年度次年 3 月 31 日前提交予主管機關。網路平臺業者在本建議指引發布前，曾表明要將本建議指引相關措施具體實施可能遭遇的困難，因此主管機關為了確保並監督線上平臺營運商將配合採取上述《2018 年反資訊操縱法》第 11 條規定的措施義務，將定期發布有效性的評估，並在依據《1986 年通訊自由法》第 19 條規定之條件下，向平臺經營者搜集平臺編寫年度報告所需的所有資訊。

其次，如果發現操縱或試圖操縱且可能擾亂公共秩序，或改變選舉真實性的訊息，主管機關要求網路平臺應保留提供任何與該訊息有關可能性的資料；並建議平臺運營商在發生此類事件時，盡可能向用戶展示最大的透明度。不過，執行這項任務時，主管機關會將不同平臺模式以及每個平臺所實施的手段，是否足以影響資訊操縱現象的規模和影響，納入考量。

最後，主管機關並根據《2018 年反資訊操縱法》第 13 條，要求每個線上平臺營運商都必須指定一名法定代表人，在法國領土上行使聯絡人職能，以適用該法律第三章的規定。

（二）全面性的法令修訂

由於過往的研究報告已對法國近年的法令修訂情況進行說明[185]，本研究不再贅述。由於本研究之重要分界點在於歐盟新出爐之《數位服務法》，因而以 2022 年 11 月 16 日，歐盟正式完成《數位服務法》之立法程序作為時間分界，僅稍加彙整該期程前之相關法令後，再介紹最新的立法趨勢。

1. 歐盟《數位服務法》立法前之法國重點法令

自二十世紀末，以進入資訊社會為主軸開始展開的各項政策作為為起始，法國開始了一連串多方面的立法與修法。

就網路交易安全部分，2004 年主要為落實歐盟指令對於電子商務進行規範，制定促進法國數位經濟之專法，初步建立法國對於網路中介服務者責任規範，亦即俗稱為《LCEN 法》的《2004 年 6 月 21 日第 2004-575 號數位經濟信任法》。另一方面，亦制定《2016 年促進數位共和國法》，納入《消費法典》法律第 111-7 條，確立法國法上網路中介服務者之用語，並以《消費法典》法律第 111-7-1 條、第 111-6 條規定，命一定規模流量之網路平臺營運者負有清楚、透明與忠實義務，且使有權行政機關得以調查評估各網路平臺營運者之實績並將未遵守義務者予以公告。同時考慮到網路上智慧財產權保護，2021 年 10 月制定前已介紹之《2021 年文化作品法》。

就兒少網路安全、網路交易安全、網路霸凌防治而言，為了避免越來越多透過網路傳布違法性言論內容之網路犯罪行為，像是利用網路宣傳恐怖主義，或是涉及未成年人之色情行為，2014 年制定《第 2014-1353 號對抗恐怖主義法》（*Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme*），由法院透過緊急程序要求網路平臺將包含違法內容之言論去除或去檢索；並針對使用網路公眾通訊而直接引起恐怖主義或向公眾美化恐怖主義之行為，修改新增《刑法典》第 421-2-5 條規定課以刑事制裁。

[185] 陳志宇、林家暘、吳秦雯、江耀國、王牧寰等，前揭註 117，頁 132-151。

接著，2020 年 6 月 24 日第 2020-766 號針對恐怖主義、色情、仇恨性內容予以移除之《Avia 法》，針對透過網路傳佈具有仇恨性內容言論予以刑罰化。2021 年則在強化共和國價值，減少極端主義之立法目的下，制定第《2021-1109 號符合共和國原則法》（*LOI n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République*，以下簡稱為《2021 年符合共和國原則法》），該法同時也是作為預計於 2024 年通過並實施之 DSA 之過渡性法律，以課予內容分享平臺、社群平臺及搜尋引擎有關違法內容之內容篩檢；與主管機關合作；對處理仇恨性內容之政策與程序之透明性、風險評估；及建立通報使用者違法內容之系統等義務。

就政治不實訊息之防治部分，2018 年底通過的《2018 年反資訊操縱法》特別規範在選舉期間，由緊急審理法官在受理後 48 小時內裁決假資訊。

2. 歐盟《數位服務法》立法後之法國重點法令

早在歐盟《數位服務法》正式生效前，法國便已開始將若干相關指令轉換為本國法律，以下以本研究設定之主軸依時序進行概要說明。

（1）對抗網路霸凌、數位暴力與保護兒少之法令

根據法國公共服務網站資料顯示，在法國，20%的 8 歲至 18 歲青少年和 60%的 18 歲至 25 歲青少年已經面臨網路騷擾的情況[186]，而大量兒童、青少年輕易接近並使用社群網路，都造成嚴峻之數位暴力情況，2022 年與 2023 年分別制定新的相關法令，說明如下：

A. 《對抗校園霸凌法》

透過《2022 年 3 月 2 日第 2022-299 號對抗校園霸凌法》（*LOI n° 2022-299 du 2 mars 2022 visant à combattre le harcèlement scolaire*）之主要規範內容包括《刑法典》第 222-33-2 條到第 222-33-2-3 條（關於心理霸凌），以及《2004 年數位經濟信任法》（《LCEN 法》）第 6 條之

[186] Direction de l'information légale et administrative (Premier ministre), *Le 3018, un numéro gratuit et une application, pour les victimes de cyberharcèlement*, Service-Public.fr. (2023/02/20), https://www.service-public.fr/particuliers/actualites/A15501 (consultée le Nov. 25, 2023).

修正。

該法之主要規範對象係「透過反覆發表評論或行為來騷擾他人，其目的或效果是惡化被騷擾者之生活條件，從而導致其身心健康發生變化」之行為，可判處一年有期徒刑和 15,000 歐元罰款。倘若上述行為導致受騷擾者完全喪失工作能力超過 8 日；受騷擾者為未成年人；故意針對因年齡、疾病、虛弱、身體或心理缺陷或懷孕狀態而具有特殊脆弱性之人；使用線上公共通訊服務、透過數位或電子媒介為之；或是騷擾當場有未成年人在場時，處罰加重為兩年有期徒刑與 20,000 歐元罰款。若上述五種情形有兩種以上同時該當，則可處以 3 年有期徒刑和 45,000 歐元罰款。

換言之，如果一個網路霸凌行為係以未成人年為對象，便可能遭致 3 年有期徒刑及 45,000 歐元之罰款。另外，針對同一教育機構中的心理霸凌行為，若導致受害者自殺或企圖自殺時，處罰將增加至 10 年有期徒刑及 150,000 歐元罰款。

不過應注意的是，根據《LCEN 法》第 6 條之定義，網路中介者即網路平臺係指提供接取服務與儲存服務之業者，並不會因為網路霸凌者使用平臺之行為，就等於自己即為網路霸凌之行為人，進而因此遭受處罰。但是，若平臺實際知悉通訊服務使用者所提供之信號、文字、圖像、聲音或訊息具有違法性質時，應立刻採取行動刪除數據或禁止瀏覽，否則也將負擔民事責任及刑事責任。為了網路中介者能夠快速進行相關配合刪除數據或禁止瀏覽的措施，受害者得直接與網路中介者聯絡並進行通報，要求刪除某一特定網路霸凌行為。

簡言之，法國法令並未直接明定網路中介者的處理方式，其僅要求網路中介者必須設置相關處理機制，亦即國家的規管行為並不包括自己直接進行網路霸凌行為之封鎖、阻斷或下架。

只有在緊急情況下，可以透過電話或簡訊向警察通報網路霸凌行為[187]。為了有效處理相關向國家通報的網路霸凌行為，法國內政部設

[187] Direction de l'information légale et administrative (Premier ministre), *Cyber-harcèlement (harcèlement sur internet)*, Service-Public.fr. (2020/11/30), https://www.service-public.fr/particuliers/vosdroits/F32239 (consultée le Nov. 24, 2023).

置了單一窗口網站，亦即前述構成「網路仇恨觀察站」成員之一的「PHAROS」平臺，與簡碼電話 3018，提供每天 9 點到 23 點的服務；也可以透過在智慧型手機下載 3018 應用程式，即時透過聊天或電話直接聯繫 3018 專業人員；將遭受騷擾的證據（螢幕截圖、照片、URL 連結等）儲存在安全的數位保險箱中，並將該證據的全部或部分傳輸給 3018 團隊；也可以快速存取「PHAROS」平臺製作之網路騷擾實用情況說明書，了解自身權利並理解如何應對。

該應用程式還有「我是否受到騷擾？」測驗，協助可能的受害者對自己的情況進行自我評估，並鼓勵受害者尋求幫助。最後，受害者可以將透過 3018 應用程序完成的通報傳輸到社群網路，以便他們快速，通常是在幾個小時內，刪除有問題的帳戶或內容，且針對最嚴重的案件，也可以直接傳輸到「PHAROS」平臺，直接通報網路上違法內容的入口網站[188]。

3018 自 2022 年啟用以來，相關機關平均每日收到 20 件通報，2022 年一年內收到 25,000 通電話；相較於 2021 年相關統計資料，增加 39％的通報電話數；已經有 10,000 則內容被下架，比起 2021 年相關統計資料，增加 234％[189]。

B. 《設定數位成年人與打擊網路仇恨法》

根據法國獨立行政機關「資訊與自由委員會」（National Commission on Informatics and Liberty, CNIL）之調查，法國年輕人首次在社群網路上註冊的年齡平均約為 8 歲半。由於父母對孩子在這些社交網路上的存在知之甚少，其數位活動往往遭到低估，且難以衡量其程度。另一方面，社群網路也是傳播假訊息的主要載體，對未成年人帶來許多危險。

面對年輕受眾中數位實踐的大眾化和賦權，立法者以《2023 年 7 月 7 日第 2023-566 號設定數位成年人與打擊網路仇恨法》（*LOI n° 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à*

188 Premier minister, *supra* note 186.

189 *Id*.

lutter contre la haine en ligne）[190]提供了一個新框架。

《設定數位成年人與打擊網路仇恨法》之內容主要係修改《LCEN 法》第 6 條，同時新增第 6-7 條，以保護未成年人免受社群媒體之影響。

該法明文將 15 歲作為法定社群媒體平臺上註冊的「成年年齡」。在法國運營的線上社群網路服務提供者不得為 15 歲以下的未成年人提供註冊服務，除非該未成年人的法定代理權持有者之一對該註冊給予授權。15 歲以下之青少年與兒童在獲得家長至少其中一方之同意，方得使用社群媒體。註冊時，社群媒體應向 15 歲以下之青少年或兒童與家長盡相關風險告知義務並告知相關使用規範；使用期間社群媒體亦應對上開青少年或兒童提供上線時間控制機制，家長亦得隨時提出要求社群媒體暫時凍結其子女之帳號。

為驗證用戶的年齡和確認是否取得家長之同意，社群媒體必須實施符合 ARCOM 制定之參考標準之技術解決方案，並在諮詢 CNIL 後進行。如業者未遵守此義務，可能面臨罰款，最高可達全球營業額的 1%。此外，該法還包含改善預防、追究線上犯罪行為：除了宣揚恐怖主義行為、煽動仇恨、性騷擾或校園霸凌之內容外，現在更包括婚姻或精神騷擾、勒索（如性敲詐）、侵犯隱私（如傳播私密內容或個人數據）與侵犯人格形象（如深度偽造）等行為相關之內容。另外，社群媒體也應傳播反網路霸凌熱線電話之訊息，並讓所有使用者舉報更多違法內容，以便刪除。

最終，該法更明文規範，在刑事偵查之場合中，社群媒體和其他線上平臺必須在 10 天內回應有關電子內容（文字、影像、影片等）的司法請求，而若在「存在對人身嚴重危害的迫切危險」之情況下，則為 8 小時內[191]。

---

[190] *LOI n° 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne (1)*, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047799533 (consultée le août 24, 2023).

[191] Protection des mineurs - Majorité numérique et haine en ligne: la loi est publiée – Veille, La Semaine Juridique Edition Générale, n° 28, 17 juillet 2023, act. 861.

（2）確保網路交易安全之法令

由於網路平臺上之商業活動，往往係透過瀏覽量達一定規模、具有影響力之「網紅」進行，除可能導致一般大眾（尤其年紀較輕之網路使用者）之理性選擇受到影響，危害網路交易安全，亦可能形成網路霸凌，法國於 2023 年 6 月 9 日通過第 2023-451 號《規範商業影響力並打擊社群網路中具影響者之濫用行為之法律》（*LOI n° 2023-451 du 9 juin 2023 visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux*）[192]。該法自同年 1 月初提案開始，僅花費 5 個月時間即完成制定，上下兩議院對於該等規範之高度共識可見一斑。

受網紅影響而鼓勵購買的產品、服務的性質或品質，通常並不能真的由網紅進行控制與確保，甚至，網紅也未必真的在意販售商品的品質，而可能只是試圖引導那些追隨他們並信任他們的人的意見和願望[193]，倘若消費者在購買後對商品不滿意而提出爭議，在新立法之前，通常僅能依據《消費者法典》法律第 132-1 條至第 132-9 條規定，主張網紅的行為該當欺騙性商業行為。因此，該法第 1 條首先定義，具有商業影響力的活動是由「自然人或法人收取費用，利用其在受眾中的知名度，透過電子方式向公眾傳播旨在直接或間接宣傳的內容」。

同時該法律規定，要求此等商業宣傳活動必須簽訂書面契約，書面契約當中包含若干強制性條款：必須載明委託任務、報酬條件、當法國訂戶成為商業宣傳目標時要求遵守法國法律；如果兒童成為任何一個網路平臺的商業影響者，兒童也受到勞動法的相關保護，其法定代理人必須與廣告商簽訂契約，並將收入一部分存入兒童的帳戶[194]。

---

[192] *LOI n° 2023-451 du 9 juin 2023 visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux (1)*, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047663185 (consultée le Nov. 1, 2023).

[193] Isabelle Corpart, *La loi n° 2023-451 du 9 juin 2023, pour une utilisation plus sécurisée des réseaux sociaux*, Lextenso (2023/07/11), https://www.actu-juridique.fr/ntic-medias-presse/la-loi-n-2023-451-du-9-juin-2023-pour-une-utilisation-plus-securisee-des-reseaux-sociaux/ (consultée le Nov. 1, 2023).

[194] *Loi du 9 juin 2023 visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux*, Vie-publique.fr (2023/06/12), https://www.vie-publique.fr/loi/288793-loi-influenceurs-proposition-de-loi-delaporte-vojetta (consultée le Nov. 1, 2023).

該法也建立加強打擊濫用和詐騙的責任平臺，同時建構監管框架。

為了具有可辨識性與增加透明性，新法規定以社群網路影響者必須以清晰、易讀或可識別的方式在宣傳圖像或影像上出現，並在整個促銷過程中標示「廣告」或「商業合作」。對於任何由人工智慧修改或產生的圖像，必須標明「圖像後製」或「虛擬圖像」，以及禁止未成年人觀看的內容，應該要標示「禁止 18 歲以下」。如果只是以主題標籤像是#ad（廣告）和#sp（贊助）不被認為足夠明確揭露內容具備促銷性質，因為大多數人無法充分理解該主題標籤之涵義。若缺乏此類標示，將被處以 1 年有期徒刑及 4,500 歐元之罰款。

同樣地，新法並未直接認定刊載有商業影響力資訊之網路中介者與刊載者負擔相同的刑事與民事責任，其義務仍然為接受通報。當受害人或相關人向平臺通報違規內容後，平臺僅有在不採取行動之情況下方被追究責任。網路中介可以選擇向消費者顯示警告訊息、在社群網路上刪除帳戶、限制存取或封鎖社群網路上的帳戶。

另外，本法第 10 條至第 12 條亦於《LCEN 法》新增第 6-4-1 條、第 6-4-2 條與第 6-6 條，除了課予儲存服務提供者，建置用戶通報網紅違法行為之建置義務外，另需依歐盟《數位服務法》第 22 條規定，課予線上平臺營運商，優先處理認證舉報者之通報機制，並責成主管機關至少每六個月列出符合本法定義之違法服務或商品的網站清單（黑名單），提供網路中介者參考使用。。

另外，本法較為特別者，在於制定了一項由競爭、消費者和詐欺控制總局（*Direction générale de la concurrence, de la consommation et de la répression* des *fraudes*, DGCCRF）實施的新控制措施。透過新增《消費法典》之規定，本法於 DGCCRF 內設置一個專門的團隊負責監控社群網路，並進行審查，一方面可以要求網紅改善，另方面也可要求網路中介者進行改善、刪除相關資訊，若出現全部或部分不履行或逾期執行的情況，DGCCRF 會依據違反的嚴重程度，適用《消費者法典》法律第 522-5 條之規定，先進行警告，如果認為該當欺騙性商業行為，則將案件移交檢察官，可能導致兩年有期徒刑和最高 30 萬歐元的罰款。

當 DGCCRF 要求網紅中止其違法行為時，倘若不遵守禁令，個人最高將被處以 75,000 歐元罰款、法人則是 375,000 歐元罰款，同時也會公布該網紅之姓名。另外，DGCCRF 也可併同要求需改善之網紅必須配合播送自己遭受裁罰之影像圖示。至於網路服務提供者，若其不配合處理用戶的警示通報，DGCCRF 則有權下令阻斷引用其內容的網路連結，甚至網域被封鎖三個月；如果違法行為持續存在，DGCCRF 可以發布禁令刪除或轉讓網域名稱。

另外，為了讓商業影響者知悉自己的商業行為規範，經濟部在經過公共審議的諮詢過程後，發布了《內容影響者與作者之良好指引指南》（*Guide* de *bonne conduite : influenceurs et créateurs de contenu*），供網紅們理解自己的行為規範與界線[195]。法國應該是歐洲第一個對商業網紅進行法令規範的國家，其未來發展值得觀察。

（3）最新立法草案

法國兩議院刻正審議之《數位空間規範與安全法》（*loi visant à sécuriser et réguler l'*espace *numérique*，未來可能簡稱為《SREN 法》），係 2023 年 5 月由經濟與數位發展部所提出之法案。其規範重點預計包括：授權設立實施反詐騙網路安全過濾器，以保護法國人免受欺詐性調閱個人資訊或用於惡意目的的金融機構資訊；強化制裁實施數位暴力之行為人；增加色情網站的瀏覽限制以保護兒童；對於未能刪除網路色情內容的網站進行制裁；恢復雲端市場的商業公平，試圖打破該市場集中在少數手中之現象；提供新的保護措施，防止因播放受國際制裁打擊的媒體而造成的虛假資訊和外國干涉；持續調整國家法律，使法國在 2022 年擔任歐盟理事會主席期間通過的兩項主要歐洲法規：《數位服務法》及《數位市場法》得以無困難地在法國適用[196]。

正如法國總統在擔任歐盟理事會主席期間將數位革命描述為「本

[195] Bercy infos, *Guide de bonne conduite: influenceurs et créateurs de contenu*, economie.gouv.fr (2022/12/19) https://www.economie.gouv.fr/guide-bonne-conduite-influenceurs-createurs-contenu# (consultée le Nov. 25, 2023).

[196] Projet de loi visant à sécuriser et réguler l'espace numérique (ECOI2309270L), *Compte rendu du Conseil des ministres du 10 mai 2023*, Compte rendu du Conseil des ministres (2023/05/10), https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000047533100/ (consultée le Nov. 25, 2023).

世紀的第二個挑戰」，法國因應數位革命，採取了保護、監管數位空間，避免不公平競爭的態度，尤其在風險和創新迅速倍增的不斷變化環境中致力於確保公民的安全，降低訊息操縱、交易風險與數位暴力行為，不但一方面盡力將歐盟層級之《數位服務法》更細緻地轉換為法國內國法，甚至更進一步致力於各種網路商業行為的規管。

三、第三方監督或產業自律機制

歐盟的監管架構下，與事實查核組織之合作，似具有不可或缺的重要性。不過，法國並未組織特別具備規模的事實查核外部或第三方組織，因為媒體聘用專業記者的工作任務之一，即是依據事實進行報導；針對事實進行查證，其實本為新聞傳播工作的核心。所以，第三方監督，雖然有媒體事業成立的事實查核編組，但並非是外於媒體的純第三方之方式出現。

不過，透過政府規管法令的指引，公私協力的模式，以及產業在政府規劃路徑架構下的自我規管行動，究竟產生如何的效果，對於此些受到規管的網路服務營運商又產生如何的困難，ARCOM 在今年 2023 年 7 月 23 日針對網路服務營運商面對網路上傳播仇恨內容的相關措施，進行評估與調查，提出調查研究報告[197]，以下將參考該份報告進行相關說明，以理解目前的產業自律規範究竟發生如何的實效性。

（一）以媒體產業為主的事實查核

隨著政治話語的多樣性，以及為了透過驗證和糾正誤導性或令人困惑的斷言來澄清公眾辯論，法國若干媒體因此設立專門的機構，特別是在選舉期間，由專門的記者進行對於事實的真實性進行考核。

在法國，2007 年創設的媒體觀察網站「*Arrêt sur Images*」是該類型的先驅之一。歐洲事實查核準則計畫規劃下，法國的合作夥伴「法

[197] Arcom, *Lutte contre la diffusion de contenus haineux en ligne : bilan des moyens mis en oeuvre par les plateformes en ligne en 2022 et perspectives*, Études, bilans et rapports de l'Arcom (2023/06/24), https://www.arcom.fr/nos-ressources/etudes-et-donnees/mediatheque/lutte-contre-la-diffusion-de-contenus-haineux-en-ligne-bilan-des-moyens-mis-en-oeuvre-par-les-plateformes-en-ligne-en-2022-et-perspectives (consultée le Nov. 25, 2023).

新社」(*L'Agence France-Presse*, AFP)，設置 AFP Factuel 專門網站[198]，針對所有受歡迎的主題進行查證後刊登相關新聞。各大傳統紙本媒體都有類似的特殊部門，讓記者專門從事這項唯一的任務[199]，像是法國《解放報》(*Libération*) 於 2008 年設置 *Désintox*，2014 年法國《世界報》(*Le Monde*) 設置 *Les Déocoders* 專欄[200]，2017 年《二十分鐘報》(20 Minutes) 也設置 Fake Off。目前也有國際人道組織成立針對 YouTube 影像的真實性進行驗證之網站 Citizen Evidence[201]。也有像是 HoaxBuster，以協作平臺的方式提供確認事實查核[202]。

（二）由政府引導的公私協力機制強化產業自律

現今網際網路及數位現象的發展特色之一，在於網路行動者們往往因為技術發展而超出原本國家規管的範圍，以國家為主導的由上而下式的監控，有時候可能有緩不濟急或過度監管的情況發生，也可能欠缺產業各自發展的彈性。因此，法國即使目前的監管模式顯現出強大的國家主導地位，在法制設計上，仍然留給產業各自形成內部規範的空間。

然而，依據《消費法典》法律第 111-7 條，所有「任何由第三方所提供，且其活動於法國境內的連結次數高於命令所訂流量的線上公共通訊服務，這種服務無論是否設置於法國境內，只要旨在對於內容進行線上分類、網路索引或資料分享」，都是受規管之網路平臺營運者；依據《2021 年符合共和國原則法》第 42 條授權的子法《2022 年 1 月 14 日命令》(*décret n° 2022-32 du 14 janvier 2022*)，亦即網路平臺營運者如果每月平均流量超過一千萬人，就屬於受規管的對象，倘若流量超過 1,500 萬人，更有須配合司法或行政機關執法之額外義務。

---

198 *See* AFP, https://factuel.afp.com/ (consultée le Nov. 25, 2023).

199 CLEMI, Le fact-checking, ou journalisme de verification, https://www.clemi.fr/fr/ressources/nos-ressources-pedagogiques/ressources-pedagogiques/le-fact-checking-ou-journalisme-de-verification.html (consultée le Nov. 25, 2023).

200 *See* Le Monde, https://www.lemonde.fr/les-decodeurs/ (consultée le Nov. 25, 2023).

201 *See* Youtube DataViewer, https://citizenevidence.amnestyusa.org/ (consultée le Nov. 25, 2023).

202 Internet Sans Crainte, Fake news: 5 sites incontournables pour ne plus se faire piéger !, https://www.internetsanscrainte.fr/dossiers/fabrique-de-linformation-0/conseils/fake-news-sites-incontournables-pour-ne-plus-se-faire-pieger（最後瀏覽日：2023/11/25）

目前包括：Google（針對 Google Search 及 YouTube）、LinkedIn、Meta（針對 Facebook 與 Instagram）、Microsoft（針對 Bing）、Pinterest、Snap、TikTok、Twitter、Wiki 媒體基金會、Yahoo（針對 Yahoo Search）還有 Dailymotion。值得注意的是，後兩者其實並不屬於歐盟《數位服務法》定義下的非常大型線上平臺或非常大型線上搜尋引擎，但是仍符合法國法自身的定義。

上述這些網路平臺營運者，都必須在保護網路交易安全、兒少保護、遏止網路霸凌等目的，適用《LCEN 法》第 6-4 條之規定，與公權力主管機關進行合作，亦即網路平臺必須制定內部政策以達到對抗仇恨性言論之公開義務、自行評斷風險、並設立相關制度以偵測並辨識使用者之非法言論。

目前這樣的義務已經在先前的研究報告中說明，內容包含：「網路平臺營運者須配合司法或行政機關執法之義務；建立舉報機制，使任何人得以舉報其認為有非法內容之資訊；建立並說明內部處理非法內容資訊之程序，以迅速回應舉報並在最佳期限內審查與通知；網路平臺營運者應建立申訴機制，告知違法內容資訊之作者說明此一決定是否透過自動化系統所判斷、該營運商內部之紛爭處理程序，及違法內容資訊可能遭受的民事與刑事責任；網路平臺營運者得對於違法內容之資訊提供者暫停使用或刪除該使用者之帳號現址，避免其重複發布違法訊息」[203]。

ARCOM 於 2023 年 7 月 23 日研究報告中，提出目前網路平臺營運者在履行相關法令義務的四個困境：第一，如何認定網路平臺營運者是否被納入法令義務適用，計算數據的標準仍有疑義；像是 Yahoo 就覺得自己不應該被納入適用。且每個營運平臺對於義務履行的完成度也有不同認定。其次，目前的規範法制未考慮平臺差異。像是 Wiki 媒體基金會認為維基百科的是採取分散協作的方式，而 Bing 不會儲存用戶內容或納入被認為違法的內容。第三，網路平臺營運者雖然已經擴大透明性，但是網路平臺營運者認為在揭露資訊的同時，資料的相關性可能會因此減損。第四，法令設定的回應時間對網路平臺營運

[203] 前揭註 108，頁 161-162。

者認為不易達成。

總結 ARCOM 的報告，以國家法令設置的網路平臺協力義務，必須透過經營者正視並反思自己的社會責任方有達成之可能。然而網路平臺的經濟模式主要就是基於廣告，因此無限制地捕捉使用者的注意力，且操作架構就是基於所呈現的內容（包括廣告），對收集到的個人資料進行大規模演算法處理，正是非常大型線上平臺及非常大型搜尋引擎的兩個特點，而這樣的特性，儘管在獲取資訊、參與公共辯論上具有重要的作用，但同時也帶來風險。然而，使用者透過網路平臺獲得好處的同時，也連帶形成各種網路暴力與色情資訊的危害，儘管這未必是網路平臺經營直接造成的，但是網路平臺經營者卻不能逃避其因為獲得經濟利益而需負擔的責任。目前在國家政策要求與社會壓力下，網路平臺經營者因應提出的自律方案，事實上不容易在國家社會期待資訊透明的情況下，與平臺期待獲得經濟最大利益的一定營業秘密取得平衡。

ARCOM 負責確保相關國家法律的正確實施，並與營運商建立穩定對話，強化發展線上平臺監管方面的專業知識，有助於營運商更理解自己的責任，慢慢展現出規管的一定成效[204]。

四、小結

從二十世紀末進入資訊社會之初，到現在二十一世紀初期，網際網路服務，對於當代社會的影響層面可能遠大於一開始的想像，為了因應這樣的挑戰，法國一開始原本採取寬鬆規管、自由競爭、市場經濟的模式，漸漸發現這樣的產業自律模式，造成沒有預料到的網路交易風險、網路暴力、兒少權益侵害，甚至大量假訊息影響民主社會的運作。目前，整個法國的治理與規範態度，顯然已經導向國家主導、透過法令框架，課予網路行動者義務，一種主導型的公私協力方式進行。

[204] Lutte contre la diffusion de contenus haineux en ligne, Bilan des moyens mis en œuvre par les plateformes en ligne en 2022 et perspectives, Acrom 2023, p.28-31.

第四節 英國

一、監理脈絡

為將數位政策納入國家發展之主軸，英國原交由數位、文化、媒體暨運動部（Department for Digital, Culture, Media & Sport, DCMS）主責電信政策、資料保護、網路安全、數位能力、媒體與創意產業等政策之發展。然 2023 年初為使英國處於全球科技發展及經濟創新成長之領先地位，英國將前 DCMS 與數位相關之業務與商業、能源及「產業策略部」(Department for Business, Energy and Industrial Strategy, BEIS）整合改組為「科技創新部」(Department for Science, Innovation & Technology, DSIT）[205]，負責推動競爭與促進創新之關鍵立法與監理改革，及虛實基礎設施（如高速寬頻網路）之監理，並加強國際間之科技合作，以支持英國經濟、公共服務、國家安全和政府優先事項。

而英國通訊傳播主管機關則為英國通訊管理局（Office of Communications, Ofcom），其係依《2002 年英國通訊管理局法》(Office of Communications Act 2002）所設立，並依照《2003 年通訊法》（Communications Act 2003）所賦予之權能，職掌範疇囊括電信、傳播及郵政等業務，機關屬性為具有公權力的法人，依法賦予其在法定職責範圍內獨立自主判斷決定之權能，且僅對國會負責，進而不受其他政府部門與產業之影響。

前 DCMS[206]與 Ofcom 間之關係則為，DCMS 部長對 Ofcom 依法具有在規範內之政策指示權，於此規範內 Ofcom 應按照該政策指示而執行法定職權；至於針對其它法定之核心職責，Ofcom 則享有獨立自主之判斷權限。現因組織改造，由 DSIT 接手《數據保護和數位資訊法》(The Data Protection and Digital Information Bill）、《數位市場、

[205] GOV.UK, *Department for Science, Innovation & Technology*, About US, https://www.gov.uk/government/organisations/department-for-science-innovation-and-technology/about (last visited June 21, 2023).

[206] 由於將數位相關業務移轉至 DIST，改組後之 DCMS 更名為「文化、媒體暨運動部」，參 GOV.UK, *Department for Culture, Media and Sport*, About US, https://www.gov.uk/government/organisations/department-for-culture-media-and-sport/about (last visited June 21, 2023).

競爭暨消費者法》（Digital Markets, Competition and Consumer Bill）草案及人工智慧監管等法制政策推動，甚至是《線上安全法》（Online Safety Bill）草案最後之立法階段，而 Ofcom 亦與 DSIT 有效合作[207]，共同保障英國人民，特別是兒童之線上安全。

不實訊息在英國並非一個新的現象，早在 1688 年英國樞密院（Privy Council of the United Kingdom）即曾發布過禁止散播不實訊息的公告。隨著現代技術的發展，傳統的訊息渠道被數位和社群媒體平臺取代，不實訊息傳播的問題與 1688 年相比變得更加嚴重。前 DCMS 於 2018 年即將不實訊息定義為「故意創建和散布虛假或操縱的訊息，旨在欺騙或誤導觀眾，以造成傷害或謀求政治，個人或經濟利益」[208]。同時期前 DCMS 亦公布《數位權利書》（Digital Charter）政策強化對於線上有害內容之防範、對不實內容的因應、網路安全之強化、促進資料經濟以活絡數位市場運作、發展人工智慧與數據的創新與倫理、規範線上平臺的法律責任，推動數位經濟發展[209]。

然而，在英國脫歐前，並未針對通訊傳播不實訊息及假新聞設立專法處置，亦未設置專責主管機關來監管線上平臺和內容，歷來皆由 Ofcom 處理相關事務，作為立場超越自律之專責機構。對於數位中介服務提供者之主要規範依據，則係歐盟《電子商務指令》（Directive on electronic commerce, 2000/31/EC, ECD）[210]，及轉換為其內國法之《2002 年電子商務管制法》（The Electronic Commerce (EC Directive)

---

[207] GOV.UK, *Making Government Deliver for the British People*, Policy Paper (2023/02/07), https://www.gov.uk/government/publications/making-government-deliver-for-the-british-people/making-government-deliver-for-the-british-people-html?_cldee=M5321QKQK01ii5V_yXGdskZuH-AI-o0Hve6nzTGsfFFdNoa1pwkfbNki7vN4OcaK&recipientid=contact-eda20ad0fe864d5bab07e9ad0e7c4bd3-a8333ba040ff4aed9683cb549d81dae6&esid=bdd69c2a-28a9-ed11-aad1-000d3adea432 (last visited June 21, 2023).

[208] House of Commons, Digital, Culture, Media & Sport Committee, *Disinformation and 'fake news': Interim Report: Government Response to the Committee's Fifth Report of Session 2017–19* (Oct. 17, 2018), available at https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1630/1630.pdf.

[209] GOV.UK, *Digital Charter*, Policy Paper (Updated 2019/04/08), https://www.gov.uk/government/publications/digital-charter/digital-charter (last visited June 21, 2023). 須注意的是，因組織改造，此等數位事項劃歸為 DIST 業務範圍。

[210] European Commission, Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

Regulations 2002, ECR）[211]，後者之規範對象基本上仍循歐盟之架構，將作為資訊服務媒介的網際網路服務提供者（Internet Service Provider, ISP）區分為三種型態，包括連線服務提供者（Mere conduit）[212]、快速存取服務提供者（Caching）[213]、資訊儲存服務提供者（Hosting），[214]分別課予相應之義務，並設置安全港免責規範[215]。具體而言，服務態樣涵蓋電商平臺、通訊服務、網路搜尋引擎、視聽服務串流等。

此處安全港之發動要件，在於服務提供者得知存在違法之活動或資訊時，應立即採取有效手段阻斷接取。然而，由於並未定義何謂「得知」，亦未定義何為「違法活動或資訊」[216]，使得安全港與通知取下義務等制度之實施帶來一定程度之不確定性，亦難以回應數位時代下，大量違法或不利使用者身心健康之有害內容透過社群媒體、搜尋引擎等線上服務快速傳播下，對社會大眾所引發之種種負面影響。

縱使數位平臺修訂服務條款、增加審核團隊之人員配置，甚至創建獨立之監督委員會，當社會大眾仍認為有所不及，部分使用者濫用服務而導致越來越多民眾對數位平臺之商業營運模式產生質疑，像是利用 Facebook 及 WhatsApp 的社團（groups）功能煽動對緬甸洛興亞人（Rohingya）之種族清洗（ethnic cleansing）[217]，引發民眾不滿 Facebook 透過演算法推波助瀾仇恨性言論，亦未能妥善刪除煽動暴力貼文[218]；甚至因 14 歲的英國少女 Molly Russell 不當仿效經由 Instagram 及 Pinterest 演算法所推薦之自戕圖片而導致自殺身亡事件，英國政府更是斷定社群媒體平臺為致死之主因。

---

[211] The Electronic Commerce (EC Directive) Regulations 2002. [hereinafter ECR]
[212] ECR, Reg. 17.
[213] ECR, Reg. 18.
[214] ECR, Reg. 19.
[215] ECR, Reg. 20.
[216] Id.
[217] Ross Anderson & Sam Gilbert (with a preface from Diane Coyle), The Online Safety Bill: Policy Brief, University of Cambridge & Bennett Institute for Public Policy Cambridge, p.1 (2022).
[218] Dan Milmo, Rohingya sue Facebook for £150bn over Myanmar genocide, The Guardian (2021/12/06), https://www.theguardian.com/technology/2021/dec/06/rohingya-sue-facebook-myanmar-genocide-us-uk-legal-action-social-media-violence (last visited June 21, 2023); AFP in Yangon, Myanmar's genocide against Rohingya not over, says rights group, The Guardian (2020/11/23), https://www.theguardian.com/world/2020/nov/23/myanmar-is-still-committing-genocide-against-rohingya-says-rights-group (last visited June 21, 2023).

因此，前 DCMS 除與內政部（Home Office）於 2019 年 4 月提出「線上危害白皮書」（Online Harms White Paper）[219]，提出針對數位時代之網路治理與未來之立法目標政策建議，並希望能建立保護線上安全之專責機關，故於 2020 年 2 月正式指定由 Ofcom 擔任網路內容之獨立監管機關，透過數位中介服務平臺之外部監督機制，以積極處理涉及恐怖主義、兒童性剝削與虐待（child sexual exploitation and abuse, CSEA）等線上違法或有害之內容[220]。

而在英國政府積極籌備前述工作後，各界均在觀望其將如何解決過往對網路中介服務提供者欠缺問責之缺陷。是以，DCMS 為昭示網路世界並非法外之地，且期使英國擁有全世界最安全之線上環境，於 2021 年 5 月 12 日提出指標性之作為，即起草《線上安全法》（Draft Online Safety Bill）草案，以展現雄心壯志，訂立較為早期與最為全面的立法[221]，期以對抗在數位環境下所普遍擔憂之錯誤訊息（misinformation）、極化（polarisation）、對青少年有害、資助恐怖主義（terrorist finance）、監視（surveillance）及其他危及線上安全情境，與監管困境等問題[222]。而該法目前已完成，並定名為《線上安全法》（Online Safety Act）[223]，詳後述。

[219] GOV.UK, Online Harms White Paper, Consultation Outcome (2019/04/08), https://www.gov.uk/government/consultations/online-harms-white-paper (last visited June 21, 2023).
[220] Id. (last Updated 2020/12/15).
[221] GOV.UK, Draft Online Safety Bill, Regulation (2021/05/12), https://www.gov.uk/government/publications/draft-online-safety-bill (last visited June 21, 2023).
[222] Ross Anderson & Sam Gilbert, *supra* note 217, p.1.
[223] Online Safety Act (2023 CHAPTER 50). [hereinafter OSA]

二、政府機關法制政策作為

《線上安全法》嘗試刻劃透過課予網際網路服務（internet service）提供者處理網路危害內容之義務框架，授權 Ofcom 針對違法內容進行調查，且得對違法之業者最高可裁處 1,800 萬英鎊（約新台幣 6.6 億元），或 10%全球營業額之罰鍰，二者擇一高者罰之[224]；並得向法院聲請與核可後採取各種「營運阻斷措施」（business disruption measures）[225]之權限，促使受規管服務之提供者承擔責任，以營造安全、友善之網際網路使用環境[226]。

DCMS 將《線上安全法》草案提交版[227]送予下議院後，下議院已於 2023 年 1 月 17 日通過三讀[228]。緊接著，對本法磨拳擦掌已久的英國上議院（House of Lords of the United Kingdom），於翌日（即 2023 年 1 月 18 日）便火速通過一讀，且於同 9 月 6 日完成三讀[229]。

至此，本法之架構已大致底定，草案訂有 12 大編，共計 242 條條文，尚有 17 項附表[230]，以勾勒整全性之規範藍圖。目前已於 2023 年 10 月 26 日通過御准[231]，仍分作 12 大編，共計 241 條條文[232]，維

---

[224] OSA, Sec.143 & Schedule 13.

[225] OSA, Sec. 144-148.

[226] GOV.UK, A guide to the Online Safety Bill, Guidance (2022/12/16), https://www.gov.uk/guidance/a-guide-to-the-online-safety-bill (last visited June 21, 2023).

[227] Online Safety Bill (Bill 209) 2022.

[228] 下議院已於 2022 年 3 月 17 通過一讀，旋即於同年 4 月 19 日通過二讀。然因議會屆期不連續之故，下議院再次於同年 5 月 11 日通過一讀與二讀，且於 5 月 24 日起交由公共草案委員會（Public Bill Committee）進行審查，並經過 13 次之修訂，委員會已於 6 月 28 日提出《線上安全法》草案委員會調修版（Bill 121），並於 12 月 6 日提出報告階段（report stage）調修版（Bill 220）後，於 2023 年 1 月 17 日通過三讀。

[229] 上議院於 2023 年 2 月 1 日完成二讀，並於 4 月 19 日完成委員會階段（committee stage），再於 7 月 6 日完成報告階段（report stage）。

[230] UK Parliament, Public Bill Committees, https://www.parliament.uk/mps-lords-and-offices/offices/commons/scrutinyunit/public-bill-committees/ (last visited Aug. 15, 2023).

[231] Tom Bristow, POLITICO Pro Morning Tech UK: Budget hopes - Ofcom's next move - DSIT portfolios, POLITICO (2023/03/15), https://www.politico.eu/newsletter/morning-tech-uk/politico-pro-morning-tech-uk-budget-hopes-ofcoms-next-move-dsit-portfolios/ (last visited June 21, 2023).

[232] 刪除原 OSB (HL Bill 164) 第 64 條，該條責成主管大臣於本法通過之日起 6 個月內須審核與虐待動物有關內容之條文（如 2006 年《動物服務法》），以確定若在受管制之服務上傳散鼓勵或協助虐待動物行為、或分享與虐待動物有關之內容是否構成犯罪。如是，則主管大臣須在可行之情況下儘速將此等犯罪指定為附表 7 之犯罪行為。然而，倡議組職有鑑於 BBC 調查團隊追蹤並拍攝揭露全球虐猴影片產業鏈之紀錄片，指稱來自美國、英國及其他地區之民眾，訂閱頻道付費觀看由印尼之虐猴人以極其殘忍的手法將幼猴凌虐致死，甚至由 YouTube 遁入較為私密地 Telegram 群組之事件，作為支持立法強化動物保護及線上安全防護之論據。故此，御准版將此等泯滅人性之犯罪行為，劃歸與恐怖主義、復仇式色情等行為同一級別之「優先犯罪行為」。可

持 17 項附表。

（一）規範對象

為達成使英國成為世界上最安全之線上場域的策略目標，考量使用者上傳與分享內容之線上平臺，諸如等社群媒體（如 Facebook）或視訊分享平臺（如 YouTube），以及搜尋引擎服務（如 Google、Bing 等）[233]類型之影響力日益增加，故基於不同之服務型態、使用者數量與功能，以及傳播影響力與風險之差異，課予服務提供者寬嚴不同之法定義務。並令 Ofcom 應針對相關規範制訂指南及實踐準則，以協助服務提供者完備相關法令遵循工作。

進一步而言，本法欲納管之線上服務，主要分為兩大態樣：「使用者對使用者服務」（user-to-user service）、「搜尋服務」（search service），且該服務須於英國境內擁有龐大之使用者數量；或以英國為該服務的重點市場或唯一之市場。

1. 使用者對使用者服務

有關使用者對使用者服務之定義，係指於該服務上直接生成（user generated content, UGC）、上傳或分享[234]之內容，可被該服務之其他使用者觸及（包括閱讀、觀看、收聽或其他體驗內容之方式）之網際網路服務[235]。

除此之外，「使用者對使用者服務」又會再依使用者數量規模及內容傳播風險，區分為管制密度較高的「第 1 類服務」（Category 1 services）[236]與管制密度較低的「第 2B 類服務」（Category 2B services）

參陳曉慈，虐待幼猴、錄製影片、下游分銷 BBC 揭全球虐猴影片產業鏈，世界新聞網（2023/06/20），https://www.worldjournal.com/wj/story/121488/7248694（最後瀏覽日：2024 年 1 月 11 日）；Lex Talamo, Victory! UK Online Safety Bill Becomes Law, Will Help Stop Animal Torture Videos, Lady Freethinker (2023/10/31), https://ladyfreethinker.org/victory-uk-online-safety-bill-becomes-law-will-help-stop-animal-torture-videos/ (last visited Jan. 11, 2024)。

[233] OSA, Sec. 3.

[234] 不問是否實際發布或與其他使用者共享，且也不問由使用者所生成之比例為何，縱使為透過人工智慧（AI）服務或工具所產生之內容，亦屬於使用者生成之內容。

[235] OSA, Sec. 3(1)-(3), (7).

[236] 所謂第 1 類服務（Category 1 services）指依第 95 條第 2 項第 a 款登記在冊的受規管之使用者對使用者服務，見 OSA, Sec. 95(10)(a)。

[237]，兩者除皆須負擔與「搜尋服務」相同的義務外，「第 1 類服務」尚須額外負擔疊加及其他義務（如保護重要民主/新聞內容、用戶身分驗證等）[238]。

「第 1 類服務」與「第 2B 類服務」之具體門檻則於附表授權交由主管大臣綜合考量不同服務之使用者數量、服務功能、性質等因素後，訂定此一區別標準[239]。

此外，針對前述服務類型，本法於附表 1 訂有豁免條款，將特定服務型態排除於納管範圍之內。因此，簡訊、多媒體簡訊、一對一即時語音服務、企業內部服務、功能限定服務、公共服務等服務態樣不在本法監管範疇之下[240]。

2. 搜尋服務

有關搜尋服務之定義，搜尋服務係指本身即是或包含搜尋引擎（search engine）之網際網路服務[241]，須包括可供使用者搜尋複數或所有網站或資料庫之服務或功能；故若使用者僅能搜尋單一網站或資料庫，則不屬之[242]。此等服務如屬於符合一定門檻之服務，則進一步稱為「第 2A 類服務」（Category 2A services）[243]。

3. Ofcom 就規範對象之權責

（1）自我檢視簡易指南

隨著《線上安全法》通過御准且預計於 2024 年底前陸續生效，Ofcom 發布一項簡易指南，提供線上服務之服務提供者自我檢視是否處於法律之適用射程範圍之內。其透過「是否與英國建立連結？」、

[237] 所謂第 2B 類服務（Category 2B services）指依第 95 條第 2 項第 c 款登記在冊的受規管之使用者對使用者服務，見 OSA, Sec. 95(10)(c)。

[238] 如 OSA, Sec. 10(9)之綜整服務中最新違法內容風險評估結果義務、Sec. 12(13)之綜整服務中最新有兒童風險評估結果義務等。

[239] OSA, Schedule 11.

[240] OSA, Schedule 1.

[241] OSA, Sec. 3 (4)-(6).

[242] OSA, Sec. 239.

[243] 所謂第 2A 類服務（Category 2A services）指依第 95 條第 2 項第 b 款登記在冊的受規管之使用者對使用者服務，見 OSA, Sec. 95(10)(b)。

「是否提供相關服務？」及「是否具有豁免事由？」等三大面向加以判斷，若前兩者均為肯定且亦無豁免事由，則可能屬於受規管之服務提供者，應負擔本法所課予之義務[244]。

其一，線上服務提供者應考量其所提供之服務「是否與英國建立連結？」，亦即若符合以下兩項要件，則為肯定：

- 英國使用者[245]為服務之目標市場；或
- 服務擁有大量的英國使用者。

其二，線上服務提供者所提供之服務若屬於「使用者對使用者服務」、「搜尋服務」或「發布或展示色情內容服務」等情形，惟應注意的是，法規僅適用其中「相關」部分之服務[246]，進一步例示如下：

- **「使用者對使用者服務」**：諸如社群媒體網站或應用程式 APP、照片或視訊分享服務、聊天或即時通訊軟體服務（如約會應用程式）、線上遊戲或手機遊戲服務等。
- **「搜尋服務」**：包含著重於特定主題或內容之「垂直式」搜尋引擎（如僅針對某些網站或資料庫中之學術文章予以索引之態樣）；提供蒐羅來自許多不同網站或資料庫結果之比較網；或生成式人工智慧（Generative artificial intelligence, GenAI）模式亦可構成搜尋服務，即使用外掛程式（plug-ins）允許接取原始訓練資料集（Training Dataset）外之外部或合作夥伴的數據資料以加強 GenAI 模式之功能者，亦屬之，惟須注意的是，若所嵌入之外掛程式係由第三方所控制之搜尋引擎，則係由該第三方遵守本法之規範。

---

[244] Ofcom, Check if the Online Safety Act applies to you, Online safety (2023/11/09), https://www.ofcom.org.uk/online-safety/information-for-industry/guide-for-services/check#links (last visited Dec. 20, 2023).

[245] *Id.* 英國使用者係指服務之造訪者或互動者為任何位於英國之民眾，身分別就屬顧客（customer）、客戶（client）、訂閱者、訪客或其他名稱，則非所問。再者，使用者可以是自然人或實體（如組織），且是否有註冊（即建立帳戶），均在所不問。

[246] *Id.* 例如線上服務題中者為經營零售網站，使用者可透過網站購買商品，因使用者間無法進行互動，故係屬「不相關」的服務，惟若同一零售網站中設有聊天室/討論區，則又因允許使用者間互動而屬於「相關」的服務，因此在考量是否適用本法時，僅關注於該聊天室/討論區即可。

- **發布或展示色情內容：**服務之特色為在自己的服務上提供色情內容者。而其製作視訊、音訊或圖像形式之色情內容，原則上僅僅是以引起性欲（sexual arousal）為目的，排除簡訊或書面文字形式之內容。包含透過軟體、自動化工具或演算法等方式於其服務上發布或展示，甚至於第三方資訊儲存之伺服器上添加視訊或圖像之縮圖（thumbnail）。應注意的是，此種服務與「使用者生成之內容」有別，亦構成豁免之例外的情形[247]。

其三，線上服務提供者所提供之服務，若符合「豁免」[248]之情事，如有使用者透過線上服務之進行交流受到限制、或使用者可透過線上服務生成或分享之內容類型受到限制等情形，則不在本法之打擊範圍[249]。具體而言又可分從兩個面向，一為根據內容類型之豁免態樣：

- 若使用者透過服務進行交流的唯一方式是透過電子郵件、簡訊、多媒體訊息、和/或一對一即時語音通訊（包含 VoIP）之服務[250]；
- 若使用者僅得與服務提供者所發布之內容進行互動，互動模式包括評論、按讚、評分或回饋（含表情貼或星等評分）[251]；

二為根據服務類型之豁免態樣：

- 使用者對使用者服務係屬事業內部業務之服務（包括事業內部網路、生產力與協作工具、內容管理系統或客戶關係管理系統等）[252]；
- 使用者對使用者服務或搜尋服務係由公部門（如議會、英國公共機構或外國政府）提供之服務[253]；

[247] OSA, Part 1 of Schedule 1, Sec. 6.
[248] OSA, Schedule 1.
[249] Ofcom, *supra* note 244.
[250] OSA, Part 1 of Schedule 1, Sec. 1-3.
[251] OSA, Part 1 of Schedule 1, Sec. 4.
[252] OSA, Part 1 of Schedule 1, Sec. 8.
[253] OSA, Part 1 of Schedule 1, Sec. 9.

- 使用者對使用者服務或搜尋服務係由英國教育或兒童照護機構提供[254]。

（1）登記制度

根據本法規定，Ofcom 應針對受本法監管之服務建置登記制度，服務提供者於登記時，須載明服務名稱，並說明所提供服務之商業型態與營運模式等內容，且須維護登記冊，檢視相關服務是否符合受監管之門檻條件而滾動式調整之[255]。

而 Ofcom 為制訂相關指南及實踐準則，故於 2023 年 7 月 11 日至 9 月 12 日期間進行公眾諮詢，向各界蒐集相關資訊，如針對服務之使用者數量與功能[256]，以及該服務可能造成之風險進行通盤研究，以利後續針對「第 1 類服務」、「第 2A 類服務」、「第 2B 類服務」之納管標準分別提出次級立法之政策建議[257]，以供進一步作為主管大臣訂定適宜之規管門檻標準之參考依據。然而，本次尚未公告公眾諮詢結果，Ofcom 表示預期將再開公眾諮詢，就此仍應持續關注。

總而言之，未來受本法所監管之服務提供者均應向 Ofcom 辦理登記，而若服務提供者對於其被納入本法之監理範疇，或對於 Ofcom 認定應持續納管之行政決定不服，可依法向高等法院（Upper Tribunal）提起救濟[258]。

（2）風險評估

Ofcom 依職責須就受管制服務之提供者進行風險評估，並依據不同服務類型之使用者數量、商業模式、風險等級等要素，分別訂定相關規範與實踐指引，以充分瞭解受管制服務所提供之內容對個人所帶來之風險，並應確保相關風險評估持續進行更新，以有效掌握市場動

---

[254] OSA, Part 1 of Schedule 1, Sec. 10.

[255] OSA, Secs. 94-97.

[256] 更細緻的區分門檻設定基準，對「第 1 類服務」及「第 2B 類服務」將依據使用者數量和功能加以評估，而「第 2A 類服務」則是以使用者數量為基準。

[257] Ofcom, Call for evidence: categorisation - research and advice, Consultations (2023/07/11), https://www.ofcom.org.uk/consultations-and-statements/category-1/call-for-evidence-categorisation-research-and-advice (last visited Jan. 11, 2023).

[258] OSA, Secs. 167-168.

態，並落實科學化管理[259]。

（一）義務規範框架：共通義務

《線上安全法》課予受管制之「使用者對使用者服務」及受管制之「搜尋服務」注意義務，其核心在於要求服務提供者負擔針對線上有害或違法內容進行充份的評估違法內容造成傷害之風險、評估有害內容對兒少造成傷害之風險，並採取有效措施以降低造成傷害之風險及於服務條款中明確說明相關保障措施且設置受理使用者通知有害或違法內容與申訴機制，於此同時，也要承擔保障服務使用者之言論自由及隱私，並保存相關紀錄以供查閱之義務[260]。

1. 線上有害或違法內容之定義

（1）違法內容

有關違法內容之定義，係指由受監管服務所提供之特定文字、影像與音訊內容，已涉及犯罪、犯罪相關行為，或散播內容之行為已構成相關犯罪[261]。而此處之犯罪，蓋指涉及恐怖主義者、涉及兒少性剝削與暴力者，以及「優先違法內容」（priority illegal content）等犯罪內容[262]。

所謂「優先違法內容」，係指恐怖主義內容[263]、CSEA 內容[264]，及附表 7 所公告之內容[265]，即其他經主管內閣首長依法評估特定違法內

---

[259] OSA, Secs. 98-99.

[260] Ofcom, New rules for online services: what you need to know, Online Safety (2023/12/05), https://www.ofcom.org.uk/online-safety/information-for-industry/guide-for-services (last visited Dec. 20, 2023).

[261] OSA, Secs. 59(2)-(5).

另依據該條第 4 項，相關犯罪行為係指優先犯罪或符合第 5 項之犯罪。而第 5 項則訂定若干條件，若該當本項所定要件者即為相關犯罪行為：犯罪行為非屬優先犯罪，且受害者或預期之受害者為單一或複數之個人。

[262] OSA, Sec. 59(7).

[263] OSA, Schedule 5.

[264] OSA, Schedule 6.

[265] 諸如：加工自殺（Assisting suicide），恐嚇殺人（Threats to kill），公共秩序犯罪、騷擾、跟追與暴力之挑唆或使人畏懼（Public order offences, harassment, stalking and fear or provocation of violence），毒品或精神成癮物（Drugs and psychoactive substances）、槍枝或其他武器（Firearms and other weapons），幫助非法移民（Assisting illegal immigration）、性剝削（Sexual exploitation）、性影像（Sexual images）、贓物（Proceeds of crime）、詐欺（Fraud）、金融服務（Financial services）、外國干預（Foreign interference）、動物福利（Animal Walfare）等犯罪行

容之盛行率（prevalence）、造成個人或社會傷害之風險程度、傷害之嚴重程度等要件後，所指定者而言。且賦予主管大臣具有調修附表 7 之權限[266]。

然而，前述所指之相關犯罪行為，並未包含涉及侵害智慧財產權之犯罪、不安全與不合格之商品，以及由非適格之服務提供者所提供之服務，前述之犯罪行為將回歸各行為之作用法進行管理[267]。

（2）對兒少有害之內容

有關有害兒少身心健康、發展內容之定義，除須為本法納管服務所提供之內容外，並須為本法或相關法制所訂定之有害兒少內容[268]；除此之外，若服務提供者認為該內容之「本質」（nature）或「傳播方式」（dissemination）將為兒少族群之生理或心理帶來直接/間接之嚴重影響時，具體如導致身體層面的損傷、心理層面的焦慮、恐懼，或長期感到沮喪、壓力等症狀；或已構成針對特定使用者之霸凌、恐嚇行為時，均為本法所稱之有害內容。

本法更進一步詳列「對兒童之主要優先有害內容」[269]及「對兒童之優先有害內容」[270]。更責成 Ofcom 負有審查受監管服務中出現相關有害內容之發生機率，且需將審查結果做成報告並發布之，報告須包含針對兒童主要優先及優先有害內容之具體修改建議，並將報告副本送交主管大臣[271]。

應注意的是，本法起草時，原規定「第 1 類服務」之提供者須額外負擔為本法所規範之有害成人之內容的注意義務[272]，即應於其服務使用條款中載明，其如何處理其服務上優先呈現的成人有害內容，以及其他方經風險評估界定為有害成人之內容。然因立法過程期間，就是否應將保護與風險評估範圍擴及至有害「成人」之內容爭議過大，

為，以及本附表所列犯罪行為之未遂、教唆、幫助與共謀等初始罪犯（Inchoate offences）。

[266] OSA, Sec. 59(10).

[267] OSA, Sec. 59(6).

[268] OSA, Sec. 60.

[269] OSA, Sec. 61.

[270] OSA, Sec. 62.

[271] OSA, Sec. 63.

[272] OSB (Bill 121), Sec. 54(2)-(3); Draft OSB, Sec. 46.

故已於下議院委員會報告階段修訂版（bill 220）刪除此項注意義務。

2. 第 3 編服務之提供者的注意義務

（1）違法內容安全管理

根據本法之規劃，受管制之「使用者對使用者服務」與受管制之「搜尋服務」（合稱第 3 編服務[273]）均被課予處理違法內容之義務，第 3 編服務之提供者須將其服務上呈現優先排序之違法內容，進行最少化呈現（minimise the presence），以降低其呈現時間與傳播能力，減輕、有效管理相關內容對個人造成傷害之風險[274]。具體而言，服務提供者應使用適當之系統與流程而盡量減少任何違法內容持續在其服務上流通、或當任何人通知或以其他方式使服務提供者知悉存在任何違法內容時，應儘速刪除之。

此外，本法依據服務之類型，另課予不同之義務。「使用者對使用者服務」須於其服務移除已確認、將確認以及可能為違法之內容[275]；「搜尋服務」則須公開說明該服務為保護個人免受網路危害內容，所實施之政策、程序規範，並確保法規範與實務執行之一致性[276]。

（2）有害兒少內容安全管理

A. 兒少族群服務使用與接取評估

根據本法之規範，受本法所納管服務之服務提供者應進行評估，以釐清該服務或該服務之一部分是否可能由兒少族群所接觸、使用[277]；其次，若兒少族群得以使用該服務，則應進一步釐清是否有大量兒少使用者使用該服務，以及該服務是否可能吸引大量兒少使用者[278]，以作為落實本法有關有害兒少內容安全管理相關規範之依據。

[273] OSA, Sec. 4(3).
[274] OSA, Secs. 10 & 27.
[275] OSA, Sec. 10
[276] OSA, Sec. 27.
[277] OSA, Secs. 11 & 28.

此外，為協助納管服務之提供者執行評估工作，Ofcom 將發布相關指南，服務提供者除獲得例外許可，應於 3 個月內完成相關評估工作，以有效保障兒少族群之權益[279]。

B. 有害兒少內容安全管理

根據本法之規範，「使用者對使用者服務」之服務提供者須針對經風險評估認定之有害兒少內容，依據不同年齡層分別進行風險管理，避免使兒少族群易於接觸有關內容，以減輕危害內容對於不同年齡之兒少族群所帶來的負面影響[280]。

在「搜尋服務」的部分，服務提供者須採取相應之系統、措施，於所有年齡層之兒少族群於使用搜尋服務時，盡可能降低兒少族群因搜尋結果所帶來之風險，並應公開說明為處理有害兒少內容，該服務所採取之營運政策與措施，以有效降低、管理對兒少族群所帶來之負面影響、傷害之風險[281]。

（3）風險評估

根據本法之規範，納管之服務提供者負有針對違法內容，以及兒少可能接觸之服務內容進行風險評估之義務，並確保相關風險評估措施將持續更新，並應於服務之營運與設計將發生重大改變時，執行進一步違法內容風險評估[282]。

具體而言，風險評估應基於該服務所掌握之使用者數量、規模，以及服務所具備之功能，妥適考量其使用者接觸恐怖主義、兒少性剝削與暴力等內容之風險、有關內容快速、廣泛傳播的難易程度，以及該服務對於個人、兒少族群產生傷害之性質與嚴重程度，以釐清使用者可能接觸網路危害內容之風險等級。

[279] OSA, Secs. 13 & 30.
[280] OSA, Sec. 12 & 29.
[281] OSA, Sec. 29.
[282] OSA, Secs. 9 & 26.

（4）受理使用者通知暨處理機制

根據本法之規劃，使用者對使用者服務與搜尋服務之服務提供者，均應建置對應之申訴機制，以提供使用者、受影響之對象與利害相關人得以針對潛在之違法內容、有害兒少之內容等進行檢舉[283]。

而有關此一檢舉機制之設計，其設計應符合易於接觸、使用，並兼具透明性等原則，且須提供被檢舉人回應檢舉內容之機會[284]。

（二）義務規範框架：疊加與其他義務

除上開重要的注意義務之規範外，尚有課予各類受管制服務之提供者疊加之義務或其他非處理違法或有害內容之義務，其分述如下：

1. 疊加義務

（1）保護具民主重要性之內容

根據本法之規定，「第 1 類服務」之提供者應採相關措施，以落實民主政治體制運作下的言論自由保障。而所謂「民主重要性之內容」係指由新聞媒體於本法納管之服務所發布之內容，且內容發布之主要目的係為促進英國民主政治環境下的議題研討、辯論[285]。

因此，服務提供者應就相關內容是否下架、是否限制使用者接觸，以及是否針對使用者生產、上傳與分享等行為採取限制措施等環節訂定辦法，並採取相關措施，以確保政治言論之多元性，且相關措施之用語、設計須清晰易懂並具一致性。

[283] OSA, Secs. 21 & 32.
[284] OSA, Sec. 72(6).
[285] OSA, Sec. 17.

（2）保障新聞自由

為保障民主社會下的新聞自由[286]，避免新聞內容[287]無正當事由而遭到下架，或有限制媒體所生產、上傳與分享之內容之情事，而不利於民主政治之發展，故本法特訂定規範，課予「第 1 類服務」之提供者義務，業者應訂定相關措施，於決定是否將內容下架，或是否對使用者接取內容之權限做出限制時，充分考量有關措施是否有違言論自由保障[288]。

而言論自由保障之基礎，即在於有關內容之管理模式，故為協助服務提供者便利管理其服務上之新聞內容，本法之規範亦要求服務提供者應於其服務使用條款說明，該服務如何辨識、認定新聞內容，其進行內容下架、限制等決策時將如何顧及新聞自由之保障，以及該服務在處理新聞內容檢舉時所採取之政策與措施[289]。

最後，由於實務上仍有實施新聞內容下架、限制接取等措施之可能，為保障新聞自由，本法另課予服務提供者義務，應提供新聞、新聞內容創作者完善之申訴管道。而若有關檢舉、申訴成立時，應儘速於其服務上復原已下架之新聞內容，或撤銷原對使用者採取之限制[290]。

---

[286] 根據 OSA, Sec. 56(1)，所謂「受認證之新聞發布者」之定義如下：

A. 英國廣播公司（British Broadcasting Corporation, BBC）。

B. 威爾斯語公共電視台（Sianel Pedwar Cymru, S4C）。

C. 依據《1990 廣電法》（Broadcasting Act 1990）或《1996 年廣電法》（Broadcasting Act 1996）領有執照，並依該執照之授權發布新聞內容之業者。

D. 新聞發布者之營運措施需符合以下要件：(A) 所發布之新聞內容係由不同人所創作，且新聞發布者對內容負有編輯、控制之權限。(B) 不論是否基於營利目的，其營運係以發布相關新聞內容為主。(C) 其營運受標準作業手冊所拘束。(D) 為處理使用者檢舉，設置有對應之政策與措施。(E) 在英國境內有經註冊之辦公室或其他聯絡地址。(F) 服務提供者對於其所發布之內容負有法定責任。(G) 服務提供者需公告其營運相關資訊，包含服務名稱、聯絡方式與註冊編號等。

[287] 有關新聞內容之定義，依據 OSA 第 55 條第 8 項至第 10 項之規範，係指由新聞媒體所直接生產，並於本法規範之服務平臺進行上傳、分享，且須符合以下 3 個要件：A. 該內容為複製原始新聞媒體業者所發布之全文，且非該文章或該文章之部分螢幕截圖或照片；B. 該內容為新聞媒體所發布；C. 為特定文章、由新聞媒體所撰寫、發布之原生內容的網頁鏈結，或由新聞媒體播送之特定內容。

[288] OSA, Secs. 17-18.

[289] OSA, Secs. 17(3)-(5) & 18(10)-(13).

[290] OSA, Secs. 17(7).

（3）用戶身分驗證

依本法之規定，「第 1 類服務」之提供者必須向該服務之所有成人用戶提供驗證其身分之選項，包含本法課予之義務開始前之所有使用該服務之成年用戶。而驗證機制之型態並無限制，惟須於服務條款中以清晰易懂之方式，說明該驗證工具之運作原理[291]。

本法亦有規範 Ofcom 必須諮詢技術人員，以妥適之制訂相關指南，以協助服務提供者遵守此項規範[292]。

（4）處理廣告詐騙

處理線上廣告詐騙為下議院審查階段所新增之義務，加強對網路使用者之保護，免於受到不實廣告之潛在性傷害，包括不法人士竊取個資、詐取財物等情事。而所謂付費廣告（paid-for ad）指服務提供者為該廣告直接自廣告主或間接自他人收取金錢或非金錢之對價；以及廣告之投放由該廣告之契約各方皆同意的系統或處理流程決定。而本法授權主管大臣得以命令調整詐欺違法行為之範圍[293]。

本法分別針對「第 1 類服務」之使用者對使用者服務[294]與「第 2A 類服務」之搜尋服務[295]訂有最小化詐騙廣告留存（加速處理）、知悉即移除（加速移除），以及避免在服務中顯示以防止使用者觸及之義務規範。

（5）處理色情內容

處理線上某些色情內容（certain pornographic content）為下議院審查階段所新增之義務，旨在防止兒少觸及線上色情內容。不但希望屬於儲存用戶生成之內容服務或提供用戶互動服務（包含視訊、圖片共享、評論與直播等）之線上平臺，也希望將本身即提供色情內容之平臺納入捍衛行列，一同承擔注意義務，並應採取有效之措施（例如年齡驗證或相同級別之保護機制），以達到防免兒少觀看色情內容之

[291] OSA, Sec. 64.
[292] OSA, Sec. 65.
[293] OSA, Sec. 40.
[294] OSA, Sec. 38.
[295] OSA, Sec. 39.

目的[296]。

2. 全體受規管服務之提供者的其他義務

（1）繳交涉及 CSEA 內容予 NCA

根據本法規定，受管制服務之提供者必須盡可能將在確保服務安全的過程中（僅適用於本法生效日或之後）檢測所得之涉及「CSEA 內容」，依循主管大臣所規範格式及時間內，提交報告予被喻為美國聯邦調查局（Federal Bureau of Investigation, FBA）之「國家打擊犯罪調查局」（National Crime Agency, NCA）。而若報告中之重要內容有虛偽之資訊，則可能為刑事有期徒刑或罰金所相繩[297]。

（2）繳交透明度報告

根據本法規定，受管制之服務提供者，負有每年提交、公布透明度報告之義務，服務提供者並應於指定期限內進行繳交。此一義務之目的，旨在協助使用者瞭解服務提供者為提供安全網路環境所採取之措施，並提供 Ofocm 監理工作推動所需之資料，以建立企業、政府與公民社會間的監督、互信關係[298]。

此外，本法亦規定，Ofcom 應就透明度報告撰寫發布相關指南，以協助業者撰寫透明度報告，完備相關法令遵循之工作[299]。

（3）繳交行政規費

在《2017 年數位經濟法》（Digital Economy Act 2017）之規範下，Ofcom 運作之財務資金來自於其所監管之單位，故下議院於調修時新增關於為填補 Ofcom 為準備行使線上安全職責所產生之成本，而向受管制服務之提供者收取規費的相關規定。

根據本法之規定，當服務提供者之全球營收，或已達指定標準時，

---

[296] OSA, Secs. 79-82.
[297] OSA, Secs. 66-70.
[298] OSA, Sec. 77.
[299] OSA, Sec. 78. Ofcom, *Looking ahead to online regulation: It's time to rethink transparency reporting*, News Centre (2023/01/31), https://www.ofcom.org.uk/news-centre/2023/looking-ahead-to-online-regulation-transparency-reporting (last visited June 21, 2023).

除應主動通知 Ofcom 外，並應繳交當年度之行政規費[300]。而有關前述全球營收標準門檻之訂定程序，主管大臣將提供 Ofcom 研提標準之指南，由 Ofcom 就有關資料進行研究、擬定後，經主管大臣核准後公布，並定期檢視相關標準之訂定是否合宜，以決定是否進行修正。

（三）Ofcom 之權責

1. 制定實踐準則之藍圖

有關線上有害或違法內容之處理機制上，本法除課予納管服務提供者就線上危害內容負擔注意義務外，並正式任命 Ofcom 為線上危害內容之主管機關，並要求其擔負對應之功能與角色，Ofcom 應確保受監管之服務提供者，於其系統或服務應提供適當之防護措施，以降低因線上危害內容擴散所衍生之風險。

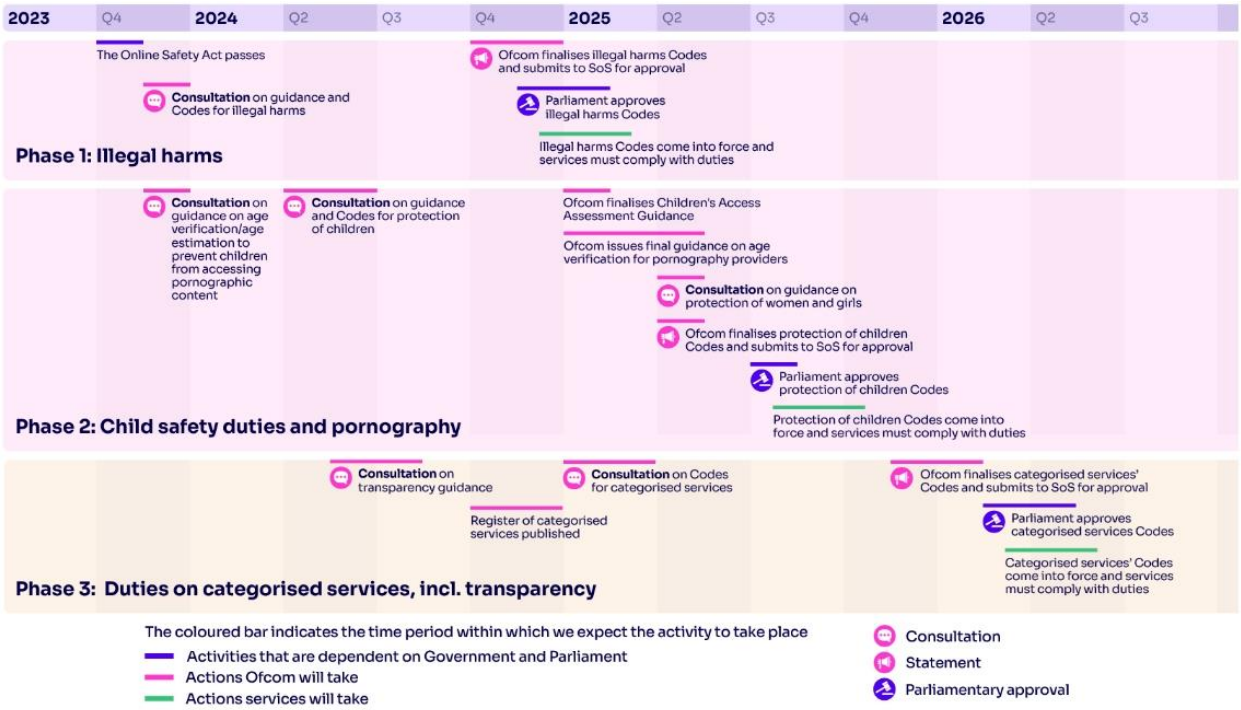


圖 1：Ofcom 執法與制定實踐準則之階段性規劃示意圖
資料來源：Ofcom[301]

[300] OSA, Secs. 83-90 & Schedule 10.
[301] Ofcom, *supra* note 260.

隨著《線上安全法》通過立法，Ofcom 分為三大階段就受管制之服務提供者法遵予以指導並制定相關實踐準則，其規劃分述如下：

（1）第一階段

此階段將針對有害或違法義務起草相關之實踐準則與指南，即於 2023 年 11 月起開始著手分析線上有害或違法內容之原因與影響，以利服務提供者進行風險評估，並起草風險評估之流程之建議指南，亦起草受管制之服務提供者可得採取因應違法或有害內容之有效措施的實踐準則，以及 Ofcom 執法方法的指南。

而陸續就公告的實踐準則與指南草案進行公開諮詢，並規劃於 2024 年秋季發布最終決定之聲明，接著再將實踐準則提交給 DCMS 大臣，經核准後，再送交議會[302]，並自議會頒布後 21 日開始施行[303]。

（2）第二階段

此階段規劃針對保護兒少相關之職責。首先因《線上安全法》第 5 編要求線上色情服務必須使用年齡認證（age assurance）機制防止兒少接觸色情內容，故預計將於 2024 年春季發布建議並供公眾諮詢，尤其是希冀線上色情服務之服務提供者及相關利害關係人得以就有關年齡認證指南之草案提供回饋[304]。接著再將實踐準則提交給 DCMS 大臣，經核准後，再送交議會，並自議會頒布後 21 日開始施行[305]。

再者，也將就分析線上對兒少造成傷害之原因與影響，並於 2025 年春季發布有害兒少內容之風險評估指南草案與保護婦女及女童之指南草案，且就相關草案進行公開諮詢，以利制訂行為準則供服務之提供者遵循[306]。

---

[302] Ofcom, *Ofcom's approach to implementing the Online Safety Act*, Online Safety (2023/10/26), https://www.ofcom.org.uk/online-safety/information-for-industry/roadmap-to-regulation (last visited Jan. 1, 2024).

[303] Ofcom, Ofcom's approach to implementing the Online Safety Act, p.12 (2023).

[304] *Id.*, p.13.

[305] Ofcom, *supra* note 302.

[306] *Id.*

（3）第三階段

此階段任務在著重於，若有受管制之服務提供者因符合次級立法（secondary legislation）所訂之門檻而被指定為「第 1 類服務」、「第 2A 類服務」及「第 2B 類服務」者，因要求其製作透明度報告、提供使用者賦權工具、依照服務條款營運、保護某類型之新聞內容及防止詐欺廣告等疊加義務。

因此，Ofcom 規劃於 2024 年初開始收集證據，首先就三類服務之門檻向主管大臣提供建議，以利在 2024 年夏季完成次級立法，從而得於 2024 年末公告三類服務並予以登記造冊；假設順利完成上開排程，接著，於 2024 年中先就《透明性指南》草案進行公開諮詢，復於 2025 年中公告《透明性指南》；最後則預期於 2025 年初發布對三類服務所課予疊加義務之建議草案[307]。

2. 處理有害或違法內容機制

基此，賦予 Ofcom 得針對特定內容於必要且適當時對服務提供者發出預警通知（warning notice）、暫時性通知（Provisional notices）與確認裁決（confirmation decisions）[308]，且當服務提供者仍未改善時處以罰鍰，並視情形施以各種「營運阻斷措施」，包含聲請（暫時）限制服務令或（暫時）限制接取令，尚有相關配套措施，以避免線上危害內容持續擴散。以下分別就前述機制予以說明：

（1）預警通知

按本法第 7 編第 5 章，若 Ofcom 基於必要且適當之合理事由，有關違法內容安全管理之規範，證明該服務確實涉及恐怖主義、兒少性剝削與暴力內容之傳播，且該內容持續存在於該服務之上時，可發布預警通知（warning notice），要求服務提供者進行改善[309]。

該通知之效力自送達日起，至多可延續 36 個月，而若服務提供者未能遵守前述通知所要求遵循之內容，Ofcom 將可要求業者進行限

[307] *Id*.
[308] OSA, Secs. 130-138.
[309] OSA, Secs. 121-123.

期改正，違者得連續進行處分並科以罰鍰。此一機制之設計係為確保納管業者遵守相關規範，惟若業者對相關處分之決定不服時，可向高等法院提起救濟[310]。

（2）限制服務令與暫時限制服務令

第 3 編服務之提供者，若未能遵守本法之規範與課予之義務，或未能遵守 Ofcom 所發布之預警通知，且該狀況為延續性時，Ofcom 可向法院申請限制服務令（service restriction order），其須指明應受命令之與第 3 編服務相關之輔助性服務（ancillary service）提供者（如提供資金轉移、廣告展示等功能之服務），及命令之要求內容，並提出相關證據；且於法院核發命令後應儘速通知主管大臣[311]。

法院將審酌相關事由，決定是否發出限制服務令，亦即，如認可防止英國境內個人免受傷害之風險，且命令與該風險具有適當性，則得核發服務限制令，要求提供輔助服務之提供者（如提供網路金流、廣告服務等業者），中斷提供予違法服務營運所需之服務，並應載明命令之期限[312]。

此外，若第 3 編服務之提供者若未能遵守本法之規範與預警通知之要求，以致於可能為英國民眾帶來立即性之重大風險，或依該傷害之性質與嚴重程度無法等到服務限制令核發時，Ofcom 可向法院申請暫時限制服務令（interim service restriction），以避免因未能及時申請限制服務令，以有效處理有關事件惡化所帶來之負面影響[313]。

法院於審查後，若認為符合聲請要件且初步證據顯示可成功聲請服務限制令時，則得核發暫時服務限制令。應注意的是，暫時服務限制令於已迄指定日期、或針對同一人所聲請之服務限制令核發或駁回時失效[314]。

---

310 OSA, Secs. 124-126.
311 OSA, Sec. 144.
312 *Id*.
313 OSA, Sec. 145.
314 *Id*.

（3）限制接取令與暫時限制接取令

當前述之限制服務令與暫時限制服務令均已失效，或未能有效防止對英國境內個人造成重大傷害時。Ofcom 得向法院申請限制接取令（access restriction orders），其須指明應受命令與受管制服務相關之接取設施（access facilities）之服務提供者，及命令之要求，並提出相關證據；且於命令核發後應儘速通知主管大臣[315]。

法院於審酌聲請事由後，如認可防止英國境內個人免受傷害之風險，且命令與該風險具有適當性，則得核發接取限制令，藉此命提供違法業者接取設施（access facility）服務之業者撤除、調整或操作以阻擋英國使用者接取受管制服務（或其部分服務），如停止提供受管制服務之網路接取服務，或 APP Store 停止開放下載或以其他方式存取 APP 等，以防止英國之使用者繼續利用該服務，並應載明命令之期限[316]。

此外，若受管制服務之提供者若未能遵守本法之規範，或依據本法所發布之限制服務令或暫時限制服務令，可能並不足以有效預防英國之使用者受到的立即性危害時，Ofcom 得向法院申請暫時限制接取令（Interim access restriction orders）[317]。

法院於審查後，若認為符合聲請要件且初步證據顯示可成功聲請接取限制令時，則得核發暫時接取限制令。應注意的是，暫時接取限制令於已迄指定日期、或針對同一人所聲請之接取限制令核發或駁回時失效[318]。

（4）資料調閱權

本法授權 Ofcom 可向受管制服務之提供者發布資料調閱通知（information notice），要求服務提供者提供相關資料。資料調閱之目的僅限於以下範疇[319]：

---

[315] OSA, Sec. 146.
[316] *Id*.
[317] OSA, Sec. 146.
[318] *Id*.
[319] OSA, Sec. 100.

- 為了訂定不同受管制服務之提供者之區別條件、標準所需之資料。
- 為評估受管制服務之提供者履行法定義務，遵守相關規範之情形。
- 為決定受管制服務之提供者應繳納行政規費之門檻，或評估受管制服務之提供者是否確實通知 Ofcom 其年度營收，並履行行政規費繳納之義務。
- 為瞭解受管制服務之提供者之全球營業額之概況，以作為罰鍰額度訂定之基礎。
- 為處理重大申訴所需之資料。
- 為籌備、訂定實踐準則或執行指南，以及進行有關網路安全事宜之研究、報告撰寫等所需之資料。
- 為確認受管制服務之提供者是否遵守、執行促進媒體素養義務之情形。

（5）調查及實地查核等權

而除了前述資料之調閱權限外，本法亦授權 Ofcom 為判定受管制服務之提供者是否有未遵守相關法令，得以另行啟動正式調查，以取得進一步之相關資訊[320]，包含得基於調查兒童死亡事件之情形，要求檢察官或法醫等相關人員提供有關之報告資料[321]。本法亦賦予 Ofcom 得於受監管之服務提供者未能遵守法規相關要求時，通知服務提供者之代表到指定地點晤談之權限[322]。

另外，Ofcom 可授權特定個人向法院申請令狀並進行實地檢查（inspection）。即當 Ofcom 合理懷疑受管制服務之提供者未能遵守或已違反本法預警通知與資料調閱通知之規範。或是合理懷疑該場所內有文件、紀錄、可用該場所之設備進行察看之內容或硬體設備與

[320] OSA, Sec. 105.
[321] OSA, Sec. 101.
[322] OSA, Sec. 106.

Ofcom 所進行之調查相關[323]。

就此，若 Ofcom 已於 7 天前通知該場所之使用人，將前往進行檢查，惟 Ofcom 要求於合理之時段前往該場所，並遭到以不合理之事由拒絕進入或雖 Ofcom 獲准進入該場所，但該場所之使用人於無合理事由之前提下，拒絕配合 Ofcom 派出之代表所提出之要求；或是 Ofcom 未能進入該場所；或是 Ofcom 有緊急進入該場所之需求等情，便可申請令狀為之。

此外，若 Ofcom 符合確信該場所係受監管之服務提供者提供服務之場所或 Ofcom 已於 7 天前通知該場所之使用人，將前往進行檢查符合之要件，亦擁有以無令狀形式進行實地檢查之權力，惟須於合理之時間行使之[324]。

（6）處理重大申訴

根據本法之規範，若使用者對於納管之服務有以下情形時，可依據本法之規定向 Ofcom 提起重大申訴（super-complaints），而具體之態樣，如為服務使用者、會員，或社會特定群體帶來嚴重危害；或嚴重影響使用者、會員，或特定社會群體之言論自由權利造成嚴重侵害、影響；或致使用者、會員，或特定社會群體之隱私受到侵害；或對於使用者、會員，或特定社會群體帶來嚴重不利之影響[325]。

而為有效處理相關申訴作業，以維護使用者與受影響者之權利，依據本法之規定，Ofcom 將針對重大申訴訂定相關之實務指南，以利相關程序之進行[326]。

[323] OSA, Secs. 107-108.
[324] OSA, Sec. 107.
[325] OSA, Secs. 169-170.
[326] OSA, Sec. 171.

（四）《線上安全法》與其他法規之整合

1. 調整 Ofcom 職權

因已指定 Ofcom 為線上危害內容之獨立監理機關，且本法中亦賦予 Ofcom 大量之權限與職責，故有必要配合其職權範圍、功能之擴張而修正《2003 年通訊法》（Communications Act 2003）第 3 條，於該條第 2 項新增第 g 款，作為執法之法源依據[327]。

此外，且基於此一職責之賦予，Ofcom 並負有執行影響評估工作之職責，故將同步修訂《2003 年通訊法》第 7 條，擴張其執行影響評估之範圍，並應依大幅擴張 Ofcom 制訂對應之實踐準則（code of practice）以說明適宜之執行方法，以及相關指南之權限。

2. 刪除《2003 年通訊法》相關章節

為配合歐盟 2018 年通過之《修正視聽媒體服務指令》，英國於 2020 年 9 月完成《2020 年視聽媒體服務管制法》（AVMSR），並於 2020 年 11 月正式生效。此次主要係擴大規管範疇，新增《2003 年通訊法》第 4B 章，將「視訊分享平臺服務」納入規範，同時拉齊線性與非線性服務對於有害內容之管制密度，並強化煽動暴力、仇恨，以及公開煽動恐怖主義罪刑之規範[328]。

本法定義之「視訊分享平臺服務」（video-sharing platform services, VSPs）係指以商業行為為基礎而透過電子通訊網路（ECN）向公眾提供無編輯責任，僅透過演算法等自動化工具決定節目之陳列、排序與標註之影音服務，且影音服務係屬該服務或該服務之可分離部分之主要目的，並已構成該服務之關鍵功能（essential functionality）。此外，服務提供者須位於英國政府的管轄範圍內[329]。

具體而言，《2020 年視聽媒體服務管制法》之修訂，並非對於內容進行直接性管制，而是課予視訊分享平臺業者相關義務，如透過設置特定服務之使用模式、條件、建立加註警語系統、年齡驗證機制、

[327] OSA, Sec. 91.
[328] OSA, Secs. 209-211.
[329] OSA, Schedule 17.

內容評分機制，以及家長控制系統等。具體而言，諸如保護未成年人免於遭受有害身心健康與道德發展之內容、廣告影響；保護大眾免於遭受煽動暴力、仇恨性之有害內容、廣告影響；或是保障大眾免於遭受涉及違反歐盟法律規範下之犯罪行為之內容與廣告影響等。

然而，因《線上安全法》已將視訊分享平臺納入規管對象，故配合刪除《2003 年通訊法》4B 專章有關視訊分享平臺之規範[330]。

3. 廢止《2017 年數位經濟法》相關章節

英國政府考量科技的轉變將改變經濟、社會與政府，故強化推動數位服務與基礎設施投資等，以擴大設施之近用、政府服務數位化並訂定相關保護孩童及消費者之規範，同時鞏固監理機關 Ofcom 之監理權限以完善監理機關之權力，特訂定《2017 年數位經濟法》(Digital Economy Act 2017)，就有關電子通信服務之關鍵議題，亦即數位經濟，訂定數項管制。

該法修訂涵蓋範圍涉及五項領域，包括近用數位服務、數位基礎設施、線上色情、智慧財產、與數位政府，其中有關數位中介服務之不法內容管制機制主要落在線上色情領域之限制與兒少保護面向。

《2017 年數位經濟法》規範線上色情網站年齡驗證機制，主要針對英國國內、外具色情內容之營利性網站進行管制，且營利性網站包含進入網站需付費與免費網站但需付費購買產品二種。管制架構引入傳統分級標準以作為色情網站內容分級依據，違反者將裁以民事責任為主。此管制要求網站應設有年齡驗證制度並與金流業者合作（如信用卡業者），以防免色情網站對兒童造成潛在的危害，主管機關並將依技術發展隨時調整管制涵蓋之範疇，以達完善維護兒童身心健康發展。

然而，由於《線上安全法》已針對違法內容與涉及兒少性剝削與暴力之線上危害內容訂定相關規範，故刪除《2017 年數位經濟法》

[330] OSA, Schedule 16.

（Digital Economy Act 2017）中有關網路色情之規範[331]。

三、第三方監督或產業自律機制

數位平臺可能是導致社會問題加劇的主因之一，是英國政府積極立法而促使數位平臺需要履行依法所課予之職責，然而單靠數位平臺無法解決某些根深蒂固的社會問題，因此線下合作或解決機制作為配套措施有其重要性，諸如解決虐待兒童或弱勢群體問題需要當地警察機關、社會福利機構及學校的參與，因此需要打造一個法律框架，彙集線上與線下之力[332]，共同守護線上使用環境之安全。

（一）第三方監督

於 2017 年《數位經濟法》修法前，英國監督線上違法網站之運作模式，原係由民間業者所成立之「網路觀察基金會」（Internet Watch Foundation, IWF）進行過濾，經由使用者或消費者回報後，再由網路服務提供者（internet service provider, ISP）封鎖，也即阻斷內容之接取，以降低網路上違法內容之影響效果，並特別著重於有害兒童心理健康之色情網站。

英國政府正式於 2018 年 2 月 21 日指定獨立的非營利組織「英國電影分級基金會」（British Board of Film Classification, BBFC）[333]，擔任線上色情年齡驗證之監理機構。年齡驗證監理機構將有權向 ISP 發出通知（notice）要求封鎖網站，亦處以 25 萬英鎊罰鍰。經由政府之介入，使年齡驗證監理機關能列出主要不合規範之網站與應用程式（APP），並通過符合標準之色情網站業者、付費服務業者、及輔助服務業者間的合作，摧毀不合規範之色情網站業者的收入來源，並導正其成為符合標準之業者。

英國政府的網路治理與第三方機構的緊密共管機制，建立在既有的法規架構與不斷因應數位環境轉變之體制背景，從 2017 年《數位

[331] OSA, Sec. 212.
[332] Ross Anderson & Sam Gilbert, *supra* note 217, p.1.
[333] BBFC, https://www.bbfc.co.uk/ (last visited July 24, 2023).

經濟法》立法指定非營利組織 BBFC 作為法定監理機構，再到《線上安全法》擴充 Ofcom 於線上危害內容監理之職權，英國的網路監理機制逐步從自律與他律結合的共管走向，賦予相關網路非營利組織之監管權力，以強化網路執行的效力與專業度，提升網路治理之公正且獨立的處理途徑。

此外，為對抗線上違法或有害內容對網路生態日益嚴重地侵害，亦透過媒體素養之培育而提升民眾之媒體素養，就此英國政府履行「線上危害白皮書」之承諾，由 DCMS 先於 2021 年 7 月公布第一年「線上媒體素養戰略」（Online Media Literacy Strategy）作為政策推行之指南，並於次年 4 月更新第二年之行動計畫[334]。並將其納入目前最新版本之《線上安全法》當中，除調修《通訊傳播法》第 11 條之規範以促進媒體素養[335]外，並要求 Ofcom 監督媒體素養與出具相關報告[336]，預期透過雙管齊下，以達加倍防護之效能[337]。

（二）產業自律機制

英國有關線上安全自律之第三方機構，與前開《線上安全法》所關心的線上議題大致相同，諸如兒少性虐待、網路暴露狂（cyberflashing）、不實訊息、賭博、網路霸凌、網路挑戰（Internet challenge）[338]。有鑑於此，英國網路安全中心（UK Safer Internet Centre,

---

[334] GOV.UK, *Year 2 Online Media Literacy Action Plan (2022/23)*, Policy Paper (2022/04/16), https://www.gov.uk/government/publications/year-2-online-media-literacy-action-plan-202223 (last visited July 24, 2023).

[335] OSA, Sec. 165.

[336] OSA, Sec. 166.

[337] 英國 DCMS 於 2019 年成立「對抗不實訊息部門」（Counter Disinformation Unit, CDU），藉由該部門與政府、民間第三方組織之通力合作，並配合《線上安全法》和「線上媒體素養戰略」共同抵禦錯誤訊息、不實訊息及惡意訊息。尤其是 Covid-19 大流行期間及烏克蘭戰爭事件影響，加劇不實訊息（如應燒毀 5G 電線杆以防止病毒傳播）之傳散，故透過此部門掌握不實資訊之內容和人為操縱訊息之意圖，以確保政府了解有害之錯誤訊息、不實訊息及惡意訊息之範圍，並得以對之採取適當的行動。而後 CDU 改名為「線上國安資訊小組」（National Security Online Information Team, NSOIT），專責關注線上社群平臺中涉及有害國家安全和公共安全風險之資訊，政府不會採取強制作為，而是通報各該平臺，讓平臺按其服務條款或社群守則決定處置之方式。See GOV.UK, Fact Sheet on the CDU and RRU, Government response (2023/06/09), https://www.gov.uk/government/news/fact-sheet-on-the-cdu-and-rru (last visited Jan. 15, 2024); John Whittingdale, Counter Disinformation Unit, TheyWorkForYou (2023/11/14), https://www.theyworkforyou.com/wrans/?id=2023-11-07.43.h (last visited Jan. 15, 2024).

[338] 網路挑戰係指經由社群媒體或其他線上平臺發起之線上挑戰，「挑戰」內容各異，但經常是會鼓勵挑戰者在現實世界中傷害自己、他人或毀損財產，通常也是為了引起恐慌而設計，且對

UK SIC）應運而生，其成立於 2011 年，係由網路觀察基金會（Internet Watch Foundation, IWF）、西南學習網（South West Grid for Learning,SWGfL）與兒童網（Childnet）[339]等三個公益組織所組成，旨在讓網路成為美好而安全之地，志在做為政府、執法單位、產業與社會間的橋梁，共同識別線上威脅與危害，制定與提供有關確保兒少及成人線上安全之重要建議、資源、教育與干預措施。此外，該組織亦是英國網路安全日（Safer Internet Day）之榮譽協調官（proud coordinator）[340]。

1. 網路觀察基金會

網路觀察基金會（IWF）為英國網際網路產業於 1996 年成立之網際網路自律協會。成立宗旨在於戮力降低網路有害內容，監督網路空間的不法與不道德行為，進而保護兒少身心[341]。

IWF 制定行為準則，詳細訂明其職責範圍與處理之潛在犯罪內容，並成為該等內容之「通知與刪除」機構，識別與刪除網路空間裡的性虐待之影像及圖片紀錄，阻止線上傳散違法或有害內容之行為持續存在。重要的是，ISP 一經通知，即有義務根據 ECR 快速刪除或阻斷該等犯罪內容之接取並透過刪除違法或有害內容與維護網路空間的良善環境，避免對受害者的二度傷害[342]。

整理網路觀察基金會相關作為如下：

（1）強化科技技術：網路觀察基金會透過先進技術運用，提升識別與刪除網路上之兒童性虐待影像與圖片。

於年輕世代而言，似乎極具有吸引力。*See* UK Safer Internet Centre, *Online Challenges: De-escalating and responding to harmful online challenges*, https://saferinternet.org.uk/online-issue/online-challenges (last visited Jan. 06, 2024).

[339] Childnet 與 3 歲至 18 歲之兒少族群及其家長或照護者、教師與專家合作，透過對話了解兒少在網路世界之經歷與體驗，用於制定相關法制政策，藉此為兒少打造美好兒安全之網路空間。*See* Childnet, What we do, https://www.childnet.com/what-we-do/ (last visited Jan. 11, 2023).

[340] *See* UK Safer Internet Centre, *Making the internet a great and safe place for everyone*, https://saferinternet.org.uk/about (last visited Jan. 06, 2024).

[341] Internet Watch Foundation, *Who we are*, https://www.iwf.org.uk/about-us/who-we-are/ (last visited July 24, 2023).

[342] Internet Watch Foundation, *Our history*, https://www.iwf.org.uk/about-us/why-we-exist/our-history/ (last visited July 24, 2023).

（2）**專業分析團隊**：網路觀察基金會的分析團隊之經驗、評估模式、相關知識獨步全球，目前基金會計有 70 多名不同領域之人員，包含分析師與圖像分類評估人員夜以繼日的觀測受性虐待兒童之影片與圖像。

（3）**多方協力合作**：舉凡政府、執法部門、舉報專線、慈善機構、科技界都是網路觀察基金會之重要合作夥伴，合作對象不僅限於英國境內，亦與世界各地相關機構、政府機關合作。

（4）**設置 IWF 專線**：網路觀察基金會提供民眾安全且匿名之專線，使其得以通報其職權範圍內之線上可疑之內容（含影像或圖片），基金會再據以通知 ISP 刪除該等違法或有害內容。

網路觀察基金會作為英國非營利組織，透過協助政府制定與線上危害相關法律規範，以回應科技帶來的快速變化。在 IWF 成立之初，全球大約有 18%之兒童性虐待圖像於英國線上流竄，透過多年努力，至今大幅降低到 1%以下，可見 IWF 消弭網路違法或有害之訊息對兒童與社會大眾之侵害有成，其將持續推廣執行經驗，力促全球友善之網路環境[343]。

2. 西南學習網

英國西南學習網（SWGfL）係非以營利為目的之公益組織，其組織內之專家數量，高達英國網路安全中心（UK SIC）的三分之一[344]。透過彙集教育與培訓之產品與服務資訊、活動辦理，特別是與教育機構合作，運用科技促進線上安全。

此外，相比網路觀察基金會特別著重線上兒童色情問題，SWGfL 則偏重線上成人安全保護，處理合法但有害之內容。其亦設置各式求助專線與通知機制，提供免費建議予受到網路傷害之受害者，相關簡介如下：

---

[343] Internet Watch Foundation, *supra* note 341.

[344] *See* SWGfL, About SWGfL, https://swgfl.org.uk/about/ (last visited Dec. 20, 2023).

（1）復仇式色情熱線

「復仇式色情熱線」(Revenge Porn Helpline,RPH)成立於 2015 年，由 SWGfL 所經營，是目前英國唯一提供成年人（18 歲以上）有關濫用親密影像[345]之服務。迄今已協助上千名深受非自願性私密影像(Nonconsensual Distribution of Intimate Images, NCII)散布的受害者，並成功從網路上，移除超過 20 萬張以上非自願性散布的私密影像，影像下架率高達 9 成以上[346]。

（2）「StopNCII.org」平臺

SWGfL 與復仇式色情熱線推出免費的「StopNCII.org」平臺，為 NCII 之受害者提供幫助[347]。

「StopNCII.org」平臺處理色情內容之流程為：基於個人隱私保護，從當事人之行動裝置中就挑選（即平臺並不會下載與儲存）之影像產生數位指紋（代碼）後建立案件，並在參與計畫之合作平臺上搜尋匹配之數位指紋內容，再依據該合作平臺之政策或服務條款採取相應措施，且可隨時查詢追蹤或撤銷案件[348]。

（3）有害內容通報熱線

有害內容泛指任何在網路上引起痛苦或傷害之內容，因此 SWGfL 透過有害內容通報熱線（report harmful content），導引使用者前往正確之通報機制，並督促平臺落實服務條款/社群守則[349]。

此外，SWGfL 也整理各大社群平臺常見違反服務條款/社群守則

---

[345] *See* SWGfL, Revenge Porn Helpline: The UK's only service dedicated to providing expert support for adult victims of intimate image abuse (last visited Jan. 11, 2024). 濫用親密影像亦稱為復仇式色情，指行為人未經同意，意圖以透過線上或線下分享或威脅分享受害當事人之親密圖像或視訊，造成當事人之痛苦的行為。

[346] 參見 StopNCII.org, 關於我們，https://stopncii.org/%E9%97%9C%E6%96%BC%E6%88%91%E5%80%91/ （最後瀏覽日：2024 年 1 月 11 日）。

[347] *See* SWGfL, *StopNCII - Preventing Intimate Image Abuse*, https://swgfl.org.uk/helplines/stopncii-org/ (last visited Dec. 20, 2023).

[348] *Id*.

[349] *See* SWGfL, *Report Harmful Content*, https://swgfl.org.uk/helplines/report-harmful-content/ (last visited Dec. 20, 2023).

之內容[350]，諸如恐嚇、冒名頂替（Impersonation）、霸凌或騷擾（Harassment）、自殘或自殺內容、網路濫用行為、暴力內容、非圖像的不受歡迎之性行為[351]及色情內容等有害內容。

（4）「Minerva」平臺

西南學習網初期以人工方式審查線上濫用行為，其後與英國 DCMS 合作開發「Minerva」平臺，藉由人工智慧技術與自動化刪除跨平臺之有害內容。並且作為線上受害者通知之中心樞紐，做成通報事件之相關報告，其中亦整合上開 StopNCII、復仇式色情熱線及有害內容通報網之資訊，一方面幫助受害者採取下一步行動，一方面也協助執法單位掌握相關事件之時序及與平臺互動之紀錄[352]。

四、小結

隨著數位平臺服務深入日常，英國之監理機關與公民社會也開始關注搜尋引擎及社群媒體等服務，並試圖課予相關服務提供者進一步的法定義務，以避免使用者受到線上危害內容之影響，並促使數位平臺服務可接受外部監督，以解決此類型服務過往欠缺民主課責性不足之缺陷。

根據「線上危害白皮書」之規劃，一方面希望建立遠超越自律之新的線上安全監理框架，使服務提供者為使用者之安全承擔更多之責任，並非僅是遵守所課予之最低義務規範要求，而是進一步鼓勵服務提供者開發與分享新的技術解決方案，以保護使用者（尤其是兒童）免受違法或有害內容攻擊之安全，及維護言論自由等權利。

基此，英國採取較高密度之管制模式，諸如預期透過《線上安全法》作為整合式之規範：一方面考量服務之型態、使用者數量與功能

---

[350] *See* Report Harmful Content, *Why these 8 harms?*, https://reportharmfulcontent.com/harms/ (last visited Dec. 20, 2023).

[351] *See* Report Harmful Content, *Unwanted Sexual Advances*, https://reportharmfulcontent.com/advice/unwanted-sexual-advances/ (last visited Dec. 20, 2023).

[352] SWGfL, Minerva - Record Online Abuse: A secure platform for recording and reporting online abuse, https://swgfl.org.uk/helplines/minerva/ (last visited Jan. 11, 2024).

等要素，將現代社會最具傳播影響力之「使用者對使用者服務」與「搜尋服務」兩類服務納入監理範疇，再依照不同內容類型所構成之風險及傳播能力與影響力，區分為第 1 類服務、第 2B 類服務及第 2A 類服務等三類登記造冊，並須課予其負擔寬嚴不等之法定義務；另一方面，藉由指定 Ofcom 對受管制服務之提供者進行監理，賦予相當程度之執法權限，並可針對違法業者裁處高額罰鍰，甚至可進一步採取限制服務令或限制接取令，以有效維繫安全之網路環境。

另外，就位於英國管轄境內之隨選節目服務（on-demand programme service, ODPS）亦於《2003 年通訊法》第 368 節 Part 4A（主要集中於第 368E 條至第 368I 條）設置有害內容、廣告、贊助與商品置入等規範，並由 Ofcom 發布《隨選節目服務提供者監理與非拘束性規範指南》（Rule and Guidance: Statutory Rules and Non-Binding Guidance for Providers of On-Demand Programme Services (ODPS)）[353]，進一步將法規明確化，其中就有害內容之具體規範，如不得提供涉及針對種族、性別、宗教與國籍等煽動仇恨之內容[354]；除配置有效之內容接取控制系統（Content Access Control System, CAC System）以進行年齡驗證外，不得提供不適宜兒少接取之特別限制內容[355]等。

整體而言，英國政府相當重視有害內容的管理，從管制脈絡來看，其並不信任數位平臺自律，故已從產業自律轉向立法他律，並賦予主管機關 Ofcom 監管權限，監督視訊平臺落實其管理責任，甚至認為《線上安全法》，亦可適用於元宇宙（Metaverse）[356]，而英國政府目前已於 2023 年秋季完成立法，至此，Ofcom 之階段性執法動態深值持續關注。

---

[353] Ofcom, *Rule and Guidance: Statutory Rules and Non-Binding Guidance for Providers of On-Demand Programme Services* (2021/12/10), *available at* https://www.ofcom.org.uk/__data/assets/pdf_file/0029/229358/ODPS-Rules-and-Guidance.pdf.

[354] ODPS, Rule 10.

[355] ODPS, Rule 11.

[356] Ryan Browne, *Meta and Microsoft can't self-regulate their metaverses, UK regulator warns*, CNBC (2022/10/26), https://www.cnbc.com/2022/10/26/meta-and-microsoft-cant-self-regulate-their-metaverses-ofcom-warns.html (last visited Aug. 15, 2023).

第五節　美國

一、監理脈絡

在當前的網際網路生態下，數位傳播平臺已是與民眾生活密不可分的存在，各種新興服務如虛擬貨幣、線上支付、社群媒體等，已改變當代民眾的日常生活型態。而隨著網路服務提供者如 Meta（Facebook / Instagram）、Twitter、Reddit 帶給使用者的功能從分享個人社交生活、交流意見轉變為帶動輿論及提供廣告投放之場域後，網路服務提供者是否應受到監管、又應如何監管的討論也開始成了各界關切的重點。

與世界其他主要國家相比，美國既作為催生 Google、Amazon、Meta、Apple 等科技巨頭之發源地，又具備向全球輸出政治、經濟、文化之長久優勢，其對於網路服務提供者監管所採取之態度自然也傾向寬鬆甚至消極。然而，自從 2016 年發生劍橋分析公司（Cambridge Analytica）經由 Facebook 取得使用者數據、繼而製作及投放政治廣告影響美國總統大選之事件後，社會上關於保護使用者數據之倡議、提醒社會大眾留意網路服務提供者是否濫用使用者個人資料之呼籲便相繼而起，亦有倡議團體及政治人物開始要求政府加強對此類科技巨頭之監管。

然而，政府對於網路服務提供者之監管，向來須考量言論自由、產業創新、公平競爭、著作權保護、使用者之隱私權保護等議題之均衡，其監管方式及監管力道往往會使政策制定者陷於左支右絀之處境。就此而言，美國的政策討論主要聚焦於網路服務提供者是否應在第三人利用其服務散布不法內容時負責之問題，並從「一般不法內容」及「侵害著作權之不法內容」兩個不同面向切入，分別以 1996 年制定之《通訊端正法》（Communications Decency Act of 1996，以下簡稱「CDA」）第 230 條，及 1998 年制定之《數位千禧年著作權法案》（Digital Millennium Copyright Act，以下簡稱「DMCA」）第 512 條為相應規範，以下將分別說明兩者之內容與發展。

二、政府機關法制政策作為

（一）CDA 第 230 條之爭議與修法動態

自 1990 年代網際網路服務萌芽之初，網路中介業者是否應就第三人侵權內容負法律責任的爭議便從未止息。1995 年，紐約州最高法院在 *Stratton Oakmont v. Prodigy Service* 一案中處理了電子佈告欄（Bulletin Board System, BBS）[357]的法律責任爭議。按法院在判決中之見解，當 BBS 經營者設有板主、過濾系統等措施，對於論壇上張貼之內容具有審查控制能力，卻未善盡其管理義務時，即應就使用者發表之誹謗言論負「出版人」責任。但該判決在實質上卻造成了網路平臺服務提供者進退維谷的困境——若積極管理平臺內容，恐將因構成出版人責任而須為第三方發表的言論負責；若完全放任平臺自行運作，則又可能導致用戶處於不當內容充斥的使用環境。

在前述判決的影響下，為了促進網際網路發展，1996 年通過的 CDA 第 230 條遂創設了「善良撒馬利亞人」（Good Samaritan）的免責規定：若平臺業者刪除特定內容或限制對特定內容之訪問，即可不必對第三人的侵權內容承擔民事責任。CDA 第 230 條透過此一「安全港」（Safe Harbor）條款鼓勵網路服務提供者主動就第三方侵權內容採取合理措施，進而為使用者清除違法內容，維護良好的網路空間。

CDA 第 230 條的規範內容概可分為以下兩部分討論：

1. 適用主體

按 CDA 第 230 條(c)(1)規定：「互動式電腦服務之提供者或使用者，就其他資訊內容提供者所提供之資訊，不應被視為出版人及發表人」[358]。

所謂「互動式電腦服務」（Interactive Computer Service），係指：「提供或讓多數使用者電腦得以連結至同一電腦伺服器之任何資訊服務、系統、或接取軟體，具體而言包括提供網際網路接取的系統或

[357] *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710 (N. Y. Sup. Ct. 1995).

[358] 47 U.S.C. § 230(c) (1). No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

服務，以及由圖書館或教育機構所經營的這類系統或提供的服務」[359]，故適用 CDA 第 230 條的典型網路中介者，包括社群平臺如 BBS 討論版、Facebook、Twitter 等，也包括資訊中介平臺（如租屋媒合網站）、電子商務平臺等。

2. 免責條件

根據 CDA 第 230 條(c)(2)規定：互動式電腦服務提供者或使用者，無須因下列原因負責。包括：針對服務提供者或使用者認為猥褻、邪惡、淫亂、過度暴力、騷擾性或其他令人不快之內容，無論該內容是否受到憲法保護，為了限制其接觸或取得而基於善意（good faith）、自願（voluntarily）採取之任何行為；或任何採取科技方法以限制接取上述內容之行為。

3. 排除適用

根據 CDA 第 230 條(e)所設立之排除規範：本法不妨礙聯邦層級之刑事法規範、著作權法規、州法、包括 1986 年《電子通訊隱私法》（Electronic Communications Privacy Act）在內之通訊隱私法規、以及以性剝削為目的之人口販運（sex trafficking）相關法規之適用。

4. 司法實務對於免責範圍之見解

自從 CDA 第 230 條在 1996 年立法通過後，網路中介者應適用的具體免責界線便屢屢受到廣泛的討論與挑戰。

舉例而言，在 1997 年的 *Zeran v. American Online* 一案中，初審法院便認定，CDA 第 230 條不只免除了網路平臺作為「出版人」之責任，同時免除其「散布者」之責[360]，聯邦第四巡迴上訴法院亦維持其判決[361]，使本案正式推翻先前 *Stratton Oakmont v. Prodigy Service* 的見解，為網路言論的責任判斷立下了新的標竿。然而另一方面，針對

[359] 47 U.S.C. § 230(f) (2). The term "interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

[360] *Zeran v. America Online, Inc.*, 958 F.Supp. 1124 (E.D. Va. 1997).

[361] *Kenneth M. Zeran v. America Online*, 129 F.3d 327 (4th Cir. 1997).

網路中介者是否應依被害人請求而主動移除相關侵權內容的爭點，*Zeran* 案雖指出網路中介者可自行決定之，但在 2003 年的 *Doe v. GTE* 案中，聯邦第七巡迴上訴法院卻採取了不同的見解[362]，認為當網路中介者未採行任何限制或移除的措施時，縱其符合 CDA 第 230 條所規範之主體定義，被害人仍得就網路中介者散布第三人侵權言論之行為向其請求賠償[363]。

其他關於 CDA 第 230 條之重要司法見解尚有：

（1）關於演算法推播之爭議

在歷來涉及 CDA 第 230 條的指標性案件中，2012 年的 *Force v. Facebook* 案[364]除了係以新興社群平臺為被告，更論及平臺使用演算法篩選、排序之手段是否將影響其身分判斷與安全港適用的議題，法院在判決中採取的立場值得注意。

本案原告為哈瑪斯（Hamas）襲擊以色列時的多名受害者及家屬，其指控 Facebook 未能取締其平臺上的恐怖分子帳號，亦無法有效防堵恐怖主義的宣傳內容，成為恐怖分子的幫兇，此舉已違反美國《反恐法》（Anti-Terrorism Act）之規定，應為恐怖分子在社群平臺上的宣傳內容負責。有鑑於過往判決中，互動式電腦服務提供者經常援引 CDA 第 230 條主張免責，本案原告遂採取不同主張，未強調 Facebook 管理平臺內容的責任，而是著眼於 Facebook 的推播及媒合服務（“networking” and “brokering” links and communications），認為這項功能係依據個人資料的數據分析，將特定內容推播給其他喜好相似之用戶，這種基於演算法的自動化媒合功能應使 Facebook 被視為內容的「創造者」（developer）。換言之，原告主張，平臺上恐怖分子交流及散布的內容，應被視為 Facebook「自己」發表的內容，而非「第三方」資訊內容提供者之內容，平臺應就此負責。

然而按一審判決，Facebook 所使用的演算法僅為一種中立的工

362 *Doe v. GTE, Corp*., 347 F.3d 655 (7th Cir. 2003).

363 郭戎晉，網路言論傳播中介者責任與其免責規範之研究－以美國通訊端正法實務發展爲中心，科技法律透析，第 23 卷第 4 期，頁 42（2011）。

364 *Fo7rce v. Facebook, Inc.*, No. 18-397 (2d Cir 2019).

具，且 Facebook 本身也受到其使用者政策的束縛，針對何人可使用平臺、可在平臺發表什麼言論，Facebook 並不具有自行決策的空間，是故按 CDA 第 230 條規定，Facebook 不必為平臺上第三方的言論負責。上訴法院亦同意 Facebook 使用演算法來顯示及媒合用戶提供的內容，屬於 CDA 第 230 條所欲保護之態樣，因此視為「非出版人」，全然不必為第三方資訊服務提供者的內容負責，原告因此敗訴。

在 2023 年 5 月的 *Gonzalez v. Google* 一案中，聯邦最高法院也處理了類似的事件。本案肇因於 2015 年 ISIS 在法國巴黎發起、造成 130 人喪命的恐怖攻擊事件。其中一位美籍交換生 Nohemi Gonzalez 的家屬在事件發生後向 Google 提起民事損害賠償訴訟[365]，主張 ISIS 係透過 Google 旗下的 YouTube 服務招募成員，因此 Google 教唆（abet）、共謀（conspire）了該起恐怖攻擊行動的發生，應就 Gonzalez 的死亡負有賠償責任。

聯邦最高法院的多數意見認為：雖然原告指稱 Google 並未採取「足夠」的行動，從平臺上數以億計的全球使用者及巨量內容中移除與 ISIS 相關的帳號或內容，但原告也無從證明 Google 係蓄意為該起攻擊行動提供實質協助、甚或蓄意參與其中。尤其 YouTube 使用之演算法僅係中立性地將任何內容（包括與 ISIS 相關的內容）與任何可能瀏覽該內容之使用者進行媒合，單就此點而言，並無法將 Google 對攻擊行動的被動協助轉化為主動的教唆。

雖然 *Gonzalez v. Google* 一案的主要爭點皆圍繞在平臺是否就恐怖攻擊事件構成《反恐法》相關損害賠償的責任判斷，而未直接針對 CDA 第 230 條進行討論，但外界仍普遍認為這則判決象徵著科技公司與利益遊說團體的勝利。在當前民主黨憂心社群網站恐成不實訊息溫床及破壞民主社會的武器、共和黨憂心使用者言論遭刪除卻求助無門，兩者皆對數位平臺責任劃定有所疑慮的現狀下，CDA 第 230 條應存廢或修正的戰場將再度回到國會殿堂[366]。

---

[365] 18 U. S. C. §2333(a).

[366] Washington Post, *Supreme Court rules for Google, Twitter on terror-related content* (2023/5/18), https://www.washingtonpost.com/politics/2023/05/18/gonzalez-v-google-twitter-section-230-supreme-court/ (last visited Aug.12, 2023)

（2）性剝削人口販運相關規範之競合

CDA 第 230 條近年引起的另一個爭議在於其(e)項的排除規範。如前所述，本條文之排除規範並不妨礙《2018 年打擊線上性販運法》（Fight Online Sex Trafficking Act of 2018, FOSTA, 18 U.S.C. §1591）等法規之適用，使互動式電腦服務不得在觸犯性剝削之人口販運等嚴重罪行時主張免責，進而提昇兒少保障。作為 2018 年 FOSTA 立法工作之一環，CDA 第 230 條(e)項增修之目的本即在於限縮法律提供給互動式電腦服務的保障，然而因其文字解釋爭議，在 2022 年 10 月的 *Jane Does v. Reddit, Inc* 一案中，聯邦第九巡迴上訴法院的判決還是做出了有利於互動式電腦服務之解釋[367]。

本案係一起由家長團體代未成年被害人所提起之集體訴訟。被告 Reddit 為美國熱門論壇，其網站設有供使用者搜尋及創設子討論串進行討論之功能；針對違反其服務及使用政策之內容，Reddit 亦雇有管理員執行審核、移除等內容調控機制。原告在本案中主張：由於被害人之性剝削影像或影片遭 Reddit 使用者張貼至其論壇板塊，但 Reddit 卻未嚴格執行其內容調控機制，導致原告在歷經數以百計之大量申訴後，仍有部分影像未被刪除，或是影像在遭到站方刪除後又在短時間內重新被使用者上傳張貼。原告遂主張：Reddit 透過此類含有兒童性影像之討論串創造爭議、吸引讀者，繼而賺取廣告收益，已觸犯 FOSTA 禁止透過性販運營利之規範。

然而，聯邦第九巡迴上訴法院在判決中指出，按照 FOSTA 之條文用字，其所適用對象應僅止於對性販運行為明確「知悉」，且確實對性販運行為提供「協助、支持或促進」之人。換句話說，Reddit 站方必須確實有參與某一性販運罪行之環節，才有因被 CDA 第 230 條(e)項而被免除保障之可能。而本案係作為第三人之網站使用者於 Reddit 張貼構成性販運罪行之影像或影片，無法單純據此認定 Reddit 透過違法影像營利。

法院並強調，透過「知悉」要件設下門檻的確會阻礙 FOSTA 立

[367] *Jane Does, et al v. Reddit, Inc.*, No. 21-56293 (9th Cir. 2022).

法時意圖限制 CDA 第 230 條適用之效果，但無法否認的是，此一效果也是立法者明文寫入條文本身的「瑕疵」或「特點」，司法權並不具備改寫法條文字的權力。

值得注意的是，本案原告雖於 2023 年 1 月請求移審，但已於同年 5 月 30 日遭到聯邦最高法院駁回[368]，未來 *Jane Does v. Reddit, Inc* 一案是否將促成立法者重新調整相關法律文字，以限制 CDA 第 230 條在此類第三人張貼嚴重違法內容情況下之適用，進而課予互動式電腦服務更高之責任，則有待持續觀察。

5. 存廢爭議與強化平臺問責之討論

如前所述，網路服務提供者之免責制度，原係為鼓勵網路服務提供者主動採取合理的管制措施，維護良好之網際網路環境。而隨著科技之發展，漸有論者認為原本訂定之免責制度似乎過於保護提供網路服務提供者，尤其 CDA 第 230 條，因條文較為簡短，使司法實務逐漸走向過於寬鬆之認定標準，又，網路服務提供者皆為私人企業，將網路言論全權交予私人企業管制，而未有任何監督管理機制，恐影響民主之實踐與發展。

隨著 Twitter 於 2020 年 5 月 26 日將川普總統之貼文標註警語，並附上與其言論持相反意見之報導連結，而川普以「防止網路審查行政命令」之發布作為回應，CDA 第 230 條的長年爭議與數位平臺責任也再次成為美國總統大選期間的熱烈議題。除了司法部提出修正建議，認為有修法限縮 CDA 第 230 條適用範圍之必要外，國會亦有諸多關於強化數位平臺問責之提案，可參考以下表整：

[368] Trending Law blog, *The Supreme Court Declines Another Opportunity to Consider Section 230* (2023/06/14), https://trendinglawblog.com/2023/06/14/the-supreme-court-declines-another-opportunity-to-consider-section-230/ (last visited Dec. 12, 2023).

表 1：近年美國關於 CDA 第 230 條修正及平臺問責之討論

時間	修正意見
2019 年	
6 月	共和黨參議員提出《停止支持網路審查法》草案。
7 月	共和黨參議員提出《禁止審查法》草案。
2020 年	
5 月 26 日	Twitter 標註川普總統 2 則推文有問題。
5 月 28 日	川普總統發布「防止網路審查行政命令」。
6 月	美國司法部之修法建議報告。
7 月 27 日	美國商務部下轄之 NTIA 向 FCC 提交法規制定請願書。 民主黨參議員提出《平臺課責及消費者透明法》草案。
8 月 3 日	FCC 開啟 CDA 230 公眾諮詢。
9 月	共和黨眾議員提出《網路自由及觀點多樣性法》草案。
2021 年	
1 月 4 日	共和黨 Scott DesJarlais 提出《保障憲法權利不受線上平臺審查》草案（Protecting Constitutional Rights from Online Platform Censorship Act）[369]
1 月 12 日	共和黨 Ted Budd 提出《將 230 條免責對象限縮於善良撒瑪利亞人》草案（Limiting Section 230 Immunity to Good Samaritans Act）
1 月 22 日	民主黨 Joe Manchin III 提出《2021 年線上即見即報法》草案（See Something, Say Something Online Act of 2021）
2 月 5 日	共和黨 Louie Gohmert Jr.提出《终止線上審查法》草案（Abandoning Online Censorship Act, AOC Act）
3 月 23 日	民主黨 Tom Malinowski 提出《保護美國免於危險演算法危害》草案（Protecting Americans from Dangerous Algorithms Act）
7 月 13 日	共和黨 John Kennedy 提出《莫來招惹》草案（Don't Push My Buttons Act）
7 月 14 日	共和黨 Steve Daines 提出《保障線上政治言論法》草案（Preserving Political Speech Online Act）[370]
10 月 7 日	共和黨 Lindsey Graham《廢除 1934 年通訊傳播法第 230 條》草案（A bill to repeal section 230 of the Communications Act of 1934）

[369] H.R.83 - Protecting Constitutional Rights from Online Platform Censorship Act, https://www.congress.gov/bill/117th-congress/house-bill/83/text (last visited Aug. 2, 2023).

[370] S. 2338: Preserving Political Speech Online Act, https://www.govtrack.us/congress/bills/117/s2338 (last visited Aug. 2, 2023).

2022 年	
2 月 9 日	民主黨 Amy Klobuchar 及共和黨 Cynthia Lummis 共同提出《促進使用者驅動社群媒體良好體驗法》（Nudging Users to Drive Good Extperiences on Social Media Act），簡稱為《社群媒體 NUDGE 法》（Social Media NUDGE Act）草案。
2 月 18 日	民主黨 Lori Trahan 提出《2022 年數位服務監督與安全法》（Digital Services Oversight and Safety Act of 2022）。

資料來源：本研究自行整理

（二）DMCA 之安全港條款

除了前述的 CDA 第 230 條外，1998 年美國《數位千禧年著作權法》（Digital Millennium Copyright Act, DMCA）第 512 條亦設有相似的安全港規範。當網路服務提供者知悉平臺上有著作侵權之內容，並且願意協助將侵權內容即時移除（Notice and takedown），即可對他人使用其服務侵害著作權之行為免責[371]。

1. 適用主體與免責要件

DMCA 所規範之網路服務提供者（service provider）共分為以下四種類型，分別對應不同免責要件：

（1）連線服務提供者

指服務提供者對透過其所控制或操作的系統或網路，進行資料的傳輸、繞送路徑及連結，或於上述資料傳輸、繞送路徑及連結之際形成之中介（intermediate）或暫時儲存，所導致的侵害著作權行為。

連線服務提供者之免責要件包括：一、資料的傳輸係由服務提供者以外之他人所發動或指示。二、傳輸、繞送路徑、連結之提供或儲存，經由自動化科技所完成，服務提供者並未對資料進行篩選。三、服務提供者並未選擇資料之接收者。四、服務提供者所做之資料複本，未以非預期接受者之人通常可接觸之方式保存。五、傳輸之資料的內容未經修改。

[371] 章忠信，網路服務提供者著作權侵害責任限制之立法思考與方向，律師雜誌，第 347 期，頁 36（2008）。

（2）快速存取服務提供者

指應使用者之要求傳輸資訊後，透過所控制或營運之系統或網路，將該資訊為中介及暫時儲存，以供其後要求傳輸該資訊之使用者加速進入該資訊之服務者。

快速存取服務提供者之免責要件包括：一、資料由服務提供者以外之他人向嗣後使用者傳輸而內容未經修改。二、服務提供者以業界一般接受的資料傳輸協定對資料進行重新整理、再傳或更新。三、若嗣後使用者已經自他人取得該資料，而服務提供者不干擾該資料回傳給他人的技術能力。四、若他人設有接觸資料之條件（如提供費用、密碼或其他資料），服務提供者亦遵守之。五、接獲通知時，迅速地回應以移除或使無法接觸資料。

（3）資訊儲存服務提供者

指透過所控制或營運之系統或網路，應使用者之要求提供資訊儲存之服務。資訊儲存服務提供者之免責要件包括：一、未實際知悉該筆資料或利用該筆資料所從事之活動造成侵權；或於知悉或察覺此等情況，即迅速地採取行動移除或使無法接觸該資料。二、在服務提供者有權利與能力控制侵權活動之情況下，並未直接自侵權活動中獲得財務上之利益。三、接獲通知時，迅速地回應以移除或使無法接觸資料。

（4）搜尋服務提供者

指提供使用者有關網路資訊之索引、參考或連結之搜尋或連結之服務者。搜尋服務提供者之免責要件與資訊儲存服務提供者相同。

2. 通知及取下程序

DMCA 責任安全港之特色在於「通知及取下」之程序，著作權利人應以書面方式通知 ISP 業者，且 ISP 業者應依該通知移除或阻斷該侵權資料或活動之存取，以達到免除間接之侵權責任。

簡言之，此一機制係藉由著作權利人主動發現侵權活動並踐行通知，免除 ISP 業者之主動監控義務；相對地，課予 ISP 業者後續取下及轉通知之義務，再藉由轉通知程序讓使用者能為自己行為主張抗辯之權利，建立 ISP 業者、著作權利人與被指控為侵權人之間的合作模式[372]。

3. 著作權責任安全港之實質審查

透過 2018 年 *BMG Rights Management v Cox Communications* 一案，可窺美國法院對於責任安全港實質審查之衡量標準[373]。

本案原告為音樂著作權管理公司（BMG Rights Management, BMG），被告 Cox Communications 則為提供寬頻上網服務之電信業者。原告控訴，被告明知其用戶涉及使用點對點分享軟體 BitTorrent 非法上傳與下載音樂後，卻未採取適當措施以阻止該侵權行為，應負間接侵權責任[374]。

Cox Communications 表示，雖然接獲著作權利人發送的侵權通知，但由於相關涉案人尚未被起訴，不足以證明 Cox Communications 知悉相關用戶有侵權行為，而有義務暫時或永久終止其服務。同時，其依循 DMCA 責任安全港之規範，制定內部的用戶守則，以對侵權者進行停權及暫停使用，例如，當收到相關的檢舉時，在 6 個月內又收到第 2 次至第 7 次檢舉後，會以電子郵件通知該用戶；在接到第 8 次與第 9 次檢舉後，用戶上網時會被導引至特定的網頁，告知相關警語，但用戶只要點取網頁上的連結，即可繼續接取網際網路服務；在第 10 次至第 13 次檢舉通知時，用戶將被暫時停權，必須主動向 Cox Communications 聯繫，才能夠復權；累計至 14 次檢舉後，將會審查該用戶的使用紀錄，以決定是否停止其服務，並與該用戶終止契約。

---

[372] 行政院經濟建設委員會，網際網路服務提供者法律責任與相關法制之研究，2003 年 12 月，https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvNTc0NC81NjQ0LzAwMDI2NTkucGRm&n=57ay6Zqb57ay6Lev5pyN5YuZ5o%2BQ5L6b6ICF5rOV5b6L6LKs5Lu76IiH55u46Zec5rOV5Yi25LmL56CU56m2LnBkZg%3D%3D&icon=..pdf，頁 22-23（最後瀏覽日：2022 年 8 月 29 日）。

[373] 鄭嘉逸，網路中介者的「合理」責任避風港義務—由美國最新發展簡評臺灣高等法院 100 年度上字第 752 號判決，科技法律透析，第 32 卷第 3 期，頁 59（2020）。

[374] *BMG Rights Management v. Cox Communications*, 881 F. 3d 293 (4th Cir. 2018).

是故，可受 DMCA 安全港之免責保護。

本案初審法院認為[375]，Cox Communications 阻止重複侵權發生的用戶守則，其適用範圍不宜限於已受到起訴的侵權人，換言之，ISP 業者不能被動的等待侵權人被起訴或判決確定後，才終止其使用權限，而是在知悉時，就必須採取必要的措施。又法院認為在實踐用戶守則方面，Cox Communications 亦沒有徹底執行終止用戶使用權的規定，反而在終止後又應用戶申請復權的請求，恢復使用，自不得享有責任安全港的免責。

本案上訴至第四巡迴法院，上訴法院亦持相同見解[376]，認為 Cox Communications 雖然形式上制定了用戶守則，但實際上根本沒有防制重複侵權之功用，因此無法進入責任安全港。

三、第三方監督或產業自律機制

（一）聖塔克拉拉原則

2018 年 5 月 17 日，以電子前線基金會（Electronic Frontier Foundation,EFF）為首的全球網路人權組織共同發布「聖塔克拉拉原則內容審查透明度及問責制度原則」（Santa Clara Principles on Transparency and Accountability in Content Moderation，以下簡稱「聖塔克拉拉原則」）[377]，以敦促網路服務提供者（社群平臺）將言論審查之標準透明化。此原則推出之初，僅有 Reddit 論壇有完全遵守原則之規範，其他如 Facebook、YouTube 及 Twitter 都未能符合此原則之規範。而後，為因應愈趨複雜的內容管制問題，聖塔克拉拉聯盟（Santa Clara Principles coalition）於 2019 年開始進行公眾諮詢及改版之相關作業，並於 2021 年 12 月發布「聖塔克拉拉原則 2.0 版」（Santa Clara

[375] *BMG Rights Management (US) v. Cox Communications*, 149 F. Supp.3d 634 (2015).
[376] *BMG Rights Management v. Cox Communications*, 881 F. 3d 293 (4th Cir. 2018).
[377] EFF, *The Santa Clara Principles on Transparency and Accountability in Content Moderation, The History of the Santa Clara Principles*, https://santaclaraprinciples.org/history/https://santaclaraprinciples.org/ (last visited Aug. 11, 2023).

Prinles 2.0）[378]。

「聖塔克拉拉原則 2.0 版」可分為「基本原則」以及「操作原則」兩個面向為規範。

基本原則包括：網路服務提供者於內容管制時，應考量人權與正當程序；網路服務提供者之內容管制政策應清楚明確；處理申訴案件的工作人員，應了解該國家之語言、文化、政治以及社會背景；當有任何國家參與網路服務提供者之內容管制政策的執行時，網路服務提供者須詳實的向使用者為報告；以及網路服務提供者應確保其可正常執行其內容管制政策。

操作原則包括：網路服務提供者應公布於疫情期間或社會事件期間遭移除及停用之貼文數量與使用者數量；網路服務提供者應告知使用者被移除／停用／降级之內容管制政策依據及平臺檢測刪除內容之方法等；網路服務提供者應確保其申訴機制具有清楚且易於近用的流程等。

（二）產業自律

為因應外界對網路服務提供者對不法內容與假訊息為處理之期待，網路服務提供者自 2016 年底開始，各自開始發展其內容管制機制，包括事實查核機制、假帳號之管理以及進行內容標籤等作法，茲分述如下。

1. Meta（Facebook、Instagram）

為了使用戶易於辨識不實內容，Facebook 自 2016 年 12 月起，新增了標示不實訊息之功能，一旦用戶質疑平臺上訊息之真實性，可向 Facebook 舉報，Facebook 工作小組即會啟動確認檢查。對於無法確認是否為不實訊息之內容，則會交由第三方事實查核機關進行內容審查，並由該機關回報。因此，Facebook 積極與「國際事實查核聯盟」（International Fact-Checking Network, IFCN）合作，並訂定《國際事實查核準則》（International Fact Checking Code of Principles），以確保

[378] EFF, *The Santa Clara Principles on Transparency and Accountability in Content Moderation, Santa Clara Principles 2.0: Chapeau*, https://santaclaraprinciples.org/ (last visited Aug. 11, 2023).

獨立性與公正性[379]。

根據 Facebook 之「第三方事實查核計畫」（third-party fact-checkers program）[380]，對於違反 Facebook 社群守則（Community Standards）之言論，如垃圾訊息、不實報導、媒體操縱等違反誠信和真實性之內容，將會將其移除；其次，Facebook 也持續與第三方事實查核夥伴密切合作，減少平臺上的不實內容；另外，利用標籤與警示的方式，告知用戶多方資訊，以供其判斷。

2. Twitter（更名為 X）

根據 Twitter 的社群守則，用戶不得濫用 Twitter 的服務而操縱、干預選舉或其他公民程序，特別是張貼或分享誤導他人之言論[381]。Twitter 會在誤導性言論旁加註事實查核標籤，讓用戶知悉，近年來 Twitter 標註的不實內容包括美國總統川普關於郵寄投票的誤導性說法，以及 COVID-19 的貼文等[382]。但由於 Twitter 未建立第三方事實查核機制，亦缺乏透明化的查核標準，因此其事實查核標籤之公正性備受爭議[383]。

3. Google

Google 則是針對搜尋引擎與新聞平臺之搜尋與瀏覽過程，於訊息旁附註事實查核的標記與評論，一旦確認屬假消息，Google 有權將其移除。相對於 Facebook，Google 合作的事實查核組織較為多元，並

---

[379] Alex Heath, *Facebook is Going to Use Snopes and Other Fact-checkers to Combat and Bury 'Fake News'*, BUSINESS INSIDER (2016/12/15), http://www.businessinsider.com/facebook-will-fact-check-label-fake-news-in-news-feed-2016-12 (last visited July 21, 2023).

[380] FACEBOOK, *Facebook's Third-Party Fact-Checking Program*, https://www.facebook.com/journalismproject/programs/third-party-fact-checking (last visited July 21, 2023).

[381] TWITTER, *The Twitter Rules*, https://help.twitter.com/en/rules-and-policies/twitter-rules (last visited Aug. 1, 2023).

[382] 推特加註事實查核標籤 審核如何透明公開為關鍵，YAHOO 新聞，2020 年 5 月 31 日，https://tw.news.yahoo.com/%E6%8E%A8%E7%89%B9%E5%8A%A0%E8%A8%BB%E4%BA%8B%E5%AF%A6%E6%9F%A5%E6%A0%B8%E6%A8%99%E7%B1%A4-%E5%AF%A9%E6%A0%B8%E5%A6%82%E4%BD%95%E9%80%8F%E6%98%8E%E5%85%AC%E9%96%8B%E7%82%BA%E9%97%9C%E9%8D%B5-045023939.html （最後瀏覽日：2023 年 7 月 31 日）。

[383] Harrison Mantas, *Fact-checkers support Twitter labels, but more than that, they want transparency*, POYNTER (2020/05/29), https://www.poynter.org/fact-checking/2020/fact-checkers-support-twitter-labels-but-more-than-that-they-want-transparency/ (last visited Aug. 3, 2023).

不限於新聞媒體產業，美聯社（Associated Press, AP）、英國廣播公司（BBC）與全國公共電台（National Public Radio, NPR）等 100 多家新聞媒體組織與事實查核組織皆有與 Google 合作；假若不同機構審查之結果有所差異，Google 將全部呈現以供用戶自行判斷[384]。

四、小結

由於 CDA 第 230 條為互動式電腦服務提供的長年保護，美國的網際網路產業得以蓬勃發展，進而成為孕育多家跨國網路巨頭的搖籃。但隨著近年來民主、共和兩黨的對立持續升高，國內言論環境激化，疫情、烏俄戰爭下的不實訊息亦持續增長，CDA 第 230 條的修正與存廢也一再成為美國政壇高度關注的議題。雖然相關討論在 2020 年總統大選結束後已較為冷卻，但隨著聯邦最高法院在 2023 年 5 月做成有利於平臺業者的 *Gonzalez v. Google* 判決，CDA 第 230 條存廢之爭的戰場可能又將在可見的未來回到國會。

另一方面，觀察近年來立法動向，也不難發現美國立法者對於網路中介服務的態度開始從過往採取寬鬆市場管制的立場逐步走向較為嚴格的管制傾向，試圖強化網路不法內容的監理。儘管相關立法大多為草案階段，亦有許多提案因屆期不連續而未有明顯進展，仍可看出美國對於網路監理態度的轉變。

[384] Anick Jesdanun, *Google Expands Fact Checking in News Searches*, AP NEWS (Apr. 7, 2017), https://www.apnews.com/8af39d8b7c404e1bbeb9cdcc3e4475d4 (last visited Aug. 3, 2023).

第六節　加拿大

一、監理脈絡

針對網際網路相關服務提供者之責任，尤其違法內容之處理，加拿大過往的法制策略係以業者自律為主，因此現行法並無類似歐盟《數位服務法》或英國《線上安全法》等具有普遍適用性質之網際網路法制框架，亦少有專門針對網路管制之法規，而僅有在少數領域透過作用法之制定，專職處理仇恨言論、兒少保護等重點議題。

其中，宣揚大屠殺或種族仇恨之言論係受加拿大《刑法》第 318 條及第 319 條所禁止之違法內容，然該條文之適用對象並不僅限於使用網際網路傳散之仇恨言論；相對地，2011 年制定的《網際網路服務提供者強制通報兒少色情內容法》（An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service）[385]、及其授權主管機關制定之《網際網路兒少色情通報規則》（Internet Child Pornography Reporting Regulations）[386]，則明確將透過網際網路傳散之兒少色情內容作為其規範對象，進而課予網際網路服務提供者通報義務。

然而，近年來加拿大政府也開始體認到網際網路生態出現急遽變化、社群媒體主導民眾日常生活所帶來的深遠影響。2019 年，時任加拿大民主改革部部長（Democratic Institutions Minister）Karina Gould 便公開表示：過往加拿大以業者自律為主的政策方針已難以回應社會對 Facebook、Google、Twitter（更名為 X）等科技巨頭應負責任的期待，法制上的策略應有所改變[387]。

除此之外，近年頻傳的恐怖攻擊、族群暴力衝突、兒少性虐待等

---

[385] An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service, S.C. 2011, c. 4.

[386] Internet Child Pornography Reporting Regulations, SOR/2011-292.

[387] Hamilton Spectator, *Canadian Government Says It's Considering Regulating Facebook and Other Social Media Giants*, The Hamilton Spectator (2019/04/09), https://www.thespec.com/news/canada/canadian-government-says-its-considering-regulating-facebook-and-other-social-media-giants/article_212ed47d-6927-5f39-a2ea-4a9c2cfff8bb.html (last visited July 12, 2023).

事件也令加拿大政府開始思考加強平臺問責以遏止極端言論傳散之可能，加拿大司法部遂於 2021 年提出「C-36」法案，意圖透過既有法規之更新，明文將相關違法內容之管制擴張至網路場域[388]。

可惜的是，C-36 法案雖因屆期不連續而失效，然加拿大政府目前仍持續進行新版草案的擬定與諮詢作業，以推動新時代下的網際網路規範框架[389]。

二、政府機關法制政策作為

（一）網際網路服務提供者通報兒少色情內容之義務

如前所述，加拿大多年來對於網際網路相關服務之政策雖係採取業者自律之主調，但在兒少保護方面，加拿大早在 2011 年通過的《網際網路服務提供者強制通報兒少色情內容法》中，便已設有針對網際網路內容及服務提供者課責之法制框架。

根據該法第 1 條之定義，所謂的「網際網路服務」（Internet Service）係指「提供網際網路接取、網際網路內容儲存或電子郵件之服務」[390]，而該法課予網際網路服務提供者的責任主要有三：

首先，若網際網路服務提供者在向公眾提供網際網路服務的過程中，獲悉某一 IP 位址或 URL 網址有被用於向公眾提供兒少色情內容的可能，服務提供者必須儘速將該 IP 位址或 URL 網址通報於本法所指定之組織[391]。而根據本法授權制定之《網際網路兒少色情通報規則》，受理本法通報之指定組織為加拿大兒童保護中心（Canadian Centre for Child Protection）[392]。

---

[388] BILL C-36, An Act to amend the Criminal Code and the Canadian Human Rights Act and to make related amendments to another Act (hate propaganda, hate crimes and hate speech).

[389] Canadian Heritage, *The Government's Commitment to Address Online Safety*, Government of Canada (2023/01/31), https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html (last visited July 12, 2023).

[390] An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service, S.C. 2011, c. 4, S 1.

[391] An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service, S.C. 2011, c. 4, S 2.

[392] Internet Child Pornography Reporting Regulations, SOR/2011-292, S 2.

其次，若網際網路服務提供者在向公眾提供網際網路服務的過程中，合理相信其服務正被用於、或已持續被用於兒少色情相關之犯罪，服務提供者必須儘速向維持治安之官員或警察通報此一事實[393]。

其三，依法進行前述通報者，自通報起必須將所有相關之電腦資料保全 21 日，保全期限屆滿後則應儘速刪除，但有法院命令繼續保全之情況則不在此限[394]。

違反本法所定義務者，視初犯與否等情事，將面臨最低 1,000 加幣之罰鍰[395]。

值得注意者係，《網際網路服務提供者強制通報兒少色情內容法》本身所課予網際網路服務提供者的，僅有「通報」指定組織或官員、警察之義務，而未進一步要求其將相關內容阻斷接取或移除。但為求兒少保障之周延，加拿大兒童保護中心於 2017 年啟動了「蜘蛛網計畫」（Project Arachnid）。該計畫透過自動化爬蟲程式主動搜尋網路上公開的兒少性虐待內容（child sexual abuse material, CSAM），並將偵測到的圖像或影片進行分類，進而向世界各地的資訊儲存服務業者發布移除請求[396]，試圖透過業者協力之方式阻斷相關內容之接取。在過去五年來，蜘蛛網計畫已經與全球超過一百個國家、總數超過一千的服務提供者合作，成功移除了六百萬則兒少性虐待的圖像或影片[397]。

---

[393] An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service, S.C. 2011, c. 4, S 3.

[394] An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service, S.C. 2011, c. 4, S 4.

[395] An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service, S.C. 2011, c. 4, S 10.

[396] Project Arachnid, *What is Project Arachnid?*, https://www.projectarachnid.ca/en/#what-is-project-arachnid (last visited July 12, 2023).

[397] Cybertip!ca, *Child Sexual Abuse: Project Arachnid*, https://cybertip.ca/en/child-sexual-abuse/project-arachnid/ (last visited July 12, 2023).

（二）新時代法制框架之討論

考量到近年恐怖攻擊、族群暴力衝突、兒少性虐待等事件頻傳，加拿大政府也開始意識到極端仇恨言論透過網際網路服務傳散之危險性，司法部遂試圖提出既有法規之更新，欲透過 2021 年「C-36」法案新增《加拿大人權法》（Canadian Human Rights Act）第 13 條。該法案明文將「透過網路或其他通訊傳播方法」散布仇恨言論之行為列為處罰對象，使受害者可依法向加拿大人權委員會（Canadian Human Rights Commission）提出申訴；委員會經審議後依法則可對行為人處最高 50,000 加幣之罰鍰[398]。雖然本次提案後因屆期不連續而失效，但也促成了網際網路立法及網路違法內容處理的進一步討論。

2021 年 7 月，加拿大政府針對網路有害內容發布了政策文件「政府處理線上安全之承諾」（The Government's commitment to address online safety），並持續進行相關法制框架之擬定，試圖推動新時代下的網際網路規範框架[399]。

歷經數次諮詢與專家會議，目前加拿大政府最新之立法規劃及討論包括[400]：

1. 規管對象之劃定

新草案暫訂之規範對象將稱為「線上通訊服務提供者」（online communication service providers），其定義雖尚未確定，但預計將涵蓋 Facebook、Instagram, Twitter、YouTube、TikTok，甚至成人網站 Pornhub 等民眾高度使用之大型網路社群平臺。至於健身應用程式、旅遊評價網站等類型則預計被此一定義所排除；私人通訊、電信服務提供者或相類似之服務也預計被列入特別的排除條款之中，而不適用本草案所課予之義務。

---

398 BILL C-36 (2021/6/23), https://parl.ca/DocumentViewer/en/43-2/bill/C-36/first-reading (last visited Aug. 12, 2023).

399 Canadian Heritage, *supra* note 389.

400 Canadian Heritage, *What We Heard: The Government's Proposed Approach to Address Harmful Content Online*, Government of Canada (2022/02/03), https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/what-we-heard.html (last visited Aug. 12, 2023).

草案亦將有授權條款，使政府透過包含性或排除性之規範，就線上通訊服務提供者之範圍進行更進一步之釐清。

2. 課予線上通訊服務提供者遏止違法內容之義務

針對前述之「線上通訊服務提供者」，草案預計課予其各種義務，敦促其採取所有合理措施，以完全排除加拿大網路使用者對有害內容之接取。至於服務提供者應採取之「合理措施」，具體而言則可能包含透過演算法為基礎之自動化系統，針對特定類別之有害內容進行監控。

按目前草案之規劃，一旦偵測到可能有害之內容，服務提供者即需依法律之標準判斷其是否構成應阻斷接取之內容，若確已構成，即需在 24 小時內進行阻斷。除此之外，受規範之線上通訊服務提供者亦應為檢舉者及內容之提供者建立標記、通知與申訴之系統，並將相關決定之結果通知雙方。

另一方面，受草案規範之線上通訊服務提供者亦會有透明度報告之義務，需針對其專門用以處理加拿大有害內容之自動化內容調控、移除或封鎖接取措施進行詳盡說明。

3. 有害內容之種類

按現行之草案規劃，新法預計處理之對象係目前加拿大政府認定最有害性之五種有害內容，包括：恐怖主義內容、煽惑暴力內容、仇恨性言論、非合意散布之私密圖像，以及兒少性剝削內容。

加拿大政府亦反思：前述五種類型的有害內容性質彼此大相逕庭，每種類型皆會需要專門的應對方法，甚或需要完全獨立的監理制度，因此，將所有網路有害內容類型皆納入同一部法律規管，可能未必會是最適切的解決方案。

4. 成立數位安全委員會

為協助新時代網路監理框架之推行，目前草案亦規劃成立新監理機關「數位安全委員會」（Digital Safety Commission），委員會並將下設「加拿大數位安全官」（Digital Safety Commissioner of Canada）、「加拿大數位追償委員會」（Digital Recourse Council of Canada）及「諮詢委員會」（Advisory Board）。

加拿大數位安全官將負責行政、監督與執行前述之新法，並領導、參與相關之研究規劃、會議召集或與利害關係人之合作，同時協助受新法管制之線上通訊服務提供者遏止五大類型之有害內容。

加拿大數位追償委員會將專責受理加拿大民眾對於網路內容調控措施之申訴。當社群平臺等線上通訊服務提供者之使用者已用盡服務提供者內部提供之申訴手段時，即可向加拿大數位追償委員會提出外部申訴，進而由委員會做成獨立且具有拘束力之專業決定。

相對地，諮詢委員會之功能則在於支援加拿大數位安全官與加拿大數位追償委員會，為其程序及決策提供諸如產業趨勢、內容調控之技術與標準等專業性建議。

（三）最新立法動向

2023 年 10 月，加拿大發生一起 12 歲少年因網路性勒索（sexual extortion）自殺案件，使得延宕已久的法案，又再度備受矚目。

加拿大現任自由黨黨魁兼總理 Justin Trudeau 首次在 2019 年第 43 屆聯邦選舉宣傳中提出打擊網路恐怖主義內容、仇恨言論和及性剝削內容之立法倡議，之後自由黨於 2021 年 6 月 23 日提出 C-36 法案[401]，對刑事法典、青少年刑事司法法案以及加拿大人權法案進行修訂。然而因總理 Trudeau 在 2021 年 8 月解散議會，使得該法案推動

[401] Library of Parliament, *Legislative Summary of Bill C-36: An Act to amend the Criminal Code and the Canadian Human Rights Act and to make related amendments to another Act (hate propaganda, hate crimes and hate speech)*, Research publications (2021/09/08), https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/LegislativeSummaries/432C36E (last visited Dec. 20, 2023).

暫時停擺。

2021 年 9 月進行重選組成第 44 屆議會時，總理 Justin Trudeau 與自由黨也再度承諾推動該法案，然而眾多輿論質疑該法案嚴重侵犯言論自由，尤其是要求數位平臺取下貼文的機制備受爭議。儘管自由黨選後已反轉前一屆少數政府的情況，議會 338 個總席位中贏得 184 個過半席位，但仍無法於原定 100 日期程內取得共識並完成立法，至今已過 2 年，政府仍持續向專家學者諮詢修改建議，一直未有新的立法進度。

過去幾年，數位相關立法諮詢工作多由加拿大文化遺產部推動，該部也順利推動《線上新聞法》（Online News Act）[402]、《線上串流媒體法》（Online Streaming Act）[403]，然而由於網路有害內容法案較具爭議，經過 2023 年 7 月內閣改組後，該工作目前轉由司法部長負責。司法部長 Arif Virani 表示目前積極研析他國機制，希望在 2024 年期間提出網路有害內容法案的最終版本[404]，可能也將朝向創立「網路監理機構」的方式，並賦予該機關調查數位平臺之權利、命令修正之權利，以及裁罰之權利。[405]

儘管有質疑聲浪，加拿大仍有許多期許迅速立法的組織，例如：以色列猶太事務中心（Centre for Israel and Jewish Affairs）、加拿大華人正義國家委員會（Chinese-Canadian National Council for Justice）、加拿大穆斯林國家委員會（National Council of Canadian Muslims）等，鑒於近年世界局勢緊張，以色列與巴勒斯坦衝突不斷，加拿大境內反猶太主義（antisemitism）等網路仇恨言論持續發生[406]。

---

[402] Canadian Heritage, *The Online News Act*, Government of Canada (date modified: 2024/01/03), https://www.canada.ca/en/canadian-heritage/services/online-news.html (last visited Jan. 11, 2024).

[403] Canadian Heritage, *Online Streaming Act*, Government of Canada (date modified: 2023/11/27), https://www.canada.ca/en/canadian-heritage/services/modernization-broadcasting-act.html (last visited Jan. 11, 2024).

[404] Stephanie Taylor, *I don't want online harms bill that 'looks like people are trying to tell you what to think': justice minister*, NATIONAL POST (2023/12/18), https://nationalpost.com/news/politics/i-dont-want-online-harms-bill-that-looks-like-people-are-trying-to-tell-you-what-to-think-justice-minister (last visited Dec. 20, 2023).

[405] Stephanie Taylor, *Is Ottawa looking at new agency to fight online harm? Minister tight-lipped*, Global NEWS (2023/12/01), https://globalnews.ca/news/10143500/canada-online-harm-new-regulator/ (last visited Dec. 20, 2023).

[406] Raffy Boudjikanian, *At conference confronting antisemitism, justice minister promises online harms*

根據多倫多市立大學領導力實驗室政策與研究主任 Sam Andrey 在 2023 年 3 月發布的網路有害內容調查結果，當前加拿大民眾期望對於網路有害內容採取行動。根據統計，加拿大民眾對社群媒體照顧公眾利益的信任持續下降，只有十分之一的人對 Facebook、TikTok 或 Twitter（更名為 X）投以高度的信任；三分之二認為政府應要求數位平臺負責減少平臺上的有害內容；自 2021 年以來，強烈支持要求平臺刪除各類非法或有害內容的聲音顯著增加；超過 80%的加拿大人支持要求平臺迅速刪除被舉報的非法內容，封鎖自動或機器人帳戶，標記已驗證為假的訊息，並為用戶提供工具以查證或搜尋線上內容之真實性[407]。

綜上所述，基於加拿大國內近期發生社群媒體性勒索自殺事件、國際衝突情勢使種族仇恨言論加劇、學術調查研究也佐證輿論朝向支持賦予平臺取下非法內容之義務等多方壓力，網路有害內容之相關立法很可能在 2024 年度或下屆聯邦議會選舉前（2025 年 10 月）有重大進展，值得持續關注。

三、第三方監督或產業自律機制

（一）產業自律情況

如前所述，加拿大過往少有專門針對網際網路相關服務業者或網路有害內容進行直接控管之法律，而係以業者自律為政策之主要方針。相對地，網際網路產業早在 1990 年代時也已建立起一定程度之自律準則。

舉例而言，1996 年成立之「加拿大網際網路提供者協會」（Canadian Association of Internet Providers, CAIP）便以衡平多方利害關係人之利益、透過國際互助解決網際網路議題、建構安全網路環境並隔絕有害人性尊嚴之違法內容作為其基本行動方針，以協助網際網

legislation, CBC NEWS (2023/10/17), https://www.cbc.ca/news/politics/virani-antisemitism-online-hate-1.6998249 (last visited Dec. 20, 2023).

[407] Sam Andrey, *Survey of Online Harms in Canada*, Toronto Metropolitan University (2023, March), https://www.ryersonleadlab.com/survey-of-online-harms-in-canada (last visited Dec. 20, 2023).

路產業在網路接取、隱私權、電子商務利用、著作權等領域之法律遵循及正向發展。以著作權領域之議題為例，CAIP 在 2004 年參與的 *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Provider* 一案，即涉及作權集體管理團體徵收網路傳輸音樂著作權利金之議題，並促使加拿大最高法院做成網路著作侵權爭議之代表性判決[408]。

CAIP 所建立之自律行為準則包括[409]：

- 成員將致力於與政府官員、執法部門及國際組織之合作，以釐清各類網際網路公司之責任。
- 成員將致力於遵守所有實訂法規，並以自律行為準則協助各成員於內部政策落實法律之要求。
- 成員有責任對公眾進行教育，使其瞭解網際網路之善用與濫用，及網際網路科技之發展。
- 成員務必保護其使用者之隱私與個人資料，僅有在接獲執法部門命令時才得以揭露。
- 成員不得依使用者要求儲存任何違法或具有濫用性質之內容，且應當檢舉此類內容，進而對此類違反刑法之內容採取相應之行動。
- 儘管監控所有網路內容乃不可能之事，成員仍將在接獲通報的情況下，針對任何儲存非法或濫用性內容之網際網路服務採取相應之法律行動。
- 針對濫用性內容之提供者，成員在採取行動前必須遵守以下之程序：其一，應透過精確之審核獲取該內容之位置與性質資訊；其二，應利用執法部門之諮詢資源；其三，應向內容提供者發送通知，先給予 7 天之回應期，再採取進一步之行

[408] Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers, 2004 SCC 45 (CanLII), [2004] 2 SCR 427.

[409] CAIP Code of Conduct, http://www.cata.ca/files/PDF/caip/CAIP_Code_of_Conduct.pdf (last visited Aug.12, 2023).

動。

（二）「數位公民倡議」資金挹注機制

數位公民倡議（Digital Citizen Initiative）是一個多方行動策略，試圖強化加拿大公民對抗網路假訊息以及其他有害內容的韌性，以維持加拿大的民主制度和社會包容性。

確保公民能夠獲得多元且可靠的新聞和資訊，是穩固民主制度的要件之一，有利於民眾形成觀點、追究政府和個人的責任，並參與公眾辯論。有鑒於網路上（尤其社群媒體）的假消息、誤導性消息和煽動性訊息越來越多，加拿大政府透過挹注資金於公民團體，該資金挹注機制係為鼓勵各界辦理有助於提高數位素養的活動，或開發有助於改善各類網路社會問題的工具，或執行相關議題之研究。

1. 建構公民韌性

保護加拿大民主計畫－以公民為主的行動（Plan to Protect Canada’s Democracy - Citizen-focused Activities）由加拿大文化遺產部提供資金，強化公民批判性並提高辨識假訊息的能力。

「保護加拿大民主計畫」目前仍有三類基金可申請：（1）加拿大歷史基金（Canada History Fund）為促進民眾對加拿大歷史、公民社會和公共政策的了解，可申請用於製作教材、網站、行動應用程式或其他新媒體工具，亦可用於辦理會議和工作坊，建立合作夥伴關係，以及執行關於加拿大公共政策議題的研究和出版物；（2）集體倡議－加拿大期刊基金（Collective Initiatives - Canada Periodical Fund）用於支援加拿大本土雜誌以及社區型報刊產業；（3）青年領導計畫（Youth Take Charge）用於加強 7 歲至 30 歲青年對於加拿大的歸屬感以及提高他們參與公眾事務的意識。

2019 年至 2020 年期間，文化遺產部共補助執行 23 個計畫[410]，花費約 700 萬加幣，觸及超過 1,200 萬加拿大人，包括青少年、老年人、少數族裔社區、官方語言少數族裔社區等。此外，目前有關 COVID-19 及烏俄戰爭的徵件計畫皆已停止。

2. 數位公民研究計畫

數位公民研究計畫（Digital Citizen Research Program）試圖了解網路假訊息對於加拿大社會的影響，並依據研究結果來擬定未來的政策與具體行動。這項計畫期許多方參與者一同為維護數位內容的多樣性制定指導原則。

（1）數位公民貢獻計劃

數位公民貢獻計劃（Digital Citizen Contribution Program）[411]為個人及團體提供資金挹注，該計畫徵求提高公民對抗網路有害資訊、假訊息能力的具體行動及研究計畫，或結合行動與研究的計畫，每個計畫最高可獲 38 萬加幣的資金。

申請者可以是非營利組織（non-for-profit institution）、大學或教育機構（educational institution）、個人研究者（individual researcher）、研究機構（research institution），或者意圖推動符合旨意之非商業計畫的加拿大營利組織（for-profit Canadian institution），並必須至少滿足以下一項條件：（a）針對加拿大老年人以及教育機構以外的人民，開發培養數位媒體素養之工具；（b）開發能夠幫助加拿大人識別由機器人和人工智慧生成和傳播的內容之工具；（c）開發能夠預防針對婦女、女孩、2SLGBTQI+社群數位暴力的工具[412]；（d）建構支援加拿大兒童

[410] 獲得「保護加拿大民主計畫」補助金名單及計畫簡介：Canadian Heritage, Backgrounder – Helping Citizens Critically Assess and Become Resilient Against Harmful Online Disinformation, Government of Canada (data modified 2022/06/28), https://www.canada.ca/en/canadian-heritage/news/2019/07/backgrounder--helping-citizens-critically-assess-and-become-resilient-against-harmful-online-disinformation.html（最後瀏覽日：2023 年 12 月 20 日）。

[411] Digital Citizen Contribution Program, https://www.canada.ca/en/canadian-heritage/services/online-disinformation/digital-citizen-contribution-program.html (last visited Dec. 20, 2023).

[412] 「數位暴力」是指透過電子通訊技術和平臺，如社群媒體、簡訊、電子郵件等，對他人進行的心理、情感或社會的攻擊或侵犯。這種形式的暴力可以包括言語攻擊、騷擾、威脅、誹謗、恐嚇和其他的行為，可能對受害者的心理和情感造成傷害。

和家長應對和預防網路霸凌的資源庫；(e) 為中小型公民組織建立識別誤導/假訊息、仇恨言論和網路霸凌的技術能力和專業知識；(f) 開發識別網路假消息之工具，加強加拿大居民（包括僑民社群）對於來自外國政府（例如中華人民共和國和俄羅斯聯邦）的假訊息；(g) 對前述事項進行研究、工具測試或評估。

加拿大文化遺產部在 2019 年至 2021 年之間共資助 50 餘個計畫[413]，例如：阿卡迪亞區域性組織（Société de l'Acadie du Nouveau-Brunswick）提出「COVID-19 事實查核網站」計畫於 2020 年獲補助 352,500 加幣（約 820 萬新台幣）、數位公共廣場（Digital Public Square）提出之「反駁關於 COVID-19 的假訊息」計畫於 2020 年獲補助 665,734 加幣（約 1,500 萬新台幣）、考迪亞大學提出之「加拿大女性領導數位防衛行動」研究計畫[414]等各類型計畫，涵蓋假訊息、性別、種族議題等。

（2）數位公民研究之聯合行動

加拿大文化遺產部與社會科學和人文研究委員會（Social Sciences and Humanities Research Council, SSHRC）合作，提供博士後獎學金和博士獎學金等補助，數位公民研究之聯合行動（Joint Initiative for Digital Citizen Research）研究補助目的：(a) 理解網路假訊息對加拿大的影響，並以此作為政策擬定的基礎；(b) 增強加拿大執行對抗網路假訊息和網路有害內容相關研究的能力；(c) 幫助加拿大建構數位公民身份和網路假訊息的研究社群。

（3）支援公共政策論壇的「數位民主計畫」

「數位民主計畫」（Digital Democracy Project, DDP）於 2020 年啟動，任務目標為理解、預測和應對數位技術對公共領域和加拿大民主產生的影響。2023 年該計畫特別關注極端化（polarization）在加拿大

---

413 Canadian Heritage, *Backgrounder - Ongoing Support for Research and Media Literacy Projects as Canada Continues to Fight Online Disinformation*, Government of Canada (data modified 2021/02/09), https://www.canada.ca/en/canadian-heritage/news/2021/02/backgrounder---ongoing-support-for-research-and-media-literacy-projects-as-canada-continues-to-fight-online-disinformation.html (last visited Dec. 20, 2023).

414 MIGS, *Canadian Women Leaders' Digital Defence Initiative*, https://www.concordia.ca/research/migs/projects/WomenDisinfo.html (last visited Dec. 20, 2023).

如何體現，公共政策論壇（Public Policy Forum, PPF）執行此計畫之項目包含實施全國性調查、辦理社區圓桌會議、全國虛擬市政廳以及發布研究報告[415]等。

表 2：加拿大「數位公民倡議：對抗網路假訊息及其他有害內容」架構

數位公民倡議	建構公民韌性	保護加拿大民主計畫－以公民為主的行動	加拿大歷史基金
			加拿大期刊基金聯合行動
			青年領導
		COVID-19 特別徵件	--
		烏俄危機特別徵件	--
	數位公民研究計畫	數位公民貢獻計畫	--
		數位公民研究聯合行動	--
		支援公共政策論壇的數位民主計畫	--

資料來源：本研究自行整理

[415] *E.g.* Justin Ling, *Canadian Women Leaders' Digital Defence Initiative*, https://www.concordia.ca/research/migs/projects/WomenDisinfo.html (last visited Dec. 20, 2023).

四、小結

綜上所述，加拿大過往之網路政策係以產業自律及公民行動為重心，少數直接針對網路違法內容之法律規範僅有 2011 年通過之《網際網路服務提供者強制通報兒少色情內容法》。而另一方面，業界早在 1990 年代即已發展出協助整體產業推動及法遵之 CAIP 等組織，進而制定了相關之自律準則。

然而，隨著近年網際網路生態改變，加拿大政府也開始體認到極端言論內容透過網路傳散之危險性，除嘗試透過 C-36 法案修正既有之《加拿大人權法》，將透過網路或其他通訊傳播方法散布仇恨言論之行為列為處罰對象，更在 2021 年 7 月提出「政府處理線上安全之承諾」，描繪新時代的立法規劃。從當前的規劃方向觀之，未來加拿大擬課予「線上通訊服務提供者」之義務已不再只是單純的兒少色情內容通報，而是針對嚴重違法內容課予服務提供者監控、移除內容、建立申訴機制與透明度報告，其平臺問責之程度已趨近歐盟《數位服務法》之精神，且亦將成立全新的監理組織「數位安全委員會」。

整體而言，加拿大目前的網際網路相關規劃仍處於研擬、諮詢之規劃階段，尚有不確定性，但其法制策略已開始邁入轉型期，未來發展值得持續追蹤。

第七節　澳洲

一、監理脈絡

澳洲數位平臺之監理首重於完整市場調查研究，澳洲競爭與消費者委員會（Australian Competition and Consumer Commission, ACCC）利用長達近兩年的時間全面調查澳洲本土數位平臺之消費者與競爭議題，並提出「數位平臺調查」（Digital platorms inquiry, DPI）報告[416]，並且從科技發展、資料（跨境）流通、公平競爭、新聞公益性、消費者保護與個資隱私等角度切入，向澳洲聯邦政府提出《新聞議價法》、《競爭與消費者法》修法建議，以及研擬《數位平臺假新聞與新聞品質準則》、《隱私保護法》修法等。

為針對數位平臺有更全面性的數位環境之監理規劃，2020 年 2 月 10 日，澳洲政府進一步要求 ACCC 展開為期 5 年的「2020-2025 年數位平臺服務調查」（Digital platform services inquiry 2020-2025）[417]。該報告重點調查事項如下：

- 數位平臺服務市場的競爭強度，包括集中程度、供應商行為、結合與併購、參進障礙等，以及其提供服務範圍之變化；
- 可能造成消費者受害之數位平臺服務提供者之行為；
- 可能影響數位平臺服務性質與特性之市場趨勢；
- 澳洲以外數位平臺服務供應市場之發展。

ACCC 至今計已繳交 6 份中期報告[418]，並於 2023 年提交社群媒體平臺調查報告[419]，預計於 2025 年向財政部提出最終報告。

---

[416] ACCC, *Digital platforms inquiry - final report*, June 2019, https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf (last visited Aug. 14, 2023).

[417] ACCC, *Digital platform services inquiry 2020-2025 - Project overview*, https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-2025 (last visited Aug. 14, 2023).

[418] *Id.*

[419] ACCC, *Digital platforms services inquiry - Interim report 6: Report on social media services*, Mar. 2023, https://www.accc.gov.au/system/files/Digital%20platforms%20services%20inquiry%20-%20Interim%20report%206%20-%20Report%20on%20social%20media%20services_0.pdf (last

整體而言，澳洲針對平臺責任與監理可分為兩大部分，一為線上違法內容；二為平臺不實訊息之管理。前者主要訂定於《線上安全法》（Online Safety Act）要求平臺業者對於在其平臺呈現並散布涉及未成年性剝削、犯罪、恐怖主義暴力等違法內容負起一定責任，包含將違法內容下架、阻止違法內容傳播等，否則將面臨罰則；而後者在誤導、虛假與惡意訊息之不實與錯誤訊息方面，則是要求業界制定強制性自律行為準則，處理相關不實訊息之投訴。

其中，DPI 報告指出[420]，透過數位平臺獲取新聞資訊之消費者可能會因錯誤訊息（misinformaiton）、不實訊息（disinformation）、和惡意訊息（malinformation）[421]的傳播而暴露於風險之中。對此 ACCC 建議制定有關管制錯誤與不實訊息之行為準則，並更廣泛地對不真實訊息（不論故意製造、傳播與否）和新聞品質進行監測和評估，以負起監理之責。

2019 年 12 月，澳洲政府已要求數位平臺為虛假訊息和新聞品質制定自願行為準則，並要求澳洲通訊與媒體局（Australian Communications and Media Authority, ACMA）監督與指導此一準則的制定內容[422]。而後 ACMA 也於 2020 年 6 月發布「澳洲數位平臺錯誤訊息與新聞品質準則」立場文件，提供業界制定行為準則可依循之框架[423]，並於隔年 2021 年 2 月，由澳洲數位產業集團（Digital Industry Group, DIGI）推出《澳洲不實與錯誤訊息實踐準則》（Australian Code of Practice on Disinformation and Misinformation）[424]，同年 6 月 ACMA

visited Aug. 14, 2023).

[420] ACCC, *supra* note 416, at 280.

[421] 錯誤訊息（misinformaiton）在此指的是不實或不準確的資訊，但並非有意造成傷害；不實訊息（disinformation）在此指的是故意製造、傳播的不實資訊，意圖造成傷害；惡意訊息（malinformation）在此指的是故意不當地傳播正確訊息，意圖造成傷害。

[422] ACMA, *Online misinformation and news quality in Australia: Position paper to guide code development*, https://www.acma.gov.au/online-misinformation-and-news-quality-australia-position-paper-guide-code-development (last visited Aug. 14, 2023).

[423] ACMA, *Misinformation and news quality on digital platforms in Australia—A position paper to guide code development*, June 2020, https://www.acma.gov.au/sites/default/files/2020-06/Misinformation%20and%20news%20quality%20position%20paper.pdf (last visited Aug. 14, 2023).

[424] DIGI, AUSTRALIAN CODE OF PRACTICE ON DISINFORMATION AND MISINFORMATION (2021), https://digi.org.au/wp-content/uploads/2022/12/Australian-Code-of-Practice-on-Disinformation-and-Misinformation-FINAL-PDF-Feb-22-2021.pdf.

即針對該準則提出評估建議予澳洲政府[425]，而 DIGI 也依據 ACMA 之修正建議於 2022 年 12 月提出最新版實踐準則[426]，並以公私協力的模式要求採納該準則之各大平臺業者，必須共同降低線上不實與錯誤訊息造成的風險危害。

然而，儘管 2022 年末平臺承諾強化《澳洲不實與錯誤訊息實踐準則》之規範作為，2023 年 1 月 ACMA 部長 Michelle Rowland 仍指出[427]，業者自律行為準則尚無法充分改善網路問題，盼制訂新法賦予 ACMA 對平臺之監理權力，擴大監督非簽署方之網路業者，與 DIGI 建立長期打擊線上不實與錯誤訊息之合作關係[428]。而澳洲政府已於 2023 年 6 月展開《2023 年通訊法（就打擊不實與錯誤訊息）修正案》（Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023）之公眾諮詢，並已於 8 月底完成公眾諮詢[429]，文後將進一步說明該草案之內涵。

[425] ACMA, A report to government on the adequacy of digital platforms' disinformation and news quality measures, June 2021, https://www.acma.gov.au/sites/default/files/2021-11/Adequacy%20of%20digital%20platforms%20disinformation%20and%20news%20quality%20measures.pdf (last visited Aug. 14, 2023).

[426] DIGI, *supra* note 424.

[427] Paul Karp, Australia's media regulator to get new powers to crack down on online misinformation, The Gardian, Jan. 19 2023, https://www.theguardian.com/media/2023/jan/20/australias-media-regulator-to-be-get-new-powers-to-crack-down-online-misinformation (last visited Aug. 14, 2023).

[428] Minister for Communications, Consultation opens on new laws to tackle online misinformation and disinformation, June. 25, 2023, https://minister.infrastructure.gov.au/rowland/media-release/consultation-opens-new-laws-tackle-online-misinformation-and-disinformation (last visited Aug. 14, 2023).

[429] ACMA, Online Misinformaiton, last updated: 25 July 2023, https://www.acma.gov.au/online-misinformation#our-role (last visited Dec. 14, 2023).

二、政府機關法制政策作為

澳洲政府對線上平臺之網路安全維護管制與法制政策作為，主要以整全式立法模式規範於《線上安全法》中，因此以下將聚焦於該法之規範內涵與政策模式進行說明。

澳洲於 2021 年 7 月 23 日通過《線上安全法》（Online Safety Act 2021）[430]，取代先前《強化線上安全法》（Enhancing Online Safety Act 2015），並於 2022 年 1 月 23 日起實施新法。根據《線上安全法》之規定，擴張「電子安全專員辦公室」（Office of the eSafety Commissioner）之職權，賦予其更多的調查與執法權力，要求線上平臺業者應為人們所使用之網路安全負起責任，亦針對違法內容之範圍有更明確之定義，以監理非法和限制性內容。

該法案透過一套涵蓋廣泛網路危害範圍之「基礎線上安全期望」（Basic Online Safety Expectations, BOSE）[431]，提高線上服務提供者之網路安全責任，確保所有澳洲人民都能安全使用線上服務。以該期望價值為基礎，建立更深層的規範措施，要求線上服務提供者主動保護人們免於遭受線上暴力行為與有害內容的影響，並以民事處罰措施對不履行相關義務的線上服務提供者進行處罰。

該法案要求業界制定全新且具有強制力之業界規範（industry code），該規範將適用於網路產業之八大領域業者[432]，包括社群媒體平臺、電子訊息服務（electronic messaging services）、搜尋引擎、應用程式服務、網路服務提供者、資訊儲存服務提供者、接取網路服務設備之製造商與供應商以及安裝與維護設備者。相關規範經登記後，線上服務提供者可據以進行平臺監測並移除線上違法內容[433]。

---

[430] Australian Government, *Online Safety Act 2021*, https://www.legislation.gov.au/Details/C2022C00052 (last visited Aug. 14, 2023).

[431] eSafety Commissioner, *Online Safety Act 2021-Fact sheet*, Updated: January 2022, https://www.esafety.gov.au/sites/default/files/2022-02/OSA%20fact%20sheet%20updated.pdf (last visited Aug. 14, 2023).

[432] *Id.*

[433] eSafety Commissioner, *Learn about the Online Safety Act*, https://www.esafety.gov.au/newsroom/whats-on/online-safety-act (last visited Aug. 14, 2023).

《線上安全法》之重點規範整理如下：

（一）電子安全專員辦公室

電子安全專員辦公室主要由 ACMA 支持成立之獨立監管機構，Julie Inman Grant 為現任澳洲電子安全專員，除了電子安全專員外，所有受雇之職員皆來自 ACMA[434]。而 ACMA 與 eSafety 為平行對等之機關，機關分工由 ACMA 負責監督澳洲網路平臺所傳散之不實與錯誤訊息並發布相關立場報告[435]，而 eSafety 則負責管理網路危害內容並做出相應處置，其組織架構如下圖所示。

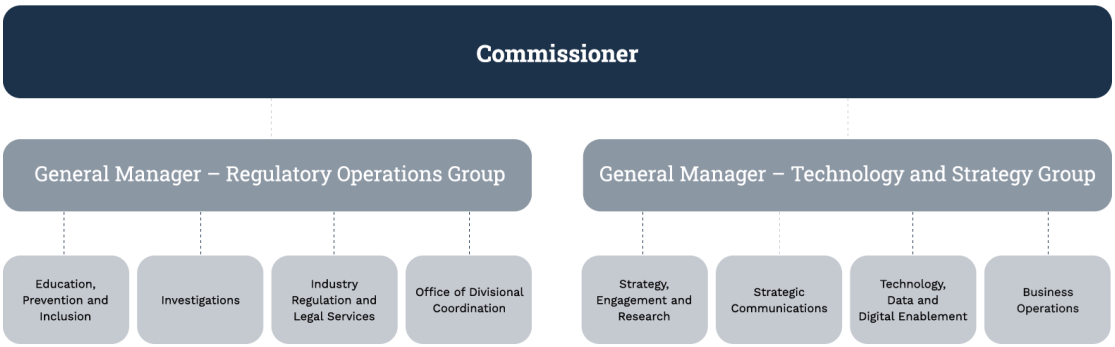


圖 2：澳洲電子專員辦公室組織架構圖

資料來源：eSafetyCommissioner[436]

電子安全專員由通訊部長（Minister for Communications）書面任命[437]，其職掌包含促進澳洲線上安全；管理針對澳洲未成年網路霸凌之線上申訴機制；管理成人網路濫用之線上申訴機制；管理未經同意分享之私密影像之申訴機制；管理線上內容管制框架；負責與聯邦各部門、有關當局和機構協調跟澳洲線上安全有關之活動。電子安全專員將會針對前述申訴開啟調查，並做出相應移除通知（removal notice）或違法內容之處置[438]。此外，根據本法，專員亦被賦予以下權力：

434 eSafety Commissioner, *Our structure*, https://www.esafety.gov.au/about-us/who-we-are/our-structure (last visited Dec. 14, 2023).
435 ACMA, *supra* note 429.
436 eSafety Commissioner, *supra* note 433.
437 Online Safty Act, Part 11, Sec. 167.
438 Online Safty Act, Part 2, Secs. 26 & 167.

- **資料蒐集權**：電子安全專員有權向社群媒體服務、相關電子服務或指定網路服務業者發布書面通知，要求於一定期限內提供終端用戶（end-user）之個人資訊與聯絡資訊[439]。若不遵循，則處以 100 單位之民事處罰[440]。
- **調查權**：電子安全專員得以調查為目的行使相關調查權力[441]，並發出書面通知傳喚個人，針對調查案件出示文件或回答問題[442]；或要求被傳喚者就調查案件之發言做出誓言或誓詞[443]。
- **資訊揭露**：特定情況下將揭露相關調查資訊，以履行專員職能或權力有關為目的之資訊揭露，包括向部長、ACMA 成員、特定單位等特定人士揭露[444]。

eSafety 運作之三大支柱[445]，包括「預防」：提供基於證據的安全資源和計劃；「保護」：監理架構之運作與調查濫用行為；以及「主動與系統性調整」：辨識新興風險，確保產業最小化危害。eSafety 成立至今，即以此三大支柱為核心，對抗網路危害，並在《線上安全法》之賦權下行使監理權力，以有效提升澳洲之線上安全。

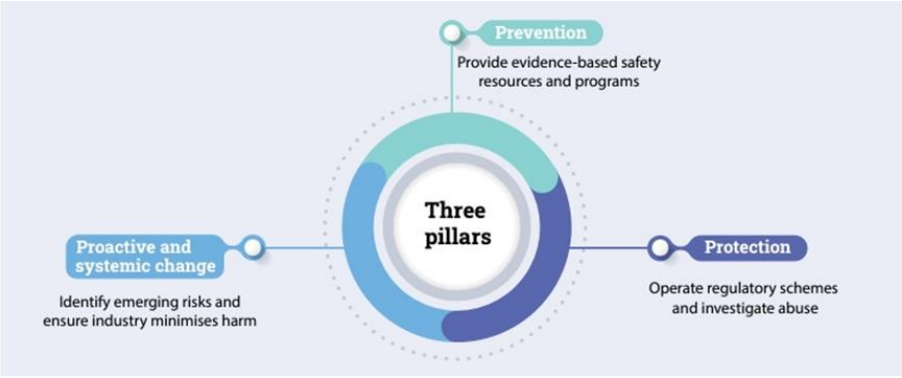


圖 3：eSafety 執行策略
資料來源：eSafety Commisssioner[446]

439 Online Safty Act, Part 13, Sec. 193.
440 Online Safty Act, Part 13, Sec. 195.
441 Online Safty Act, Part 14, Sec. 197.
442 Online Safty Act, Part 14, Sec. 199.
443 Online Safty Act, Part 14, Sec. 200.
444 Online Safty Act, Part 15, Sec. 206.
445 eSafety Commissioner, *eSafety Strategy 2019-2022*, https://www.esafety.gov.au/about-us/who-we-are/strategy (last visited Dec. 31, 2023).
446 *Id.*

（二）線上違法內容範圍與處置

1. 線上違法內容類型

（1）未成年網路霸凌內容

所謂未成年網路霸凌（cyber-bullying material targeted at an Australian child）[447]，係指於網路上（社群媒體服務、相關電子服務或指定之網路服務）針對澳洲 18 歲以下未成年人進行嚴重威脅、嚴重恐嚇、嚴重騷擾或嚴重羞辱，或其他法規所訂定之情境條件，且一般人民可合理判斷該內容可能對特定未成年人造成影響時，則可將之視為針對澳洲未成年人為標的對象之霸凌內容。

行為態樣諸如，寄送辱罵性的簡訊和電子郵件、有害的訊息、圖像或影片；在網路進行排擠與羞辱；散布令人不適的八卦和對話內容；冒名頂替；創建虛假帳戶以欺騙或羞辱某人等。

（2）成人網路暴力內容

所謂成人網路暴力（cyber-abuse material targeted at an Australian adult）[448]，係指於網路上（社群媒體服務、相關電子服務或指定之網路服務）針對年滿 18 歲或以上成年人進行威脅、騷擾或冒犯，或其他法規所訂定之情境條件，且一般人民可合理判斷該內容可能對特定成年人造成影響時，則可將之視為針對成人網路暴力內容。

行為態樣諸如，因其外貌、宗教、性別、種族、殘疾、性取向或政治信仰而受到嘲笑或羞辱；聯繫方式等個資被公開；在網上受到威脅或傷害；被網上跟踪；社交媒體、銀行或電子郵件帳戶被駭客入侵；鼓勵自殘；多次被發送淫穢訊息等。

[447] Online Safty Act, Part 1, Sec. 6.
[448] Online Safty Act, Part 1, Sec. 7.

（3）未經同意之私密影像

所謂未經同意之私密影像（non-consensual intimate image of a person）[449]，係指於網路上（社群媒體服務、相關電子服務或指定之網路服務）未經當事人同意發布私密影像。而某人發布或威脅他人散布私密影像，該行為即構成本法所指之「未經同意分享私密影像」，將處以民事處罰。

私密影像（intimate image）[450]係指無論靜態或動態之視覺影像，描繪私密部位、乳房或肛門等內容，或是從事私人活動，如裸體、使用廁所、淋浴、洗澡、從事性行為或其他類似之私人活動等內容，或是無宗教或文化意義服飾之描繪。其他解釋性條文規定，則包含無論是否為經變造之內容；或呈現某人身體部位，該內容視為描繪或可能描繪該人。

（4）違法與受限制之線上內容

違法與受限制之線上內容（illegal and restricted online content）[451]係指從極端嚴重有害之違法內容到未成年人應限制觸及之線上內容，前者像是兒童性暴力與恐怖主義行為之影像內容，後者則包含模擬性行為、裸露或具高度衝擊性之暴力內容等。

而《線上安全法》則進一步於「線上內容管制框架」（Online Content Scheme）中將此類內容分別定義為第一級內容（Class 1 material）與第二級內容（Class 2 material），保護未成年使用者免於接觸不當或有害內容。該管制框架將受管制之線上內容分成二級，第一級為宣揚恐怖主義之禁止級（Refused Classification, RC 級）之電影、出版物、遊戲等[452]；第二級為澳洲分級委員會（Australian Classification Board）歸類之色情 18 禁（X18+）、限成人觀看 18 禁（R18+）、裸露第 1 類限制（Category 1 Restricted, CAT 1）與性行為第 2 類限制（Category

[449] Online Safty Act, Part 1, Sec. 16.
[450] Online Safty Act, Part 1, Sec. 15.
[451] eSafety Commissioner, *Illegal and restricted online content*, https://www.esafety.gov.au/key-topics/Illegal-restricted-content (last visited Dec. 25, 2023).
[452] Online Safty Act, Part 9, Division 1, Sec. 106; Classification (Publications, Films and Computer Games) Act, Part 2, Division 2, Sec. 9A.

2 Restricted, CAT 2）等級之電影、出版物、遊戲等[453]。

Online Safety Act	Content	Classification Act/ National Classification Code
Class 1	Film Publication Computer game Any other material*	Refused Classification (RC)
Class 2	Film Any other material (excluding computer games)*	X18+
	Publication	Category 2 restricted
	Film Computer game Any other material*	R18+
	Publication	Category 1 restricted

*Under the Online Safety Act, material that is not a film, computer game or publication is to be classified in a corresponding way to the way in which a film would be classified.

圖 4：第一級與第二級內容分級制度

資料來源：eSafety Commissioner[454]

（5）令人憎惡之暴力內容

所謂與犯罪、暴力、恐怖主義有關之令人憎惡之暴力內容（material that depicts abhorrent violent conduct, AVM）[455]，係指宣揚恐怖主義、教唆犯罪之內容，以及由犯罪者製作的圖像、影片、錄音、紀錄等，該內容可能涉及導致嚴重傷害或死亡的行為、謀殺或謀殺未遂、酷刑、強制性交、暴力綁架或暴力威脅等[456]。

[453] Online Safty Act, Part 9, Division 1, Sec. 107; DITRDCA Australian Classification, *What do the ratings mean?*, https://www.classification.gov.au/classification-ratings/what-do-ratings-mean (last visited Aug. 14, 2023).

[454] ESAFETY COMMISSIONER, DEVELOPMENT OF INDUSTRY CODES: UNDER THE ONLINE SAFETY ACT, Position Paper, p. 19 (2021), *available at* https://www.esafety.gov.au/sites/default/files/2021-09/eSafety%20Industry%20Codes%20Position%20Paper.pdf.

[455] Online Safty Act, Part 1, Sec. 9.

[456] Criminal Code Act, Subdivision H, Sec. 474.31-474.32.

2. 線上違法內容監理與處置程序

針對上開線上違法內容之處理，《線上安全法》係設置申訴處理機制（complaints, objections and investigations）[457]，由民眾或受害人向電子安全專員進行申訴，並由專員展開調查，再做出處置決定。

電子安全專員可決定採取之措施包括：向線上服務業者發布移除通知；要求終端用戶道歉等，若違反則將對線上服務業者（如社群媒體服務業者、相關電子服務業者或指定之網路服務業者、與資訊儲存服務業者等）處以 500 單位[458]之民事處罰（civil penalty），或可針對終端用戶強制執行（如確保移除內容、道歉等）。

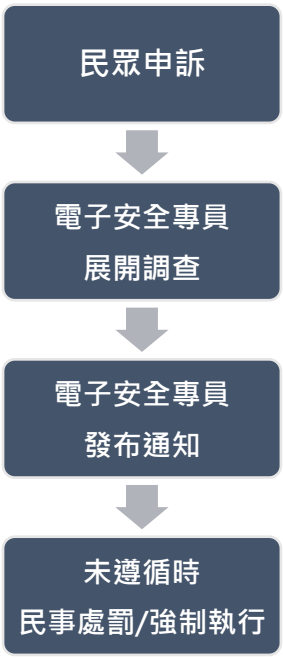


圖 5：《線上安全法》之申訴處理機制

資料來源：本研究自行整理

[457] Online Safty Act, Part 3, Division 1, Sec. 29.

[458] 每單位換算之金額係每三年調整一次，按 2023 年公布之金額，一單位為 313 澳幣，故 500 單位為 156,500 澳幣，約為新台幣 320 萬元。Crimes (Amount of Penalty Unit) Instrument 2023, Sec.5.

以下將進一步說明澳洲如何透過電子安全專員，針對本法所規範之線上違法內容進行處理。

（1）未成年網路霸凌內容之處理

當電子安全專員接獲未成年網路霸凌申訴，該申訴可能來自：合理認為網路服務曾經或正在提供網路霸凌內容之兒童、兒童之監護人、曾遭受霸凌之成年人，或向服務提供者提出申訴之網路使用者[459]，電子安全專員將啟動調查程序[460]。若認定該內容為未成年網路霸凌內容，專員有權向社群媒體服務業者、相關電子服務業者或指定之網路服務業者發出移除通知，要求移除違法內容[461]，並要求資訊儲存服務提供者停止儲存特定內容[462]。若服務提供者不遵循，則將處以 500 單位之民事處罰[463]。

另外，若該內容經申訴且為終端用戶（即訊息發布者、網路服務使用者)所發布之內容，專員即可發出終端用戶通知(end-user notice)，要求其採取一切手段避免內容繼續散布、移除與未成年人有關的違法內容，或向受害者道歉[464]。若不遵守，則依據《2014 年監理權力（標準條款）法》（Regulatory Powers (Standard Provisions) Act 2014）之強制執行規範處置之[465]。

（2）成人網路暴力內容之處理

當電子安全專員接獲成人網路暴力申訴，該申訴可能來自：合理認為網路服務曾經或正在提供網路暴力內容之成人、授權他人申訴之責任人，或向服務提供者提出申訴之網路使用者[466]，電子安全專員將啟動調查程序[467]。

---

[459] Online Safty Act, Part 3, Sec. 30.
[460] Online Safty Act, Part 3, Sec. 31.
[461] Online Safty Act, Part 5, Sec. 65.
[462] Online Safty Act, Part 5, Sec. 66.
[463] Online Safty Act, Part 5, Sec. 67.
[464] Online Safty Act, Part 5, Sec. 70.
[465] Online Safty Act, Part 5, Sec. 71; Online Safty Act, Part 10, Sec. 165.
[466] Online Safty Act, Part 3, Sec. 36.
[467] Online Safty Act, Part 3, Sec. 37.

若認定該內容為成年網路霸凌內容，專員有權向社群媒體服務業者、相關電子服務業者或指定之網路服務業者發出移除通知，要求移除違法內容[468]；亦可向張貼成人網路暴力內容之終端用戶，發布書面移除通知，要求其於發布通知之 24 小時內，採取一切手段移除該內容[469]；或向資訊儲存服務提供者發布移除通知，要求其停止儲存特定內容[470]。若前述通知對象不遵循，將處以 500 單位之民事處罰[471]。

（3）未經同意分享之私密影像之處理

未經同意分享之私密影像之申訴處理機制，如同成人網路暴力內容之程序，當電子安全專員接獲未經同意分享之私密影像之申訴時，該申訴可能來自：涉及私密影像者、或代表涉及私密影像者之他人所提出之申訴[472]，電子安全專員將啟動調查程序[473]，並發布移除通知，要求服務提供者、資訊儲存服務提供者或終端用戶，於移除通知發布之 24 小時內移除該內容[474]。若不遵循，則處以 500 單位之民事處罰[475]。

除了申訴處理機制外，涉及私密影像者、或代表涉及私密影像者之他人亦可透過拒絕散布告知（objection notice）[476]，向電子安全專員提出阻斷該私密影像於網路傳散之告知，即使原本同意分享私密影像者，亦可向專員提出，而專員則據此考量是否決定發布私密影像之移除通知[477]。

---

[468] Online Safty Act, Part 7, Sec. 88.
[469] Online Safty Act, Part 7, Sec. 89.
[470] Online Safty Act, Part 7, Sec. 90.
[471] Online Safty Act, Part 7, Sec. 91.
[472] Online Safty Act, Part 3, Sec. 32.
[473] Online Safty Act, Part 3, Sec. 34.
[474] Online Safty Act, Part 6, Secs. 77-79.
[475] Online Safty Act, Part 6, Sec. 80.
[476] Online Safty Act, Part 3, Sec. 33.
[477] Online Safty Act, Part 3, Sec. 35.

（4）違法與受限制內容之處理

當電子安全專員接獲線上違法與受限制內容之申訴，該申訴範圍可能包含：合理認為終端用戶會接觸到第一級與第二級內容之申訴、他人違反服務提供者規範之情事、或違反業界規範之情事[478]，專員會對此主動進行調查，或回應申訴而啟動調查程序[479]。

針對線上內容管制框架之內容，電子安全專員會針對不同內容級別並做出處置判斷，亦會向個別業者發布相應之處置通知[480]，如下：

A. 第一級內容

- **移除通知**

  向社群媒體服務業者、相關電子服務業者或指定之網路服務業發布移除通知，要求移除特定內容[481]；向資訊儲存服務提供者發布移除通知，要求停止儲存特定內容[482]。

- **連結移除通知（link deletion notice）**[483]

  向網路搜尋引擎業者發布連結移除通知，要求停止提供導引至特定內容之連結。

- **應用程式移除通知（app removal notice）**[484]

  向應用程式服務業者發布應用程式移除通知，要求停止讓終端用戶下載有利於在社群媒體服務、相關電子服務或指定之網路服務上發布特定內容之應用程式。

---

478 Online Safty Act, Part 3, Sec. 38-40.
479 Online Safty Act, Part 3, Sec. 42.
480 Online Safty Act, Part 9, Division 1, Sec. 105.
481 Online Safty Act, Part 9, Division 2, Sec. 109.
482 Online Safty Act, Part 9, Division 2, Sec. 110.
483 Online Safty Act, Part 9, Division 5, Sec. 124.
484 Online Safty Act, Part 9, Division 6, Sec. 128.

B. 第二級內容

- **移除通知**

  向社群媒體服務業者、相關電子服務業者或指定之網路服務業發布移除通知，要求移除特定內容[485]；向資訊儲存服務提供者發布移除通知，要求停止儲存特定內容[486]。

- **補救通知（remedial notice）**

  向社群媒體服務業者、相關電子服務業者或指定之網路服務業發布補救通知[487]，要求採取包含移除特定內容，與限制使用者造訪特定內容之限制瀏覽措施(restricted access system）[488]；向資訊儲存服務提供者發布移除通知，要求採取停止儲存特定內容與限制瀏覽措施。

若未遵守前述違法與受限制內容之處置要求（移除通知、連結移除通知、應用程式移除通知與補救通知），則將對業者處以 500 單位之民事處罰[489]。

處置方式	第一級（Class 1 material）	第二級（Class 2 material）
移除通知	✔	✔
補救通知		✔
連結移除通知	✔	
應用程式移除通知	✔	

圖 6：違法與受限制內容之處置通知

資料來源：本研究彙整

[485] Online Safty Act, Part 9, Division 3, Sec. 114.
[486] Online Safty Act, Part 9, Division 3, Sec. 115.
[487] Online Safty Act, Part 9, Division 4, Secs. 119-120.
[488] Online Safty Act, Part 9, Division 1, Sec. 108.
[489] Online Safty Act, Part 9, Division 2, Sec. 111; Online Safty Act, Part 9, Division 3, Sec. 116; Online Safty Act, Part 9, Division 4, Sec. 121; Online Safty Act, Part 9, Division 5, Sec. 125; Online Safty Act, Part 9, Division 6, 129.

（5）令人憎惡之暴力內容之處理

有關宣傳、煽動、教唆與描繪跟犯罪、暴力、恐怖主義有關之令人憎惡之暴力（AVM）內容，其處置程序與前述未成年網路霸凌、成人網路暴力、未經同意之私密影像、線上內容管制框架四大類網路內容不同，無須經過「申訴處理程序」。

電子安全專員可直接向提供網路傳輸服務之網路服務提供者（internet service provider, ISP）發出阻斷請求（blocking request）[490]或阻斷通知（blocking notice）[491]，要求業者封鎖網域（domain name）、網址（Uniform Resource Locator, URLs）或 IP 位址（IP address），阻止人民瀏覽特定網站，以防止特定人士繼續宣傳、煽動、教唆或描繪可能對澳洲民眾造成重大危害之恐怖攻擊或暴力犯罪。若違反阻斷通知，則將對業者處以 500 單位之民事處罰[492]。

《線上安全法》之網路內容監理與處置程序，綜合表整如下：

[490] Online Safty Act, Part 8, Division 2, Sec. 95.
[491] Online Safty Act, Part 8, Division 3, Sec. 99.
[492] Online Safty Act, Part 8, Division 3, Sec. 103.

表 3：《線上安全法》之網路內容監理與處置程序

違法內容	處置程序	通知對象	通知類型	處罰
未成年網路霸凌內容	➢ **申訴處理機制** 1. 民眾申訴 2. 啟動調查 3. 發出通知 4. 未遵循時民事處罰/強制執行	● 社群媒體服務業者 ● 相關電子服務業者 ● 指定之網路服務業者	移除通知：移除其服務上出現之內容	500 單位之民事處罰
		● 資訊儲存服務提供者	移除通知：停止儲存特定內容	
		● 終端用戶	終端用戶通知	強制執行（確保移除、避免發布未成年霸凌內容、為發文內容道歉）
成人網路暴力內容	➢ **申訴處理機制** 1. 民眾申訴 2. 啟動調查 3. 發出通知 4. 未遵循時民事處罰	● 社群媒體服務業者 ● 相關電子服務業者 ● 指定之網路服務業者	移除通知：移除其服務上出現之內容	500 單位之民事處罰
		● 資訊儲存服務提供者	移除通知：停止儲存特定內容	
		● 終端用戶	移除通知：移除發布之內容	
未經同意之私密影像	➢ **申訴處理機制** 1. 民眾申訴 2. 啟動調查 3. 發出通知 4. 未遵循時民事處罰	● 社群媒體服務業者 ● 相關電子服務業者 ● 指定之網路服務業者	移除通知：移除其服務上出現之內容	500 單位之民事處罰
		● 資訊儲存服務提供者	移除通知：停止儲存特定內容	
		● 終端用戶	移除通知：移除發布之內容	

	➢ **拒絕散布告知程序** 1. 民眾向專員提出拒絕散布告知 2. 專員據以決定發出通知與否			
線上內容框架之內容	➢ **申訴處理機制** 1. 民眾申訴 2. 啟動調查 3. 發出通知 4. 未遵循時民事處罰	● 社群媒體服務業者 ● 相關電子服務業者 ● 指定之網路服務業者 ● 資訊儲存服務提供者	➢ **第一級內容** 1. 移除通知 2. 連結移除通知 3. 應用程式移除通知 ➢ **第二級內容** 1. 移除通知 2. 補救通知	500 單位之民事處罰
犯罪、暴力、恐怖主義有關之令人憎惡之暴力內容	➢ **專員直接向業者發布通知**	● 網路服務提供者	1. 阻斷請求 2. 阻斷通知	500 單位之民事處罰

資料來源：本研究自行整理

（三）基礎線上安全期望與業界規範

1. 《線上安全（基礎線上安全期望）標準》

《線上安全法》針對線上違法內容除了訂有前述內容管制框架，為確保業者有效遵守相關規定並負起平臺責任，提高服務提供者之透明度與問責，在規範基礎上制訂「基礎線上安全期望」（BOSE）[493]，有關服務提供者的監理指引、如何遵守期望並回應強制性報告要求設有相關標準，並要求社群媒體服務提供者、相關電子服務業者或指定之網路服務業者向專員提交遵守線上安全期望之報告[494]，以實踐立法期望之三大原則：其一為服務提供者責任，其二為賦予用戶權力，其三為透明度與問責。

BOSE 之核心期望[495]，係期望服務提供者採取合理措施，以確保終端用戶可安全使用服務，並於決定採取措施時諮詢電子安全專員，確保減少未成年網路霸凌內容、成人網路暴力內容、未經同意之私密影像、第一級內容與令人憎惡之暴力內容，以及降低第二級內容對兒童所造成之近用影響。而服務提供者也應確保提供明確且易識別之機制，讓終端用戶能就前述內容或違反服務條款之行為，進行通報或申訴。而若電子安全專員以書面通知服務提供者，要求於指定期間提供違反服務使用條款申訴數量、移除所需時間與確保終端用戶安全使用服務之說明，則服務提供者應於通知後 30 天內遵守該要求。

2022 年 1 月，澳洲基礎建設、運輸、地區發展、通訊和藝術部（Department of Infrastructure, Transport, Regional Development, Communications and the Arts, DITRDCA）係依據《線上安全法》第 45 條制訂《線上安全（基礎線上安全期望）標準》（Online Safety (Basic Online Safety Expectations) Determination 2022，下簡稱《期望標準》）[496]，該標準對線上服務提供者規範之主要內涵如下：

---

[493] eSafety Commissioer, *Basic Online Safety Expectations*, https://www.esafety.gov.au/sites/default/files/2022-07/Basic%20Online%20Safety%20Expectations%20Table%20one%20-%20Summary%20of%20the%20Expectations%20%281%29.pdf (last visited Aug. 14, 2023).

[494] Online Safty Act, Part 4, Division 1, Sec. 44.

[495] Online Safty Act, Part 4, Division 1, Sec. 46.

[496] Australia Government, *Online Safety (Basic Online Safety Expectations) Determination 2022,*

（1）採取合理措施主動降低違法或有害內容或行為，並確保使用者可安全使用服務；

（2）避免未成年人遭受不適合觀賞內容（如色情內容）之侵害；

（3）採取合理措施防止有害使用之匿名與加密服務；

（4）建立使用者申訴機制，並明確說明其服務條款與違反處罰；

（5）與其他服務提供者合作；

（6）回應電子安全專員之資訊要求。

為協助服務提供者履行「基礎線上安全期望」所制訂之標準，電子安全專員亦公布相關指引措施[497]，該指引雖不具強制性，但線上服務提供者可以根據其服務性質，經諮詢電子安全專員，再採行合理之電子安全措施，包括：

（1）在服務的設計、開發與配置過程，進行安全風險與影響評估與安全檢測；

（2）確保針對兒童使用之服務，隱私預設機制和安全設定限制性最高之級別；

（3）與其他線上服務提供者合作偵測大量且跨平臺攻擊；

（4）納入身分認證或持有帳戶之程序；

（5）實施年齡認證機制；

（6）業者應提出採行措施報告，說明其採行措施之合理性，以及符合「基礎線上安全期望」與確保線上安全之行動。

available at: https://www.legislation.gov.au/Details/F2022L00062/Html/Text (last visited Nov. 28, 2023).

[497] eSafe Commissioner, *Basic Online Safety Expectations-reasonable steps,* https://www.esafety.gov.au/industry/basic-online-safety-expectations (last visited Aug. 14, 2023).

而電子安全專員已於 2022 年 8 月 29 日根據《線上安全法》第 56(2)條，向 Apple、Meta（和 WhatsApp）、Microsoft（和 skype）、Omegle 與 Snap 發出非定期報告通知[498]，要求前述業者概述平臺在解決兒童性剝削與虐待問題上所採取的措施。針對此次報告通知 7 家業者所收到的回覆，eSafety 已於 2022 年 12 月做成第一份透明度報告[499]，而後也持續針對其他類型之線上有害議題，向業者發布透明度報告通知。2023 年 10 月公布的透明度報告調查結果總結了 Google、Twitter（更名為 X）、TikTok、Twitch 和 Discord 的回應，包括監測與處理其服務之兒童性剝削和虐待，以及性勒索與推薦系統之安全面向所採取之措施[500]。

近年為進一步確保《線上安全法》之網路安全保護規範有效因應快速變化的網路環境（如人工智慧之迅速發展），2023 年 11 月澳洲政府即啟動《線上安全標準（基礎線上安全期望）修正案》（Online Safety (Basic Online Safety Expectations) Amendment Determination 2023）[501]之公眾諮詢[502]，試圖擴大《期望標準》所涵蓋之內容，納入確保兒童使用權益之服務、關注人工智慧帶來之違法或有害問題、監測並解決違反服務使用條款之仇恨言論，以及定期發布透明度報告等項目。DITRDCA 提出公眾諮詢之期望修正版本主要聚焦以下主題[503]：

---

[498] ESAFETY COMMISSSIONER, ESAFETY ISSUES FIRST BASIC ONLINE SAFETY EXPECTATIONS NOTICES, *available at* https://www.esafety.gov.au/sites/default/files/2022-08/Basic%20Online%20Safety%20Expectations%20first%20notices_0.pdf.

[499] ESAFETY COMMISSSIONER, *BASIC ONLINE SAFETY EXPECTATIONS-SUMMARY OF INDUSTRY RESPONSES TO THE FIRST MANDATORY TRANSPARENCY NOTICES* (December 2022), *available at* https://www.esafety.gov.au/sites/default/files/2022-12/BOSE%20transparency%20report%20Dec%202022.pdf.

[500] eSafety Commisssioner, *Responses to transparency notices-Online service providers are required to report on how they are implementing the Basic Online Safety Expectations set out by the Australian Government,* https://www.esafety.gov.au/industry/basic-online-safety-expectations/responses-to-transparency-notices (last visited Aug. 14, 2023).

[501] DITRDCA, *Albanese Government takes major steps forward to improve online safety (Nov. 2023),* https://minister.infrastructure.gov.au/rowland/media-release/albanese-government-takes-major-steps-forward-improve-online-safety (last visited Nov. 28 2023).

[502] Australia Government, *Online Safety (Basic Online Safety Expectations) Amendment Determination 2023,* https://www.infrastructure.gov.au/have-your-say/online-safety-basic-online-safety-expectations-amendment-determination-2023 (last visited Nov. 28, 2023).

[503] DITRDCA, *Online Safety (Basic Online Safety Expectations) Amendment Determination 2023,* https://www.infrastructure.gov.au/department/media/publications/online-safety-basic-online-safety-expectations-amendment-determination-2023 (last visited Dec. 31, 2023).

- 生成式人工智慧、推薦系統與使用者控制；
- 保障兒童的最大利益，並限制其在線上接觸不適合觀賞的內容；
- 商業與資源決策之安全影響；
- 線上仇恨言論；
- 透明度；
- 使用條款之執行；
- BOSE 標準之具體化與改進措施。

《期望標準》之修正提案現已進入公眾諮詢階段，未來將於 2024 年 2 月 16 日關閉諮詢，也將進一步提出修正報告。

2. 線上內容管制框架之業界規範與業界準則

根據《線上安全法》之線上內容管制框架規定[504]，為監管有害之線上內容，產業協會應主動制定業界規範（industry code），並由電子安全專員將該規範進行登記；而在特定情況下，電子安全專員亦可自行就有害線上內容制定業界準則（industry standard）。因此在本法通過後，澳洲之電子安全專員便逐步針對線上內容管制徵詢相關產業機構之意見，使其規範框架更加符合實際產業需求，透過與業界共同建立之規範作為《線上安全法》之監理基礎，以由下而上的方式確保網路環境符合線上安全之立法期待。

（1）業界規範之制定

根據《線上安全法》第 140 條，業界規範之產生，係由代表線上產業之特定機構或協會主動制定。該規範需適用於行業本身，內容涵蓋一或多項線上活動，且應就該線上活動制定妥適之處理或保障方式。而就產生程序而言，業界規範之草案需經電子安全專員確認、進行公眾諮詢並考量產業參與者提供之諮詢意見，才會由 eSafety 進行登記並於網路公告。

[504] Online Safety Act, Part 9, Division 7.

eSafety 也得透過書面通知之方式，要求代表線上產業之特定機構或協會制定業界規範[505]。業界規範完成登記後，eSafety 得向違反該規範者發出書面通知或正式警告，不遵循則處以民事處罰[506]。

另一方面，在法定的特殊情況下，eSafety 也得自行就有害線上內容制定業界準則[507]，包括：產業機構或協會未遵守 eSafety 提出制定業界規範之要求；產業機構或協會所制定之規範草案並未包含適當的保障措施、不符合目標的達成，以致 eSafety 拒絕其登記；eSafety 發布要求制訂業界規範通知後，期限內未出現任何相關機構或單位；業界規範已登記至少 180 天，但 eSafety 認定該規範並不充分等。此處之「不充分」係指：該規範未就線上活動相關之事項提供恰當的社群保障，或未適當管理該產業部門之參與者[508]。

（2）業界規範發展現況

2021 年 9 月，電子安全專員發布業界規範立場文書（industry code position paper）[509]，協助網路產業制定業界規範，並於 2022 年 4 月 11 日正式發布通知要求業界制定相關規範。

其中，六大產業協會所組成的指導小組，將負起監督網路八大領域之規範制定。

參與指導小組的六大產業協會如下[510]：澳洲行動電信協會（Australian Mobile Telecommunications Association）、商業軟體聯盟（BSA The Software Alliance）、通訊聯盟（Communications Alliance）、消費者電子供應商協會（Consumer Electronics Suppliers' Association）、數位產業協會（Digital Industry Group Inc.）、互動遊戲與娛樂協會（Interactive Games and Entertainment Association）。

---

505 Online Safty Act, Part 9, Division 7, Sec. 141.
506 Online Safty Act, Part 9, Division 7, Sec. 143-144.
507 Online Safty Act, Part 9, Division 7, Sec. 145(1).
508 Online Safty Act, Part 9, Division 7, Sec. 145(1A).
509 ESAFETY COMMISSIONER, DEVELOPMENT OF INDUSTRY CODES UNDER THE ONLINE SAFETY ACT-POSITION PAPER, September 2021, *available at* https://www.esafety.gov.au/sites/default/files/2021-09/eSafety%20Industry%20Codes%20Position%20Paper.pdf.
510 eSafety Commissioner, *Industry codes and standards*, https://www.esafety.gov.au/industry/codes (last visited Dec. 31, 2023).

而應遵守產業規範之網路八大領域分別為[511]：一、社群媒體平臺；二、電子訊息服務；三、搜尋引擎；四、應用程式服務；五、網路服務提供者；六、資訊儲存服務提供者；七、接取網路服務設備之製造商與供應商，以及八、安裝與維護設備業者。

業界規範立場文書為產業界提供規範起草之基礎，電子安全專員也於起草過程中與產業協會有密切合作並提出反饋與替代方案，其中，六大產業協會已於 2023 年 2 月發布第一級業界規範草案[512]，eSafety 也於同年 6 月正式登記 5 項規範[513]，包括社群媒體服務規範（如 Facebook、Instagram、TikTok）、應用程式服務規範（如 Apple IOS 和 Google Play 商店）、資訊儲存服務規範（如 Amazon Web Services、NetDC）、接取網路服務規範（如 Telstra、iiNet、Optus、TPG Telecom、Aussie Broadband）與安裝與維護設備規範（如數據機、智慧電視、電話、平板電腦、智慧家居設備、電子閱讀器等）。

另外，eSafety 曾保留對搜尋引擎規範之登記[514]，而後納入生成式人工智慧規範內涵後，才於 2023 年 9 月 12 日正式登記第 6 項搜尋引擎服務規範。

前述 6 項服務規範將於 6 個月後（分別為 2023 年 12 月 16 日、2024 年 3 月 12 日）正式生效[515]。

另外，eSafety 針對其中兩項服務規範以未提出適當的社群保護措施為由拒絕登記，分別為相關電子服務規範（包括電子訊息服務（如 SMS、MMS）、電子郵件、視訊和線上遊戲服務（如 Gmail、WhatsApp）等服務），以及指定網路服務規範（包括網站及終端用戶之儲存與分享服務，如 Dropbox、Google Drive）。故 eSatey 將著手針對此二服務

---

[511] *Id.*

[512] AMTA, BSA, CA, CESA, DIGI & IGEA, REQUEST FOR REGISTRATION OF ONLINE SAFETY CODES (2023), *available at* https://onlinesafety.org.au/wp-content/uploads/2023/04/230331_Request-for-registration-of-revised-Codes_FINAL.pdf.

[513] AMTA, BSA, CA, CESA, DIGI & IGEA, *Online Safety Codes*, https://onlinesafety.org.au/ (last visited Aug. 14 2023).

[514] *Id.*

[515] eSafety Commissioner, Register of industry codes and industry standards for online safety, https://www.esafety.gov.au/industry/codes/register-online-industry-codes-standards (last visited Dec. 31, 2023).

制定強制性業界準則（industry standard）並交付公眾諮詢，而六大產業協會也需確保相關替代方案仍能達成《線上安全法》之政策意義，以共同建立完善且強而有力的業界規範。

3. 小結

整體而言，「基礎線上安全期望」適用於各類線上服務，包括社群媒體服務提供者、相關電子服務業者或指定之網路服務業者，並提供線上服務提供者一套可依循之標準，要求業者主動採取合理措施以最大程度減少本法所規範之各類違法內容，如網路霸凌、暴力和其他有害活動與內容等，以及提供用戶明確且易遵循之申訴途徑，進而保護其用戶之線上使用安全。而 eSafety 則可依據 DITRDCA 制定之《期望標準》，有權要求線上服務提供者提出相應報告，一旦違反相關義務將處以民事處罰，或由 eSafety 公布業者名單。

此外，本法要求八大線上產業須針對線上內容管制框架之第一級與第二級內容，自行制定具強制力之業界規範，該規範經 eSafety 登記後，業者可主動偵測與移除違法內容。當線上服務提供者無法就規範達成協議時，或者所制定之規範不包含適當的保障時，eSafety 將為該產業制定業界準則。換言之，澳洲線上服務監理之共管模式，在於透過產業協會與業者協議，加上 eSafey 共同監督推動所制定之業界規範或業界準則，且該規範具強制力，若不遵守則將對業者進行處罰。

而有關內容管制框架之第一級與第二級內容，其監理層次如下圖金字塔模型所示，eSafey 的正式監理權是以共管的業界規範為基礎，並且立基於「基礎線上安全期望」中對於線上內容與活動之政府監理上，因此除了業界規範或業界標準與線上內容監理架構之規定外，亦可能透過《期望標準》解決有關第一級與第二級線上違法內容所衍生之問題。

在監理目的上，「基礎線上安全期望」是為了讓服務提供者承擔更大的責任，以確保他們向澳洲用戶提供更安全的服務，而業界規範則在確保第一級與第二級內容受到限制，或避免出現在澳洲用戶可造訪之線上服務上。而「基礎線上安全期望」與業界規範確實存在重疊

的可能性，故 eSafety 在業界規範的設計係建立在「基礎線上安全期望」基礎之上，業者在遵守業界規範的同時，也能達到《線上安全法》的核心目標。

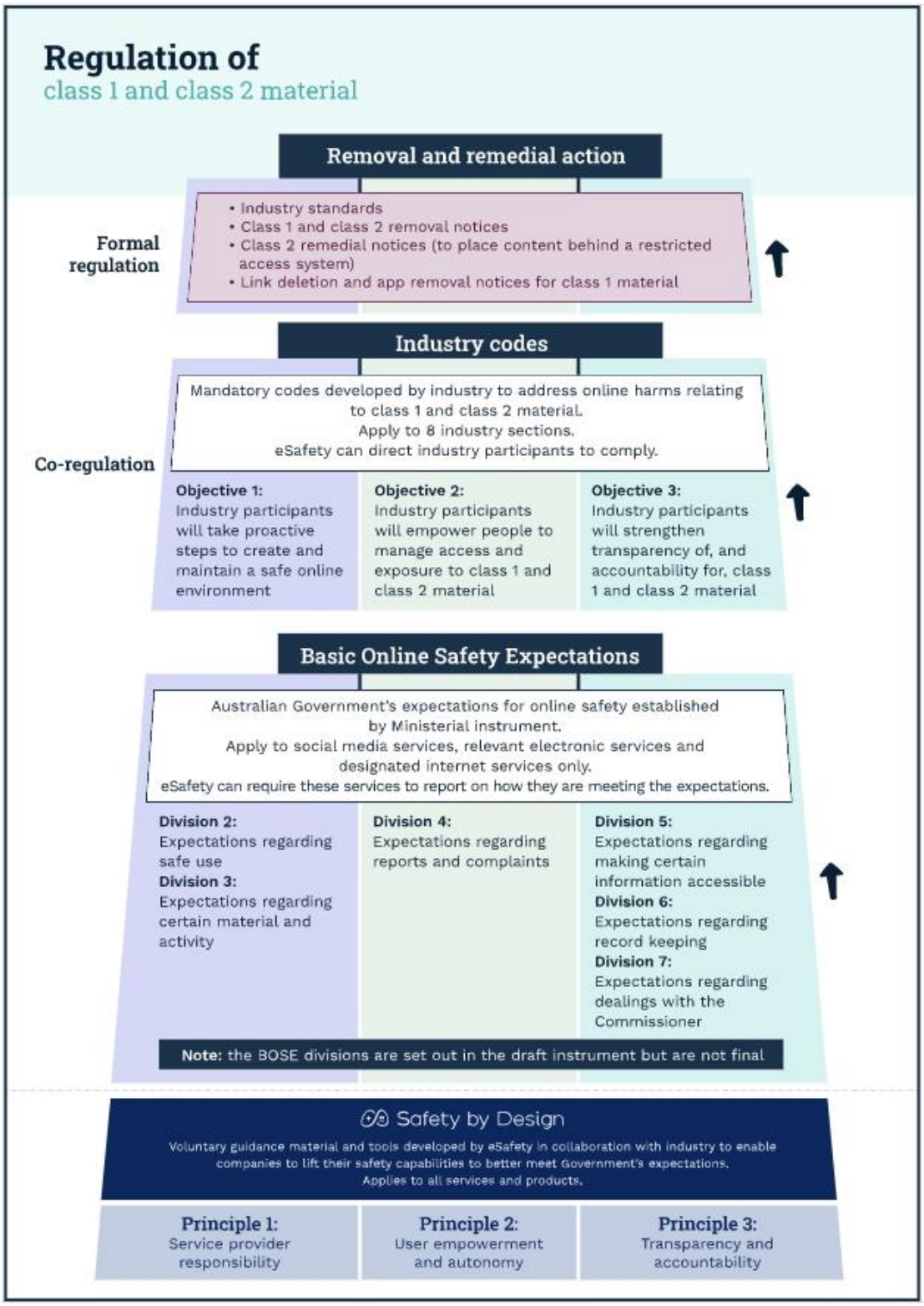


圖 7：eSafety 業界規範立場文件之線上安全規範

資料來源：eSafetyCommisssioner[516]

三、第三方監督或產業自律機制

為響應 ACCC 於 DPI 提出之政策建議與 ACMA 對於不實內容監管的立場，2021 年 2 月 22 日，澳洲數位產業集團（Digital Industry Group Inc., DIGI）發布了《澳洲不實與錯誤訊息行為準則》（Australian Code of Practice on Disinformation and Misinfromation, ACPDM）[517]，該準則之制定係奠基於 2020 年 6 月 ACMA 提出之「澳洲數位平臺錯誤訊息與新聞品質準則」，如下表整理之立場方向[518]：

表 4：「澳洲數位平臺錯誤訊息與新聞品質準則」規劃方向

立場	說明
一	ACMA 希望建立一個單一且全新聞業通用之準則，為澳洲數位平臺用戶提供適當的保護和補救措施。該準則將以消費者保護為中心，以易於公眾近用的方式呈現。
二	ACMA 期望該準則能夠解決所有類型的新聞和資訊（包括廣告和贊助內容）中的錯誤訊息，這些資訊具有公共或半公共性質，透過數位平臺傳遞，並有可能造成傷害。並期望準則能夠涵蓋考量平臺上之優質新聞資訊構成來源，以及對消費者傳播模式。
三	ACMA 期望該準則將涵蓋線上搜尋引擎、社群媒體平臺和其他在澳洲具有重要影響力的數位內容匯流服務。ACMA 將鼓勵所有平臺加入簽署準則規範。

資料來源：ACMA[519]，本研究整理繪製

此為第三方非營利數位產業協會 DIGI 發起之自律準則，要求所有簽署方承諾處理有關其服務的不實和錯誤訊息，且要求業者承諾發布年度透明度報告，並說明其在準則下所做之努力，以保障民主與公

[516] eSafety Commissioner, *The industry codes and standards environment*, https://www.esafety.gov.au/industry/codes#the-industry-codes-and-standards-environment (last visited Dec. 31, 2023).
[517] DIGI, *supra* note 424.
[518] ACMA, *supra* note 422, at 20-22.
[519] *Id.*

共利益[520]。參與簽署方包含 Adobe, Apple、Facebook、Google、Microsoft、Redbubble、TikTok 以及 Twitter（更名為 X）等平臺業者[521]。

2021 年 10 月，DIGI 引入治理委員會（Governance Committees）之獨立監督機制，組成專家小組負責解決簽署方違反準則之申訴、監督業者義務履行，以及年度透明報告之查核，並提供公眾舉報違反承諾之投訴機制，以強化準則之實踐[522]。

圖 8：《澳洲不實與錯誤訊息行為準則》之治理委員會

資料來源：DIGI[523]

[520] DIGI, *DISINFORMATION CODE*, https://digi.org.au/disinformation-code/ (last visited Aug. 14, 2023).
[521] *Id.*
[522] DIGI, *GOVERNANCE OF THE CODE*, https://digi.org.au/disinformation-code/governance/ (last visited Aug. 14, 2023).
[523] *Id.*

而後 2022 年 6 月，DIGI 啟動「2022 年準則審查」（2022 Code Review），蒐集公眾諮詢意見後，於 2022 年 12 月發布更新版之《澳洲不實與錯誤訊息行為準則》[524]。此次引入獨立評估機制與最佳透明度報告實踐指引，進一步改進透明度報告之實踐要求[525]。

（一）2022 年澳洲不實與錯誤訊息行為準則

2022 年更新版行為準則之原則與內涵整理如下[526]：

1. 保障言論自由：如果內容並未違法，則簽署方不應受到政府或它人強迫刪除內容。
2. 保護隱私：簽署方不應為解決虛假或錯誤訊息，而侵犯消費者之隱私。
3. 廣告投放政策和流程確立：簽署方應制定合宜的廣告投放與分潤政策，避免助長不實或錯誤訊息傳播。
4. 賦予用戶（消費者）權力：簽署方應賦予用戶資訊來源的知情權。
5. 確保服務與產品之完整和安全性：簽署方應確保服務與產品之完整和安全，採取禁止、監測或其他行動來避免不受信任之帳號製造與傳播不實或錯誤訊息。
6. 支持獨立研究：簽署方應支持相關之獨立性學術研究，以了解發展趨勢與應對虛假或錯誤訊息之技巧與方法。
7. 不影響其他法規：本準則不影響其他相關法規之適用。

[524] DIGI, *supra* note 424.
[525] DIGI, 2022 CODE REVIEW, https://digi.org.au/disinformation-code/code-review/ (last visited Aug.14, 2023).
[526] DIGI, *supra* note 525, at 4-5.

表 5：不實與錯誤訊息行為準則目標與對應作法

目標	對應措施例示
針對可能出現的危害提供保障措施	建立事實查核機制、標記可疑內容、降低排名、移除內容、通知或警告用戶、發展識別可疑內容之技術
降低不實與錯誤訊息之廣告與金流誘因	與第三方驗證公司合作、協助廣告商評估廣告投放之位置及其商譽風險、與廣告商共同改進廣告生態系
確保數位平臺傳輸之服務與產品之完整性與安全性	管理或封鎖假帳號與機器人帳號
讓使用者更了解內容來源與提供替代選擇	使用戶能夠選擇可靠的消息來源，或透過不同的來源來驗證事實、建立投訴機制、可靠來源優先排名
提高公眾對政治廣告之認識	提升政治廣告之透明度、讓用戶了解該廣告是否針對特定群體
加強公眾對不實與錯誤訊息之認識和支持獨立研究	資助與鼓勵研究，歡迎研究人員取得相關研究用之資料
公開透明打擊不實與錯誤訊息之措施	對外公開所採取的措施，例如相關承諾文件、倡議、白皮書、透明度報告

資料來源：DIGI[527]，本研究自行整理

ACMA 作為 ACPDM 之政府監督角色，長期與 DIGI、簽署方合作，包含評估簽署方提交之透明度報告、檢查簽署方處理用戶申訴之方式，以及鼓勵更多平臺簽署該準則等。ACMA 亦於 2023 年 7 月，針對 2022 年更新版行為準則提出第二份建議報告，本研究歸納以下相關建議與發現[528]，藉以進一步理解未來 ACPDM 可能持續精進之方向：

[527] DIGI, *supra* note 525, at APPENDIX 1, 23-29.
[528] ACMA, *ACMA releases disinformation report*, (2023/07/25), https://www.acma.gov.au/articles/2023-07/acma-releases-disinformation-report (last visited Dec. 31, 2023).

1. 業界需採取進一步措施，來檢視準則適用範圍及其適應技術和服務變化（如生成式人工智慧）之能力；
2. 應改進簽署方報告其行為準則的方式，以評估簽署方達成準則目標之實際進展；
3. 應儘速提升平臺採取措施之有效性與透明度。

最後，儘管此修訂版本確實解決了一些因應科技迫切問題，包括調整危害定義、調整透明度報告要求等，但 ACMA 針對數位平臺所做之有害內容申訴研究[529]，結果亦清楚顯示，澳洲數位平臺用戶願意申訴於數位平臺接觸之有害內容，但普遍並不滿意平臺的回應。

（二）政府與產業自律機制之實踐

為進一步解決錯誤訊息和虛假訊息對澳洲民主、社會和經濟帶來的威脅，2023 年 1 月，通訊部長宣布推出新法並賦予 ACMA 獨立監理之責，強化打擊線上不實與錯誤訊息之效[530]。也一併回應過去 ACMA 於 2021 年 6 月發布之「數位平臺虛假訊息與新聞品質措施之充分性報告」[531]，該報告提出了 5 項建議和 48 項發現，內容涉及自願性規範、其制定過程、簽署方之表現，以及澳大利亞錯誤訊息和虛假訊息環境等綜合內容，其中，報告第 3 項與第 4 項建議，即提出應擴大 ACMA 職權打擊在線上有害之錯誤訊息和虛假訊息。

[529] ACMA, *Report on digital platforms' efforts under the Australian Code of Practice on Disinformation and Misinformation*, https://www.acma.gov.au/report-digital-platforms-efforts-under-australian-code-practice-disinformation-and-misinformation (last visited Dec. 31, 2023).

[530] Exposure Draft Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023, *available at* https://www.infrastructure.gov.au/sites/default/files/documents/communications-legislation-amendment-combatting-misinformation-and-disinformation-bill2023-june2023.pdf.

[531] ACMA, A REPORT TO GOVERNMENT ON THE ADEQUACY OF DIGITAL PLATFORMS' DISINFORMATION AND NEWS QUALITY MEASURES (2021), *available at* https://www.acma.gov.au/sites/default/files/2021-11/Adequacy%20of%20digital%20platforms%20disinformation%20and%20news%20quality%20measures.pdf.

因此 2023 年 6 月 25 日，澳洲政府啟動《2023 年通訊法（就打擊不實與錯誤訊息）修正案》之公眾諮詢[532]，該草案將賦予 ACMA 打擊網路錯誤訊息與不實訊息之權力，要求數位平臺承擔相應責任，以強化打擊澳洲有害之錯誤訊息與虛假訊息的力道。草案內容大致如下[533]：

1. ACMA 能向數位平臺提供者蒐集資料，或要求平臺保留錯誤訊息與不實訊息之特定紀錄；
2. ACMA 能要求產業制定一套 ACMA 可登記與執行之行為準則（code of practice），訂定打擊數位平臺錯誤訊息與不實訊息之措施；
3. 若該行為準則無法有效打擊錯誤訊息與不實訊息，則允許 ACMA 制定並執行產業標準（更強而有力的監管形式）。

但 ACMA 無權要求數位平臺移除特定文章或貼文，其權力僅限於強化既有 ACPDM 之自律規範架構，將該準則之適用擴大至非簽署方之平臺服務[534]。

而該法案則提供一套循序漸進的方式，在自律規範架構無法有效解決線上問題時，保留 ACMA 採取行動之權力[535]。運作方式為，ACMA 有權要求產業制定新的規範（code），該規範將於登記後具有強制力；若業界未能制定規範或該規範無法保護澳洲線上安全時，作為最後手段，ACMA 可制定具更高強制執行力之業界標準（standard），要求業者遵守相關規範。

---

532 Australia Government DITRDCA, *New ACMA powers to combat misinformation and disinformation*, https://www.infrastructure.gov.au/have-your-say/new-acma-powers-combat-misinformation-and-disinformation (last visited Aug. 14, 2023).

533 *Id.*

534 *Id.*

535 Australia Government DITRDCA, *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023 Guidance Note*, (2023/07/24), https://www.infrastructure.gov.au/department/media/publications/communications-legislation-amendment-combatting-misinformation-and-disinformation-bill-2023-guidance (last visited Dec. 31, 2023).

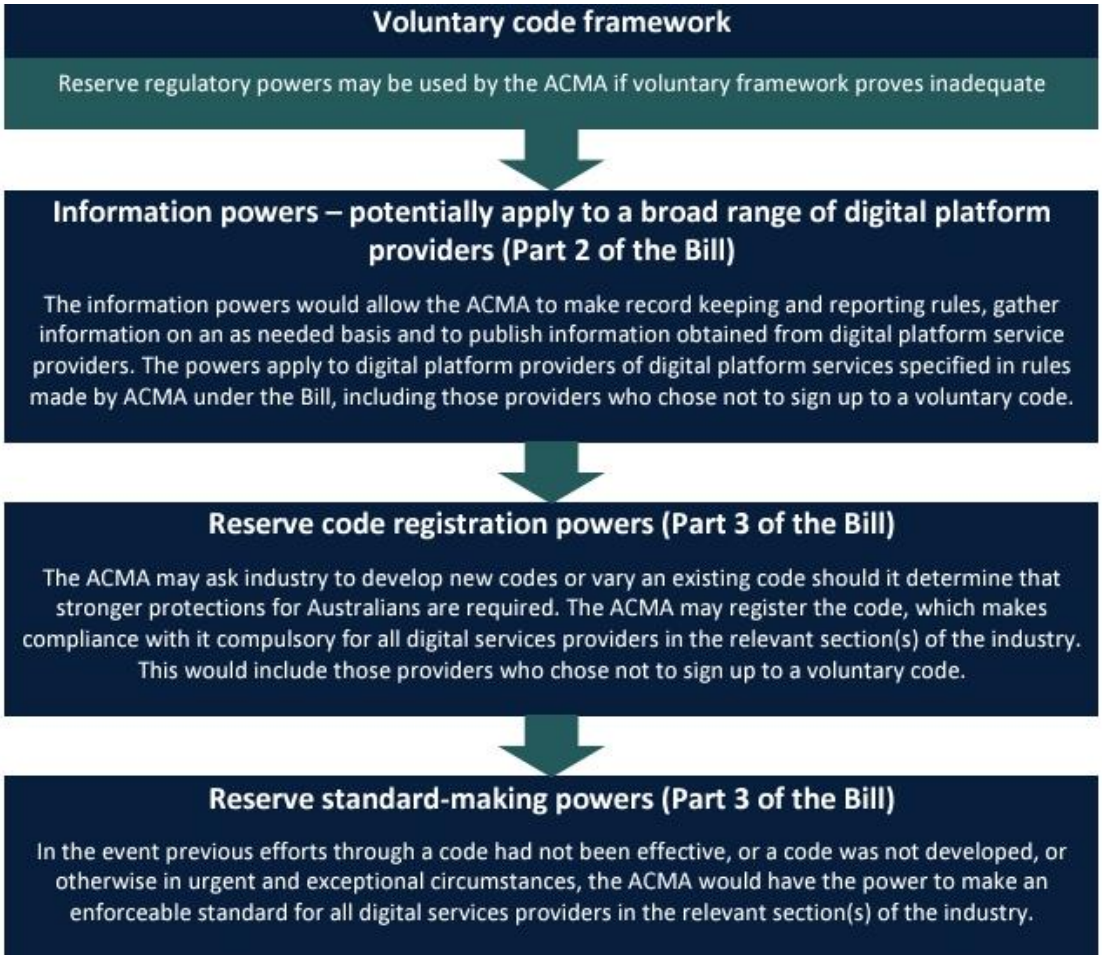


圖 9：打擊錯誤訊息和虛假訊息之 ACMA 權力行使

資料來源：DITRDCA[536]

公眾諮詢已於 2023 年 8 月 20 日結束，針對該修正案的相關意見反饋與評論主要可分為六大面向[537]，包含言論自由為民主社會基礎、反對政府對線上言論自由進行審查、錯誤訊息與虛假訊息定義模糊、政府授權內容之不對稱管制(即排除政府授權內容於審查機制之外)、反對政府作為真理之仲裁者、對錯誤與虛假訊息之限制排除「專業新聞內容」存疑、政府執法與處罰之比例性與公平性存疑。

536 *Id.*

537 Australia Government DITRDCA, *New ACMA powers to combat misinformation and disinformation-Comments on the draft Bill*, https://www.infrastructure.gov.au/have-your-say/new-acma-powers-combat-misinformation-and-disinformation (last visited Dec. 31, 2023).

整體而言，大部分意見認為應審慎對待擬議之立法，但仍對政府打擊線上錯誤、虛假訊息之努力予以肯定。澳洲後續是否將進一步研議立法，或以其他行政作為處理線上錯誤與不實訊息仍值得持續觀察。

四、小結

澳洲政府透過《線上安全法》以較為整全性之立法模式，賦予電子安全專員執法與調查權力，要求數位平臺負起相應責任，以保障澳洲用戶之線上使用安全。該法不僅對違法內容訂有明確定義，也為電子安全專員建立起與業界合作之基礎，使其可透過共管模式輔助業界制定因應產業變化之業界規範，據以支撐其執法力量，並以單一立法處理網路內容危害議題，以保護使用者不受違法內容之侵害。

而有關澳洲數位產業自律機制，則源於澳洲政府單位 ACCC 與 ACMA 對網路資訊之重視，從 2019 年發布之 DPI 產業調查報告，要求業界制定自律行為準則，再到數位產業協會 DIGI 制定《澳洲不實與錯誤訊息行為準則》，係由業者自行承諾簽署並履行義務，並透過第三方獨立機構之監督與執行，以公私協力之模式強化數位產業之自律實踐，降低網路不實與錯誤訊息之危害。此外，DIGI 也廣納各方意見（包含 ACMA 之政府監督報告、簽署方、公眾諮詢之意見等）調整既有行為準則，並於 2022 年 12 月發布更新版之《澳洲不實與錯誤訊息行為準則》，引入獨立評估機制與透明度實踐指引，以因應新興科技之發展（如生成式 AI 的出現），並不斷適應網路技術與服務之變化所帶來的線上風險。

儘管澳洲政府仍對產業自律實踐存有疑義，希望透過訂定新法擴大 ACMA 對平臺監督之責，並於 2023 上半年度推出之《2023 年通訊法（就打擊不實與錯誤訊息）修正案》進一步強化打擊線上不實與錯誤訊息之力道，管制未加入簽署準則之業者與違反網路義務之平臺，但 2023 年底公眾諮詢之結果顯示，民眾對該法仍存有政府干預線上言論自由之疑慮，故後續立法進展仍待觀察。

第八節　紐西蘭

一、監理脈絡

紐西蘭整體網路監理可從內政部建立之數位安全小組（Digital Safety Group）所執行之數位安全工作窺知一二。數位安全小組由多個團隊組成，致力解決紐西蘭網路危害之四大問題，包括兒童性剝削、有害數位訊息（如分享垃圾郵件、詐騙和非法內容等）、數位極端暴力主義，以及紐西蘭內容分級[538]，該小組透過建立企業與個人申訴機制，執行相關案件調查並在必要時採取行動[539]。

數位安全小組之工作，大致包含：一、負責 1993 年《電影和出版物分類法》（The Films Videos and Publications Classification Act, FVPCA）[540]與 2007 年《未經請求之垃圾郵件法》（The Unsolicited Electronic Messages Act, UEMA）[541]之執法，處理前述網路危害問題；二、確保商業隨選視訊服務提供者（Commercial Video On-Demand, CVoD）於平臺上使用正確分級標示[542]；三、提供企業有關垃圾郵件之法律依循規範[543]；四、管理數位兒童性剝削過濾系統（Digital Child Exploitation Filtering System, DCEFS）[544]。數位安全小組之成立也期待透過與國內外機構合作，促進與產業界之聯繫，進而以多方治理之策略，確保網路使用安全。

---

538 Te Tari Taiwhenua-Department of Internal Affairs, *About the Digital Safety Group*, https://www.dia.govt.nz/About-the-Digital-Safety-Group (last visited Aug. 14, 2023).

539 Te Tari Taiwhenua-Department of Internal Affairs, *Report harmful online content*, https://www.dia.govt.nz/Digital-Safety-Report-harmful-online-content (last visited Aug. 14, 2023).

540 Parliamentary Counsel Office, *Films, Videos, and Publications Classification Act 1993*, Version as at 12 April 2022, https://www.legislation.govt.nz/act/public/1993/0094/latest/DLM312895.html (last visited Aug. 14, 2023).

541 Parliamentary Counsel Office, *Unsolicited Electronic Messages Act 2007*, Version as at 28 October 2021, https://www.legislation.govt.nz/act/public/2007/0007/latest/DLM405134.html (last visited Aug. 14, 2023).

542 Te Tari Taiwhenua-Department of Internal Affairs, *Classification in New Zealand*, https://www.dia.govt.nz/Commercial-video-on-demand-classification (last visited Aug. 14, 2023).

543 Te Tari Taiwhenua-Department of Internal Affairs, *Spam Prevention & Messaging Compliance*, https://www.dia.govt.nz/Spam (last visited Aug. 14, 2023).

544 Te Tari Taiwhenua-Department of Internal Affairs, *Internet and website filter*, https://www.dia.govt.nz/digital-child-exploitation-DCEFS (last visited Aug. 14, 2023).

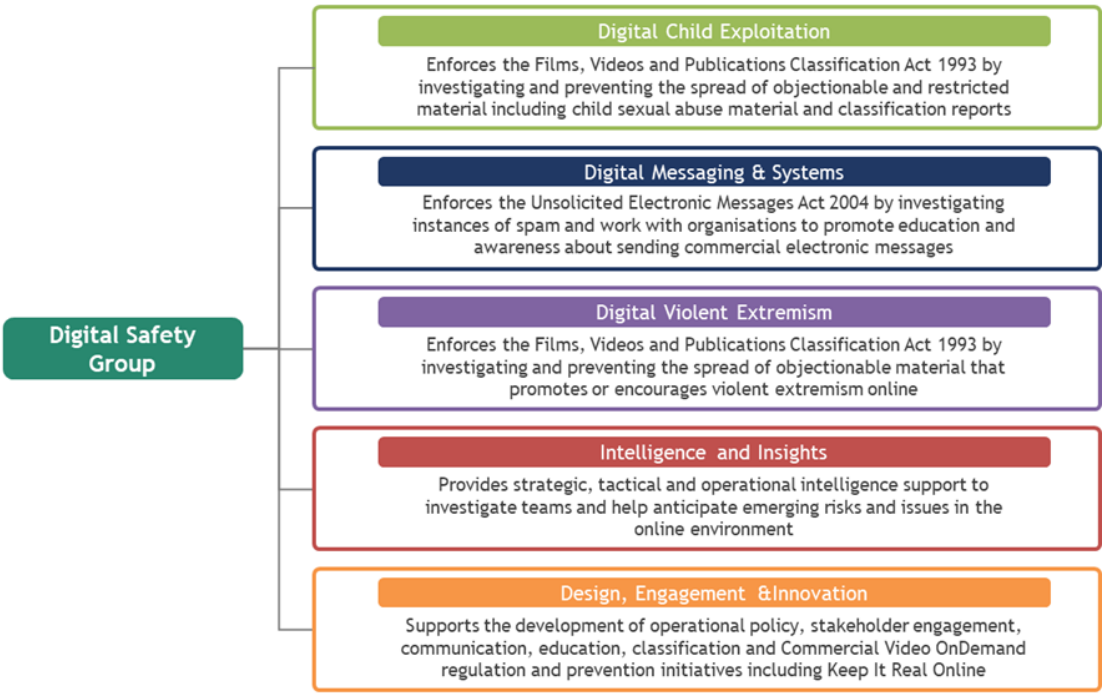


圖 10：紐西蘭數位安全小組工作綜覽

資料來源：Te Tari Taiwhenua-Department of Internal Affairs[545]

除了前述紐西蘭政府對網路安全之監理作為外，有鑑於網路霸凌、騷擾、恐嚇等情事日益嚴重，紐西蘭於 2012 年便開始關切電子通訊行為對個人造成之危害，並於當時的部長政策文件（Ministerial Briefing Paper）中提出《新媒體電子通訊》草案（Communications (New Media) Bill）[546]之立法期待，於此便展開了為期三年的立法程序，試圖針對數位通訊上之有害活動與犯罪行為提出解決與補救辦法[547]。後續正式更名為《有害數位通訊傳播法》（Harmful Digital Communications Act, HDCA）[548]，該法奠定紐西蘭在網路活動的處理模式並延續至今，因此以下將側重《有害數位通訊傳播法》之法制內涵，說明紐西蘭對於網路有害內容與平臺之監理政策與規範模式。

545 Te Tari Taiwhenua-Department of Internal Affairs, *supra* note 538.

546 PARLIAMENTARY COUNSEL OFFICE, COMMUNICATIONS (NEW MEDIA) BILL, *available at* https://www.lawcom.govt.nz/sites/default/files/publicationAttachments/communications_new_media_bill.pdf.

547 Post, S.. NZWLJ, Harmful Digital Communications Act 2015, 2017, 1, 208.

548 New Zealand Government-Parliamentary Council Office, *Harmful Digital Communications Act 2015*, https://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html#DLM5711814 (last visited Aug. 14, 2023).

二、政府機關法制政策作為

紐西蘭於 2015 年 7 月通過《有害數位通訊傳播法》（Harmful Digital Communications Act, HDCA），旨在預防、避免或降低數位通訊（digital communications）對個人造成的傷害，並提供受害者快速且有效之補救措施，以減少線上霸凌、數位騷擾、色情報復（revenge porn）或其他形式之虐待與恐嚇之影響。例如，傳送或發布具威脅性或攻擊性之訊息，散布有辱人格之謠言、令人不安之照片，並騷擾和恐嚇他人等。

本法之數位通訊，係指任何形式之電子通訊，包含文本訊息、文字、照片、圖片、錄音或其他以電子傳送內容；而傷害，則係指造成嚴重情緒困擾[549]。並於本法羅列十大通訊守則（communication principles）[550]，如下：

1. 數位通訊不應披露攸關個人之敏感事實；
2. 數位通訊不應出現威脅性、恐嚇性或威嚇性之內容；
3. 數位通訊不應極度冒犯易受影響之理性自然人；
4. 數位通訊不應具有不雅或淫穢之內容；
5. 數位通訊不應用以騷擾個人；
6. 數位通訊不應捏造不實指控；
7. 數位通訊不應包含違反保密規定而發布之事項；
8. 數位通訊不應煽動或誘使任何人向他人傳送造成傷害之訊息；
9. 數位通訊不應煽動或鼓勵個人自殺；
10. 數位通訊不應因膚色、種族、族群、血統、宗教、性別、性向或殘疾而詆毀他人。

[549] Harmful Digital Communications Act 2015, Part 1, Subpart 1, Sec. 4.
[550] Harmful Digital Communications Act 2015, Part 1, Subpart 1, Sec. 6.

紐西蘭總督可依據司法部長建議命令核准任何個人、組織、部門或官方實體作為執行本法之認證機構（approved agency）[551]，該機構之職權包含接收與評估數位通訊對個人造成傷害之申訴、調查申訴，以及處理解決申訴問題，並維繫與國內外服務提供者、線上內容資訊儲存服務提供者（online content hosts）與代理機構之關係，提供有關線上安全和網路行為政策教育與建議，並履行本法命令之職能[552]。

其中，NetSafe 為紐西蘭政府依據本法授權之認證機構，得依法行使相關權力[553]。且 Netsafe 有責任協助解決涉嫌違反十大通訊原則之行為，其實務作為如下[554]：

- 與國內外網站資訊儲存服務提供者（website hosts）、網路服務提供者和其他內容資訊儲存服務提供者（content hosts）聯絡，並要求他們移除或調控（moderate）明顯令人反感之貼文。
- 視情況以建議、談判、調解和說服方式來解決申訴問題。
- 當 Netsafe 無法解決申訴問題時，通知人們可向地方法院針對有害內容之作者或發布者申請移除命令（takedown），但須由 Netsafe 提供申請者一份事件摘要（Netsafe Summary）以向法院證明完成相關流程。

其中，本法規定任何因數位通訊而遭受傷害之個人、受影響人之父母或監護人、註冊學校之代表人，或警方，皆可向地方法院（District Court）申請命令[555]。惟前三類申請人之申請需先經由認證機構評估處置後，才能向法院提出申請[556]。而法院亦可將該申請轉回至認證機構，或要求認證機構提供相關訊息，以進行法庭程序[557]。

---

551 Harmful Digital Communications Act 2015, Part 1, Subpart 2, Sec. 7.
552 Harmful Digital Communications Act 2015, Part 1, Subpart 2, Sec. 8(1).
553 Netsafe, *WHAT IS THE HDCA?*, (2021/09/01), https://netsafe.org.nz/what-is-the-hdca/ (last visited Aug. 14, 2023).
554 *Id.*
555 Harmful Digital Communications Act 2015, Part 1, Subpart 2, Sec. 11.
556 Harmful Digital Communications Act 2015, Part 1, Subpart 2, Sec. 12.
557 Harmful Digital Communications Act 2015, Part 1, Subpart 2, Sec. 13-14.

而地方法院將處理 Netsafe 未能解決之有害數位通訊案件。法院可對被告人做出一項或多項命令[558]：

1. 移除或禁止內容之命令；

2. 被告人停止或不得從事相關行為之命令；

3. 被告人不得鼓勵其他任何人與受影響人進行類似通訊行為；

4. 發布更正命令；

5. 予以受影響人答辯權之命令；

6. 發布道歉之命令。

另外，地方法院可以根據申請案件，針對線上內容資訊儲存服務提供者資訊做出以下一項或多項命令[559]：

1. 移除或禁止公眾接取已發布或傳送之內容之命令；

2. 向法院揭露匿名或假名通訊作者身分之命令；

3. 以法院指定之任何方式發布更正命令；

4. 以法院指定之任何方式，予以受影響人答辯權之命令。

除此之外，法院得命令網路通訊協定地址提供者（Internet protocol address provider, IPAP）公開匿名通訊傳播者身分資訊[560]。

任何無視地方法院命令的人都可能受到起訴和處罰。HDCA 之刑事處罰，將對個人處以最高 6 個月的有期徒刑或最高紐西蘭幣 5,000 元的罰款，對法人團體最高處以紐西蘭幣 20,000 元的罰款[561]。另外，若某人在未經受害人同意下發布私密影像（intimate visual recording），或發布未滿 16 歲之私密影像，則將處以最高 2 年有期徒刑或最高紐西蘭幣 50,000 元之罰款，若為法人團體則處以最高紐西蘭幣 200,000

[558] Harmful Digital Communications Act 2015, Part 1, Subpart 2, Sec. 19(1).
[559] Harmful Digital Communications Act 2015, Part 1, Subpart 2, Sec. 19(2).
[560] Harmful Digital Communications Act 2015, Part 1, Subpart 2, Sec. 19(3).
[561] Harmful Digital Communications Act 2015, Part 1, Subpart 2, Sec. 21.

元罰款[562]，且法院可就該罪刑於法律程序中做出民事命令，以要求移除或禁止相關內容[563]。

而本法也針對線上內容資訊儲存服務提供者之責任劃定安全港規範，即不利用使用者發布之內容則不因該特定內容而生任何民事與刑事責任[564]。但仍需對特定內容進行責任保護措施，並於收到申訴後48小時內通知作者或移除該內容[565]。

三、第三方監督或產業自律機制

為了要求科技公司降低線上有害內容對紐西蘭人造成風險傷害，Netsafe於2021年4月首次提出自律框架(self-regulatory framework)之計劃，並於2021年12月公布準則以公眾諮詢徵求反饋，開啟Netsafe與各種利益相關者之磋商，以確保該實踐準則能夠解決與紐西蘭人有關之線上有害內容[566]。

而後於2022年7月25日，Netsafe和NZTech共同提出《紐西蘭線上安全及危害行為準則》(Aotearoa New Zealand Code of Practice for Online Safety and Harms)[567]之倡議，該準則之核心意義涵蓋四項毛利原則，為團結(mahi tahi)、平衡(kauhanganuitanga)、人性(mana tangata)與尊重(mana)[568]。

該行為準則主要由紐西蘭既有產業規範以及其他國家實踐準則發展而來[569]，諸如歐盟《因應不實訊息之實踐準則》(Code of Practice

---

562 Harmful Digital Communications Act 2015, Part 1, Subpart 2, Sec. 22A.
563 Harmful Digital Communications Act 2015, Part 1, Subpart 2, Sec. 22B.
564 Harmful Digital Communications Act 2015, Part 1, Subpart 2, Sec. 23.
565 Harmful Digital Communications Act 2015, Part 1, Subpart 2, Sec. 24.
566 Netsafe, *AOTEAROA NEW ZEALAND CODE OF PRACTICE FOR ONLINE SAFETY AND HARMS DRAFT*, https://netsafe.org.nz/aotearoa-new-zealand-code-of-practice-for-online-safety-and-harms-draft/ (last visited Aug. 14, 2023).
567 Netsafe& NZTech, *The Code - Aotearoa New Zealand Code of Practice for Online Safety and Harms*, July 2022, https://thecode.org.nz/wp-content/uploads/sites/38/2023/06/THE-CODE-DOCUMENT-FINAL.pdf (last visited Aug. 14, 2023).
568 NZTech, *About the Code*, https://thecode.org.nz/about-the-code/ (last visited Aug. 14, 2023).
569 Aotearoa New Zealand Code of Practice for Online Safety and Harms, July 25, 2022, https://nztech.org.nz/wp-content/uploads/sites/8/2022/07/FINAL-NZ-Code-of-Practice-for-Online-Safety-and-Harms-25-July-2022.pdf (last visited Aug. 14, 2023).

on Disinformation）、歐盟《打擊線上非法仇恨言論行為準則》（Code of Conduct on Countering Illegal Hate Speech Online）與澳洲《不實訊息與錯誤訊息實踐準則》（Code of Practice on Disinformation and Misinformation），以及「數位信任與安全夥伴最佳實踐框架」（the Digital Trust & Safety Partnership Best Practice Framework），因此參與制定該準則之數位平臺，大多數已是其他準則之簽署方或成員。而目前 Meta（Facebook 和 Instagram）、Google（YouTube）、TikTok、Twitch 和 Twitter 皆已採用《紐西蘭線上安全及危害行為準則》。

（一）《紐西蘭線上安全及危害行為準則》之自律框架與運作

《紐西蘭線上安全及危害行為準則》為業者建立一具監督性之自律框架[570]，明確規定權力、結構和監督機制。該準則賦予管理者（Administrator）與多方利害關係人之監督委員會（Oversight Committee）監督之責，且可向管理者建議終止簽署方之成員資格，並透過使用者申訴機制，允許使用者向管理者報告簽署方違反承諾之情形。另外，監理委員會亦須評估平臺業者之年度報告與遵守情況，定期審查並提出改進準則之建議。

1. 管理者

管理者係由簽署方共同同意並指派之機構，負責與準則相關之行政管理[571]。職責包括：管理多方利益相關者之監督委員會並促成辦理定期會議、推動簽署方建立申訴機制並發布年度透明度報告、促使簽署方遵守年度報告提交流程、推動準則審查之進行、維護一個公開可造訪之準則網站、更新準則之新簽署方。

而 NZTech 作為一非營利組織，匯聚來自紐西蘭 20 個技術社區與 1600 多名成員，成員包括新創公司、本地科技公司、跨國公司、教育機構、金融機構、網路提供者、高科技製造商與政府機構等[572]。NZTech 即為本準則之管理者[573]，試圖將準則納入其現有產業協會框

[570] *Id.*
[571] Aotearoa New Zealand Code of Practice for Online Safety and Harms, Sec. 5.1 & 6.1.
[572] NZTech, About NZTech, July 21, 2022, https://nztech.org.nz/reports/creating-collective-impact/ (last visited Dec. 31, 2023).
[573] Aotearoa New Zealand Code of Practice for Online Safety and Harms, appendix 4.

架中加以管理。

2. 監督委員會

監督委員會係由多方利益相關人組成，包括簽署方代表、毛利文化合作夥伴、公民社會，以及其他經過同意之利益相關者（如政府和學術界）。每年至少召開一次會議，以審查簽署方履行承諾之情況，包括評估簽署方的年度報告、經由申訴機制所提交之申訴案件，以及準則之進展[574]。

2022 年 7 月版本之《紐西蘭線上安全及危害行為準則》，將原本由管理者行使的權力轉移至監督委員會，並由當選之獨立監督委員會主席行使。監督委員會主席可行使以下權限，以確保簽署方遵守準則[575]：

（1）對新簽署方之錄取做出具約束力之決定（需得到簽署方的同意）；

（2）對違反準則承諾之簽署方，基於反覆違反之情形，做出具約束力之終止決定（須根據監督委員會成員建議做成決定）。在對簽署者進行公開終止宣布之前，監督委員會主席將對相關簽署方進行諮詢；

（3）對準則發表公開評論，並可依據相關證據，點名個別簽署方於準則承諾之正面或負面進展。監督委員會主席進行公開評論前，必須提前合理通知並諮詢相關簽署方。

（4）根據監督委員會成員建議，並獲得簽署方同意，對準則進行修訂。

此外，《紐西蘭線上安全及危害行為準則》之組織自律機制運作模式，係由 NZTech、Netsafe 和簽署方聯合推薦監督委員會之人選，擔任任期 2 年之職務，並負責委員會成立階段之提名與任命等制訂及

[574] Aotearoa New Zealand Code of Practice for Online Safety and Harms, Sec. 5.2 & 6.2.
[575] *Id.*

施行程序[576]。委員會之職責如下：

（1）調查並解決簽署方違反本準則承諾之申訴；

（2）就解決潛在系統性問題或嚴重違反本準則之問題，向受影響之簽署方提供報告與建議；

（3）於必要時，提出改進申訴機制之建議；

（4）定期審核本準則，確保能不斷回應快速變化之網路環境；

（5）選任擔任本準則之發言人；

（6）審查並核准本準則之新簽署方。

[576] NZTech, Governance of the Code, https://thecode.org.nz/governance/ (last visited Dec. 31, 2023).

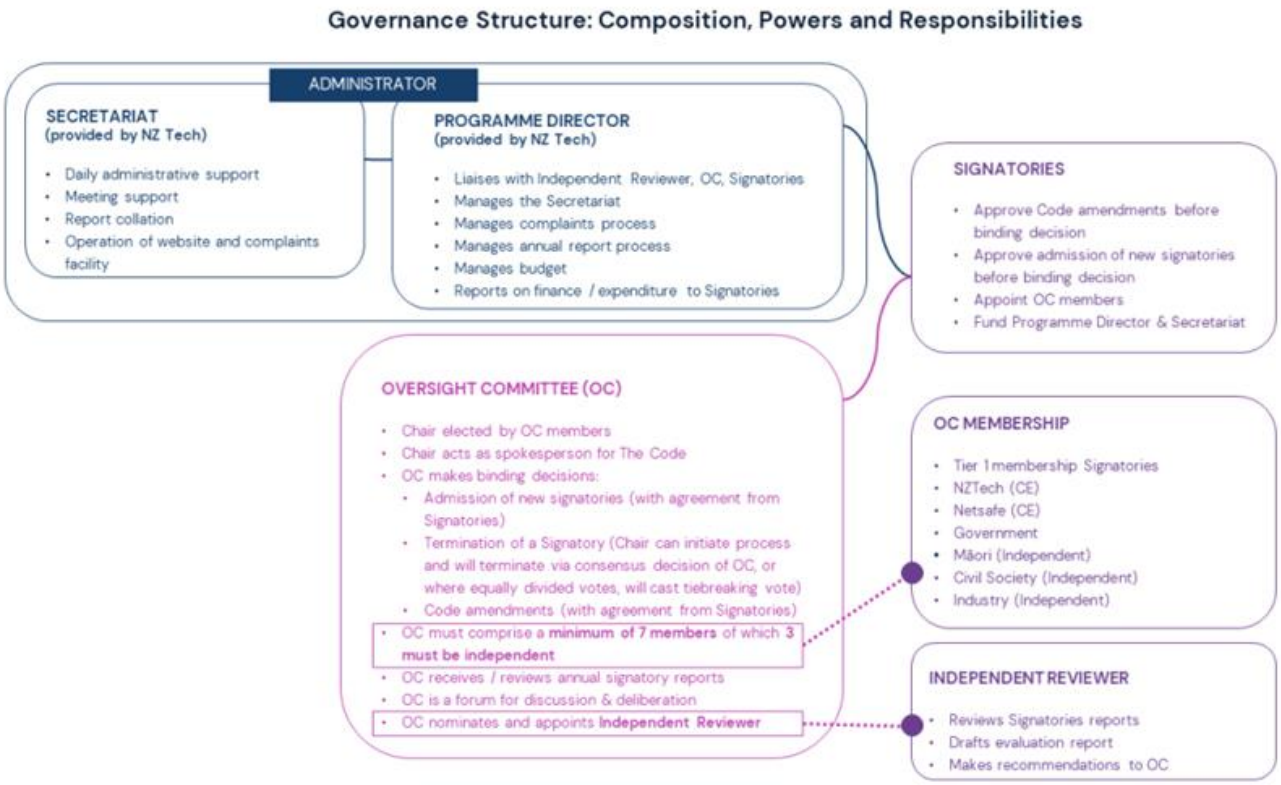


圖 11：《紐西蘭線上安全及危害行為準則》之權力與責任分布架構圖

資料來源：NZTech[577]

[577] *Id.*

3. 公眾申訴機制

申訴機制（complants mechanism），係為管理者將與簽署方共同合作建立之申訴政策、機制、違反定義/標準與申訴資格，讓紐西蘭使用者可對違反準則承諾之簽署方進行申訴[578]。

惟須注意，管理者只會接受與準則承諾相關之申訴，不會接受針對簽署方平臺內容之申訴，包括特定內容應該保留或移除的問題[579]。管理者也將制定並發布一份年度透明度報告，可能包含針對簽署方年度報告與申訴機制進行分析之綜合報告。

4. 年度報告

年度合規報告（annual compliance reporting），係為簽署方向監督委員會提交之年度報告，針對《準則》要求之四大承諾所做之實施措施和相關進展進行詳細說明[580]。針對四大承諾，《紐西蘭線上安全及危害行為準則》亦完整列舉業者執行之指導原則，即簽署方應提交之「合規」報告內容，並將於後續章節（第八節、三、(二)）詳述之。

5. 審查

《紐西蘭線上安全及危害行為準則》將於運作 12 個月後由監督委員會進行審查，之後每兩年審查一次。審查將奠基於簽署方和其他同意之利益相關者（如公民社會組織、學者和政府機構）之意見，任何因審查而對準則所做之變更或修訂，必須於生效前，經過監督委員會和所有簽署方同意[581]。

578 Aotearoa New Zealand Code of Practice for Online Safety and Harms, Sec. 5.3.
579 *Id.*
580 Aotearoa New Zealand Code of Practice for Online Safety and Harms, Sec. 5.4.
581 Aotearoa New Zealand Code of Practice for Online Safety and Harms, Sec. 5.5.

（二）《紐西蘭線上安全及危害行為準則》之四大承諾

該準則要求簽署方必須遵守相關指導原則並做出四大承諾[582]，包括：1. 減少線上有害內容之傳散、2. 賦予使用者更多控制權以知悉後做出選擇、3. 提升政策、程序及系統之透明度、4. 支持獨立研究和評估。以下將進一步針對此大承諾說明該準則對簽署方要求之承諾內涵。

1. 減少線上有害內容之傳散

目的在於減少網路七大類有害內容，包含兒童性剝削與性虐待（child sexual exploitation and abuse, CSEA）、霸凌或騷擾、仇恨言論、煽動暴力、影像暴力、錯誤訊息（misinformation）與不實訊息（disinformation）[583]。其中有關七大類有害內容，準則中亦明列具體措施，提供業者評估與執行如下表。

表 6：《準則》承諾之減少線上有害內容傳散措施

	結果（達成事項）	措施
1	提供保護措施以減少來自線上兒童性剝削與性虐待（CSEA）之風險危害	措施 1 實施、執行和/或維護政策、程序、產品和/或程式，以防止已知的兒童性虐待內容於其平臺和服務上供使用者接取
		措施 2 實施、執行和/或維護政策、程序、產品和/或程式，以防止搜尋結果出現兒童性虐待內容
		措施 3 實施、執行和/或維護政策、程序、產品和/或程式，力求採取強化的安全措施，保護兒童在網上不受進行有害性活動之同儕或成人影響（如網上誘導與掠奪性行為）
		措施 4 實施、執行和/或維持政策、程序、產品和/或程式，以減少更多兒童性虐待或剝削之可能

582 Aotearoa New Zealand Code of Practice for Online Safety and Harms, Sec. 4.

583 Aotearoa New Zealand Code of Practice for Online Safety and Harms, Sec. 4.1.

		措施 5 努力展開跨業合作並與其他相關利害關係人合作，以應對不斷變化的威脅
2	提供保護措施以減少來自網路霸凌或騷擾之風險危害	措施 6 實施、執行和/或維護旨在減少個人（包括未成年人和成人）或團體成為網路霸凌或騷擾目標之政策與程序
		措施 7 實施和維護旨在減少個人或群體成為網路霸凌或騷擾目標之產品和/或工具
		措施 8 實施、維護並提升用戶對產品或服務相關政策和工具之認識，以報告網路霸凌或騷擾內容
		措施 9 支持或維護旨在教育和提升對於如何減少或阻止網路霸凌或騷擾行為之認知計劃、倡議或功能
3	提供保護措施以減少網路仇恨言論之風險危害	措施 10 實施、執行和/或維護旨在禁止或減少仇恨言論傳散之政策和程序
		措施 11 實施和維護旨在禁止或減少仇恨言論傳散之產品和工具
		措施 12 實施、維護並提升用戶對產品或服務相關政策和工具的認識，以便用戶報告潛在仇恨言論
		措施 13 支持或維護旨在鼓勵批判性思維和教育用戶如何減少或阻止散播網路仇恨言論之計劃和倡議
		措施 14 努力展開跨業合作並與其他相關利害關係人合作，以支持應對網路仇恨言論不斷帶來的危害
4	提供保護措施以減少網路煽動暴力之風險危害	措施 15 實施、執行和/或維護旨在禁止或減少潛在傳散煽動暴力內容之政策和程序

		措施 16 實施和維護旨在禁止或減少潛在傳散煽動暴力內容之產品和工具
		措施 17 實施、維護與提升用戶對產品或服務相關政策和工具的認識，以便用戶報告潛在煽動暴力內容
		措施 18 支持或維護旨在教育用戶如何減少或阻止散播煽動暴力之網路內容之計劃和倡議
		措施 19 努力展開跨業合作並與其他相關利害關係人合作，以支持應對煽動暴力之線上內容不斷帶來的危害
5	提供保護措施以減少影像暴力之風險危害	措施 20 實施、執行和/或維護旨在禁止和/或減少散播網路影像暴力內容之政策和程序
		措施 21 實施和維護旨在禁止和/或減少散播網路影像暴力之產品和工具
		措施 22 實施、維護並提升用戶對產品或服務相關政策和工具之認識，以便用戶報告潛在影像暴力內容
6	提供保護措施以減少錯誤訊息之風險危害	措施 23 實施、執行和/或維護旨在減少散播網路錯誤訊息之政策、程序和/或產品
		措施 24 實施、執行和/或維護政策和程序，力求懲罰那些重複發布或分享違反相關政策錯誤訊息之用戶
		措施 25 支持或維持旨在鼓勵批判性思維和教育用戶如何減少或阻止散播錯誤訊息之媒體素養計劃和倡議
		措施 26 支持或維持旨在支持民間社會、事實核查機構和/或其他致力於打擊錯誤訊息的相關組織之計劃和/或倡議。

		措施 27 努力展開跨業合作並與其他相關利害關係人合作，以支持應對錯誤訊息不斷帶來的危害
7	提供保護措施以減少不實訊息之風險危害	措施 28 實施、執行和/或維護政策、程序和/或產品，以終止、移除、禁用或懲罰使用誤導性、欺騙性和/或可能造成傷害之假帳號
		措施 29 實施、執行和/或維護政策、程序和/或產品，以移除重複散播不實訊息之帳號（包括個人簡介、網頁、用戶名、頻道等）。
		措施 30 實施、執行和/或維護政策、程序和/或產品，以提供有關公眾帳號（public account）（包括簡介、網頁、用戶名、頻道等）之訊息，使用戶能夠做出知情決定（如帳號簡介建立日期、主要帳號訊息變更日期、追蹤人數）
		措施 31 實施、執行和/或維護政策、程序和/或產品，以提供具透明度之付費政治內容（例如廣告或贊助內容），並提供用戶更多背景和資訊（例如付費政治或選舉廣告標籤或為廣告付費者）
		措施 32 實施、執行和/或維護政策、程序和/或產品，以中斷廣告和/或減少從不實訊息獲利之用戶誘因
		措施 33 努力展開跨業合作並與其他相關利害關係人合作，以支持應對不實訊息不斷帶來的危害

資料來源：NZTech[584]，本研究自行整理

[584] *Id.*

2. 賦予使用者更多控制權以知悉後做出選擇

由於線上用戶有不同的需求、忍受度和敏感度，這些因素影響其線上體驗和互動，單一服務標準可能無法滿足或保護所有用戶。因此簽署方應提供用戶更多控制權，使其於網路內容和/或線上體驗和互動中做出選擇，並承諾提供工具、計畫、資源和/或服務，以保護用戶之線上安全[585]。《紐西蘭線上安全及危害行為準則》明列之具體指導原則，如下表所示。

表 7：《紐西蘭線上安全及危害行為準則》促進使用者知悉權之承諾

	結果（達成事項）	措施
1	用戶有能力就平臺上所看到的內容做出知情決定	措施 34 實施、執行和/或維護政策、程序、產品和/或計畫，幫助用戶對所看到的內容做出知情決定
		措施 35 實施、執行和/或維護政策、程序、產品和/或計畫，促進有關社會重大議題之準確可信資訊，以及與數位平臺用戶社群相關資訊（例如公共健康、氣候變化、選舉）
		措施 36 支持透過教育計畫和/或倡議，提高對虛假訊息、錯誤訊息和其他危害內容之意識，例如媒體/數位素養活動
2	用戶在他們看到的內容和/或線上體驗和互動方面擁有控制權	措施 37 實施、執行和/或維護政策、程序、產品和/或計畫，提供用戶對其看到的內容、動態消息以及/或線上社群有適當控制權
		措施 38 推出並維護產品，提供用戶對其看到的廣告有適當控制權

資料來源：NZTech[586]，本研究自行整理

585 Aotearoa New Zealand Code of Practice for Online Safety and Harms, Sec. 4.2.
586 *Id.*

3. 提升政策、程序及系統之透明度

透明度有助於建立信任並促進平臺問責。簽署方應承諾公開其有關線上安全和內容審查的政策、程序和系統，以及這些措施對減少用戶風險的有效性[587]。《準則》明列之具體指導原則，如下表所示。

表 8：《紐西蘭線上安全及危害行為準則》對於提高透明度之承諾

	結果（達成事項）	措施
1	透明化政策、系統、程序和計畫，以降低線上危害風險	措施 39 發布並提供用戶簽署方之安全與危害相關政策和服務條款
		措施 40 發布並提供相關政策、程序和產品資訊（例如透過部落格文章、新聞稿和/或媒體文章），減少線上有害內容之傳散
2	定期發布透明度報告，提出降低有害內容傳散與相關 KPIs/指標所做之努力	措施 41 發布帶有 KPIs/指標的定期透明度報告，提出基於政策、程序和產品所採取的行動，以減少有害內容傳散（例如違反政策而全球性移除之定期透明度報告）
		措施 42 根據《準則》之年度合規報告要求，向管理者提交報告，並詳細列出簽署方承諾所為之措施和進展

資料來源：NZTech[588]，本研究整理繪製

[587] Aotearoa New Zealand Code of Practice for Online Safety and Harms, Sec. 4.3.
[588] *Id.*

4. 支持獨立研究和評估

由學者和其他專家進行獨立的在地、區域或全球研究，以全面了解有害內容對社會的影響、強化線上安全並減少有害內容，這些研究對於持續改進數位生態系統之保護工作至關重要。簽署方應支持或參與這些研究工作，並承諾對實施之系統、政策和程序進行獨立評估[589]。《準則》明列之具體指導原則，如下表所示。

表 9：《紐西蘭線上安全及危害行為準則》支持獨立研究與評估之承諾

	結果（達成事項）	措施
1	有助於了解影響線上安全或有害內容對社會影響的獨立研究，和/或有關新技術強化線上安全或減少有害內容的研究	措施 43 在適當的情況下，支持或參與研究人員、公民社會和其他相關組織（例如事實查核機構）所發起的計畫和倡議，且可能包括由簽署方展開更廣泛的區域或全球研究計畫，並有益於紐西蘭
		措施 44 支持或每年至少召開一次活動，促進多方利害關係人對話，特別是與研究社群有關，且涉及線上安全與有害內容主題。且可能包括由簽署方展開更廣泛的區域或全球活動，並與紐西蘭相關
2	支持對已實施的系統、政策和程序進行與《紐西蘭線上安全及危害行為準則》相關之獨立評估	措施 45 承諾選擇一個獨立的第三方機構來審查簽署方提交之年度合規報告，並評估報告所列之承諾、成果和措施呈現之進展

資料來源：NZTech[590]，本研究整理繪製

589 Aotearoa New Zealand Code of Practice for Online Safety and Harms, Sec. 4.4.
590 *Id.*

四、小結

紐西蘭《有害數位通訊傳播法》主要從數位通訊之使用規範出發，訂定十大通訊守則，直接要求網路使用者皆須遵守數位通訊基本使用原則，並賦予第三方認證機構執行評估與處置網路有害內容之責，以共管模式處理違反十大通訊守則之情事，惟有當該機構無法處理，才會轉由法院裁定，針對被告或線上內容資訊儲存服務提供者發布相關處置命令，若違反法院命令，則將處以刑事處罰。

另外，由第三方非營利組織 Netsafe 和 NZTech 發起之《紐西蘭線上安全及危害行為準則》，共同訂定了網路七大類有害內容與具體實踐錯施，要求簽署方承諾解決網路有害內容所帶來的風險危害，並交由多方利害關係人組成之監督委員會審查平臺執行成果。該準則奠基於他國已施行之行為準則，也因跨國大型平臺皆已加入簽署他國之自律規範，將有效促進業者自律實踐之成果。此外，該份準則報告中也提到，儘管此自律規範與現行紐西蘭法律所規範之有害內容概念部分重疊、但並不衝突，而是希望透過法律、自律與他律之多元治理概念，共同建構紐西蘭友善且安全使用之網路環境。

第九節　日本

一、監理脈絡

在網際網路的監理政策上，日本一向採取較為保守的態度，最大限度的奉言論自由為監管之圭臬。因此，日本的政策通常非常重視產業界的自律精神。本節將從日本網際網路環境觀察出發，並從日本政府召開的研究專家會議說明日本的監理脈絡。

（一）網際網路環境之觀察

日本是個網路環境發展相對發達的國家，不但從資訊科技的發展可以見得，即使是從網路使用率的角度來看，都能夠看出端倪。

根據總務省每年固定進行的「通信使用動向調查」（通信利用動向調查）結果可見，日本在令和 4 年（2022 年）的網路使用率約為 83.1%，其中年齡在 15～59 歲的範圍內，網路使用率更高達 95%以上[591]，可見日本的網路已經達到極為普及之程度。由於這個調查每年均會進行一次，故從這個調查也可以發現，日本的網路普及率，尤其是高齡使用者的方面，也呈現著逐漸向上成長的趨勢（見下圖）。

[591] 総務省統計局，令和 4 年通信利用動向調査　世帯構成員編，e-stat 政府統計の総合窓口，https://www.e-stat.go.jp/stat-search/files?page=1&toukei=00200356&tstat=000001204921（最後瀏覽日：2023 年 10 月 2 日）。

全年齡層　　65～69 歲　　70～74 歲　　75～79 歲　　80 歲以上

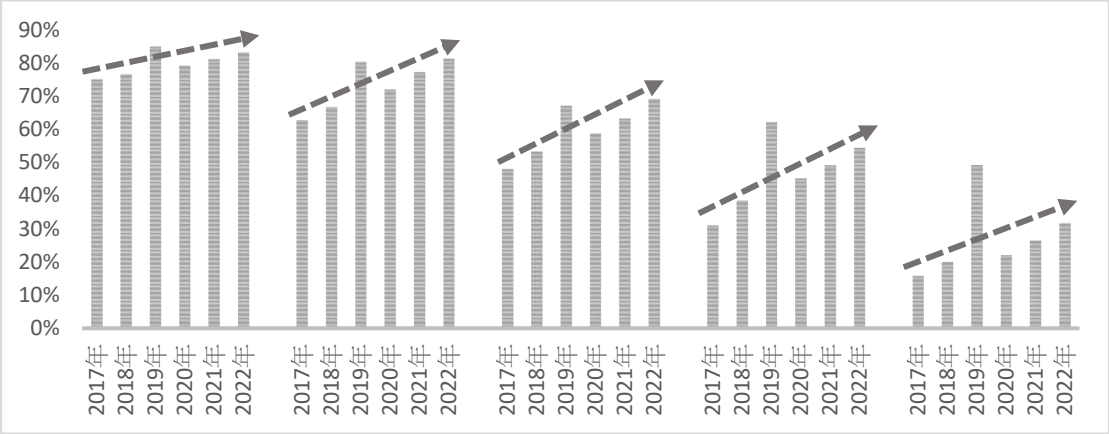


圖 12：日本 65 歲以上民眾之網路使用率變化

資料來源：総務省[592]

正因為網路在日本變得普及，例如錯假資訊的流竄、誹謗侮辱言論的傳播、智慧財產權侵害行為態樣的變化等，許多負面的社會現象也應運而生。隨著網路越來越普及，對被害人造成的傷害乃至於對社會造成的影響也越來越大，使得民間與政府均不得不審慎研議如何就上述情況建立對策。其中，前兩種負面現象與本研究之主軸較具關聯性，以下分別略述之。

1. 不實資訊的流竄

關於不實資訊在網路上流竄的問題，在日本已非第一次出現。早在 2011 年東日本大地震發生之時，由於災情導致的物流缺失、災區內外訊息傳遞困難、福島核電廠爆炸等，以及日本政府對災情的應對失靈，導致民眾對政府的信任感驟降，使得未經證實的「謠言」在 Twitter（更名為 X）等日本人時常使用的社交平臺上出現，錯誤資訊或虛假資訊也就隨之廣泛傳播[593]。

---

592 総務省統計局，通信利用動向調査，e-stat 政府統計の総合窓口，https://www.e-stat.go.jp/stat-search/files?page=1&toukei=0020035（最後瀏覽日：2023 年 10 月 2 日）。從這個趨勢圖也可以發現，令和元年（2019 年）曾經發生過一次網路使用率暴增的情況，而且增加的主力是發生在高齡使用者中，推測是因為搭上當年「改元」風潮的緣故。同時也可以發現，令和 2 年（2020 年）網路使用率並沒有顯著提升，反而因為前一年改元的緣故，而有顯著下降趨勢，可見新冠病毒疫情對於高齡者或全國國民的網路使用率，並未造成顯著影響。

593 鍋島啓太、渡辺研斗、水野淳太、岡崎直観、乾健太郎，訂正パターンに基づく誤情報の収

近年來，由於受到新冠病毒疫情之影響，諸如醫院、衛生所、新聞業會透過網路服務將疫情相關報導、病毒預防方法等資訊傳遞給民眾，政府也透過網際網路對公眾進行疫情的公開及政策宣示。不過，網際網路畢竟是任何人均得共同發表與接收的公共言論空間，例如「施打疫苗將導致不孕[594]」、「喝熱開水可以預防病毒[595]」等未經查核之錯誤或虛假資訊也被帶到網際網路中廣泛傳遞，加上透過通訊軟體等社群平臺分享的方式越來越容易，任何人都能「隨手分享」，使得這樣的資訊傳播達到了氾濫的程度[596]。

根據調查，日本人認為最常獲得錯假資訊的媒體場域，就是網路社群服務（SNS），而這樣的調查結果並非日本獨有，而是廣泛出現在全世界的現象[597]。然而，與前面的調查相互輝映，當日本人希望在網路上獲得新聞資訊時，網路社群服務總是日本人繼新聞網站以後的第二優先選擇[598]。因此，如何使民眾辨識在網路社群平臺廣為流傳的不實資訊，並從根源阻絕不實資訊的流傳，不管對於日本的民眾或政府而言，均是日漸重要的課題。

2. 誹謗、侮辱言論之傳播及網路霸凌

除了不實資訊外，日本關於網路誹謗中傷言論的狀況，也是一直以來備受討論的議題。所謂誹謗中傷之言論，係指對他人所為之批判或貶抑等人格上貶損之言論，也就是對他人有所損傷之言論[599]，至於是否屬於事實上之陳述，則在所不問[600]。

集と拡散状況の分析，自然言語処理，第 20 巻第 3 号，頁 461（2013）。

[594] “ワクチンで不妊”のデマ　なぜ拡散し続けているのか，NHK NEWS（2021/08/10），https://www3.nhk.or.jp/news/html/20210810/k10013192071000.html（最後瀏覽日：2023 年 10 月 2 日）。

[595] ＜みなぶん＞教えて！新型コロナ　２　これって本当？編　「お湯を飲んで予防」ネット情報にデマ，北海道新聞，2020 年 2 月 27 日，https://www.hokkaido-np.co.jp/article/397358/（最後瀏覽日：2023 年 10 月 2 日）。

[596] 総務省，令和 5 年版情報通信白書，頁 31-32（2023）。

[597] 総務省，令和 4 年度国内外における偽情報に関する意識調査，頁 14（2022）。

[598] 総務省，前揭註 596，頁 34。

[599] 総務省，前揭註 596，頁 31。

[600] 與我國《刑法》第 310 條所規定之「誹謗罪」在概念上較為接近的，是日本刑法第 230 條之「名譽毀損罪」。因為定義上之不同，日本的「誹謗中傷」行為通常只能構成刑法第 231 條之「侮辱罪」（相當於我國刑法第 309 條之「公然侮辱罪」）。

在日本，因網路誹謗中傷的言論產生的社會新聞仍時有所聞，而當誹謗中傷的言論在網路上廣為傳遞，並出現集體攻擊的現象時，就很容易形成網路霸凌。因此，網路霸凌事件與誹謗、侮辱攻擊事件，通常會一起討論。

根據統計（見下圖），由總務省委託負責協助民眾諮詢、處理相關事件的「違法、有害資訊諮詢中心（違法・有害情報相談センター）」，其受理之案件量不僅有增長之趨勢，近年的案件量更是十年前的四倍，使得日本政府不得不對此社會現象加以重視[601]。

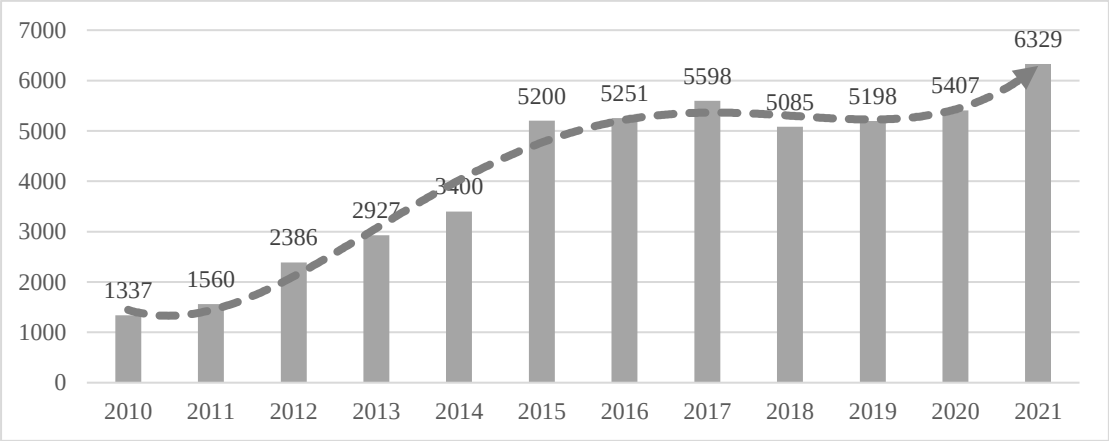


圖 13：違法、有害資訊諮詢中心處理諮詢案件數變化（單位：件）

資料來源：総務省[602]

（二）專家會議之政策意見

針對上述議題，總務省曾經召集相關之專業人士及學者組成「平臺服務研究會」（プラットフォームサービスに関する研究会，以下簡稱研究會），並由該研究會分析、研究相應之手段，並做成研究報告，作為未來施政之參考依據。

601 渡辺健策，デジタル情報空間の汙染にどう向き合うか，放送研究と調査，第 73 巻第 4 号，頁 3（2023）。

602 総務省プラットフォームサービスに関する研究会，第二次とりまとめ，https://www.soumu.go.jp/main_content/000831346.pdf，頁 8（2022）。

1. 不實資訊

就不實資訊之傳播，研究會在其作成之《第二次論點整理》（第二次とりまとめ）中明確表示仍以平臺自律作為政策推動之主基調，並且表示不贊同以課予法律強制義務之方式進行資訊之監管[603]。根據研究會的研究成果，研究會認為與其推動具備法律強制力的監管手段，透過與產業合作以及溝通，並為產業提供自律策略，一方面能夠與業者之間交換政策意見，二方面也能方便政府機關掌握產業動態及監管成效。

從《第二次論點整理》中，研究會共計羅列了十點不同的政策方向建議，如下圖所示。由研究會提出的政策方向建議可見，比起具體且強制的監管措施，研究結論更著重在與業者的合作和技術研發上，這樣的結論也可以體現出日本政府及學者在研究規劃網際網路監管之政策時，仍舊保持較為保守的態度，盡可能不以直接規制的方式對言論自由加以限制。

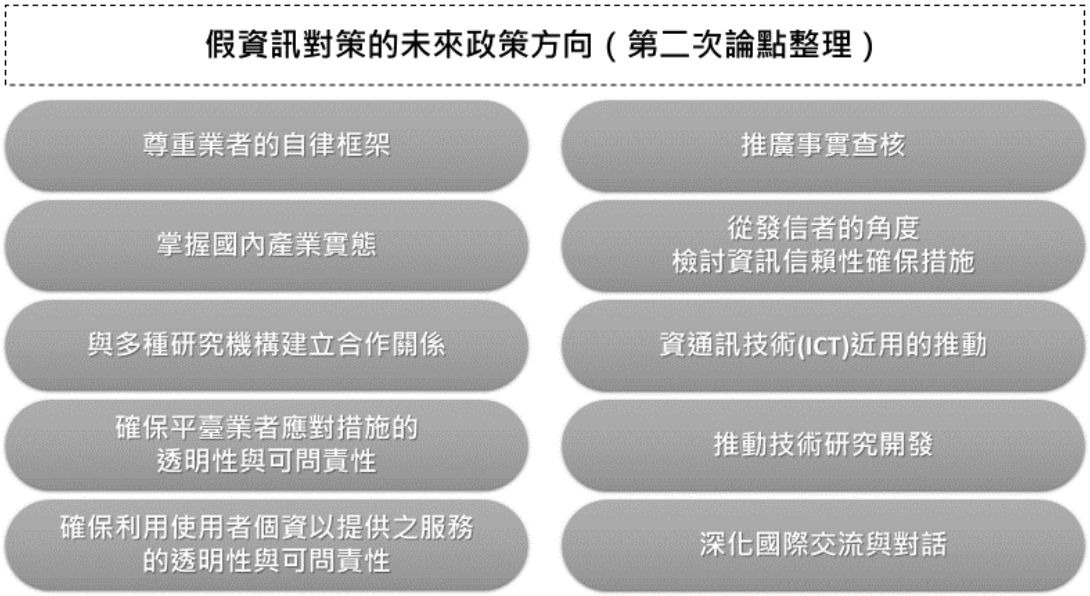


圖 14：假資訊對策的未來政策方向建議

資料來源：總務省プラットフォームサービスに関する研究会[604]

[603] 総務省プラットフォームサービスに関する研究会，前揭註 602，頁 81。
[604] 総務省プラットフォームサービスに関する研究会，前揭註 602，頁 81。

本文以下即就《第二次論點整理》所提及的十項政策方向建議，取其精要，分為「官民合作」、「促進信賴」、「技術升級」三個部分加以說明分析。

（1）官民合作

誠如前述，研究會意見並不認同政府直接制定具法律強制力（罰則）的規範，將手直接深入言論市場的政策是優良的監管措施。相反的，研究會意見的重點仍著重在與業者在政策上的合作中，透過業者自行制定的內規、使用者規範等措施，促使使用者遵守由業者制定的監管規範，並由平臺業者作為刪除文章、刪除帳號等措施的決定者[605]。

至於政府的角色，則是在最前面制定監管方針，並在後端對於業者執行之成效給予評價以及提供修正方向。透過這樣的方式間接達到監管效果，而非直接行使公權力，對於使用者（民眾）的言論自由較不易形成過度之衝擊[606]。

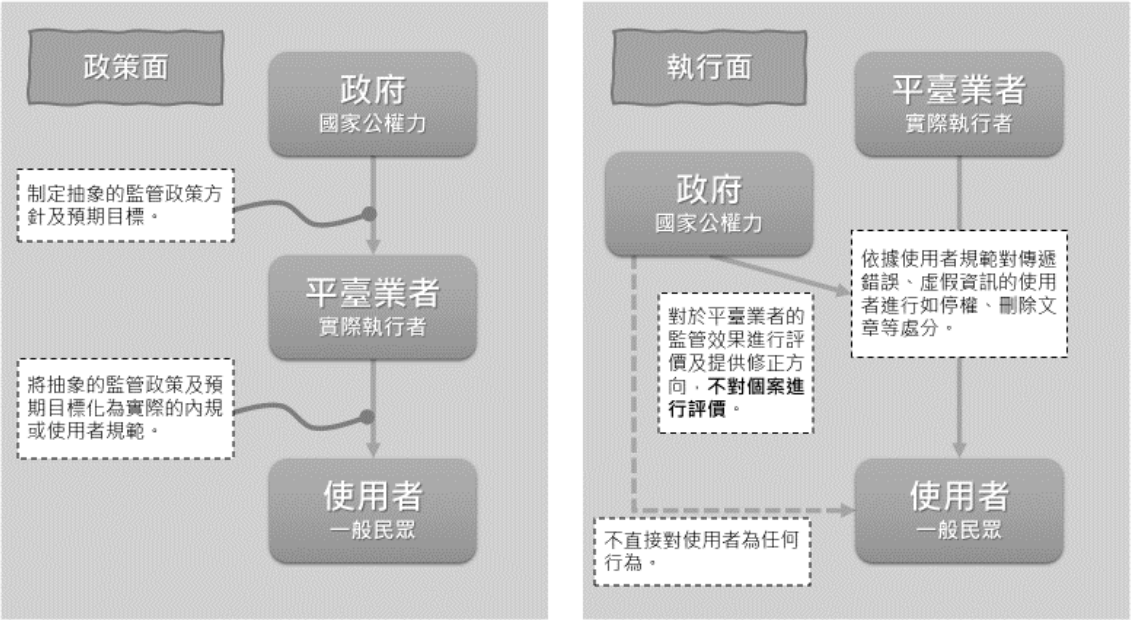


圖 15：研究會提出的自律框架及執行程序

資料來源：本研究自行整理

605 総務省プラットフォームサービスに関する研究会，前揭註 602，頁 81-82。

606 総務省プラットフォームサービスに関する研究会，前揭註 602，頁 82。

除了與業者合作以外，研究會亦指出與研究單位合作也是一個值得採取的方式。日本如 Disinformation 對策論壇（Disinformation 対策フォーラム）、Innovation Nippon 等研究機構對於不實訊息的研究已經行之有年，故將這些研究機構納入政策分析與研究的合作對象，對於監管政策之形成具有正向之意義[607]。

（2）促進信賴

所謂的促進信賴除了民眾與政府之間的信賴外，也包括民眾與業者之間的信賴。有鑑於近年平臺業者常常在使用者發出虛假或錯誤資訊時，以使用者違反規範為由，進行諸如刪除文章、刪除帳號等措施，卻沒有明確提供具體違反使用者規範的條款內容，導致平臺業者與使用者之間，常因此出現對立的狀況。

因此，研究會意見認為業者的管制政策應採透明化，明確規範使用者規約的文字，且應具備可問責性，使得使用者在受到平臺業者處分之時，能夠明確知悉自己被處分之原因，並有完整暢通的申訴機制。

此外，由於平臺業者收集使用者個人資料的同時，亦會活用其所收集之個人資料，例如透過使用者的活動軌跡（個人資料）掌握使用者的需求或興趣，並精準投放廣告等。在此情況下，研究會意見認為平臺業者有義務提供相應之資訊，確保使用者知悉自己有多少個人資料被平臺業者掌握並運用，促進資訊對等，以提升平臺業者與使用者之間的信賴，有助於正當化平臺業者的權限行使[608]。

（3）優化環境

所謂優化環境，指的是讓資訊環境能夠維持優良的狀態，也就是使得正確的資訊被凸顯、錯誤的資訊被隱藏。為了達成這個效果，研究會意見認為必須要推廣事實查核措施，並透過改良、研發資訊技術的方式，減緩虛偽、錯誤資訊的傳遞效果。

在技術開發方面，研究會指出政府應嘗試與大型平臺業者（如

[607] 総務省プラットフォームサービスに関する研究会，前揭註 602，頁 83。
[608] 総務省プラットフォームサービスに関する研究会，前揭註 602，頁 84。

Google、Meta、Twitter 等）合作，設計並開發能夠過濾不實資訊或能夠協助使用者進行事實查核的機制，協助使用者避免接觸不實資訊或便於尋求事實查核之資源。

在社會環境營造方面，研究會也認為應加強事實查核資源的運用，例如培育事實查核的人力資源、凸顯事實查核機構的存在等，並結合對一般民眾媒體素養的養成，提供相應的教育資源等。另外，亦可透過強化資通訊技術近用的方式，養成一般民眾對於資訊獲取及辨識的能力，以建構優質的媒體與資訊環境。

2. 誹謗、侮辱言論與網路霸凌

針對誹謗、侮辱言論與網路霸凌之現象，「平臺服務研究會」（プラットフォームサービスに関する研究会，以下簡稱研究會）亦有組成「因應誹謗侮辱等違法、有害資訊工作小組」（誹謗中傷等の違法・有害情報への対策に関するワーキンググループ），研議相關之政策並作成《因應誹謗侮辱等違法、有害資訊工作小組政策調修方向》（誹謗中傷等の違法・有害情報への対策に関するワーキンググループ今後の検討の方向性）之政策文件（以下簡稱政策文件），提供總務省作為未來施政之參考依據。

由政策文件的內容可見，該小組之見解仍採取較為保守的規制立場，雖有提及如具有法律強制力之違法資訊刪除義務、違法帳號停權義務等附罰則手段，惟基於保障言論自由之立場，政策文件仍以平臺自律為主要規制之原則。

舉例而言，針對「違法資訊刪除義務」，政策文件有提供二種不同的刪除方式，即「基於自律之資料刪除義務」與「基於法律之資料刪除義務」，而該小組的研究結論仍偏向採用前者之措施，說明如下。

（1）基於自律之資料刪除義務

所謂「基於自律之資料刪除義務」，係指由平臺業者制定關於刪除違法、有害言論之自律規範，明確規定何種言論會遭到平臺刪除，並將該自律規範作為平臺使用契約之一部，而使用者在此之地位，則為契約之一方當事人。在此情況下，使用者所發表之內容遭到刪除，係因使用者違反使用契約而導致之刪除結果，而非違反法律導致之刪除結果[609]。

以現況而言，實際上各大平臺均已具備類似之機制，惟使用者常反應其發文或言論常因不明原因而被刪除，平臺業者所制定之所謂「刪除標準」，有被指摘缺乏透明性之問題。然而，針對是否應制定具體明確之刪除基準，平臺業者（尤其跨國平臺業者）則普遍採取反對之立場。業者指出，若具體明確制定並公布其刪除標準，將使得惡意之使用者規避刪除標準明文禁止之內容，而繼續為該等有害資訊之傳播，對於所欲達到防制誹謗、侮辱乃至霸凌之目的，恐有相悖[610]。

此外，目前絕大多數的平臺業者雖然都設有申訴窗口，但一直以來均被反應窗口位置不明顯、無法以日語申訴請求刪除、無法完整說明申訴理由等情形，即使成功申請，其申請案之內容亦如石沉大海，無法確認調查進度與結果。準此，政策文件亦建議平臺業者應將申訴窗口以明顯之方式標示，並將其申訴案之處理進度適當透明化及設定申訴處理時間，使得申訴人能夠得知申訴進度並預期處理結果作成時間，以解決前開疑慮[611]。

（2）基於法律之資料刪除義務

相較於基於自律的資料刪除義務，由政府制定法規命令或由國會制定法律之方式建構，並附有罰則等法律強制力之資料刪除義務，研究會採取反對之立場。

---

[609] 総務省プラットフォームサービスに関する研究会事務局，プラットフォームサービスに関する研究会誹謗中傷等の違法・有害情報への対策に関するワーキンググループ今後の検討の方向性，https://www.soumu.go.jp/main_content/000909499.pdf，頁 10（2023）。

[610] 総務省プラットフォームサービスに関する研究会事務局，前揭註 609。

[611] 同上註 609，頁 11-14。

研究會認為，不論是制定法律課予平臺業者在其平臺中隨時監測、發覺涉及誹謗、侮辱或霸凌之言論資料並自主刪除之義務(刪文)，或是將帳號予以監視、標記、停用（封帳號）等，雖然可以有效降低此等言論之出現與傳播，惟站在平臺業者的角度而言，為使平臺業者免於受罰，平臺業者的執行標準勢必會提高到比政府原先期待的更高之程度，反而形成執法過度之問題，對於使用者的言論自由（包括將來之言論自由）將會形成過高之限制[612]。

若非由平臺業者自行監測，而是由公共機關（如法務省下屬之人權擁護機關[613]或警察廳委託之網路熱線中心（インターネット・ホットラインセンター）等）監測、發覺涉及誹謗、侮辱或霸凌之言論資料後，向平臺業者請求刪除時，平臺業者才有刪除義務者，由於公共機關具備一定的審查能力，平臺業者若因此就公共機關所提出之申請，怠於審查即予以刪除時，對使用者之言論自由亦將形成實質上的制約效果[614]。

至於日本法現有的「通知－取下」原則[615]，由於僅以「通知後七日內發表者無應答」為刪除要件，並不涉及言論內容本身之違法性判斷，可能使未必具備違法性的內容也遭到刪除，而對使用者的言論自由造成侵害，研究會意見也認為此種政策需要慎重考慮[616]。

政策文件也舉了由第三方機構進行違法性判斷與刪除請求等機制與訴訟外紛爭解決機制等多元的處理方式，惟此類機制目前仍欠缺法律整備，研究會見解認為均非救急之方案，不宜貿然使用[617]。

綜上所述，針對以具備法律強制力的手段所規範的資料刪除義務，由於涉及限制言論自由之問題，在研究會做成之政策文件中，仍

---

612 同上註，頁 16-18。

613 包括法務省（人權擁護局）、法務局（人權擁護部）、地方法務局（人權擁護課）、法務局及地方法務局支局等行政機關，及由法務大臣委任之人權擁護委員，以及人權擁護委員組織成立的機構，包括各市町村（或相鄰之市町村合併組織）組織之人權擁護委員協議會，及由相同都府縣（北海道則為同一區域之市町村）之協議會組織而成的聯合會等。

614 総務省プラットフォームサービスに関する研究会事務局，前揭註 609，頁 16-17。

615 《服務提供者責任限制法》第 3 條第 2 項第 2 款。

616 総務省プラットフォームサービスに関する研究会事務局，前揭註 609，頁 19。

617 同上註，頁 19-20。

採取反對之見解。

二、政府機關法制政策作為

日本現行網際網路內容之管理法規，共有《青少年網際網路環境整備法》（青少年が安全に安心してインターネットっを利用できる環境の整備等に関する法律）及《特定電信業務提供者之損害賠償責任限制寄發訊人資訊開示法》（特定電気通信役務提供者の損害賠償責任制限及び発信者情報開示に関する法律，官方簡稱「プロバイダ責任制限法」，以下依據官方簡稱，簡稱為《服務提供者責任限制法》）二部法律，說明如下。

（一）《青少年網際網路環境整備法》

日本於 2008 年通過並實施《青少年網際網路環境整備法》，其主要規範內容在於要求網際網路接取業者（IASP）應提供過濾青少年有害內容（青少年有害情報）之服務，並作為家長為青少年申辦行動門號時選用之參考依據。

本法所規定之有害網路內容，係指可受公眾閱覽且對於青少年有顯著阻礙之內容而言，例如直接且明示之承攬、仲介或引誘犯罪或違反刑事法規、使人興奮或引發性慾之性描寫，以及殺人、處刑或虐待等場面有殘虐描寫等之內容[618]。

然而，本法在制定後成效不彰，選用過濾服務的用戶數量並不多，故日本於 2018 年時修正本法之規定，對於 IASP 業者課予使用者身分確認義務、過濾措施說明義務及過濾措施實施義務。

根據修正後《青少年網際網路環境整備法》之規定，IASP 業者所應履行之法定義務主要分成三個階段。首先，就使用者身分確認義務，IASP 業者在新訂行動網路契約或續約時，應先行確認契約當事人是否為青少年；即使契約當事人非青少年，IASP 業者亦應近一步確認該契約所憑依之門號使用者或終端設備使用者是否為青少年，確

618 《青少年網際網路環境整備法》第 2 條第 3 項、第 4 項。

保每一位使用 IASP 業者服務的青少年都被業者所掌握[619]。

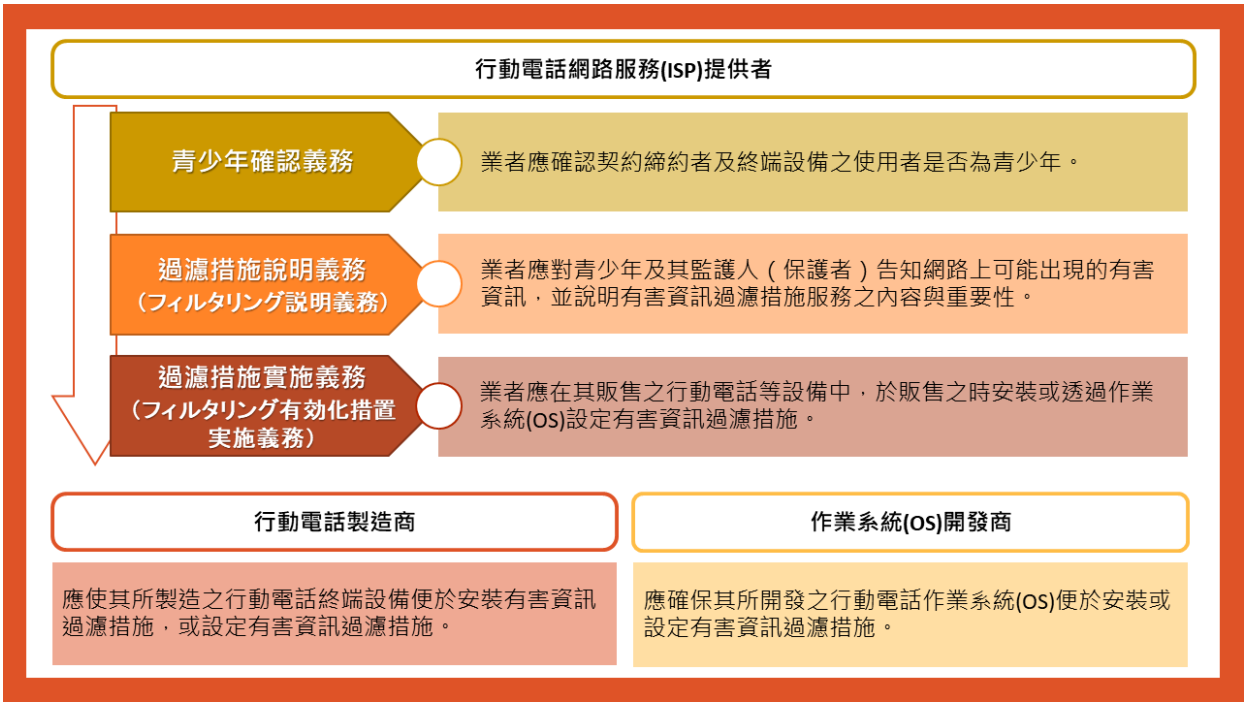


圖 16：《青少年網際網路環境整備法》修正條文賦予之義務

資料來源：こども家庭庁[620]

若 IASP 業者已能掌握契約當事人或終端設備使用者為青少年時，IASP 業者即應對青少年本人及其監護人（保護者）說明青少年使用網際網路時可能接觸到的有害資訊，並說明有害資訊過濾措施之內容及其重要性[621]。

最後，除青少年之監護人明確提出不希望受到該措施之過濾外，IASP 業者均應使有害資訊過濾措施在青少年的設備及裝置中有效運作，例如在其販售之行動電話等終端設備中安裝或設定有害資訊過濾措施等[622]。

然而，在法律修正後，有害資訊過濾措施的使用率不但未能上升，

619 《青少年網際網路環境整備法》第 13 條。

620 参見こども家庭庁，青少年インターネット環境整備法改正の概要，https://www.cfa.go.jp/assets/contents/node/basic_page/field_ref_resources/f71e3886-64d9-4781-9d3a-0d2f07332b82/e1951151/policies_youth_kankyou_internet_torikumi_hourei_doc_01.pdf。

621 《青少年網際網路環境整備法》第 14 條。

622 《青少年網際網路環境整備法》第 16 條。

反而出現下降趨勢[623]，且在中學及高中階段（約 14 歲至 18 歲）的使用者解除過濾措施的比率亦有提高之趨勢[624]。可見《青少年網際網路環境整備法》的規定尚有檢討之空間。

（二）《服務提供者責任限制法》

日本在 2001 年時即通過《服務提供者責任限制法》之立法，明文界定網際網路服務提供者（Internet Service Provider, ISP）業者的責任範圍。該法引入「通知及取下」（Notice and take out）模式，一方面賦予 ISP 業者相關之作為義務，另一方面也免除履行作為義務之 ISP 業者的責任，並對發訊人、送訊人及相關權利人間之權利義務明確規範，同時確立發訊人資訊揭露的要件。本段將從服務提供者的定義出發，細部解說本法的運行機制，並說明其在修法過後新增的發訊人資訊揭露程序。

1. 名詞定義

根據《服務提供者責任限制法》第 1 條之規定，本法的適用範圍限於「特定電信」（特定電気通信）之情形，而所謂特定電信，根據同法第 2 條之規定，以使不特定人收訊為目的而傳輸（不包括以公眾直接收訊為目的之傳輸）之電氣通信而言[625]。而根據總務省對本法所作成之解說可見，本法所要規範的範圍，係指網頁或網路電子公布欄（BBS）等在網路上使不特定人得以收訊為目的之情形，而不包括如電話通訊（對特定人通訊）、廣播通訊（以公眾直接收訊為目的）等情況[626]。

---

[623] 參見総務省青少年インターネット環境の整備等に関する検討会，青少年インターネット環境の整備等に関する検討会報告書（案）について～改正法附則に基づく検討～，https://www.soumu.go.jp/main_content/000710963.pdf，頁 3（2020）。

[624] 総務省，「我が国における青少年のインターネット利用に係るフィルタリングに関する調査」報告書，https://www.soumu.go.jp/main_content/000746234.pdf，頁 42（2021）。

[625] 日本《服務提供者責任限制法》第 2 條第 1 款。

[626] 総務省，特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律－解説－，https://www.isplaw.jp/vc-files/isplaw/000461787.pdf，頁 1（2017）。

不過，隨著科技日漸發達，數位匯流技術逐漸演進使得本法對於特定電信的定義有過時而不堪適用之情況。例如，儘管廣播（放送）被本法明文排除，但透過網路進行的網路廣播（インターネット放送）服務並未因此而受排除，使得後續如隨選型串流服務（例如 Netflix 等）、即時型串流服務（例如 Twitch 等）等在法律上的定性如何，即有疑問。在此爭點上，有學者認為網路廣播之情況，實與在網頁上揭露資訊無異，僅是形式上的不同而已，故仍應屬於特定電信之範圍[627]。準此，則各類透過網頁或 APP 網際網路視聽服務等，均會被列為特定電信之範圍。

至於「特定電信服務提供者」（特定電気通信役務提供者）之範圍，在日本亦曾經有過爭議。在 2010 年的「NTT DOCOMO 案」[628]中，就曾經以網際網路接取服務提供者（IASP）是否屬於特定通信服務提供者為爭點，有過爭執，其爭議的目的在於判斷 IASP 業者是否屬於本法發訊人資訊揭露義務的範圍。這個爭議在第一審與第二審均認為「特定電信」的判斷基礎在於網站的伺服器，而不包括伺服器與使用者中間連結的 IASP，故 IASP 業者並不屬於特定電信服務提供者。

不過，這個見解在最高法院被推翻，理由有三：（1）依文義解釋，凡發訊人供不特定人觀覽的資訊流通過程，均為特定電信之範圍，自然包括負責資訊流通的 IASP。（2）由於 IASP 通常是付費服務，故 IASP 業者對於使用者的資料應較能把握，基於保障被害人的觀點，認定 IASP 業者屬於特定電信服務提供者的見解，較能達成本法保障被害人之目的。（3）若 IASP 業者不屬於本法所稱特定電信服務提供者，則有悖於本法第 3 條之本旨與電信事業法第 3 條保障通訊秘密之本旨[629]。根據上述見解，IASP 業者也被認為是特定電信服務提供者的範圍，有本法之適用而有相應之義務，且該見解也被編入判例中，

[627] 飯田耕一郎，プロバイダ責任制限法解説，三省堂，頁 35-36（2002）。

[628] 最高裁判所第一小法廷，平成 22 年 4 月 8 日（平成 21(受)1049），民集，第 64 卷第 3 号，頁 676。[発信者情報開示請求事件]

[629] 森亮二，「経由プロバイダの抗弁」に関する最高裁判決——最一判平成 22・4・8 民集 64 巻 3 号 676 頁，收錄於堀部政男監修，別冊 NBL No.141　プロバイダ責任制限法 実務と理論－施行 10 年の軌跡と展望－，頁 102-105（2012）。

作為權威的實務見解。

應注意的是，「特定電信」的判斷基準是以「使不特定人收訊為目的」，並非所有透過網際網路達成的行為均屬於行為。換言之，例如網路通訊服務（例如 LINE 等）或電子信箱（E-mail）等，由於該通訊行為乃以「特定人」收訊為目的，而非屬於特定電信服務[630]。

2. 特定電信服務提供者之責任限制

由於特定電信服務提供者（以下簡稱服務提供者）與發訊人之間通常具備契約關係，若服務提供者任意揭露發訊人資訊，將使服務提供者陷入違約之風險。又若發訊人透過服務提供者提供之服務發表侵害被害人權利之言論時，若服務提供者毫無作為，則間接對被害人之權利造成侵害，而陷入訟爭之風險中。

為使服務提供者無須陷入前開進退兩難之窘況，《服務提供者責任限制法》將服務提供者對於被害人與發訊人之間的責任加以限縮，奇具體限縮之內容如下：

（1）特定電信服務提供者對於被害人責任之限制

根據《服務提供者責任限制法》第 3 條第 1 項之規定：「若因特定電信所生之資訊流通，致使他人權利受有侵害時，以特定電信設備提供服務之電信服務提供者(本項以下簡稱「關係電信服務提供者」)，若技術上對侵害權利之資訊得採取措施以防止侵害時，除有下列各款情形外，不負損害賠償責任：一、該關係電信服務提供者知悉該特定電信之資訊流通將造成他人權利侵害。二、該關係電信服務提供者知悉該特定電信之資訊流通，且有理由足資認定其可知悉該資訊流通將導致他人權利受有損害」。

準此，可見在《服務提供者責任限制法》之下，服務提供者對於使用者原則上無需負損害賠償責任，惟阻止權利侵害之措施，在技術上可行的情況下，若服務提供者明知或可得而知因其提供之服務所生

[630] 関原秀行，基本講義プロバイダ責任制限法，加除出版，頁 198（2016）。

資訊流通，對他人之權利將造成侵害時，服務提供者則例外負損害賠償責任。

應注意的是，此處所謂「權利侵害」範圍非常廣，包括財產權、人格權、隱私權、肖像權、著作權、商標權、專利權等，並不局限於某一特定權利，屬於普遍性的規範模式。惟本法所保護之範圍只包括「權利」[631]，與日本《民法》第 709 條關於侵權行為（不法行為）同時保護權利與利益之規定有別[632]，故如廣告不實、誇大廣告、身份冒用（なりすまし）等行為，除影響其所關聯之具體權利外（例如冒用他人身分發表不當言論，致被冒用人名譽權受侵害等[633]），均不在本法之適用範圍。

（2）特定電信服務提供者對於發訊人責任之限制

服務提供者對發訊人應負之責任，即服務提供者依契約應使發訊人發表之文章不被任意刪除之契約義務，若發訊人所發表之文章被服務提供者所刪除，服務提供者自應依契約負相應之責任。是以，為使服務提供者願意主動感知並刪除或被動依申請而刪除侵害他人權利之文章，限制服務提供者對發訊人應負之責任即有其必要。

關於服務提供者對發訊人責任之限制規定，在《服務提供者責任限制法》第 3 條第 2 項定有明文：「特定電信服務提供者，於防止特定通信所生之資訊流通而為措施時，若因該措施而使發訊人受有損害時，在該措施係為防止對不特定人傳輸資訊必要限度之範圍內，而有下列情形之一者，免除賠償責任：一、該特定電信服務提供者有理由足資相信該特定電信資訊流通將對他人權利造成不當侵害。二、因該

631 日本《服務提供者責任限制法》第 3 條第 1 項：「特定電気通信による情報の流通により他人の**権利が侵害された**ときは……（後略）」（若因特定電信所生之資訊流通，致使他人**權利受有侵害**時……（後略））。

632 日本《民法》第 709 條：「故意又は過失によって**他人の権利**又は**法律上保護される利益**を侵害した者は、これによって生じた損害を賠償する責任を負う。」（因故意或過失，致使**他人之權利**或**依法保護之利益**受侵害者，應負損害賠償責任）。

633 參見 東京地方裁判所，令和 2 年 6 月 26 日（平成 31(ワ）8945 號）民事判例。該判例所涉事實如下：被告Ｘ冒用原告Ｙ之名義，在推特（Twitter，今更名為Ｘ）開設帳號，以Ｙ之照片作為該帳號之頭像，並以該帳號發文惡意辱罵Ｙ之同學Ｚ。原告Ｙ最終主張適用服務提供者責任限制法揭露Ｘ資訊之依據，並非Ｘ冒用Ｙ身分之行為，而是Ｘ冒用Ｙ身分之後所為辱罵他人之後續行為造成Ｙ之肖像權與名譽權侵害。

特定電信資訊之流通而使自己權利受有損害之人，表明侵害之資訊、被侵害之權利及受侵害之理由（以下於本款簡稱侵害之資訊等）並請求特定電信服務提供者為防止侵害之資訊流通之措施（以下於本款簡稱流通防止措施）時，特定電信服務提供者對該侵害之資訊之發訊人表明侵害之資訊等並為同意該流通防止措施與否之照會，而在發訊人接收照會後七日內未能從發訊人處取得不同意之回應者」。

由此可見，服務提供者對發訊人權利造成侵害時，其責任限縮之要件，可分為「主動感知並取下」和「被動受通知而取下」兩種情況，說明如下。

本項第 1 款規定即主動取下之情形，由於服務提供者擁有特定電信服務（平臺）之絕對控制能力，若服務提供者透過其人力主動感知，或透過其製作之軟體或技術（如演算法、人工智慧軟體等）感知並判斷發訊人所發表之文章有侵害他人權利之情況時，服務提供者即可自行下架，且因之對發訊人所受之損害，不負賠償之責。

本項第 2 款規定即被動取下之情形，也就是所謂的「通知及取下」（Notice and Take down）條款，其具體的運作流程，則如下圖所示：

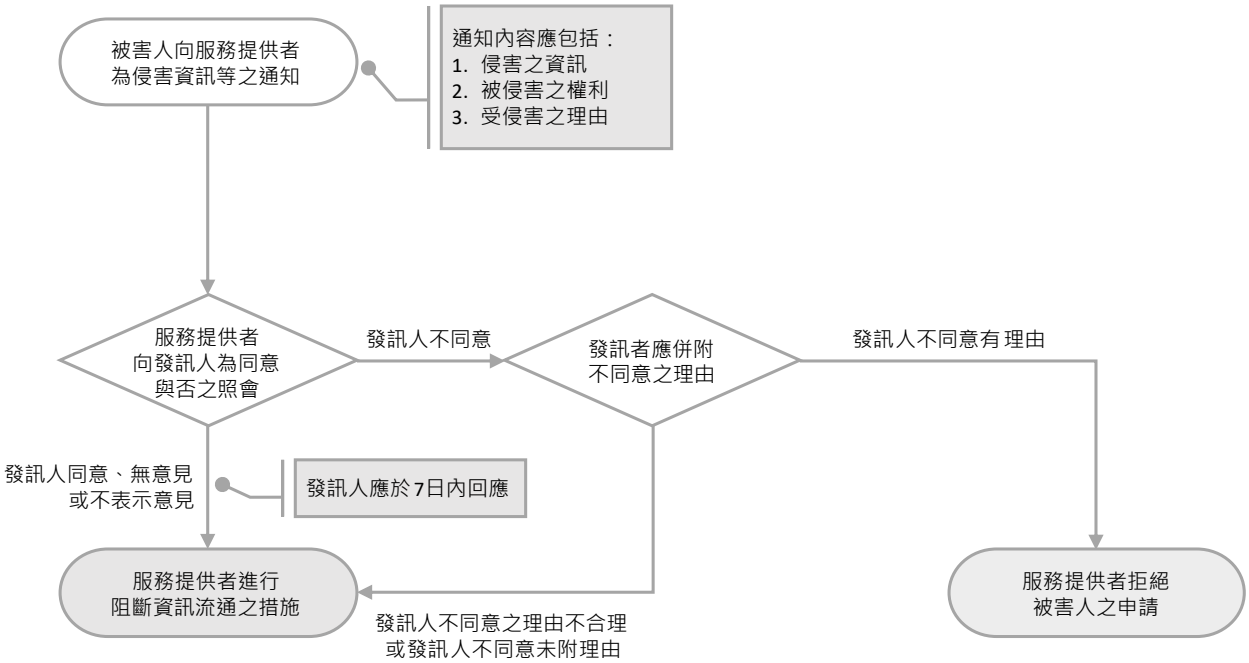


圖 17：日本服務提供者責任限制法「通知及取下條款」運作流程圖

資料來源：本研究自行整理

透過被害人通知服務提供者其權利受到發訊者所發表之文章侵害，並藉以請求刪除時，服務提供者在照會發訊人後，除發訊人附正當理由不同意之情況下，服務提供者刪除發訊人之文章或其他足以阻止資訊流通知措施，對發訊人造成之損害，不負賠償之責。

3. 發訊人資訊揭露程序

近年，《服務提供者責任限制法》經歷了大幅度的修正，而修正案於 2021 年經國會通過，並於 2022 年 10 月起實施。此番修正最主要的修正重點，即為將「發訊人資訊揭露程序」加以完善，使得使用者（被害人）的發訊人資訊揭露請求權得以被完整主張。

所謂發訊人資訊揭露請求權，則是當被害人之權利在網路上受到他人侵害時，為使被害人能夠順利行使救濟權（包括和解、訴訟等）以回復其權利，而特別賦予被害人在法定要件與程序下，得請求網際網路服務提供者揭露發訊人資訊之權利。此番權利，於《服務提供者責任限制法》修法前第 4 條、修法後第 5 條中均定有明文。

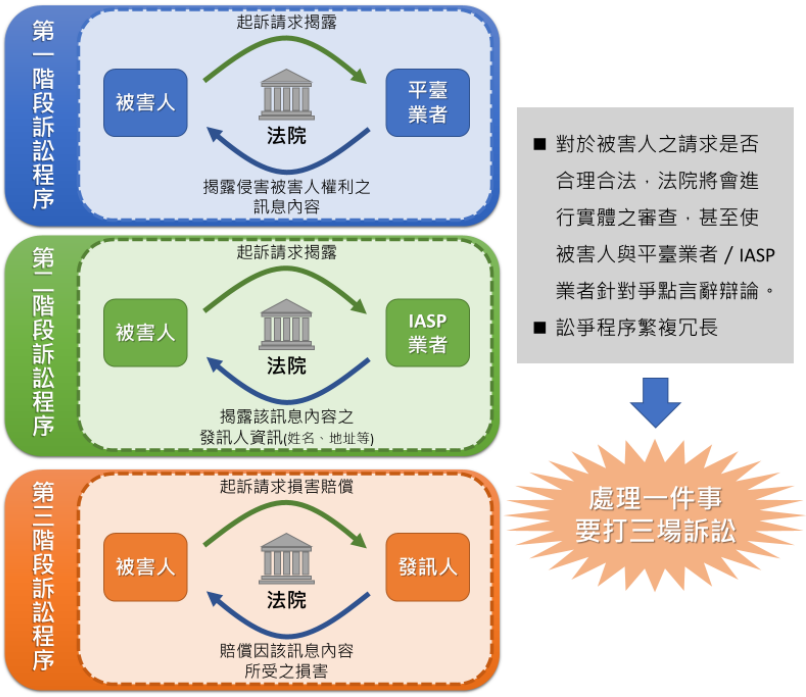


圖 18：修法前之發訊人資訊揭露程序（第三階段並非資訊揭露程序）

參考資料：總務省[634]

在修法前，《服務提供者責任限制法》只對發訊人資訊揭露請求權加以規定，卻未規定行使該權利之具體程序，使得被害人行使該權利時，僅能透過一般民事訴訟程序解決。在這樣的法律程序規範下，日本逐步形成了所謂的「二階段的發訊人資訊揭露」訴訟程序。以被害人在某論壇被散布不真實且有人格貶損性質之資訊為例，被害人必須先起訴該論壇之經營者，請求揭露發訊人的通訊紀錄，勝訴後再依該通訊紀錄，起訴 IASP 業者請求揭露發訊人的個人資料（姓名、住居所等），再根據該資料起訴發訊人，以請求損害賠償。這樣的程序顯然冗長而缺乏效率，且因程序冗長，證據及相關資訊隨時有滅失之風險。

為因應上述情形，本法在 2022 年之修正包含以下重點：

634 総務省，プロバイダ責任制限法の一部を改正する法律（概要），https://www.soumu.go.jp/main_content/000836903.pdf，頁 0（2021）。

（1）創設發訊人資訊揭露之非訟程序

在發訊人資訊揭露請求權的實體權利上，該次修法並未有任何更動，惟在行使該權利之程序規定，則有較大幅度的修正。有別於修法前僅能透過訴訟方式請求之程序，修法後則改為得透過非訟程序得到解決。

根據修法後《服務提供者責任限制法》第 8 條規定，若被害人因自己權利受到他人在特定電信流通資訊之侵害，而向法院聲請時，法院接獲聲請後，得命揭露關係服務提供者基於該法之規定，揭露發訊人之個人資訊。這裡所稱的「揭露關係服務提供者」指的即是依同法第 5 條所規定被請求揭露發訊人資訊的特定電信服務提供者，搭配前面提及的特定電信之範圍，可知在修法後，被害人即得逕向法院聲請對平臺業者（例如 Twitter）或 IASP 業者發布發訊人資料揭露命令。

另外，本法對於程序已經有特別規定，並以非訟事件之形式規範之，自無須依照舊法適用普通民事訴訟之方式處理，而是以非訟事件之程序，透過法院向服務提供者發布命令的方式處理之[635]；同時，在採用非訟程序後，被害人請求發訊人資訊揭露時，即可一次性對多數人（業者）向法院聲請，而無須如舊法一般透過二階段的訴訟方式行使權利。

[635] 同上註，頁 7。

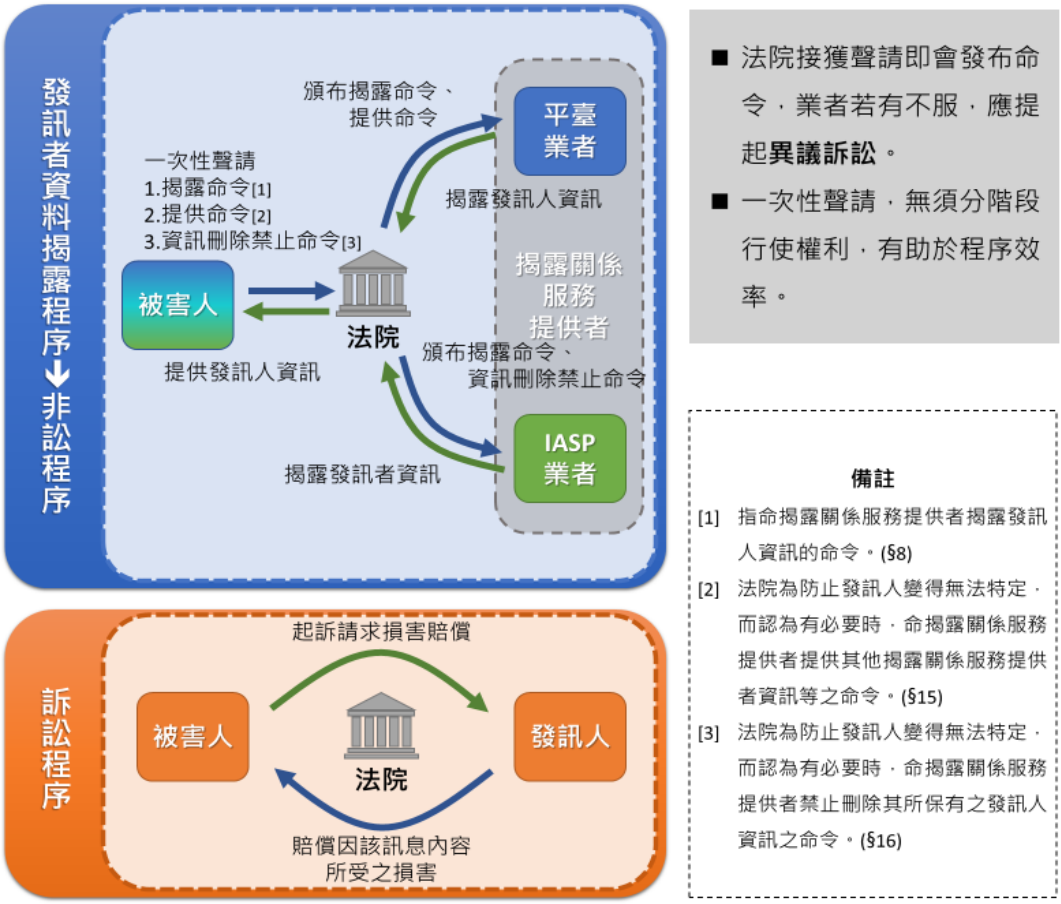


圖 19：修法後之發訊人資訊揭露程序（訴訟程序並非資訊揭露程序）

參考資料：總務省[636]

在前開法律修正之後，由於不再適用訴訟程序之規定，且二階段訴訟程序亦得到減縮，使得被害人在主張發訊人資訊揭露請求權時，得直接一次性向法院主張，不須分別向平臺業者及 IASP 業者請求或起訴，降低了被害人尋求救濟的門檻，也提升了被害人尋求救濟的效率。

（2）得請求揭露資訊範圍之擴張

現在有部分網際網路留言板、論壇等網路平臺的營運模式，雖採用會員制設計，惟使用者在留言的當下，則為匿名之身分，而不能被被害人所辨識、特定，進而無法請求揭露該留言之發訊人資訊。在舊法之下，這種情況由於法院無法特定該當事人（即發訊人），而無從

[636] 同上註，頁 6。

判斷如何要求業者履行其揭露義務，導致被害人依舊無法主張其權利。

修法後，被害人得請求揭露之範圍，除原有之發訊人資訊外，若個案情形屬於上述匿名留言之情況，被害人在向法院聲請揭露發訊人資訊時，得揭露之範圍也將擴張至發訊人登入時的資訊。換言之，修正後的資訊範圍將使匿名發布的言論，能夠依據法院的裁定而被揭露發訊人資訊[637]。

另外，舊法時代被認為難以受到《服務提供者責任限制法》規管之身分冒用（なりすまし）行為，在修法之後也將受到規管。所謂身分冒用，係指在網路留言板（如 2ch、5ch 等）等無須登入之全匿名制平臺上，透過偽稱或暗示自己是某特定人之方式發表言論之行為。由於新法使全匿名之網站發訊者資訊也能被追蹤並揭露，故縱使發生身分冒用之行為，也能透過發訊人資訊揭露程序，將冒用身分之發訊人資訊揭露出來，以使因身分冒用而受有損害之被害人得以請求損害賠償。

（3）拒絕揭露資訊時之理由告知

按揭露發訊人資訊之行為，對於發訊人之權利而言，勢必會造成限制或侵害，故特定電信服務提供者在揭露發訊人資訊前，應向發訊人照會，以使發訊人得以陳述意見。此照會之制度，在修正前既已存在，並非新設之規定。

本次修正重點在於，倘若發訊人所陳述之意見本旨，係拒絕或不同意揭露其資訊時，根據修正後本法第 6 條第 1 項之規定，發訊人應告知拒絕之理由，否則應視為消極同意揭露。

[637] 総務省，前揭註 634，頁 0。

（三）網路霸凌相關規範

雖然因為網路霸凌而導致的憾事時有所聞，日本至今對於網路霸凌事件尚無針對性的規範，惟對於與兒童有關的霸凌事件，日本於 2013 年通過《霸凌防止對策推動法》（いじめ防止対策推進法），從教育、環境與懲戒三個面向出發，協助兒童身心之健全成長，避免使兒童身陷霸凌環境，使其人格發展產生危害。應注意的是，《霸凌防止對策推動法》所保護的範圍是兒童霸凌之情況，尚不及於成人。

在《霸凌防止對策推動法》第 2 條第 1 項中，對於所謂「霸凌」（いじめ）定義如下：「本法所稱霸凌，係指由與兒童等具備一定人際關係之其他兒童，對於該兒童等所為之行為，造成該兒童心理上或物理上之影響（包括透過網際網路之行為），使該兒童身心感到苦痛而言。」由該定義可見，該法所要規管之霸凌行為，也包括網路霸凌行為在內。

《霸凌防止對策推動法》所規範的措施，可歸納為四種範疇，整理如下圖：

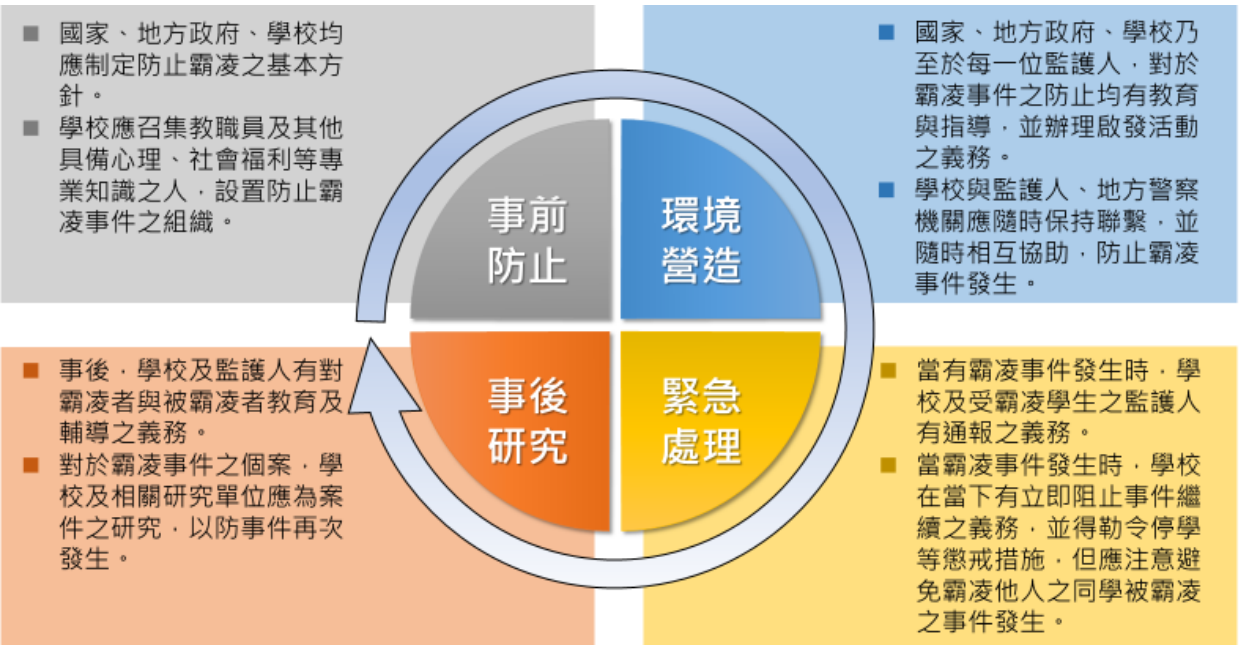


圖 20：日本《霸凌防止對策推動法》規範內容

資料來源：本研究自行整理

就網路霸凌之部分，《霸凌防止對策推動法》並沒有額外之特別規定，而是根據該法第 19 條之本旨，透過教育及啟發活動之方式防止事件發生，而當事件發生時，則依同條第 3 項之規定，回歸適用前述《服務提供者責任限制法》的規定處理，並未有刪除網路霸凌言論內容之直接規範。

總體而言，《霸凌防止對策推動法》之立法宗旨不在於個案事後的損害填補或加害人懲戒，而是在事前透過環境營造與啟發之方式防止霸凌事件之發生，事後透過教育之方式防止事件之再度發生，藉此根除霸凌事件。

然而，由於《霸凌防止對策推動法》尚有對於霸凌定義不夠明確、對於學校及其教師課予過重之負擔等問題，導致法律推動效果不彰[638]，亟待修正之必要。

（四）仇恨性及歧視性言論相關規範

仇恨性、歧視性言論在日本並非罕見，且並不限於對非本國籍人的歧視，如「部落民」等古來即受到日本文化歧視的族群[639]，或在日朝鮮人等因歷史因素而在日本繁衍之非日本民族族群等，至今仍受到日本環境之歧視[640]。

所謂部落民，係指在明治維新以前從事農耕、獸屍處理、皮革加工等手工業等較為低下職業者，在織豐、江戶時代被認為社會地位低賤，甚而有「穢多」（エタ）、「非人」之稱，並廣受日本其他族群之歧視[641]。儘管在明治維新後，日本政府發布了所謂「解放令」，試圖透過憲政體制建立一個人人平等的社會，依舊難以擺脫數百年來日本民眾對於部落民

638 松永邦裕，いじめ防止対策推進法施行後の学校現場の新たな課題，福岡大学研究部論集 B：社会科学編，第 11 号，頁 17-21（2019）。

639 明石一朗，「同和問題を考える」：人権問題論の講義から，関西外国語大学人権教育思想研究所紀要，第 20 号，頁 59-63（2017）。

640 姜冠霖，【特別報導】「我也想當日本人！」被歷史留下的「在日朝鮮人」是誰？為何至今仍飽受歧視？，換日線（2023/04/13），https://crossing.cw.com.tw/article/17516（最後瀏覽日：2023 年 12 月 27 日）。

641 明石一朗，前揭註 639，頁 62；のびしょうじ，被差別民社会論　序説，人権問題研究，第 14 号，頁 104（2014）。

的歧視心理，甚至在法院裁判上對於部落民也或多或少有差別待遇[642]。

為解決長久以來根深柢固的部落民歧視問題，日本於 2016 年制定《部落歧視消除推動法》（部落差別の解消の推進に関する法律，簡稱部落差別解消推進法），宣示了消除部落民歧視遭遇的決心，惟該法的內容大多屬於宣示性規定，例如宣示國家教育義務、要求國家與地方政府應建立諮詢體制等，卻無相應之罰則或其他法律強制力之規範，對於問題之解決效果有限[643]。

在對於非日本國籍人之歧視或仇恨言論部分，為籌辦 2020 年東京奧運，聯合國種族歧視消除委員會（Committee on the Elimination of Racial Discrimination, CERD）在 2014 年時要求日本政府制定「綜合性的禁止種族歧視法律」。作為回應，日本於 2016 年制定《仇恨言論消除法》（本邦外出身者に対する不当な差別的言動の解消に向けた取組の推進に関する法律，簡稱ヘイトスピーチ解消法）。

《仇恨言論消除法》從其法律全名及第 2 條之名詞定義可見，所要保護的是「對外國出身之人」，也就是「本國（日本）之外的國家或地區出身者及其子孫」。該規定並非以國籍作為界定是否受到保護的判斷基準，可見立法者所欲保護不受歧視之範圍，除外國人以外，也包括外國出身但已歸化為日本籍，或因歷史原因繼續在日本生活而未取得日本國籍者（如前述在日朝鮮人等）。

該法雖有七條，惟深究其內容可見，該法的體例及用詞與同年稍後通過的前述《部落歧視消除推動法》有異曲同工之妙。將《仇恨言論消除法》和《部落歧視消除推動法》的內容加以對比，將更為明顯。

---

642 吉田徳夫，法制史上より見た部落問題，關西大學法學論集，第 53 卷第 6 号，頁 1268-1269（2004）。

643 法務省人権擁護局，部落差別の実態に係る調査結果報告書，https://www.moj.go.jp/content/001327359.pdf，頁 186-187（2020）。

表 10：《仇恨言論消除法》與《部落歧視消除推動法》條文比較

規範內容	條文位置與概要說明	
	《仇恨言論消除法》	《部落歧視消除推動法》
立法目的	第 1 條：揭示本法所要消除者，是對外國出身之人（不限於外國籍人）的歧視和仇恨言論。	第 1 條：揭示本法所要消除者，是對部落民的歧視情形，包括但不限於言論、差別待遇或其他行為，以期待打造日本憲政體制下人人生而平等之國度。
名詞定義	第 2 條：定義本法所稱「外國出身之人」的範圍。	（無規定）
基本理念	第 3 條：揭示本法制定之理念，乃基於使國民充分理解禁止對外國出身之人歧視之重要性。	第 2 條：揭示本法制定之理念，乃基於使國民充分理解每位國民人人平等享有基本人權及尊重之重要性，以實現消除部落歧視之社會。
國家及地方政府之責任	第 4 條：揭示國家與地方政府有積極制定與推動政策，以改善輿論環境之義務。	第 3 條：揭示國家與地方政府有積極制定與推動政策，以促使達成基本理念之義務。
諮詢體制之完善	第 5 條：國家與地方政府應完善諮詢體制，共同承擔針對外國人不當言論之諮詢工作，並協助處理紛爭。	第 4 條：國家與地方政府應完善諮詢體制，並共同分擔諮詢工作，以回應國民對該法實施與部落歧視狀態之諮詢。
教育活動	第 6 條：國家與地方政府應努力透過教育活動消除對外國人的歧視與偏見。	第 5 條：國家與地方政府應努力透過教育活動與啟發活動等方式，消除對部落民及部落出身者或相應地區的歧視與偏見，並促使國民深知消除歧視之重要性。
啟發活動	第 7 條：國家與地方政府應透過啟發活動等能夠宣傳政令之方式，使國民深知消除不當言論的重要性。	
歧視狀況之調查	（無規定）	第 6 條：國家應與地方政府協力，調查部落歧視的實際情況。

資料來源：本研究自行整理

透過上表可看出，兩者之間體例幾乎相同，故也有著相似的缺點。換言之，《仇恨言論消除法》與《部落歧視消除推動法》的性質都偏向政令宣示性的規範，試圖透過教育和啟發民眾良知的方式，逐漸達到立法目的，而缺乏關於罰則等法律強制力之規定。

因此，當仇恨言論、歧視言論出現時，在刑事責任上，僅能回到如《刑法》關於名譽毀損罪、侮辱罪之規定處理，並依前開罪名之構成要件加以檢驗與論斷其刑事責任；而在民事責任上，則應依《民法》第 709 條以下關於名譽侵害之損害賠償責任之規定處理，而不能直接適用《仇恨言論消除法》與《部落歧視消除推動法》對加害人論處。

此外，由於《仇恨言論消除法》與《部落歧視消除推動法》屬於廣泛性的規定，就網路仇恨言論或歧視言論之問題，則並未有細部之特別規範。因此，就網路仇恨言論與歧視言論，仍應回歸各該相應之責任條文（如《民法》、《刑法》等）或《服務提供者責任限制法》的相關規定處理。

三、第三方監督或產業自律機制

（一）產業自律機制

如前所述，當涉及言論自由爭議時，日本的制度較避免直接使用法律強制效力予以規制，而是常以透過產業自律的方式達到類似的規制效果。是以，本部分將針對日本現行的自律機制，以不實訊息為例加以說明。

就不實訊息的處理方式，日本採行的政策係由政府先行制定政策方針及目標後，由各平臺業者自行決定具體政策，以達到打擊、消除不實訊息及其影響之政策效果。總務省於 2020 年時公布了《平臺服務研究會最終報告書》（プラットフォームサービスに関する研究会最終報告書），其中即揭示了政府對於不實訊息的對應政策方針，仍以平臺自律作為施政核心[644]。

[644] 総務省，プラットフォームサービスに関する研究会最終報告書，頁 35-50（2020）。

由於大部分平臺業者採行之措施大同小異，故以下就日本最常使用的入口網站 Yahoo! JAPAN 及最常使用之通訊軟體 LINE 二家平臺業者所執行之自律機制說明之[645]。

1. Yahoo! JAPAN

Yahoo! JAPAN 是日本市占率最高的入口網站[646]，除搜尋引擎服務外，亦提供如新聞、股市、天氣預報等資訊服務，且在營運上與 Yahoo! 美國母公司完全切割，已有日本本土化之性質[647]。

除了新聞服務外，Yahoo!自早期即開發了 Yahoo!知識＋的服務，該服務的運作方式，係由使用者在網站上發問，由其他使用者針對該問題提供答案，並由其他非發問者與答覆者之使用者們票選最佳解答之服務。在該服務最初設計的流程架構下，資訊的提供與獲取均由使用者們自行達成，Yahoo!則扮演著提供媒合發問者與回答者的平臺之角色。

雖然該服務已在世界上大多數的國家停止提供，惟日本是唯一尚未停止該服務的國家（以「Yahoo!知恵袋」的名稱提供服務）[648]，且每日仍有許多使用者在該平臺上發問與回答[649]，故維護該平臺上資訊的品質，便成為維持該平臺運作時最重要的課題。

---

[645] 本部分之內容，參考自総務省プラットフォームサービスに関する研究会，偽情報対策に係る取組集 Ver. 1.0， https://www.soumu.go.jp/main_content/000868124.pdf（2023）。

[646] 依據 similarweb 網路流量分析公司的數據，在 2023 年 11 月，Yahoo! JAPAN（yahoo.co.jp）是日本流量次高之網站（最高為 google.com）。值得注意的是，由於 Yahoo! JAPAN 旗下的各項服務分屬子網域不同，在該流量分析上被界定為不同之網站，例如其新聞服務（news.yahoo.co.jp）為第 7 名，購物服務（shopping.yahoo.co.jp）則為第 30 名。參見 similarweb，https://www.similarweb.com/zh-tw/top-websites/japan/（最後瀏覽日：2023 年 12 月 29 日）。

[647] 2023 年 10 月起，日本雅虎與 LINE 等 5 間企業合併為 LINE 雅虎股份有限公司（LINE ヤフー株式会社，LY Corporation），並以日本為主營業所之所在地。

[648] Yahoo!知識＋自 2012 年末起停止韓國之服務，2013 年起停止中國大陸之服務，除日本外其他國家或地區的該服務則自 2021 年 5 月 4 日起停止提供。日本 Yahoo!知識＋的服務網站至今仍在運作中，詳見 https://chiebukuro.yahoo.co.jp/（最後瀏覽日：2024 年 1 月 2 日）。

[649] 以 2024 年能登半島地震之事件為例，本研究於 2024 年 1 月 2 日下午 2 時（約為地震發生後 23 小時）以「能登」為關鍵字於「Yahoo!知恵袋」搜尋 24 小時內發問的問題，共有 594 條發問，其中 88 條已被回答，且大多與地震相關，如地震與海嘯對當地核電廠是否有影響乃至於地震使家貓受驚嚇不願進食該如何處理等，問題繁多且五花八門，可見該服務至今仍有穩定的使用率。

準此，作為日本最大入口網站之服務提供者，Yahoo! JAPAN 在打擊不實訊息的部分，有以下策略與具體作為。

（1）提供高度信賴性的資訊[650]

由於不實訊息的持續流通，當在相同主題上有不同結論的資訊在資訊空間流通時，對於使用者而言就會造成諸多困擾與不便。以近年新冠病毒（Covid-19）疫苗為例，光是「疫苗究竟有沒有施打必要」這個問題，正反兩面都有不同的資訊，且後面都有著不同的立論基礎（不管這個立論基礎是否正確）。

這個狀況在 Yahoo!知識＋服務中尤其常見，由於該服務係由使用者自行發問、自行回答，沒有任何答案驗證或事實查核措施，故當緊急事件發生又缺乏穩定的資訊提供管道時，這樣的狀況就極容易使使用者感到困惑。

因此，Yahoo!在其所提供之新聞服務中，針對不同主題設計特別主題網站（特設サイト），並由相關領域的專家提供資訊內容，例如防災資訊[651]、性教育[652]、戰爭[653]等，透過由專家提供的資訊建立值得信賴的資訊環境。

至於在 Yahoo!知識＋服務中，當系統偵測到有相關主題的問題時，系統便會自動在該問題的下方註記相關政府機關的網站，例如在與新冠肺炎有關的問題中，系統即會在該問題下方註記厚生勞動省（厚生労働省）等與防疫有關主管機關之官方網站，確保使用者能夠獲得正確的資訊。

另外，作為全日本最大的入口網站，Yahoo!則透過將使用者誘導到將各媒體提供之新聞資訊集中刊登的主題網站之方式，提供關乎生命財

---

650 総務省プラットフォームサービスに関する研究会，前揭註 645，頁 1。

651 9.1 防災の日＃災害に備える，https://www.bosaiguide.jp/bosainohi/?cpt_n=yj_news&cpt_m=all&cpt_s=hotissue_bnr（最後瀏覽日：2024 年 1 月 2 日）。

652 みんなの性教育，https://news.yahoo.co.jp/pages/20221118a（最後瀏覽日：2024 年 1 月 2 日）。

653 つなぐ＃戦争の記憶，https://wararchive.yahoo.co.jp/2023/（最後瀏覽日：2024 年 1 月 2 日）。

產之重大事項。在緊急事件發生時，則提供如首相記者會等影片在首頁，確保使用者能夠從速獲取重要資訊。同時，當如地震等重大緊急事故發生時，Yahoo!也將配合政府同步以最快的速度，發布相應的警報措施。

（2）推動媒體識讀措施[654]

在媒體識讀方面，Yahoo!則透過開設備有媒體識讀教材之「Yahoo!新聞健診」網站，提供使用者學習破解不實資訊的學習管道，並與大學等教育機構協同合作，繼續提供各年齡層針對事實查核對策的媒體識讀業務，同時在如選舉等重大活動接近時，開設相應的主題網站，並與專業人士一同維護主題網站的內容查核，從媒體面強化媒體識讀措施。

（3）消除不實訊息[655]

如前所述，不實訊息在網路上流傳的情況甚篤，尤其是未有監督機制的 Yahoo!知識＋服務更是如此。當不實訊息持續在平臺上流通時，輕則誤導民眾，重則與生命財產安全攸關。是以，Yahoo!除了在其新聞服務中，禁止留言可能影響他人生命財產或健康安全之錯誤資訊外，若 Yahoo!知識＋的回答內容顯然與事實違誤，或其內容可能招致社會混亂時，Yahoo!將會從速查證並予以刪除。

2. LINE

LINE 是日本使用率最高的網路通訊服務之一，且除了通訊服務外，亦有如 LINE NEWS 等提供資訊的新聞服務。是故，LINE 旗下的服務除了可能成為不實訊息的溫床外，也可能透過其通訊服務，成為不實訊息流通的管道。為防不實訊息的擴散，LINE 制定並實行了以下策略。

（1）刪除不實資訊[656]

作為 LINE 最主要的功能與最初開發的，個人之間的通訊即 LINE 開發最初的功能。而 LINE 在通訊上的功能，可以分成「個人聊天」、「群

[654] 総務省プラットフォームサービスに関する研究会，前揭註 645。
[655] 総務省プラットフォームサービスに関する研究会，前揭註 645。
[656] 総務省プラットフォームサービスに関する研究会，前揭註 645，頁 2。

組聊天」及「社群聊天」（オープンチャット，Openchat）三種功能，由於加密技術上的不同，這三種聊天功能可以大致分為二類，即「個人與群組」和「社群」二種模式。這二種模式之間有著許多的不同點，本研究將與不實訊息的刪除相關兩種模式不同之處整理如下表，並於後段接續說明。

表 11：LINE 群組（グループ）與社群（オープンチャット）功能差異

主要差異	LINE 群組	LINE 社群
人數上限	500 人	5,000 人
管理員	無	有
歷史訊息可讀性	新成員無法 閱讀歷史訊息	新成員可以 閱讀歷史訊息
點對點加密	有	無 （屬於公開聊天室）
溝通內容限制	採最高隱私的 訊息加密技術	■ 需遵守 LINE 社群守則 ■ 透過人工智慧技術過濾違規內容 ■ 管理員可設定要過濾的關鍵字

資料來源：LINE[657]

從上表的加密技術可見，LINE 群組（一對一的個人聊天亦如是）傳訊功能採用的是點對點加密技術，基於保障個人之間秘密通訊自由之本旨，LINE 企業並未有將經點對點加密技術加密的訊息予以解密之能力。而這樣的加密技術在 LINE 社群功能並不適用，故 LINE 官方對於在 LINE 社群上進行的訊息傳輸能夠直接閱讀並干預，而有能夠對社群內訊息加以處理之權限。是以，本部分 LINE 所採行的刪除策略，專指在 LINE 社群上面的訊息刪除，不及於個人聊天室與群組聊天室，合先敘明。

657 【LINE 社群】搶先看！全新網路聊天室「LINE 社群」將在台推出，LINE 官方部落格（2020/05/07），https://line-tw-official.weblog.to/archives/82874924.html（最後瀏覽日：2024 年 1 月 3 日）。

由於 LINE 社群功能大多具備公開（或半公開[658]）的特性，成員來自四面八方且管理員不一定認識，加上人數上限眾多，人多嘴雜難免形成不實訊息的溫床。因此，LINE 在其社群規則中強調禁止真偽不明之資訊擴散，並積極針對煽惑人心的謠言或假新聞予以刪除。

根據 LINE 所公布的訊息刪除基準，當使用者所發表之訊息符合下列事項之一者，LINE 即會予以刪除，並透過人工智慧予以過濾：(1)對健康可能造成深度危害之錯誤資訊，或恐生社會混亂者；(2)經政府官方否定的資訊，或依據該資訊而衍生之其他主張者。除此之外，管理員遇有不實訊息或疑似不實訊息出現時，亦可透過刪除訊息或將部分關鍵字列入社群黑名單之方式，阻止相關訊息擴散。

（2）假新聞的防堵與消除[659]

在 LINE 新聞方面，每逢重大事件發生，即常有不實訊息乃至於假新聞（フェイクニュース，Fake news）在資訊世界中迅速流通，而新聞製作具備時效性，倘每則在資訊世界中流通的訊息均需徹底確認真實性後方為刊登，則有悖於時效性之情況；但未經確認真實性之資訊即製作成新聞後從速發表，又對新聞之真實性有所忽略。是以，LINE 亦積極擬定此種狀況之對策。

由於 LINE 新聞編輯部人手不足，為衡平上述新聞時效性與真實性之拉扯，LINE 新聞之報導文章中，除報導文本本身外，亦將諮詢專家並在報導網頁明顯處提供相關中央省廳之網站，或提供 NHK 針對相同事件之新聞報導之連結等，確保使用者除了以 LINE 新聞作為資訊來源外，亦有其他可信的資訊來源可供參考。

除此之外，LINE 也接受了政府的補助，開設了 LINE 新聞的官方帳號，提供經 LINE 新聞編輯部事實查核之新聞資訊，並以通知的方式向使用者推播，傳達更為真實的資訊。

---

[658] 同上註。LINE 社群的加入方式共有三種，除最常見的開放公眾直接加入外，亦有輸入參加密碼和管理員核准等另外二種，分別屬於公開、半公開（知道密碼即可邀請他人加入，不限管理員）與不公開三種性質。

[659] 総務省プラットフォームサービスに関する研究会，前揭註 645，頁 2-3。

（3）推動媒體識讀[660]

就不實訊息之遏止方面，除了透過阻斷訊息之傳遞外，透過培養公眾媒體識讀能力的方式，更能從傳遞者的角度直接掐斷資訊的傳遞，並能有效促使正確資訊的流通。準此，LINE 公司與其他民間機構一樣，開展與推動媒體識讀相關之啟發活動，改善公眾看待媒體的模式，並打造完善的媒體流通場域。

為達到前述效果，LINE 透過其出資成立的「財團法人 LINE 未來基金會」（一般財団法人 LINE みらい財団）製作可供公眾廣泛閱讀、使用之媒體識讀教材，並刊登於其首頁上，不僅歡迎公眾無償使用外，亦積極與地方政府接洽，希冀推廣其教材至各地方各形式之教育場域中。

（二）事實查核機構

除了產業自律機制外，為了阻斷不實訊息的傳遞，日本亦有如社團法人安全網路協會（一般社団法人セーファーインターネット協会，以下簡稱 SIA）、日本事實查核推廣協會（特定非営利活動法人ファクトチェック・イニシアティブ，以下簡稱 FIJ）等非營利組織，提供事實查核業務。

SIA 成立了日本事實查核中心（日本ファクトチェックセンター，JFC），並專責事實查核工作，針對網際網路上流通之不實訊息進行查核，並透過社群平臺與新聞網站等管道發布其查核報告[661]。

而 FIJ 所執行之業務，則較專注於擔任媒體業者背後的協力角色，透過其開發的自動偵測系統「Fact Checking Console, FCC」自動收集網路上流竄的真偽不明資訊，加以判讀、查核，並將查核後的結果儲存於其開發的資料庫「Claim Monitor」中，提供給媒體業者參考[662]。

---

[660] 総務省プラットフォームサービスに関する研究会，前掲註 645，頁 2。
[661] 総務省プラットフォームサービスに関する研究会，前掲註 645，頁 8。
[662] 総務省プラットフォームサービスに関する研究会，前掲註 645，頁 9。

四、小結

爬梳日本的網路監管制度可以發現，基於保障公眾言論自由之目的，也為了防止寒蟬效應之發生，日本的網路監管法制仍比其他國家保守，仍舊以產業自律作為其監管政策的定海神針。雖然不是沒有討論過是否改變現有的保守監管制度，惟目前的學界與研究建議都依舊採行反對的觀點。

日本目前的監管政策，係以政府透過政策推動的方式標定一個方向，而產業界則依循該方向建立自己的自律政策，或共同建立自律框架等，政府對於自律政策、自律框架則採不干預之態度，因而未有制定任何具備法律強制力之監管條文。

另一方面，雖然日本制定了許多法律條文，試圖透過法律的制定推動網路環境乃至於公共言論場域的改善，惟這些法律通常不具備法律強制力，惟 ISP 業者能夠透過《服務提供者責任限制法》的規定，在符合特定要件或為特定措施之情況下，得主張免除其民事責任。

不過，由於網路言論環境每況愈下，日本也漸漸有希冀政府管理不實訊息或網路霸凌等聲音，故日本接下來會如何調修其既有之條文，值得後續追蹤。

第十節　韓國

一、監理脈絡

2020 年起，韓國以打造公平網路平臺環境出發，陸續提出《網路平臺通訊銷售中介交易公平法》(온라인 플랫폼 통신 판매 중개거래의 공정화에관한법률)、《網路平臺中介交易公平法》(온라인 플랫폼 중개거래의 공정화에관한 법률)、《網路平臺使用者保護法》(온라인 플랫폼 이용자 보호법) 等涉及數位平臺規範之草案，期望課予數位平臺業者較強之事前與事後規範，強化小型企業與使用者之保護，但國會歷經一年多的爭論，卻依舊無法達成共識。

在 2022 年 5 月就任的第 20 任總統尹錫悅公布的「120 大國政課題」[663]中，對於平臺相關政策一改過往徘徊在重成長與重法規之間的兩難，明確訂定以政策支援擴大成長動能，並以競選時期提出的「平臺改革應是社會發展主導的重要角色之一」為主軸，確認推動平臺產業自我管理的政策，由企劃財政部 (기획재정부) 主導，科學技術資訊通訊部 (과학기술정보통신부)、公平交易委員會 (공정거래위원회)、通訊傳播委員會 (방송통신위원회) 等組成「跨部門平臺政策合議 (범부처 플랫폼 정책협의체)」[664]，商討平臺產業中長期政策，集結各能量協助制定平臺市場自律規範。

（一）平臺自律規範政策

前述提及之「跨部門平臺政策合議」以「平臺自律規範與政府支援自律規範之法律依據」為重點，於 2023 年完成各部會間協商後，提出《電信事業法》部分修正案，並由科學技術資訊通訊部與通訊傳播委員會提出立法預告，在 9 月 21 日至 30 日接受利害關係人等之建

[663] 詳見大韓民國政策簡報，政策資料→國政課題，https://www.korea.kr/archive/govVisionList.do（最後瀏覽日：2023 年 7 月 12 日）。

[664] 詳見大韓民國政策簡報，제 1 차 범부처 플랫폼 정책협의체 개최（召開第 1 次跨部門平臺政策會議），新聞稿（2022/07/06），https://www.korea.kr/briefing/pressReleaseView.do?newsId=156515280（最後瀏覽日：2023 年 7 月 12 日）。

言，後續向國會提出修正案，如順利通過，2024 年即可施行。

同時在協助平臺自律規範上，亦從 2022 年 8 月一路支持「民間平臺自律組織」的組成與運作，透過自律組織將原本平臺與進駐中小型商家之間的手續費、廣告費等契約條件透明化、防止購物平臺詐騙，以及推動快速應對體系等成果。這回的修正案是為民間自律規範活動、政府相關支援、政策提供法律依據，更具體的內容為協助建立、推動健全的交易秩序、消費者保護與共生協力等自律規範業務，並提供自律組織設立與運行之根據。通訊傳播委員會委員長指出「為嚴正應對平臺使用者利益侵害與不公平行為，同時因應技術與市場快速變化，難以將規範訂定於法律，期望透過本次修正案積極協助自律規範」，科學技術資訊通訊部部長也指出「透過此次的修法，可為政府與民間準備共同推動溝通、協力體系，更積極的應對民生問題」[665]。

不過公平交易委員會先於 2023 年 7 月 20 日表示，針對平臺獨寡佔制裁法案推動已在 1 月成立專家小組，並已大致論議完成，目前尚未確認是要修法、還是制定新的特別法[666]。後續又在 9 月 21 日宣布正在準備《線上平臺公平相關法》(온라인 플랫폼 공정화에 관한 법률)，並強調在交易環境與使用者保護端，賦予企業自律可讓企業之間有公平競爭環境，但獨/寡占問題就需有嚴正地應對措施，方可讓平臺、進駐業者與消費者可享受自律規範的成果[667]。公平交易委員會指出「目前正集中關注以電子商務、旅遊、住宿等核心平臺是否有違法的疑慮，預計年底前會完成調查」、「從 1 月到 6 月與專家小組歷經九次討論」、「關於平臺業者的不公正行為依舊會採行嚴厲的事後應對方針，但也需要事前的規範」。

---

[665] 이정현，'플랫폼 자율규제' 전기통신사업법 개정안 국무회의 의결，聯合新聞（2023/11/14），https://www.yna.co.kr/view/AKR20231114066800017?input=1195m（最後瀏覽日：2023 年 11 月 20 日）。

[666] 김성현，한기정 공정위원장 "플랫폼 규제 법제화 미정…계속 논의 중"，ZDNET Korea（2023/07/20），https://zdnet.co.kr/view/?no=20230720121526（最後瀏覽日：2023 年 11 月 20 日）。

[667] 김경미，정부, 플랫폼 자율규제 법제화 시동…“독과점엔 엄정 대응”，中央日報（2023/09/21），https://www.joongang.co.kr/article/25194088（最後瀏覽日：2023 年 11 月 20 日）。

相關業者期待平臺自律規範政策的啟動，但對於公平交易委員會在事先規範的立法準備，以及強化監控平臺業者不公平的行為措施備感混亂，相關業者指出「目前政府希望業者能自律規範，但卻又想對平臺產業進行法律規範的想法令人疑惑」、「從國家資源創造數位平臺政府，希望出口數位技術，但卻又認為需要事先規範，實在難以理解政策方向究竟為何」[668]。

對此，SHIN & KIM 律師事務所在「平臺自律規範相關立法與政策動向」[669]中整理了兩大注意事項：

其一，科學技術資訊通訊部與通訊傳播委員會提出《電信事業法》部分修正之立法預告，讓尹政府的平臺自律規範又再次獲得動力，期待業者可以更積極的擴大自律規範，但對於平臺獨寡佔的立法與平臺自律規範有所衝突的疑慮，有待政府與國會持續協調。

其二，自律規範需要業者積極參與並提出意見，才能更具體化這一政策的可行性，執行可能性也較立法高、同時亦能應對市場的多變性。此次在《電信事業法》部分修正案中，獎勵措施是依據自由規範的參與程度，應可期待實際成效，但若獎勵也無法鼓勵自律規範時，可能就會再次出現法制化之論議，因此就平臺業者立場看來，必須在遵守自律規範規約的同時，持續關注政府與國會的規範動向。

（二）韓國網路使用實情調查

根據「2022 網路使用實情調查報告」[670]，韓國全體國民的網路使用率在全韓國 2,136 萬戶中，有 2,136 萬戶有網路，占全體 99.96%。

---

[668] 김나볏，자율 규제냐 사전 규제냐…정책 엇박자에 플랫폼 업계만 '혼선'，newstomato（2023/09/15）：https://www.newstomato.com/ReadNews.aspx?no=1201440（最後瀏覽日：2023 年 11 月 20 日）。

[669] 법무법인 유한 세종，플랫폼 자율규제 관련 입법 및 정책동향，SHIN & KIM 律師事務所官方部落格（2023/10/04），https://blog.naver.com/shinkimlaw/223227806990（最後瀏覽日：2023 年 11 月 20 日）。

[670] 2022 인터넷이용 실태조사최종보고서，詳見韓國智慧資訊社會研究院（NIA）網站，https://www.nia.or.kr/site/nia_kor/ex/bbs/View.do?cbIdx=99870&bcIdx=25521&parentSeq=25521（最後瀏覽日：2023 年 7 月 14 日）。本調查報告為年度常態調查報告，2022 年的調查期間為 8 月 1 日～9 月 30 日，滿 3 歲以上之常住家戶人口，排除軍隊服役者、長期滯留海外者、受刑人等，調查方式為家戶拜訪訪談。

就網路使用人數來說，滿 3 歲以上的國民中有 5,081 萬人，近一個月內有使用網路者的比例高達 93%，約有 47,253,345 名使用人數；就性別來說，男性的使用率（94.5%）較女性使用率（91.5%）多 3.0%；在年齡層部分，近五年間 60 歲以上高齡者的網路使用率有增加的趨勢。至於行動裝置上網之使用率，相較 2018 年亦增加 1.6%，達到 92.0%。

在韓國 17 個行政區中，有 14 個行政區的網路使用率達到 90%以上；週平均的網路使用時間比 2018 年增加 5.6 小時，達到 22.1 小時。

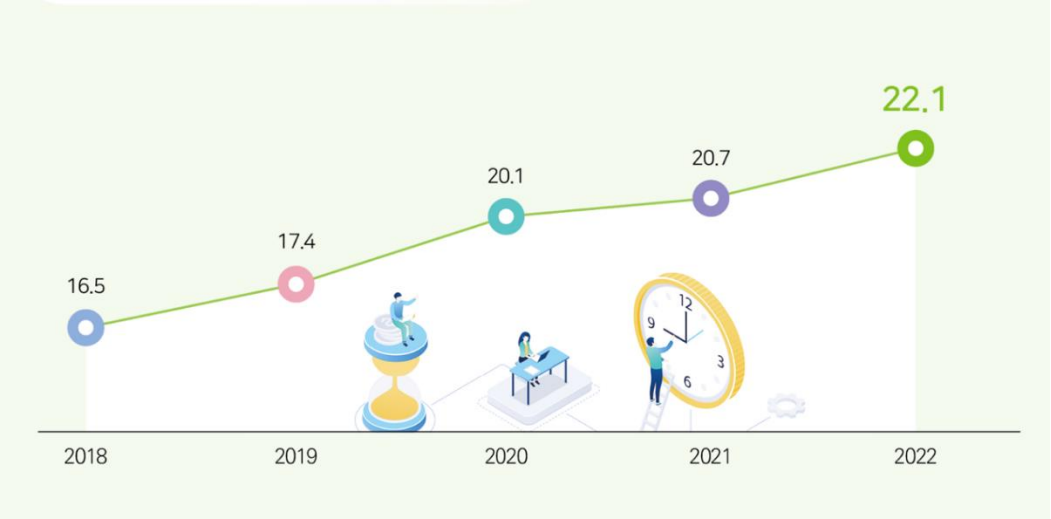


圖 21：韓國民眾週平均網路使用時間歷年變化

資料來源：2022 網路使用實情調查報告[671]

年滿 6 歲以上的網路使用者大多數（98.5%）都使用即時訊息，除了對話（100%）外，依序是檔案分享（82.4%）、聲音與影像通話（63.5%）、網購（38.3%）、確認配送資訊（35.9%）、地圖與位置分享（35.3%）、遊戲（30.2%）、匯款服務（29.9%）等；在網路購物使用率，滿 12 歲以上的網路使用者，在 Covid-19 以來，網路購物的頻率與購買費用都有增加的趨勢，從 2019 年的月平均使用 3.3 回、平均購買費用 114,163 韓元，增加到 2022 年的月平均使用 6.3 回、平均購買費用 192,759 韓元；網路銀行的使用率，也是在 Covid-19 以來持

[671] 同上註。

續成長，從 2018 年的 63.7%到 2022 年的 79.2%。

另一方面，年滿 3 歲以上的網路使用者在影片服務的使用率也是過去三年間持續增加，從 2020 年的 92.7%成長至 2022 年的 96.1%，而每天利用影片服務一次以上的使用者比例，則達 76.2%。最後，是因應 Covid-19 的線上教育系統使用率，在滿 3 歲以上網路使用者是 39.8%，而學生的使用率是 94.1%。

就這一份年度調查報告可看出，如今是可說是影片的全盛時代，96.1%的韓國國民使用影片服務，智慧型電視與 OTT TV 平臺的利用比率也有擴大的趨勢，使用者使用的平臺也因使用者增加而在平臺的選擇上逐漸多元化，同時在 1 人家庭增加與高齡社會的影響之下，70 歲以上使用影片服務的比率也逐步增加，從 2019 年的 47.1%攀升至 2022 年的 82.4%，四年間就增加了 35.3%，其中增加幅度最明顯是影片服務平臺 YouTube，從 2019 年的 43.8%到 2022 年的 77.2%，幾乎是以每年增加 10 個百分點的趨勢增加。

再者就是以數位為基礎的經濟、社會活動也持續擴散，網路購物的使用率也持續增加至 73.7%，網路購物的結帳方式在信用卡部分從 2019 年的 73.0%下降到 2022 年的 63.8%、Check Card[672]則是從 2019 年的 36.6%下降至 2022 年的 26.4%，然而電子支付從 2019 年的 39.6%上升至 2022 年的 56.1%、網路銀行從 2019 年的 64.9%上升至 2022 年的的 79.2%。

二、政府機關法制政策作為

（一）主管機關

韓國目前在《電信事業法》（전기통신사업법）之主管機關係科學技術資訊通訊部及通訊傳播委員會（방송통신위원회）;《資通訊網路使用促進與及資訊保護法》（정보통신망이용촉진및정보보호등에한법률，以下簡稱《資通訊網路法》）之主管機關則係通訊傳播委員會。科學技術資訊通訊部主管通訊傳播業務，政策方向係為促進通訊

[672] Check Card 是一種與銀行帳戶連動的卡片，類似我國的簽帳金融卡。

傳播產業之發展[673]，而通訊傳播委員會負責通訊傳播產業之監管與使用者保護，同時為保障傳播產業之自由、公共性與公益性，推動相關政策[674]。

（二）線上違法內容處理機制

根據《通訊傳播委員會設置暨營運法》(방송통신위원회의 설치 및 운영에 관한 법률）第 18 條成立的通訊傳播審議委員會（방송통신심의위원회)，其職務明定於同法第 21 條，包含受理《放送法（방송법)》第 32 條，以及《資通訊網路法》第 44 條之 7 的審議申訴，因此通訊傳播審議委員負責受理電視廣播類申訴、資訊通訊的違法、有害資訊申訴、網路受害救濟，以及全年無休受理數位性犯罪申訴，透過即時審議在 24 小時內提出修正要求(刪除、阻斷連線)，且要求國內、外業者基於自律規範而儘速處理[675]。

1. 《資通訊網路法》

根據《資通訊網路法》第 44 條之 7 的第 1 項所列出的非法流通資訊可分為兩大類。第一類是第 44 條之 7 第 1 項的第 1 款到第 6 款、第 6 款之 2 與第 6 款之 3：

- 散布、販售、租任或公然展示色情符號、文字、聲音、圖像及影像內容之資訊（第 1 款)。
- 以誹謗他人為目的，揭露含有損害他人名譽之事實或虛偽不實內容之影像（第 2 款)。
- 反覆送達當事人，致心生恐懼、不安之符號、文字、聲音及圖像之資訊（第 3 款)。

673 科學技術資訊通訊部主管業務，詳見官網：https://www.msit.go.kr/contents/cont.do?sCode=user&mPid=131&mId=198（最後瀏覽日：2023 年 7 月 12 日)。

674 通訊傳播委員會之願景及任務，詳見官網：https://kcc.go.kr/user.do?page=A04010400&dc=K04010400 （最後瀏覽日：2023 年 7 月 12 日)。

675 通訊傳播審議委員會綜合申訴中心，http://www.kocsc.or.kr/PageLink.do（最後瀏覽日：2023 年 7 月 14 日)。

- 無正當事由而以毀損、滅失、變更或偽造等方法，妨礙資訊通訊系統、數據檔案或電腦程式等之內容資訊（第 4 款）。
- 以盈利為目的，不履行確認使用者年齡、標示義務，提供含有《青少年保護法》規範之有害青少年視聽物之內容資訊（第 5 款）。
- 法令禁止之賭博行為的內容資訊（第 6 款）。
- 違反本法與個人資訊保護法規範之個人資訊交易之內容資訊（第 6 款之 2）。
- 可製作槍砲、彈藥（包含會危及生命、身體之具有爆炸物）的方法或設計圖等資訊（第 6 款之 3）。

上述各款，根據同條第 2 項，經過審議委員會審議，得責令資訊通訊服務提供者或營運管理者拒絕、終止、限制；但第 1 款、第 2 款、第 3 款不得違背受害者意願。

第二類是第 44 條之 7 第 1 項的第 7 款到第 9 款：

- 洩漏依據法律規範為秘密等的國家機密之內容資訊（第 7 款）。
- 《國家安全法》禁止之行為，如何執行之內容資訊（第 8 款）。
- 此外，以犯罪為目的、或教唆、幫助的內容資訊（第 9 款）。

上述各款，根據同條第 3 項，通訊傳播委員會在符合下列 3 款情況時，應責令資訊通訊服務提供者或營運管理者拒絕、終止、限制。

- 相關部門首長的請求（第 9 款資訊中，包含對《性暴力犯罪特別法》第 14 條所規範的影像照片、其複製物與複製物的複製物的搜查機關首長的請求）。
- 第 1 款請求起 7 日內經過審議委員會審議後，根據《通訊傳播委員會設置暨營運法》第 21 條第 4 款提出修正要求。
- 資訊通訊服務提供者或營運管理者不理會修正命令。

再者，根據同法第 4 項，通訊傳播委員會於第 2 款、第 3 款時，應給予相關業者說明機會，但若涉及下列情況，則可不給予機會。

- 基於公共安全與福利需緊急處置時。
- 聽取說明明顯有困難或明顯不需要，由總統令訂定之。
- 明白表示放棄說明機會。

2. 《資通訊審議規定》（정보통신에 관한 심의규정）

本行政規範是規範通訊傳播審議委員會根據《通訊傳播委員會設置暨營運法》第 24 條第 2 項執行同法第 21 條第 3 項（即為《資通訊網路法》第 44 條之 7）、第 4 項的必要事項與基準。

在本規範中，第 4 條為審議的基本原則。第 1 項中，要求委員會以最少規範原則、公平客觀原則、迅速原則、個人資訊暨私生活保護原則為審議基準；同時在審議時應考量下列情況：

- 考量違反國際和平秩序、憲政秩序、犯罪，以及違反法律、善良風俗、社會秩序的比重。
- 考量社會倫理、文學、藝術、教育、醫學、科學的不同特性。
- 是否危害健全倫理、法律意識、社會通念。
- 資訊的表現樣式、性格與影響、內容與主題、整體脈絡。

3. 杜絕數位性犯罪貼文之法律修正[676]

自 2020 年以來，韓國雖已通過多部數位性犯罪相關法案，但「威脅兒童與青少年，製作性壓榨影片的 L 事件」、「與大邱非面對面小額借貸相關的性壓榨影片」等數位性犯罪的事件依然層出不窮，其中又以 2020 年 3 月之 Telegram「N 號房事件」引發社會廣泛討論。該案件係 2019 年 2 月在隸屬於海外 SNS 所開設的團體聊天房中，有生

[676] 趙英基（조영기，音譯），數位性犯罪發文根絕了嗎？事前處置義務的現況與限制（디지털 성범죄 게시물은 근절되고 있나? -사전조치 의무의 현황과 한계），KISO JOURNAL，第 50 期，頁 2-6（2023）。

產、交易、散佈淫亂物的數位性犯罪事件，透過N號房製作、散布包含未成年人、女性的性壓榨淫亂物，數千個影片透過虛擬貨幣交易，爾後 Telegram N 號房嫌疑人陸續被逮補，2021 年 10 月 N 號房的主嫌被宣判 42 年有期徒刑，也讓國會通過《兒童暨青少年性保護相關法》(아동·청소년 성 보호에 관한 법률）與《性暴力犯罪處罰特別法》(성폭력 범죄의 처벌 등에 관한 특례법）的制定與修正。

先談及《性暴力犯罪處罰特別法》的修訂，在第 14 條第 4 項中明訂擁有、或僅是觀看非法影片亦可處罰；第 14 條之 2 訂出深偽技術（deepfake）處罰規範，也在第 14 條訂出就算是拍攝者是受害者自己，但與受害者意志無關，只要散布即可處罰，為數位性犯罪提供一嚴懲的法律根據。又因網路特性使然，數位性犯罪物一但散布，就會造成受害者無限的痛苦，所以《電信事業法》、《資通訊網路法》、《性暴力犯罪處罰特別法》、《兒童暨青少年性保護相關法》等被稱為「N號房防止法」的通過，也進一步強化業者快速阻斷，將傷害降到最小的責任，同時也明定網路業者在數位性犯罪上的義務。

「N號房防止法」強化業者快速阻斷，將傷害降到最小的責任，同時也明定網路業者在數位性犯罪上的義務，首先是《電信事業法》在 2020 年 5 月的修正，平臺營運業者必須阻止非法影片散布，並協助檢舉與刪除，為了能事前防止這一類散布，可採用技術與監管的處置（第 22 條之 5 及第 22 條之 6)，適用對象包含硬碟業者與前一年度賣出額度達 10 億韓元以上，或以前一年度末為基準之前的 3 個月，每日平均使用者數達到 10 萬名以上規模，以及提供 SNS 的加值電信業者，且向一般不特定或多數大眾（包含向公眾開放之聊天室)(《電信事業法施行令》第 30 條之 6)；在《資通訊網路法》可稱為「深偽技術（deepfake）防止法」，開發能識別深偽技術之技術工具，並普及之（第 4 條)，防止非法影片散布讓受害者受到二次受害（第 44 條之 9 等)，以及與其他法律競合時的優先適用（第 5 條)。

不過，實際上數位性犯罪事件可能比上述規模還小，且若發生在沒有於韓國境內登記為加值電信業者時，因現行法律無法涵蓋，執行上就會有所受限，例如發生在 Telegram 的事件；且就算課予平臺防

止非法資訊散布的義務，現行法上也只有具一定規模以上的業者，才適用國家提供的過濾技術，做出事前處置的義務。

再者，目前政府嘗試允許事前將使用者內容與既有的數位性犯罪物資料庫結合過濾，期望達到預防數位性犯罪的效果，但這難以透過強制施行而達到實際效果。就適用對象來說，除了先前提及的大規模業者外，若為國外業者，僅能要求協助調查，從現實層面的數據看來，目前 2 萬 6 千多件案件中，僅有 58%回應並積極協助調查，因此需要積極強化國際協力與國外協助。

再來就是過濾技術的限制，內容過濾技術是系統以特定關鍵字與模式，判定是否進行過濾、阻斷，但這一方法時而可能導致正當的內容遭到過濾、阻斷，目前國家資料庫採行的方式是一旦匹配就立即阻斷，所以難以掌控有否誤判的情況，而當過濾系統出現誤判，將使用者的正常內容阻斷時，可能讓使用者產生不滿，也拉低該使用者對該使用平臺的信任感。

另一方面，過濾技術是基於已發現的性犯罪物數據資料，所以當有新的類型出現時便難以迅速反應；又，若使用者變更內容，例如變更、或壓縮解析度，單純的匹配技術可能無法識別。更不用說因杜絕數位性犯罪而投入的幾項措施，包含「監控」與「過濾」兩項技術僅適用部分大型業者，且有違憲法賦予國民的權利，所以在這幾部修正案提案的當下，不斷有人提出對於預先審查的擔憂、且以不具司法權的通訊傳播審議委員會審議、議決的內容，就阻斷相關發言的話，確實有侵害言論自由的疑慮，但相關法案依舊通過，業者也必須遵守相關法律，只是儘管採取了這些嚴格措施處置，數位性犯罪依舊透過各種管道持續發生。

從預防數位性犯罪的角度切入，確實獲得相當程度的共鳴，不過現今的處置義務從網路業者的角度看來，可能誤判正常內容為非法內容，除了會讓使用者產生不滿外，阻斷即導致內容毀損，所以針對誤判的賠償責任也是不得不面對的現實；而針對使用者在發表內容前，就可偵測的預先審查，也有法律責任的疑慮，以及採用過濾系統時，因傳輸過載導致使用者上傳或使用時產生不便，直接影響使用者的使

用經驗，事實上在測試階段，也發生過幾秒遲延的情況，不過最重要的是會增加企業的費用支出。

最後，從立法達成的角度看來，賦予業者的義務已經超過必要範疇，但當問題發生時，卻難以透過現行的規範要求業者達成要求，依舊有許多漏洞。縱使同意此一立法目的，仍不該以目的作為合理化這些行政規範與刑事處罰的根據，過度壓制或阻斷現代社會的網路訊息的傳播，始終是違反憲法基本權，因此不得不思考有否更有效的替代方案。

（三）假新聞與虛偽捏造資訊

原本韓國對於輿論的不實報導、違反《個人資訊保護法》、《刑法》等法律之內容，在官方有「輿論仲裁委員會」(언론중재위원회)、，在民間則有「韓國記者協會」(한국기자협회，下稱韓國記協)，前者處理輿論受害之救濟與報導審議（含選舉報導），協助調解、仲裁；後者則針對記者的不實報導、違法行為與違反記協規範進行懲戒。但由於近年來網路媒體興盛，假新聞與虛偽捏造資訊的問題逐漸浮上檯面，針對這一問題，除了是否危及新聞自由與言論自由外，法律是否有相關依據也是論爭焦點，不過這一論爭目前尚未有結論。

本節介紹輿論仲裁委員會、韓國輿論振興基金會（한국언론진흥재단)、通訊傳播審議委員會在這一議題中的職權、轄下相關單位，以及相關爭議內容。

1. 輿論仲裁委員會

關於假新聞與虛偽捏造資訊，在韓國訂有《輿論仲裁暨被害救濟等相關法》(언론중재 및 피해구제 등에 관한 법률)。本法目的為因媒體等相關輿論報導或媒介導致名譽、或權利受侵害，抑或在法益上有所爭議時，得以公正有效之救濟制度，確保言論自由與公義責任。並依據同法第 7 條成立「輿論仲裁委員會」。該委員會之業務主要分為兩大類，一是輿論被害救濟[677]與報導審議、二是輿論仲裁學院。在

[677] 輿論仲裁委員會→輿論仲裁救濟程序→輿論被害諮商，

輿論被害救濟部分，申請人只需是該報導的相關關係人，就算沒有公開全名，該報導內容足以讓周遭人士知曉即可申請調解或仲裁。

對於尚未報導的內容，亦可向法院請求禁止播放或出版，近期較為知名的案例即為 2021 年年底的「金建希 7 小時錄音事件」[678]。2022 年 3 月即將舉行第二十任總統選舉投票前，時為在野黨國民力量之總統候選人尹錫悅的夫人金建希與「首爾之聲」的記者長達 7 小時的通話錄音，MBC 原訂分兩集播出，播出之前，金建希選擇向法院提出禁止播放的假處分申請，最終法院核定無關公益、涉及私人的部分不得播出，其他尊重新聞自由，最終 MBC 選擇刪除法院核定不得播出的部分後播放，但原訂的兩集，僅播放一集。

在報導審議部份，設有一般報導與選舉報導相關審議委員會，針對相關新聞提出修正建議，但不具強制性。在研究刊物部分，有學術雜誌《媒體與人格權》(미디어와 인격권)、季刊《輿論仲裁》(언론중재)、網路雜誌《輿論人》(언론사람)、《年度輿論相關判決分析報告》(언론관련판결분석보고서)[679]、《海外言論法制研究報告/海外輿論判決集》與相關研討會的資料。

2. 韓國輿論振興基金會

韓國輿論振興基金會係依據《新聞等振興相關法》(신문 등의 진흥에 관한 법률) 第 29 條，為新聞暨網路新聞之健全發展與擴大閱讀文化與振興新聞產業)設置，主管機關為文化體育觀光部。於 2023 年 5 月 9 日[680]設立「假新聞被害申請、諮詢中心」(가짜뉴스 피해

https://www.pac.or.kr/kor/pages/?p=191&b=B_1_4&cate=F20&scate= （最後瀏覽日：2023 年 11 月 19 日）。

[678] 박효실，김건희 7 시간 녹취록에 갈린 입장... MBC'스트레이트' 방송취소, '열린공감 TV' 전체보도，스포츠서울（2022/01/21），https://www.sportsseoul.com/news/read/1092710?ref=naver （最後瀏覽日：2023 年 11 月 19 日）。

[679] 輿論仲裁委員會→資訊資料室→研究刊物→輿論相關判決分析報告：https://www.pac.or.kr/kor/pages/?p=201&magazine_new=M01&cate=MA05 （最後瀏覽日：2023 年 11 月 19 日）。

[680] 聯合新聞「가짜뉴스 신고·상담센터 출범…구제기관·법적 대응 안내」，聯合新聞（2023/05/09），https://www.yna.co.kr/view/AKR20230509076500005 （最後瀏覽日：2023 年 11 月 19 日）。

신고·상담센터）[681]。

該中心提供輿論仲裁委員會（新聞報導、報紙報導、網路新聞報導等已登記之媒體）、通訊傳播審議委員會（電視廣播一般、社群網路服務等一般資訊）、網站等各個網路、社群媒體業者（虛偽與非法有害資訊申請）的受害諮詢與調停申請程序、網路被害救濟申請程序與民刑事應對之法律知識與程序，並計劃與律師事務所簽訂委託契約，提供更有效率的法律應對方案（限定於一般諮詢，非訴訟代理）。

在假新聞的定義部分，該中心明示目前雖有多種定義，但中心處理的是針對受害者在線上、實體散佈的假新聞、虛偽捏造資訊、流言蜚語、錯誤報導等的救濟申請與諮詢。假新聞包含新聞網站或以輿論報導形式，透過媒體散佈與事實不符的資訊；虛偽捏造資訊係為假新聞的通用概念，意圖以似是而非的捏造資訊，不限定是新聞網站，包含透過網路、社群網路服務擴散之假資訊；流言蜚語則是口傳或個人之間流傳之未經證實且難以證實出處的資訊。

3. 假新聞（虛偽捏造）快速審議中心

通訊傳播委員會委員長於 2023 年 8 月 28 日就任，三週後提出杜絕假新聞方案，擴大通訊傳播審議委員會之審議項目，成立「假新聞（虛偽捏造）快速審議中心」(가짜뉴스[허위조작콘텐츠]신속 심의，下稱假新聞中心）[682]。

在成立依據上，假新聞中心根據《放送審議相關規則》第 9 條（公正性）第 1 項與第 14 條（客觀性），以及《資訊通訊相關審議規則》第 8 條第 3 項 11 款（混亂社會）與第 4 項 3 款（名譽毀損），進行審理，前者為放送，包含無線台、有線台、網播等，後者針對網站、網路媒體對一般人公開的文章、影片等，舉凡在緊急災難事項、重大公益毀損、對個人或團體造成難以恢復之損害、金融市場等引起嚴重社

681 韓國輿論振興基金會→客戶中心→假新聞受害申請、諮詢中心，https://kpf.or.kr/front/intropage/intropageShow.do?page_id=bcf25c2f61934ea4958b4081988b1162（最後瀏覽日：2023 年 11 月 19 日）。

682 放送通訊審議委員會官網：http://www.kocsc.or.kr/main/mainPage.do# →電子申訴→假新聞申訴→假新聞（虛偽捏造內容）快速審議中心。

會混亂的重大事項，但一般違反事項不包含在內。

同年 10 月 26 日，國會的科學技術資訊通訊委員會的國政監查時間，在野黨國會議員對通訊傳播審議委員會設置假新聞中心提出質疑，且指出通訊傳播審議委員會無審議「假新聞」的權限。對此，通訊傳播委員會提出 10 月 16 日於國務會議提交的「杜絕假新聞－推動現況暨法律根據」說明對假新聞的定義、審議權限與法律根據、國外案例[683]。

（1）假新聞、虛偽捏造資訊、錯誤報導

針對假新聞，通訊傳播委員會採取的定義為「基於政治或經濟利益，故意或惡意扭曲並傳播無根據或非事實的資訊」，並與相信「假新聞」為事實，事後發現為「錯誤報導」（misinformation）做區分。

然而輿論學界指出這一假新聞的定義與基本概念不符，首先是假新聞一詞應是指基於特定意圖（商業、政治、娛樂等動機）創造一虛偽資訊，並將這一虛偽資訊以新聞報導的方式呈現，也就是偽裝成輿論媒體發布的新聞報導，才稱為「假新聞」（Fake News）。不過亦有人將輿論媒體的新聞稱為假新聞，也就是將對於公職人員的在道德、或業務上進行正當監督的輿論報導、或對於政府政策批評的新聞，視為假新聞。因此通訊傳播委員會所提出的定義，應視為「虛偽捏造資訊」，因此假新聞中心的正式名稱也據此做出相應修正[684]。

（2）假新聞審議根據是「憲法法庭判決」

除了定義外，另一爭議就是審議假新聞的法律根據或權限。放送通訊委員提出是基於《通訊傳播委員會設置暨營運相關法》第 21 條，通訊傳播審議委員會職權的第 4 項「為健全通訊倫理涵養，透過電信通訊迴路對一般人公開、流通之資訊，其必要事項可由總統令訂定資

683 박효인，“용어는 오락가락, 근거는 발췌 편집”…방통위 보고서 살펴보니 [가짜뉴스]①」，KBS News（2023/11/02），https://news.kbs.co.kr/news/pc/view/view.do?ncd=7808374&ref=A（最後瀏覽日：2023 年 11 月 17 日）。

684 2023 年 9 月 26 日是以「假新聞審議專責中心」之名進行開幕式，然而在 10 月 23 日變更為「假新聞（虛偽捏造內容）快速審議中心」。

訊審議暨修正要求」，認為假新聞符合本項規範的「健全通訊倫理涵養之必要事項」，並以 2009 年通訊傳播審議委員會要求網路業者刪除「國內產水泥有毒」的特定留言，當時刪除要求之根據即為本條，且該案最終經過憲法法庭審判確定合憲為例。

通訊傳播委員會引用憲法法庭對於本條所謂「健全通訊倫理」一詞過於概括、「不明確」的意見如下：

> *（明確性原則）《通訊傳播委員會設置暨營運相關法》第 21 條的「健全通訊倫理」之概念多少有點抽象，然在利用電信通訊傳遞資訊的部分，應有社會要求的最少秩序、或道德，考量資訊通訊領域之廣範圍、迅速變化等多元可變的表現形態難以文字化，所以上述隱含表達方式不可避，因此不違背明確認原則（2011 憲가 13，2012 年 2 月 23 日[685]）。*

對此，金波拉美律師（DIKE 律師事務所）指出：「雖然當時針對該條文作出合憲判決，但該憲法法庭判決並非許可『健全通訊倫理涵養之必要事項』之無限制審議，理當回歸以《資通訊網路法》為基準進行審議」、「因在《資通訊網路法》找不到依據條文，所以在《通訊傳播委員會設置暨營運相關法》找到憲法法庭的相關判決」。崔祐晴韓國輿論法學會副會長也指出：「通訊傳播委員會所持的根據是擴大、推論解釋『健全通訊倫理』，可能會違反『犯罪與刑罰須由法律訂定』的罪刑法定主義」，並強調「侵害個人身體、財產法益的部分，須由法律明定何種行為違法、會有何種懲罰，這就是所謂明確性原則」。

不過這些批評聲浪並沒有阻擋通訊傳播審議委員會管制網路媒體的決心，通訊傳播審議委員會於 11 月 15 日公布與韓國網路新聞協會組成「自律規範實務協議體」，推動快速應對假新聞（虛偽捏造內容），當通訊傳播審議委員會確認假新聞（虛偽捏造內容）、非法流通等情況，會將該事實與韓國網路新聞協會共享，透過自律規範快速提供受害救濟。然而假新聞中心引起內外強烈反彈也是事實，能否適用

[685] 針對「放送通訊委員會設置暨營運相關法第 21 條第 4 項」的違憲提請，詳請參考國家法令資訊中心：https://www.law.go.kr/LSW/detcInfoP.do?mode=1&detcSeq=18874 （最後瀏覽日：2023 年 11 月 18 日）。

這一協定目前仍是未知數，又假新聞中心迄今成立兩個多月，不僅無審議成果，派遣至假新聞中心之員工亦提出擔憂業務擱置、法律損害等，請求調回原部門[686]，對此通訊傳播審議委員會僅回應「沒有事實根據」，不過在 11 月 23 日正式拒絕員工「請求調回原部門」的請求，通訊傳播審議委員會指出「對於假新聞中心的設立確實在事前準備不充分、也明白員工在業務上的壓力，但會積極努力找出解決方案」[687]。

雪上加霜的是，透過假新聞中心審議的第一起網路媒體 Newtapa[688]「金萬倍錄音報導」一案，在無法律依據之下強行進行審議，輿論界批判是侵害與管制言論自由，就在通訊傳播委員會委員長強調審議此案於法有據、Newtapa 聲明「不會留下屈服於權力之非法審查的先例」而拒絕出席陳述意見之下，最終審議結果是請求移交首爾市確認是否有違反新聞法之事項[689]，然而首爾市也無法做出任何決議。本案最後僅針對引用 Newtapa 該篇新聞的電視台做出合計 1 億 4 千萬韓元的鉅額罰款度懲處[690]。

686 박재령，'가짜뉴스' 규제로 폭주하는 방심위와 침묵하는 조중동，Mediatoday（2023/11/21），https://www.mediatoday.co.kr/news/articleView.html?idxno=313932（最後瀏覽日：2023 年 11 月 21 日）。

687 임현주，방심위, 가짜뉴스 센터 직원 요구 거부..직원 반발，MBC 新聞（2023/11/23），https://imnews.imbc.com/replay/2023/nwdesk/article/6546594_36199.html（最後瀏覽日：2023 年 11 月 21 日）。

688 Newtapa 全名為「韓國實地調查新聞中心 Newtapa」，為杜絕外部壓力與干涉，不接受廣告、政府、利益團體的支援，僅接受會員自發性捐款的獨立網路媒體，詳請見官網：https://newstapa.org （最後瀏覽日：2023 年 11 月 21 日）。

689 공윤선，방심위, 첫 인터넷 언론 심의..제재 없이 서울시에，MBC 新聞（2023/11/08），https://imnews.imbc.com/replay/2023/nwdesk/article/6541604_36199.html（最後瀏覽日：2023 年 11 月 21 日）。

690 유원정，가짜뉴스 센터 잡음 방심위, 인터넷 언론 규제 가속화，Nocutnews（2023/11/15），https://www.nocutnews.co.kr/news/6046887（最後瀏覽日：2023 年 11 月 21 日）。

（四）兒童暨青少年保護與數位遺忘權

1. 兒童暨青少年保護

2022 年 7 月由女性家族部（여성가족부）主導[691]，個人資訊保護委員會（개인정보보호위원회）、教育部、衛生福利部等相關部門共同發表的「兒童暨青少年個人資訊保護基本計畫」[692]，該計畫揭示，隨著從小就接觸智慧型手機與電腦等數位產品的數位原住民（Digital Native）的成長，加上教育、文化、休閒、人際關係等日常生活大量依賴線上活動，又因 Covid-19 造成的非面對面的活動激增，透過影像、遊戲等接觸多元內容的機會越來越多，個人資訊遭受侵害的危險性也日益增加。

另一方面，相較於成年人而言，兒童與青少年對於個人資訊洩漏等可能會造成侵害的警覺心較為不足，根據 2020 年首爾市與非營利團體社團法人 tacteen[693]於同年 10 月 28 日至 11 月 30 日針對 12 歲至 19 歲（國小五年級到高中三年級）、共 1,607 位的調查結果顯示，有 36%曾收到陌生人的訊息、或是陌生人請求對話，且線上接觸的陌生人也曾提及「要求告知年齡或電話號碼等個人資訊（23%）」、或「可以簡單賺到零用錢（10%）」；在與陌生人的對話中，有 64%會告知個人資訊，而拿到個人資訊的陌生人會回覆「好漂亮」等稱讚用語或更加親切（29%）、說會給錢或零用錢（15%）、文化商品券、遊戲幣等（10%）；而這「陌生人」的年齡依序最多是「14～16 歲」的 43%、「17～19 歲」的 43%，以及「20～24 歲」的 21%，可知加害者與被害者的年齡相當，而這一情況反覆出現，極可能出現「網路誘騙（Online Grooming）」，所謂網路誘騙就是加害者以受害者個人資訊為要脅，例如持續利用照片或影片進行壓榨剝削，前述利用 Telegram 的

691 詳見大韓民國政策簡報，관계부처 합동 「아동·청소년 개인정보 보호 기본계획」발표，新聞稿（2022/07/11），https://www.korea.kr/news/pressReleaseView.do?newsId=156515904（最後瀏覽日：2023 年 7 月 11 日）。

692 아동·청소년 개인정보 보호 기본계획，詳見教育部新聞稿網站：https://www.moe.go.kr/boardCnts/viewRenew.do?boardID=294&boardSeq=91965&lev=0&searchType=null&statusYN=W&page=1&s=moe&m=020402&opType=N（最後瀏覽日：2023 年 7 月 11 日）。

693 1995 年成立，以保護兒童與青少年人權的非營利社團法人，詳見 https://www.tacteen.net（最後瀏覽日：2023 年 7 月 11 日）。

「N 號房事件」就是最具代表性的網路誘騙犯罪，且被害者報案的可能性也不高。

因網路認識的人而有受害經驗的兒童與青少年雖然只占全體受訪者的 5%，但卻有 47.9%不會在事情發生後請求援助，其原因在於「害怕謠言衍伸的問題（20%）」、「不知道該如何應對（17.8%）」、「不知道向誰請求協助（13.1%）」；主要受害的內容則是「SNS 上的誹謗（56%）」、「要脅發送性相關影片（17%）」，也有「要脅上傳已發送的性相關影片（8%）」的情況，而因被要脅而傳送影片的受害兒童與青少年有 6%[694]。

2. 數位遺忘權之試行

因「曬娃」（Sharenting）爭議而衍生的兒童個人資訊自主權而受到重視，因此兒童與青少年在自身的個人資訊上應有行使權利、受到保護的國家對策。韓國既有在《個人資訊保護法》與《位置資訊法》等明定有處理未滿 14 歲兒童的個人資訊與個人位置資訊時，須取得法定代理人同意、確認同意的規範。但未滿 14 歲兒童係以法定代理人為主進行規範，滿 14 歲以上的青少年就等同成人，顯見未考量青少年對於行使個人資訊保護的權利尚未成熟，因此須針對兒童與青少年的個人資訊保護樹立基本原則，建立以兒童與青少年為中心的個人資訊保護體制。

預備將現行法律保護對象從未滿 14 歲提高到未滿 18 歲，也就是針對未滿 14 歲之兒童須法定代理人同意、兒童版本處理方針義務公開、特定廣告限制等，而針對未滿 18 歲的兒童青少年，則是需要遺忘權、擴大顯示個人資訊搜集通知、個人檔案限制等安全措施。目前預計 2024 年完成兒童、青少年時期，本人或第三者上傳的個人資訊可請求刪除的「數位遺忘權」法制化[695]，同時個人資訊保護委員會依

[694] 鄉新聞，아동·청소년 3 명 중 1 명 “SNS 서 낯선 사람이 대화 요구（2020/12/13），https://www.khan.co.kr/national/national-general/article/202012132056005（最後瀏覽日：2023 年 7 月 11 日）。

[695] 預定新增《兒童暨青少年個人資訊保護法》（名稱暫定）。

據「兒童暨青少年個人資訊保護指引」[696]於 2023 年 1 月 13 日公布從 4 月中起試行兒童暨青少年數位遺忘權[697]，涵蓋範圍以兒童、青少年使用頻率較高的三大領域（遊戲、SNS、教育學習）為主，提供滿 24 歲以下，在兒童、青少年階段（未滿 18 歲）時期於線上累積的個人資訊（包含文字、照片、影片）等，在發生危害或有發生危害之可能時，透過個人資訊保護網站（개인정보보호포터）[698] 提供要求刪除、遮蔽與檢索排除等的協助[699]。

三、第三方監督或產業自律機制

韓國在數位規範管理上，向來是標榜嚴格國家規範，施行過去被稱為確認本人制度之「網路實名制」，大部分國家都在自律規範的前提下，以官方規範管理有害資訊（不是非法資訊），遊戲、影片等各種內容物也都是採行事前登記制度，在這一潮流下，過去兩年政府想要將線上平臺納入同一官方規範，確實引起極大爭議，不過在尹政府上任後，發布線上平臺採自律規範的方式後，這一爭論逐漸平息，然而對於自律規範是採行「自發型自律規範」、還是「強制、規範型自律規範」，依然是政府與民間業者最大的爭議。

因此有數位平臺業者以團體的方式自發性透過共同規約建立「韓國網路自律政策機構」（한국인터넷자율정책기구，KISO）[700]，這是一典型的非法定民間自律規範機構，最初成立時，是一自發性地執行表現自由、監控非法資訊等的「執行法令型自律規範機構」，近來也

---

[696] 原文指引名稱為아동 · 청소년 개인정보보호 가이드라인，詳見個人資料保護委員會新聞稿：https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=8159（最後瀏覽日：2023 年 7 月 11 日）。

[697] 個人資訊保護委員會政策宣傳 https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS212&mCode=C040030000&nttId=8557 （最後瀏覽日：2023 年 7 月 11 日）。

[698] 由個人資訊保護委員會委由韓國網路振興院營運之個人資訊保護網站：https://www.privacy.go.kr （最後瀏覽日：2023 年 7 月 11 日）。

[699] 試行政策概要參見企劃財政部 2023 年 4 月份政策介紹 https://www.econedu.go.kr/mec/ots/dif/view.do?comBaseCd=DIFPERCD&difPer1=DIFPER004&difSer=802d6ccf-2228-4d7b-b76d-06eecb6644a6&temp=2023&temp2=HALF001 （最後瀏覽日：2023 年 7 月 11 日）。

[700] 官方網站：https://www.kiso.or.kr/ （最後瀏覽日：2023 年 7 月 13 日）。

追加了人工智慧開發與利用的相關行為基準等的營業行為與相關規約，由產業界自行形成共同必須遵守的規約，即韓國網路自律政策機構政策規範」[701]（下稱 KISO 政策規範），再依據《資通訊網路法》進行必要處置的具體處理基準[702]。

（一）民間自律機構

1. KISO 之成立

韓國在 2009 年[703]由網路業者 NAVER、雅虎韓國、KTH、HanaraDream（現 SK Broadband）、Freechal（2013 年終止服務）共同發起成立之網路自律機構為「韓國網路自律政策機構」，為韓國第一個民間網路自律組織，目前會員企業有韓國主要網路入口網站業者如 NAVER、Kakao、SK Communications 等 16[704]家業者，主要透過政策與審議規範會員企業。且營運之資金來源主要係來自會員企業繳交之會費、捐款等民間企業資源，以及營利性業務收入，是一民間之網路自律組織[705]。成立之目的係為因應網路使用環境之快速變化，法規無法予以及時規範之情形下，提供一個迅速且有效率之爭議解決機制，以保護網路使用者之言論表達自由及相關權利，期使網路能夠安全且有秩序的發展。

2. KISO 歷年作為

在 KISO 成立以來的十年間，網路生態有著極大的變化，為因應嶄新的網路環境進行，以既有政策委員會為主的論議架構，修正為「使用者內容分科」、「服務營運分科」、「線上廣告分科」、「技術分科」等

---

[701] 原規範名稱是한국인터넷자율정책기구 정책규정，詳見 KISO 網站：https://www.kiso.or.kr/정책위원회/정책규정/（最後瀏覽日：2023 年 7 月 13 日）。

[702] 金賢真（김현경，音譯），數位未來社會與自律規範（디지털 미래사회와 자율규제），KISO JOURNAL，第 49 期，頁 62-65（2022）。

[703] KISO 介紹，https://www.kiso.or.kr/wp-content/uploads/2021/11/한국인터넷자율정책기구-소개자료.pdf （最後瀏覽日：2023 年 7 月 13 日）。

[704] 截至 2023 年 6 月為止，KISO 會員有 16 個。

[705] KISO 自律規制白皮書（KISO 자율규제백서） Vol.2（2013-2015），頁 23，KISO，https://www.kiso.or.kr/kiso%ec%86%8c%ea%b0%9c/%ea%b8%b0%ea%b5%ac%ec%86%8c%ea%b0%9c/%ec%9e%90%ec%9c%a8%ea%b7%9c%ec%a0%9c%eb%b0%b1%ec%84%9c/ （最後瀏覽日：2023 年 7 月 13 日）。

四個分科為主的自律規範，因應快速變化的網路生態。使用者內容分科是負責使用者作成的發言、檢索詞的相關政策與審議，在必要時，會與小審議委員會一同進行留言、檢索詞的審議；服務營運分科則是 KISO 的主軸，負責業者的服務營運相關政策，不只社群業者的會員相關政策，還有個人資訊相關等議題的服務營運相關政策；線上廣告分科目前是以不動產廣告為主要業務範疇，為杜絕不動產不實買賣廣告，而執行事前與事後驗證的政策，也想建立一個合理的網路廣告自律規則；最後是特別分科，專責適應與發掘所需的新 IT 技術自律規範，本分科目前由資料庫自律小組組成，透過資料庫主導應對網路議題[706]。

又為因應非法、有害的訊息而將自律規範擴大至假新聞、假訊息，於 2018 年成立 KISO 綜合檢舉中心[707]，包含假新聞、有害貼文、名譽毀損貼文、檢索詞、不動產連結管理，並分別接受「以媒體輿論報導方式的虛假訊息」、「不健康、非法侵害個人法益之貼文[708]」、「造成名譽毀損之留言[709]」「檢索語受害[710]」、「虛假不動產網站[711]」，以及 Covid-19 相關虛假訊息的檢舉。這部分由前述提及資料庫自律小組負責，以保護使用者、支援會員企業的服務與實現社會價值，與外部專家、會員企業共同商討，作成網路上使用的髒話、青少年有害用語、淫亂圖片，以及根據會員企業的需求與社會議題做成各種的資料庫自律規範[712]。

---

[706] KISO 分科介紹說明：https://www.kiso.or.kr/정책위원회/분과-및-소위/분과소개/（最後瀏覽日：2023 年 7 月 13 日）。

[707] KISO 綜合檢舉中心：https://report.kiso.or.kr/about/（最後瀏覽日：2023 年 7 月 13 日）。

[708] 但基於《資通訊網路法》第 44 條之 7 侵害國家法益之留言，屬於傳播通訊委員會專責項目，而不健康、非法的留言，會因使用者觀點不同而難以有明確基準，因此須經過一定判斷過程。

[709] 依據《資通訊網路法》第 44 條之 2 與 KISO 政策規範第 2 章請求臨時處置，且臨時處置亦可在確認為本人的前提下，直接向相關會員企業提出請求。

[710] KISO 會員根據 KISO 政策規範「檢索語相關政策」經營檢索語服務，使用者可根據《KISO 政策規範》第 13 條之 2 向 KISO 會員提出檢舉。

[711] KISO 原先自發性的為保護不動產仲介服務之使用者，在不動產資訊驗證上設置「不懂產買賣驗證中心」與「不動產買賣連結管理中心」，但近來（2020 年 8 月）制定了《公益仲介法》，引入利用網路進行相關仲介廣告的規範與監控。

[712] KISO 自律規範 DB：https://www.kiso.or.kr/자율규제-db-안내/（最後瀏覽日：2023 年 7 月 13 日）。

3. 舉辦論壇

2022 年 12 月 8 日，KISO 舉辦「自律規範模型，從 KISO 找尋解答」(자율규제 모델, KISO 에서 답을 찾다）論壇[713]，由 KISO 政策委員，同時也是忠南大學媒體資訊學系的李晟善（이승선）教授進行發表。李教授以現今各種活躍的線上活動為題，提出線上的各種活動已是自由言論的一部分，要進行法律上的限縮就需要慎重行事，而焦點自然就會放在自律規範與法律規範的問題上，因此李教授以「韓國型自律規範機構 KISO 的特性與課題」為題，透過 KISO 之主要活動與成果探討近來企圖規範線上平臺之立法與政策，探索可改善課題[714]，科學技術資訊通訊部也有派員參與論壇交流意見，並表達政府施政方針積極朝 KISO 的成果努力。

4. 仇恨言論指引

韓國社會早已熟悉「仇恨言論」這一詞彙，然而在各種爭論持續發生的這一刻，我們始終沒有一個明確可判斷仇恨言論的基準，讓我們在面對網路上的各種言論，難以辨別何謂仇恨言論。因此 KISO 積極於 2023 年 4 月 27 日制定《仇恨言論自律政策指引》[715]（全 13 條，下稱本指引），其特點是 KIS 會員企業作為主導主體，參與並監管網路服務中出現的仇恨言論，自律保護網路使用者，且尊重言論自由，引導創造健全的網路文化。更重要的是本指引明示何謂仇恨言論，以及如何判斷仇恨言論的具體說明。

---

[713] KISO，[보도자료] 2022 KISO 포럼 개최, “자율규제 모델, KISO 에서 답을 찾다” ，新聞稿（2022/12/06），https://www.kiso.or.kr/kiso-%EC%86%8C%EC%8B%9D/%EB%B3%B4%EB%8F%84%EC%9E%90%EB%A3%8C/?mod=document&uid=1376（最後瀏覽日：2023 年 7 月 13 日）。

[714] 詳請參考論壇手冊與線上直播：https://www.kiso.or.kr/kiso-%EC%86%8C%EC%8B%9D/%EA%B3%B5%EC%A7%80%EC%82%AC%ED%95%AD/?mod=document&uid=1375（最後瀏覽日：2023 年 7 月 14 日）。

[715] 本指引原文名稱為혐오표현 자율정책 가이드라인，詳見 KISO 網站：https://www.kiso.or.kr/정보센터/kiso-정책/guideline/（最後瀏覽日：2023 年 7 月 14 日）。

首先看關於仇恨言論的定義，根據本指引，仇恨言論的特稱是以種族、國家、民族、地區、年紀、障礙、性別、性向或宗教、職業、疾病為由，合理化、助長、強化，或以暴力言論煽動歧視特定團體或特定團體的成員，明示仇恨言論是從「種族、國家、民族、地區、年紀、障礙、性別、性向或宗教、職業、疾病」當中尋找，而仇恨言論的客體是「設定團體或特定團體的成員」、仇恨言論的內容是「合理化、助長、強化歧視、或暴力言論煽動」。雖然在定義上依舊沒有非常明確，但至少能給予 KISO 會員企業應對仇恨言論的判斷基準。

再者是仇恨言論自律政策的基本原則，在制定仇恨言論規範時，首重不得侵害使用者的言論自由，而本指引在這一部分明示了基本原則「須極大化尊重網路服務使用者的言論自由」，更進一步明示「必須保障我國社會的多元性，保護特定團體不因仇恨言論而被歧視或排斥」，同時明確指出「須快速提供因仇恨言論導致網路服務使用者受害的救濟，與預防往後可能發生的傷害」。而這些原則不僅賦予 KISO 會員企業，也包含會員企業的網路使用者，不得使用、傳播或分享仇恨言論，以此侵害其他使用者的權利或為其他使用者帶來傷害。

關於仇恨言論的判斷基準須滿足：（1）特定屬性的言論；（2）針對特定團體或特定團體成員的言論；（3）合理化、助長、強化歧視、或暴力言論煽動（需考量特定言論使用的詞彙含義、以及該詞彙的使用脈絡），才能判斷為仇恨言論。但不滿足（3）的條件，但符合「針對特定團體或特定團體成員的特定特色而輕視、戲弄的言論」時，例外的須依據本指引第 11 條處置，也就是（1）刪除；（2）遮蔽該言論或限制曝光；（3）標記警告文字、使用者注意文句；此外，亦可（4）限制仇恨言論或與之相當之處置。而檢舉與處置就依據本指引第 8 條，網路服務使用者可向會員企業、或 KISO 檢舉，若難以判斷、或對於判斷為仇恨言論後刪除，但該當事人提出異議時，可以請求仇恨言論審議委員會進行審議[716]。

[716] 根據本指引第 13 條之設置與營運仇恨言論審議委員會。

另外，關於本指引有幾點注意事項，本指引是會員企業的自律規範，可就因仇恨言論而發生、或可能發生的結果，該以何種方式進行規範這一點看來，本指引的處置方式，確實有其限制。畢竟以網路傳播速度，當意識是仇恨言論，到適當處置定案的等待時間，早已讓所屬團體、或團體成員身心疲憊、難以承擔，而本指引卻無法提出該如何補償已發生的傷害；若考量遭受仇恨言論的受害者，甚至是從其所屬團體的立場時，本指引尚需針對有問題的言論進行適切的規範，以及具體明示可保障受害的事後救濟對策。

還有當網路服務使用者的言論自由受到侵害時，即並非仇恨言論，卻依據指引判定為仇恨言論的受制裁的當事人，必須自行舉證證明不是仇恨言論，可對個人來說，這一證明行為不僅困難，指引中也沒有明確的程序，因此本指引尚需制定當事人異議程序與必要時，會員企業也能提供協助等的內容。當證明不是仇恨言論，且經過再審程序確認不是仇恨言論時，依據本指引是「可廢除」仇恨言論的處置，但最佳做法應是「應即時廢除」，因這是審議程序作成的錯誤判定導致，應給予一定保障；更進一步地說，當經過異議程序而廢除仇恨言論處置，且判定該當事人言論自由確實受到侵害時，本指引亦無明示相關的補償對策。

最後就是關於仇恨言論審議委員會的組成人員與議決方式，根據本指引第 13 條，是由 KISO 政策委員會委託不隸屬於會員企業的 3 位以上的委員，以及會員企業所屬的委員組成，同時還規範開會要件是「在職委員過半數出席」且議決要件是「在職委員過半數贊成」，且會員企業所屬委員不計入開會與議決人數，也就是仇恨言論審議委員會是由政策委員會委託非會員企業所屬委員至少 3 名，以及會員企業所屬委員組成，若要仇恨言論審議委員會開會，就須有政策委員會委託非會員企業所屬委員 3 位中，2 位出席且 2 位皆贊成才能作成議決。然而仇恨言論審議委員會針對特定言論的審議，涉及該案發言者的基本言論自由，需相關專家們經過充分的討論，所以目前對於本指引明示的組成人員、作成的議決內容上有疑慮存在。就結果面看來，難以達成本指引想達成的仇恨言論的自律規範，更重要的是，仇恨言

論審議委員會的審議結果，會產生限制、壓抑發言者的言論自由的結果，所以依據本指引成立的仇恨言論審議委員會的組成人員與審議程序皆需追加更詳細的內容[717]。

（二）官民合力自律規範

2022 年 8 月啟動的「平臺民間自律機構」[718]於同年 9 月 6 日召開第一次會議，參與者包含平臺業者、商家、消費者、從業人員等與韓國網路企業協會、中小企業聯合會、韓國消費者團體等相關協會團體，政府相關部門也與會聽取民間建言，但也有最後會變成政府主導的疑慮，無法產生實質效果，尤其在 kakao 數據中心火災導致多項服務中斷事件[719]後，對於線上平臺的法律與自律規範的原則與基準又再度受到重視。

根據個人資訊保護委員會的 2023 年業務報告[720]中指出，由於線上平臺成長速度過快，個人資訊法規無法即時更新，因此政府積極推動線上平臺自行制定規約，形成政府核准的自律規範，並根據履行的結果提供相關各項優惠措施，以符合技術環境與新產業特性。

2023 年 5 月 11 日舉辦「平臺民間自律機構自律規範方案發表會」[721]，針對四個分項「甲方乙方、消費者與使用者、數據與人工智慧、改革分享與治理」進行方案發表，參與機關有主要平臺業者與相關事業團體、中小企業、全國商會團體、消費者團體與民間專家，以

---

[717] 李貞嬋（이정념，音譯），KISO 制定「仇恨言論自律政策指引」的意義與考量（KISO <혐오표현 자율정책 가이드라인>의 제정 의의와 몇 가지 고려사항），KISO JOURNAL，第 51 期，頁 2-5（2023）。

[718] 公平交易委員會 2022 年 8 月 19 日新聞稿：https://www.ftc.go.kr/www/selectReportUserView.do?key=10&rpttype=1&report_data_no=9706 （最後瀏覽日：2023 年 7 月 13 日）。

[719] 發生於 2022 年 10 月 15 日的 kakao 數據中心火災事件，導致透過 kakao 的各項服務，包含通訊、銀行、行動支付、叫車服務等涉及日常生活的各項服務全數中斷，部分服務甚至中斷超過一天都未能復原。

[720] 大韓民國總統府政府業務報告之個人資訊保護委員會 2023 年業務報告，詳見 https://www.president.go.kr/affairs/gov_report （最後瀏覽日：2023 年 7 月 13 日）。

[721] 詳見大韓民國政策簡報，플랫폼 자율기구 자율규제 방안 발표회 개최（召開平臺民間自律機構自律規範方案發表會），新聞稿（2023/05/11），https://www.korea.kr/briefing/pressReleaseView.do?newsId=156569141（最後瀏覽日：2023 年 7 月 13 日）。

及公平交易委員會委員長、科學技術資訊通訊部部長、通訊傳播委員會常任委員等政府人員與會。

四個分項具體方案分別為 1、開放市場領域自律規範方案（甲方乙方、韓國網路購物協會）；2、開放市場消費者集體受害快速對應方案（消費者與使用者）；3、提高平臺檢索、推薦服務透明性之自律規範原則（數據與人工智慧）；4、提高平臺社會價值之八大原則（改革分享與治理）[722]。

與會的公平交易委員會委員長指出「今天發表之自律規範方案皆為各平臺業者自律參與，因此必有高度遵守的意願」、「相信透過平臺業者自律的努力，創造一共生文化並深耕健康的韓國平臺市場生態」；科學技術資訊通訊部部長「在以自律作為國家政策、打造創新與公平平臺生態系的今日，由民間主導提高平臺服務透明性與共生原則，並直接宣佈實施是件非常有意義的事情」、「不僅如此，還希望透過各個平臺業者遵守各個原則，並擴散至整個業界，並持續改進與發展」；通訊傳播委員會常任委員也指出「自律規範不是一件簡單的挑戰，透過民間自律的商討與協力展現出成果，深具意義」，因此期望「透過自律規範持續保護各平臺使用者」。

（三）韓國記者協會

前述提及，韓國在不實報導、違反《個人資訊保護法》等法律之內容，官方有輿論仲裁委員會、在民間有韓國記者協會。

韓國記者協會是由隸屬全韓國報紙、廣播電視、網路新聞等輿論媒體之現職記者組成，目前約有一萬多名會員，是韓國最大的輿論團體。在 1964 年 8 月 17 日創立之初是為守護言論自由價值、反抗當時軍事政權推動之反民主惡法「輿論倫理委員會法」，初始設置有守護言論自由、提高記者素質、擁護記者權益、祖國和平統一、國際交流等五大綱領。

目前記協在組織上設有會長、副會長、顧問團、監察（2 位），以

[722] 同上註。

及報導自由、擁護權益、調查研究、資格懲戒、國際交流、南北統一六個常任分科委員會，除了章程外，有輿論倫理憲章、綱要、實踐綱要，對於自殺報導、人權報導、國家安全危機時、性暴力犯罪、災難報導、傳染病報導、兒虐報導、選舉輿論調查、仇恨言論等等都有訂有採訪與報導準則；在新聞或報紙報導上皆會完整揭露記者姓名、網路新聞亦會標示上稿時間、修正時間，若該篇報導有侵害相關權益時，可經由韓國輿論仲裁委員會進行申請調停、仲裁或是進入法院程序；在記者資格懲戒部份，記協懲戒分別是警告、資格中止、除名，由資格懲戒分科委員會進行調查，並採行投票多數決決定懲戒方式。

四、小結

過往韓國在數位平臺的法規論議上，常徘徊在法律規範與業者自律之間，如今政府認同要讓產業得以發展迅速，應鼓勵業者採行自律規範，業者為爭取自主權也已積極成立自律團體，期盼以產業界自主形成相關自律規範達成有效的管理，目前看似略有成效，但依然有許多值得思考的課題。法律規範則是在非法行為可能發生、或發生時介入，在非法行為可能發生之情況，同步也課予業者處置義務，然而課予義務的業者範疇卻無法全面涵蓋，就國內部分僅有大型業者、國外部分僅能請求協助。

其中最大的課題為:業者可能因擔心產生多於競爭者的成本而對自律猶豫不決，法律規定則跟不上變化莫測的數位技術，且可能侵害憲法賦予人民的權利。因此，如何讓所有業者皆願意加入自律組織、遵守自律規範才是關鍵，並且應共同討論如何讓自律規範更加完善。

第十一節　新加坡

一、監理脈絡

新加坡之通訊傳播法制政策發展之架構，係由新加坡通訊及新聞部（Ministry of Communications and Information，下簡稱 MCI）主責，其掌理網路安全、國家設計發展、資通訊媒體、個人資料保護、圖書行政（包括國家圖書館、公共圖書館以及國家檔案與紀錄管理）、公共傳播與數位閱讀之政策發展，並負責推動數位經濟政策[723]。

為使新加坡於數位時代保持國際領先之地位，並有利於通訊傳播事業的成長與發展，MCI 於 2015 年便通過「2025 資通訊媒體」（Infocomm Media 2025）計畫[724]作為政策基礎，並發布「資通訊媒體產業轉型地圖」（Infocomm Media Industry Transformation Map）[725]，強化民眾之資通訊能力及提升國際之競爭力。

當中重要的是調整其轄下組織，併整原分別掌理新加坡資通訊管制與政策執行與媒體管制與政策執行之資通訊發展管理局（Infocomm Development Authority, IDA）與媒體發展管理局（Media Development Authority, MDA）此兩機關的事權，將之交由新加坡資通訊及媒體發展局（Infocomm Media Development Authority，下簡稱 IMDA）統籌[726]，由 IMDA 依照《資通訊媒體管理局法》（Info-communications Media Development Authority Act）、《1994 年廣播電視法》（Broadcasting Act 1994）、《電子交易法》（The Electronic Transactions Act）、《1981 年電影法》（Films Act 1981）、《1974 年新聞與報業法》（Newspaper and Printing Presses Act 1974）、《郵政服務法》（Postal Services Act）、《大眾娛樂法》（Public Entertainments and Meetings Act）、

---

723 Ministry of Communications and Information, *Our Organisation, Who We Are*, https://www.mci.gov.sg/about-us (last visited June 21, 2023).

724 Ministry of Communications and Information, *Infocomm Media 2025*, https://www.mci.gov.sg/portfolios/infocomm-media/infocomm-media-2025/introduction-to-infocomm-media-2025 (last visited June 21, 2023).

725 Smart Nation and Digital Government Office, *Infocomm Media Industry Transformation Map (ITM)*, Press Room (2017/11/03), https://www.smartnation.gov.sg/media-hub/press-releases/infocomm-media-industry-transformation-map-itm/ (last visited June 21, 2023).

726 IMDA, *About IMDA*, https://www.imda.gov.sg/Who-We-Are/about-imda (last visited June 21, 2023).

《個人資料保護法》（Personal Data Protection Act）、《1999 年電信法》（Telecommunications Act 1999）、《不受歡迎出版品法》（Undesirable Publications Act）[727]等法規範，落實新加坡資通訊及媒體政策之推行，並維護消費者利益與促進有利於產業之管制模式發展。

IMDA 的治理組織，以董事會為機關治理的最高單位，以法定的正式會議程序進行決議，主導 IMDA 整體之政策方針，董事會的成員依法為 6 位至 20 位不等[728]，其成員除全由 MCI 部長所選任[729]外，部長亦擁有隨時可以不具任何理由直接解除董事會成員職務之權力[730]。董事會其中 1 人為主席，1 人為副主席[731]，執行長亦為董事會成員，但主席與副主席不得兼任執行長。至於日常行政之運作，則是由執行長及各行政部門所職掌[732]。

整體而言，在政策指示權方面，MCI 為 IMDA 之責任部會，可依法對 IMDA 的機關法定職權功能為政策指示，相對地，IMDA 為 MCI 之所屬機關，應遵循 MCI 的政策指示行使職權；而在行政救濟機制方面，MCI 為 IMDA 之訴願管轄上級機關，亦即如不服 IMDA 之行政決定者，可向 MCI 部長提起訴願，由部長對 IMDA 之行政決定進行訴願決定，且部長的決定為最終的決定[733]。

就此監理架構下，關於網路管理框架，IMDA 主要係透過《廣播電視法》之分類執照[734]，針對包含藝術娛樂、電影、網路、電視與廣播，以及電玩遊戲等不同類型之服務提出不同規範與標準。而網際網路服務提供者（Internet Service Providers, ISPs）和網際網路內容提供者（Internet Content Providers, ICPs）必須遵守網際網路「分類執照」（Class License）之許可條件及《網際網路實踐準則》（Internet Code

[727] IMDA, *Regulations and Licensing Listing, Acts and Regulations*, https://www.imda.gov.sg/regulations-and-licensing-listing/acts-and-regulations (last visited June 21, 2023).

[728] Info-communications Media Development Authority Act 2016 (2020 Rev. Ed.), Sec. 10.

[729] Info-communications Media Development Authority Act 2016 (2020 Rev. Ed.), Sec. 11.

[730] Info-communications Media Development Authority Act 2016 (2020 Rev. Ed.), Sec. 16.

[731] Info-communications Media Development Authority Act 2016 (2020 Rev. Ed.), Sec. 13.

[732] IMDA, About IMDA, *Our Team*, https://www.imda.gov.sg/about-imda/who-we-are/our-team (last visited June 21, 2023).

[733] Info-communications Media Development Authority Act 2016 (2020 Rev. Ed.), Sec. 68.

[734] Broadcasting Act 1994 (2020 Rev. Ed.), Sec. 2 & Sec. 9.

of Practice）。至於線上管制較為著重之內容議題，則較為偏向公共利益、種族、宗教和對兒少有害之內容等相關問題[735]。

總括而言，IMDA 宣稱，其係以輕度（light-touch）管理思維，並採用三支柱策略[736]：其一為要求網際網路服務提供者和網際網路內容提供者自動遵循線上實踐準則之方案；其二為鼓勵產業自律，對於其所提供之內容承擔社會責任，並期待服務提供者提出相關實務準則，以擴大自律之範圍；其三則是透過有效的公共教育計劃，旨在促進家長監督兒少上網之使用情形，及提高媒體品質與網路福祉，藉以維護全民之基本價值及促進健康發展。

二、政府機關法制政策作為

新加坡作為全球上網普及率最高的國家，加上向來強調政府運作與管理之功能，故而屬於主張政府必須強制介入線上內容管理的國家之一[737]。

諸如，針對線上內容可能涉及著作權侵權之情事，新加坡於 2004 年調修《著作權法》（Copyright Act）第 193A 條以下，將「網路服務提供者」（network service provider, NSP）[738]之責任加以限縮，其立法目的乃為與美國簽訂自由貿易協定，故與美國《數位千禧年著作權法》（Digital Millennium Copyright Act, DMCA）第 512 條以下有關安全港之規範一致，定義亦與美國之「網際網路服務提供者」（Internet Service Provider, ISP）大致等同，藉此保護網路服務提供者免受著作權侵權責任的影響。

---

[735] IMDA, *Regulations and Licensing Listing*, Internet, https://www.imda.gov.sg/regulations-and-licensing-listing/content-standards-and-classification/standards-and-classification/internet (last visited June 21, 2023).

[736] IMDA, *Singapore has a three-prong approach to Internet content regulation, Internet Content Regulation*, Internet Content Regulation (2022/10/26), https://www.imda.gov.sg/Infocomm-regulation-and-guides/infocomm-regulation/internet-content-regulation (last visited June 21, 2023).

[737] 范傑臣，從多國網路內容管制政策談台灣網路規範努力方向，資訊社會研究，頁 207-208（2002）。

[738] 新加坡舊《著作權法》係第 193A 條對「網路服務提供者」（NSP）加以定義，謂線上服務或網路接取之提供者或設施經營者，與美國之「網際網路服務提供者」（ISP）大致等同。然新加坡於 2021 年再度調整《著作權法》，是《2021 年著作權法》（Copyright Act 2021）針對 NSP 之相關規定移至第 313 條以下。

而在對抗線上之虛擬或誤導之事實，新加坡先通過號稱史上最嚴格之法規範，不論是個人或非個人（如數位平臺）均為該法之規範對象。然而近年政府注意到社群媒體平臺放大線上有害內容之風險，像是使用者間發起危險行為之「挑戰」，再透過社群媒體平臺之演算法迅速傳散，並導致傷亡，或是透過直播傳散恐怖主義行為而加劇對社會之負面影響等情事，故加入德國、澳洲、歐盟及英國之立法行列，制定新法規以促使線上通訊傳播服務（尤其是社群媒體平臺）為使用者之線上安全承擔更大的責任[739]。以下分述之。

（一）2019 年《線上虛假內容與操控防止法》

新加坡國會（Parliament of Singapore, PARL）於 2019 年 5 月 8 日通過《線上虛假內容與操控防止法》（Protection from Online Falsehoods and Manipulation Act 2019, POFMA），並經 MCI 部長公告於同年 10 月 2 日生效[740]。

此法又稱《虛假新聞法》（fake news law）[741]，主要目的為遏止不實陳述（false statements of fact）於新加坡之電子通訊環境傳散，進而對公共利益造成危害，特制訂相關防堵措施。

《POFMA》共計 62 條，規範架構可分為九大編，第一編為序言，規範本法之概念定義、立法目的，以及主管機關之相關規定；第二編為規範本法所禁止事項，即禁止於新加坡傳播不實陳述之規定；第三編係規範防制不實陳述於新加坡傳播，而針對個人所為之指令與措施；第四編則係為防制不實陳述於新加坡境內傳播，而針對網路中介者（internet intermediaries）與大眾傳播媒體服務者（providers of mass media services）所規範之指令與措施；第五編則是線上位置宣告及其

[739] The Business Times, Singapore joins other places with laws regulating online content, International (2022/06/20), https://www.businesstimes.com.sg/international/singapore-joins-other-places-laws-regulating-online-content (last visited June 21, 2023).

[740] Singapore Fake News Laws: Guide to POFMA (Protection from Online Falsehoods and Manipulation Act), Singapore Legal Advice (2022/04/25), https://singaporelegaladvice.com/law-articles/singapore-fake-news-protection-online-falsehoods-manipulation/ (last visited June 21, 2023).

[741] Learning Centre: Criminal Law: Cybercrime, Singapore Fake News Laws: Guide to POFMA (Protection from Online Falsehoods and Manipulation Act), Singapore Legal Advice (2022/04/25), https://singaporelegaladvice.com/law-articles/singapore-fake-news-protection-online-falsehoods-manipulation/ (last visited June 21, 2023).

相關措施之規定；第六編為對不實線上帳號與協同性造假行為（coordinated inauthentic behaviour, CIB）之規範；第七編則為其他措施之規定；第八編為選舉期間與特定期間之監管機關代理規定；最後，第九編為附則規定。

1. 監理機關之職權

依據《POFMA》之規定，授權 MCI 部長得任命法定機構（statutory board）或任何由政府或法定機構所設之辦公室，作為本法之主管機關（Competent Authority）[742]。因此，MCI 指定 IMDA 為主管機關，並於 IMDA 轄下新設立「線上虛假內容與操控防止法辦公室」（Protection from Online Falsehoods and Manipulation Act Office，下簡稱 POFMA 辦公室）以執行該法之管制措施[743]。

該法實際運作之模式為新加坡政府各部會之部長將在其官員或是幕僚的建議下，決定系爭資訊是否虛假，並同時評估對公共利益的影響[744]。

也就是說，若判斷同時滿足「有虛假之事實陳述」及「符合公共利益」，相對應的部長們與 IMDA 合作採取執法措施。即透過 POFMA 辦公室承政府各部會部長之命令，向個人或線上平臺發布指示（directions）或通知（notices），並監督指示與通知後續之執行情形[745]。

2. 規範對象

除「個人」以外，該法所規範之對象，尚涵蓋「網路中介服務」（internet intermediary service）[746]，而依《POFMA》之定義，其係指：

---

[742] POFMA, Sec. 6.
[743] POFMA Office, About Us, https://www.pofmaoffice.gov.sg/about-us/ (last visited June 21, 2023).
[744] Chomkins，史上最嚴假新聞法案上路，新加坡對「分享者」加重兩倍刑罰、最高監禁 10 年，數位時代（2019/10/24），https://www.bnext.com.tw/article/55206/singapore-fake-news-protection-from-falsehoods-manipulation-act（最後瀏覽日：2023 年 6 月 21 日）。
[745] POFMA, Sec. 6.
[746] POFMA, Sec. 2.

（A）允許終端使用者在網路上或透過網路獲取源於第三方資料之服務；

（B）在網路或透過網路向終端使用者傳輸這些資料的服務；或

（C）向使用該服務進行線上搜尋的終端使用者顯示搜索結果索引的服務，每一個搜尋結果都可讓該終端使用者得連結到資訊儲存（hosted）或預存（stored）在與搜索結果索引地點不同的位置。

但不包括為提供以下目的或附帶提供以下目的而作出的任何行為——

（D）向公眾提供網路接取服務；或

（E）網路計算資源服務。

具體而言，網路中介服務包含：社群網路服務、搜尋引擎服務、內容整合服務、以網路為基礎的資訊服務，以及視訊分享服務等。而依其子法《防止線上虛假消息和操縱規則》（Protection From Online Falsehoods and Manipulation Regulations 2019, POFMR）則明確指出網路中介服務，即指 Google 公司（旗下擁有 Google Search、YouTube 服務）、Meta 公司（旗下擁有 Facebook、Instagram 與 WhatsApp 服務）、Twitter 國際公司（旗下擁有之 Twitter 服務）、百度公司（旗下擁有之 Baidu）、新加坡報業控股公司（旗下擁有之 HardwareZone.com 服務），以及騰訊公司（旗下擁有之 WeChat）等服務提供者[747]。

3. 法定禁止行為與罰則

為防制不實陳述（false statement）於新加坡境內傳播，《POFMA》明文規定禁止為傳播不實陳述於新加坡之行為。其中所謂不實陳述，係指陳述內容部分或全部本身或依其脈絡係虛假或誤導之內容[748]。

而該法所禁止的傳播行為，包括透過網際網路、行動多媒體訊息

[747] POFMR, Sec. 3.
[748] POFMA, Sec. 2.

（Multimedia Messaging Service, MMS）或行動文字訊息（Short Message Service, SMS）之方式傳播，使新加坡境內一位以上的終端用戶能夠取得該陳述[749]。

亦即，任何人無論是否身處新加坡，都不得於新加坡境內，傳播其明知或有理由相信該陳述為不實陳述內容，且明知或有理由相信將該不實內容之傳播，可能於新加坡造成法定公共利益危害之行為[750]。應注意的是，本條規範僅適用於個人而不適用於網路中介服務、電信服務、提供公共接取之網路服務者以及電腦資源服務（computing resource service）。

至於公共利益要件，係為避免表意行為不受到過度限制所設，可概分為六類[751]：

- 新加坡安全利益之維護；
- 公共安全、財政、公共健康與公共安寧；
- 新加坡與其他國家的友善外交；
- 防止總統、國會選舉以及投票受影響；
- 防止不同團體民眾間的仇恨、負面意識；
- 防止對於政府的公眾信心受負面影響。

而其禁止行為之態樣，依該法規定，包括：傳播不實陳述、使用機器人軟體與不實帳號傳播不實陳述以及傳播不實陳述之服務提供，就此分述如下：

（1）禁止傳播不實陳述

若行為人傳播該不實陳述，且明知或有理由相信該不實陳述之傳播於新加坡可能造成公共利益之危害者。行為人可處以 5 年以下有期徒刑，以及 5 萬新加坡幣（約新台幣 118 萬元）以下之罰金；而若任

[749] POFMA, Sec. 3.
[750] POFMA, Sec. 7.
[751] POFMA, Sec. 4.

何人使用不實線上帳號與自動化電腦軟體（bot）作為加速傳播不實陳述之目的，而違反上述行為者，則加重刑責，即行為人可處 10 年以下有期徒刑，與 10 萬新加坡幣（約新台幣 236 萬元）以下罰金[752]。

（2）禁止使用自動化電腦軟體傳播不實陳述

該法規定不得使用機器人軟體（bot），而意圖透過機器人軟體傳播不實陳述；亦不得使用機器人軟體，而意圖透過機器人軟體促使他人傳播不實陳述。違反者，可處 3 年以下有期徒刑與及 3 萬新加坡幣（約新台幣 70 萬元）以下罰金。若上述方式的不實陳述傳播行為，可能構成危及公共利益之情形者，可處以 6 年以下有期徒刑與 6 萬新加坡幣（約新台幣 141 萬元）以下罰金[753]。

（3）禁止提供傳播不實陳述之服務

該法規定任何人若期約或收受利益作為服務提供之對價，且知悉所提供之服務將被用於新加坡傳播不實陳述，可處 3 年以下有期徒刑與 3 萬新加坡幣（約新台幣 70 萬元）以下罰金；若該不實陳述之傳播可能構成危及公共利益之情形者，可處 6 年以下有期徒刑與 6 萬新加坡幣（約新台幣 141 萬元）以下罰金[754]。應注意的是，本條規定僅適用於個人而不適用於網路中介服務、電信服務、提供公共接取之網路服務者以及電腦資源服務。

4. 防制措施：針對任何人

該法規定若部長確信某不實陳述已經或正於新加坡傳播，基於公共利益之考量，認為應發布更正命令、停止傳播命令者，有權指示 IMDA 發布更正命令（Correction Direction）、停止傳播命令（Stop Communication Direction）[755]。

上開命令所適用之規制對象與地域範圍，可發布予新加坡境內或

752 POFMA, Sec. 7.
753 POFMA, Sec. 8.
754 POFMA, Sec. 9.
755 POFMA, Sec. 10.

境外之人，亦得要求該人無論於新加坡境內或境外為特定行為[756]。應注意的是，更正命令與停止傳播命令，均不適用於僅從事於網路中介服務、電信服務、提供公共接取之網路服務者以及電腦資源服務之行為[757]。

所謂更正命令，係要求傳播不實陳述之人，於特定方式（特定線上位置、報紙或其他出版品）以及在特定時間，為更正通知公告，要求更正內容包括：系爭陳述為不實之陳述，或系爭陳述內容含有不實之陳述；系爭陳述之事實，或提供可供查找系爭陳述之事實的資料文獻來源之位置[758]；所謂停止傳播命令，係要求特定人，於特定時點起停止傳播系爭陳述，亦可要求特定人，停止傳播與系爭陳述具有實質上相似性的任何陳述。即便在該人非明知或無理由相信該陳述為不實之情形下，亦得對之發布停止傳播命令[759]。

若無任何合理之理由而未遵守要求，得針對命令所發布之對象科處刑事處罰，可處以 2 萬新加坡幣（約新台幣 47 萬元）以下罰金及/或 1 年以下有期徒刑[760]。

若受上開命令發布之受處分人未遵守命令之要求；且系爭事實已由受處分人於某一線上位置傳播至新加坡境內；以及部長認為，於新加坡已有一位以上的終端用戶，已經或正使用 ISP 業者所提供之服務，接取該線上位置之情形下，部長有權指示 IMDA，對 ISP 業者發布「阻斷接取命令」（Access blocking order），命該 ISP 業者以合理的措施，阻斷新加坡之終端用戶接取該線上位置[761]。

若該 ISP 業者未遵循阻斷接取命令者，可每日處以 2 萬新加坡幣（約新台幣 47 萬元）以下之罰金，至業者完全履行阻斷接取命令前，最高可至 50 萬新加坡幣（約新台幣 1,180 萬元）罰金。

---

[756] POFMA, Sec. 13.
[757] POFMA, Sec. 11-12.
[758] POFMA, Sec. 11.
[759] POFMA, Sec. 12.
[760] POFMA, Sec. 15.
[761] POFMA, Sec. 16.

5. 防制措施：針對網路中介者、大眾傳播媒體服務者

若系爭陳述內容係包含不實陳述或由不實陳述所構成；且部長基於公共利益之考量，認為應發布針對性更正命令、中止連結命令、一般性更正命令者，部長有權指示主管機關核發上開命令，即便系爭線上內容已經過修正或已在新加坡境內停止傳播，亦得為之[762]。

上開命令所規制對象與範圍，無論該人是否在新加坡境內皆可對之發布、亦可要求該人於新加坡境內或境外履行命令所示之特定行為[763]。

（1）針對性更正命令、中止連結命令及一般性更正命令

針對性更正命令（Targeted Correction Direction）係向特定之網路中介者發布之命令，命於特定時點後，對使用其服務之終端使用者，就已經或正於新加坡傳播的系爭不實陳述，以易於察知之方式為更正通知公告[764]。

中止連結命令（Disabling Direction）係向特定之網路中介者發布之命令，命於特定時點後，將任何經由或正在該網際網路中介服務之構成或包含系爭不實陳述內容，向新加坡終端使用者為中止連結，且同時以易於察知之方式透過特定說明敘述，傳播更正通知[765]。

一般性更正命令（General Correction Direction）係對於受規管處分之網路中介者、新聞與出版媒體、廣播媒體、電信業者以及其他經規管指定之對象，要求其於網路中介服務、報紙或平面出版品、廣播、電信服務，以易於察知之方式為修正通知公告[766]。

若受上開命令所發布的對象，未遵循命令或命令之義務，部長可指示 IMDA，由 IMDA 發布阻斷接取命令，命 ISP 業者採取進一步措施，以中止新加坡的終端使用者接取該線上位置。若 ISP 業者未遵守阻斷接取命令，可按日處罰 2 萬新加坡幣（約新台幣 47 萬元）以下

[762] POFMA, Sec. 20.
[763] POFMA, Sec. 25.
[764] POFMA, Sec. 20.
[765] Id.
[766] POFMA, Sec. 23.

罰金，至該業者完全履行命令所示義務前，可處最高額 50 萬新加坡幣（約新台幣 1,180 萬元）以下之罰金[767]。

（2）線上位置宣告及其後續相關措施

若特定線上位置符合：A. 至少分別有三個以上不同內容的陳述，都已經構成上述命令之情形，或是各該陳述都已經或正於新加坡境內傳播；且 B. 該三個以上陳述，於該線上位置已傳播於新加坡境內的時間，至少達 6 個月以上之情形。部長有權對之為線上位置宣告（Declared online locations），內容包括 URL 網址、網域名稱、或其他得以辨識線上位置之特徵，並有權要求線上位置經營者或所有人（無論該人於新加坡境內或境外），應以特定方式傳達此線上位置「已受線上位置宣告」予在新加坡任何接取該線上位置的終端使用者[768]。

若受線上位置宣告的經營者或所有人未遵守該規定，可處 3 年以下有期徒刑及 4 萬新加坡幣（約新台幣 94 萬元）以下罰金。且部長亦得在一定要件下指示 IMDA 發布阻斷接取命令，命 ISP 業者採取合理方式，停止新加坡使用者皆取該線上宣告位置[769]。

此外，在發布「線上位置宣告」後，亦可禁止從事於經營受宣告線上位置之營利行為（如出售該線上位置的廣告空間）、禁止服務提供者或數位廣告中介商將受線上宣告位置內之付費內容傳播於新加坡境內或促進特定付費內容，甚至不得對該線上宣告位置提供財務支持或協助。若有違反上述行為，均可對行為人處以有期徒刑或罰金[770]。

（3）防制不實帳號與協同性造假行為之措施

若特定網路中介者提供線上帳號之功能，而有 A. 不實陳述已透過該帳號傳播於新加坡，或是 B. 已有協同性造假行為透過該帳號進行之情形，且部長在考量法定要件後已確信該線上帳號為不實帳號，或是該帳號係由機器人軟體所控制，其基於公共利益之考量，而認為

[767] POFMA, Sec. 28.
[768] POFMA, Sec. 32.
[769] POFMA, Sec. 33.
[770] POFMA, Sec. 36-38.

應發布帳號限制命令者，部長得指示 IMDA 對於特定網際網路中介者發布「帳號限制命令」（Account restriction direction），命特定網際網路中介者：不允許被限制的特定線上帳號，透過其服務於新加坡傳播任何陳述；或不允許任何人使用被限制的特定線上帳號，與其在新加坡境內網路中介服務的任何終端用戶進行互動[771]。

若網際網路中介者未遵循帳號限制命令之要求，可處 1 年以下有期徒刑，及 2 萬新加坡幣（約新台幣 47 萬元）以下罰金。若行為人持續違反之情形，可按日連續處罰最高至 10 萬新加坡幣（約新台幣 236 萬元）以下罰金。且部長亦得在一定要件下，指示 IMDA 對 ISP 業者發布阻斷接取命令，命該業者採取合理措施，中止位處新加坡的終端使用者連結至該線上位置。若 ISP 業者未遵守該阻斷接取命令，可按日處 2 萬新加坡幣以下罰金至履行該命令所示義務為止，最高可處以 50 萬新加坡幣（約新台幣 1,180 萬元）以下之罰金。

6. 救濟機制

因該法對於何謂「陳述為誤」（a statement is false）之定義說明僅簡要提及「若其為虛假或具誤導性者，則無論是全部或一部，亦無論是其本身或在其所出現之的脈絡下，均屬虛假事實陳述（false statement of fact）」[772]，並未明確說明如何確定陳述是「虛假的」（false）。

就此，對於主管機關發出的處分之判斷，必須先行向發出修正指示之部長提出申訴；若申訴失敗後，再向新加坡高等法院提起上訴予以救濟（appeals to High Court），尋求法院判斷虛假事實陳述[773]，即司法部門擁有是否為虛假陳述之最終決定權。

[771] POFMA, Sec. 40.
[772] POFMA, Sec. 2.
[773] POFMA, Sec. 44.

7. 爭議

新加坡之法務部長曾表示，已有研究證實「更正錯誤」是有效對抗虛假新聞之重要解毒劑，尤其在 Covid-19 疫情時代中發揮有效之功用，因此政府認為訂立具有強制性罰則之法規有其效益，將使網站或民眾於分享線上內容時更為謹慎，即便是在私人聊天的視窗中亦然。

實際上，於《POFMA》立法後相關爭議不時發生，其嚴厲管控不實訊息的手段，引發社會不小爭議[774]。其中社群平臺 Facebook 更是作為主戰場[775]，分享不實訊息的人，尤其是那些知名度高、具有影響力的人物，也可能被要求提出糾正或刪除虛假訊息，因為他們承擔著更大的社會責任，故被期待要更加謹慎對待可能破壞社會的內容，但有許多不同意見質疑政府的做法其實是為了壓制反對派聲音[776]。

鑑於「虛假陳述」、「公共利益」等要件之模糊性，《POFMA》基本上使各部會之部長們成為真理的仲裁者。雖然新加坡的司法機構對於依《POFMA》所為之指示具有最終決定權，然而受處分人仍然必須首先遵守，否則將面臨刑事起訴的風險。且除上訴之時間與金錢成本不斐外，就實際經驗來看，上訴成功之機率極低[777]。

除新加坡國內之異議聲浪外，國際法院也曾指出新加坡政府實施《POFMA》且未有充分司法監督之作為，與國際法中線上言論及資訊自由之人權標準，有所扞格。因此，數次呼籲新加坡政府廢止《POFMA》或對該法進行實質性之修法[778]。

---

[774] Ian Seiderman, RE: Protection from Online Falsehoods and Manipulation Bill 2019 (2019/04/12), International Commission of Jurists (ICJ), *available at* https://www.icj.org/wp-content/uploads/2019/04/Singapore-online-regulation-bill-letter-advocacy-open-letter-2019-ENG.pdf.

[775] 簡恆宇，社群平台質疑「反假新聞法」箝制言論自由 《華盛頓郵報》：新加坡藉疫情測試法規成效，風傳媒（2020/03/18），https://reurl.cc/o7ELj3（最後瀏覽日：2023 年 7 月 24 日）。

[776] Kathleen, *SPH and Mediacorp remain silent on criticisms and concerns by various statements published by different groups on POFMA*, TQC (2019/04/30), https://www.theonlinecitizen.com/2019/04/30/sph-and-mediacorp-remain-silent-on-criticisms-and-concerns-by-various-statements-published-by-different-groups-on-pofma/ (last visited July 24, 2023).

[777] Dartmouth College, *Singapore's Fake News Law: For or Against Democracy?*, Democratic Erosion (2022/05/27), https://www.democratic-erosion.com/2022/05/27/singapores-fake-news-law-for-or-against-democracy/ (last visited July 24, 2023).

[778] International Commission of Jurists, *Singapore: ICJ calls on government to repeal or substantially amend the POFMA, two years after it entered into force*, ICJ (2021/04/10), https://www.icj.org/singapore-icj-calls-on-government-to-repeal-or-substantially-amend-the-pofma-two-years-after-it-entered-into-force/ (last visited July 24, 2023).

8. 實際案例

承前所述，《POFMA》立法後的質疑不斷。新加坡政府開的第一槍即是針對新加坡前進黨（反對黨）黨員鮑耶（Brad Bowyer）2019 年 11 月底於 Facebook 發布一則貼文，內容為影射政府直接參與淡馬錫控股和新加坡政府投資公司而質疑其獨立性，旋即被新加坡財政部（Ministry of Finance, MOF）指控為虛假資訊[779]，要求修改有關內容[780]。鮑耶事後更改帖文，並附帶政府聲明連結，提醒評論國內政治及社會議題的人士務必小心謹慎，但保留提出上訴的權利[781]。

近期亦發生相類情形，亦是針對新加坡前進黨（反對黨）黨員在 Facebook 上之貼文，本次起因於新加坡總理李顯龍之胞弟李顯揚在 Facebook 提及政府爆出的多起官員涉嫌貪污而受調查之醜聞，就此，政府指出李顯揚其中提及「部長租屋砍樹事件」和「新加坡報業控股（SPH）發行流量數據造假」兩起事件屬於不實訊息[782]，故由新加坡律政部（Ministry of Law, MINLAW）依據《POFMA》讓 POFMA 辦公室向李顯揚發出更正指示，要求其必須在貼文附上更正指示的通知，且說明貼文含有不實內容。而雖李顯揚隨後在 Facebook 貼文附上更正通知。不過，他隨即再發一則貼文表示堅持更正之前的說法，甚至主張 POFMA 辦公室之更正指示具有誤導性[783]。

---

[779] Ministry of Finance, *Use of POFMA on an online posting by Mr Brad Bowyer*, Press Releases (2019/11/25), https://www.mof.gov.sg/news-publications/press-releases/use-of-pofma-on-an-online-posting-by-mr-brad-bowyer (last visited July 24, 2023).

[780] Gov.sg, *Corrections and clarifications regarding falsehoods posted by Mr Brad Bowyer: Misleading and false statements were made by Brad Bowyer on Temasek and GIC* (2019/11/24), https://www.gov.sg/article/factually-clarifications-on-falsehoods-posted-by-mr-brad-bowyer (last visited July 24, 2023).

[781] Prisca Ang, *PSP member in first Pofma case considering appeal*, STRAITSTIMES (2019/11/29), https://www.straitstimes.com/singapore/psp-member-in-first-pofma-case-considering-appeal (last visited July 24, 2023).

[782] 林偉傑，李顯揚貼文不實 接到更正指示，聯合早報（2023/07/25），https://www.zaobao.com.sg/realtime/singapore/story20230725-1417196?close=true（最後瀏覽日：2023 年 8 月 1 日）。

[783] Singapore, *Lee Hsien Yang issued POFMA order over Facebook post on Ridout Road rentals, SPH circulation data*, CNA (2023/07/25), https://www.channelnewsasia.com/singapore/pofma-order-lee-hsien-yang-facebook-post-ridout-road-rentals-sph-circulation-data-3652176 (last visited Aug. 1, 2023).

（二）2021 年《外國干預反制法》

肇因於新加坡政府認為網際網路近年成為強大的顛覆國家媒介，如新加坡內政部（Ministry of Home Affairs, MHA）即表示，現今多有外國勢力（foreign principal）將此視為陸海空軍力以外之第 4 種作戰手段，尤其新加坡之社會（如多元種族及宗教）結構，容易受到外國勢力透過線上社群媒體傳散精心策畫的內容，達成試圖撼動社會穩定與凝聚力[784]，進而對新加坡主權及國家安全構成嚴重威脅之政治目的[785]。且過往也發生多起外國勢力干涉之案例，故而 2018 年研究線上虛假內容傳散問題之特選委員會（Select Committee on Deliberate Online Falsehoods）指出需要制定一部法律加以因應[786]。

基此，2019 年 9 月 13 日新加坡政府制定《外國干預反制法》（Foreign Interference (Countermeasures) Act, FICA），並於 2021 年 10 月 4 日由議會通過、同月 29 日由總統簽署後發布[787]，共計 11 編、127 條條文。其中涉及「有害線上外國干擾活動」相關之規定先於 2022 年 7 月 7 日生效，而與「具政治影響力之人物」（politically significant persons）[788]相關之規定，後於 2023 年 12 月 29 日生效[789]。

本法之立法旨在授權主管機關（由部長指定公部門官員擔任[790]），若確定任何人之行動係出於政治目的，並意圖、明知或可得而知利用電子通訊或線上社群媒體，散布有害新加坡公共利益之資訊，將面臨刑事處罰，且未遂犯亦罰之。藉此採取反制措施，防範外國勢力透過電子通訊、政治獻金等手段對新加坡造成之影響[791]。

---

[784] BBC, 新加坡通過「防外國干預法」的爭議和影響，BBC NEWS 中文網（2021/10/8），https://www.bbc.com/zhongwen/trad/world-58842757（最後瀏覽日：2024 年 11 月 11 日）。

[785] 針對新加坡的政治目的，可參 Foreign Interference (Countermeasures) Act, Sec. 8. [hereinafter FICA]

[786] Rei Kurohi, *5 things to know about Fica, the law to counter foreign interference*, The Straits Times (2021/10/05), https://www.straitstimes.com/singapore/politics/5-things-to-know-about-fica-the-law-to-counter-foreign-interference (last visited Jan. 05, 2024).

[787] *Id*.

[788] FICA, Part 4.

[789] Ministry of Home Affairs, *Introduction to Foreign Interference (Countermeasures) Act (FICA)*, https://www.mha.gov.sg/fica (last visited Jan. 05, 2024).

[790] FICA, Sec. 105. 又第 107 條規定，主管機關可任命公職人員或公共機構（市鎮理事會除外）之受僱者為授權官員，並賦予其主管機關之全部或部分權力或職責。

[791] FICA, Sec. 2.

1. 規範對象

上開提及之「外國勢力」所指者為，外國人、外國政府、與外國政府有關之個人、外國立法機關、外國政治組織、外國公共企業或外國私人企業[792]等。

而舉凡與外國勢力訂有協議者、服務於外國勢力者、受外國勢力命令或要求者、受外國勢力控制、指示或監督者、受外國勢力資助者，以及與外國勢力合作者[793]均屬本法指涉之對象。

2. 防制措施：打擊敵意資訊活動

針對「有害線上外國干擾活動」，部長可授權主管機關發布本法第三編之命令（Part 3 directions）[794]。具體而言，第三編之命令有以下類型，且各自之適用對象皆有所不同，或為社群媒體服務提供者、相關電子服務提供者、經營網站、部落格或社群媒體專頁者，或是網際網路接取服務提供者、網際網路資訊儲存服務提供者等[795]。

- 停止終端用戶通訊傳播命令（stop communication [end-users] direction）[796]；
- 中止命令（disabling direction）[797]；
- 1 級至 4 級之必載命令（must-carry direction）與補償性必載命令（remedial must-carry direction）[798]；
- 1 級至 2 級阻斷接取命令（access blocking direction）[799]；
- 帳戶限制命令（account restriction direction）[800]；

[792] FICA, Sec. 4.
[793] FICA, Sec. 5 (1).
[794] FICA, Sec. 20.
[795] FICA, Sec. 29.
[796] FICA, Sec. 30.
[797] FICA, Sec. 31.
[798] FICA, Sec. 32.
[799] FICA, Sec. 33.
[800] FICA, Sec. 34.

- 服務限制命令（service restriction direction）[801]；
- 技術支援命令（technical assistance direction）[802]；
- 應用程式移除命令（App removal direction）[803]；
- 獲利回吐命令（disgorgement direction）[804]。

此外，若不遵守第 3 編之命令，針對上開不同命令，將可處以罰鍰或有期徒刑，或兩者併罰[805]。

3. 防制措施：禁止線上位址宣告

發布第三編之命令後，部長更可進一步針對特定線上位址發布「禁止線上位址宣告」(proscribed online location)，就該位址進行營運、支援或廣告交易之行為，皆須受刑事處罰[806]。

而本法所稱之線上位址經營者，則包含該線上位址之開發及維持者；組織、管理或監督該線上位址之利用者；對該線上位址之接取或會員資格進行管理或規範者；對該線上位址應包含或排除任何資訊、資訊應放置於該線上位址的任何位置擁有決定權限，或對該線上位址實行其他編輯控制者[807]。

其中，若個人與受禁止宣告之線上位址經營者締結廣告交易契約，而未採取足夠之措施，確保該位址之資訊內容不被新加坡之終端用戶接取，或促進、協助公眾對相關資訊內容之呈現，將面臨最高新加坡幣 2 萬元之罰金，或最高 12 個月之有期徒刑，或兩者皆罰[808]；若非個人，則處以最高新加坡幣 2 萬元之罰金。

此一機制之設計與前述之《2019 年虛假內容與操縱防止法》相似，均係以廣告交易之相對人為規範對象，透過刑事處罰之恫嚇力以

[801] FICA, Sec. 35.
[802] FICA, Sec. 36.
[803] FICA, Sec. 37.
[804] FICA, Sec. 38.
[805] FICA, Secs. 42-46.
[806] FICA, Secs. 39-41.
[807] FICA, Sec. 3.
[808] FICA, Sec. 41.

阻斷外國勢力之收入來源，進而間接達成反制外國干預之目的。

4. 再議機制

禁止線上位址宣告做成後，該線上位址之經營者（proprietor）得於 30 天內向部長申請再議，無論再議結果為維持或撤銷原宣告，皆須通知線上位址之經營者[809]。

5. 爭議

雖然內政部表示本法排除大多數的學術活動，如與海外其他人士合作、撰寫國際期刊文章及接受國際資助之情形，然而較有疑義的是本法於立法階段未經公眾諮詢或經特選委員會審查[810]，且本法由司法體系介入審查的餘地相當侷限[811]。

（三）2022 年《線上安全（其他修正）法》

新加坡政府為回應各界呼籲以更多的保護措施作為兒少等弱勢族群之防護，自 2022 年 7 月 13 日至 8 月 10 日開啟公眾諮詢[812]，並於 2022 年 10 月提出《線上安全（其他修正）法》（Online Safety (Miscellaneous Amendments) Bill）草案，次月即由議會通過該法，並於 2023 年 2 月 1 日起生效。主要是調修 1994 年《廣播電視法》中部分條文及新增第 10A 編，及調修 2010 年《電子交易法》部分條文，藉由實施針對社群媒體之一般性管制措施而加強線上安全[813]。

---

809 FICA, Secs. 261(1)-(2).

810 Rei Kurohi, *supra* note 787.

811 FICA, Sec. 104. 除非具有程序瑕疵，否則無法向任何法院表示異議、上訴、審理、撤銷。

812 MCI, *Public Consultation on Proposed Measures to Enhance Online Safety for Users in Singapore*, https://www.reach.gov.sg/Participate/Public-Consultation/Ministry-of-Communications-and-Information/public-consultation-on-enhancing-online-safety-for-users-in-singapore (last visited Aug. 1, 2023).

813 Eileen Yu, *Singapore can now order social media sites to block access, as 'online safety' law kicks in*, ZDNET (2023/01/31), https://www.zdnet.com/article/singapore-can-now-order-social-media-sites-to-block-access-as-online-safety-law-kicks-in/ (last visited Aug. 1, 2023).

1. 規範對象

規範對象主要為受管制之線上通訊傳播服務（regulated online communication services），包括於新加坡境內或從新加坡境外提供此類服務，並得由主管機關 IMDA 將具有「重大影響力」之線上通訊傳播服務指定為屬於受管制之平臺[814]，並課予指定平臺必須遵守依法要求其建構與實施之系統和流程之實踐準則，以降低新加坡之線上使用者接觸有害內容之風險[815]。

而線上通訊傳播服務係指新增之第 4 附表（Fourth Schedule）中具有電子服務或電子服務之一部分特徵者，即供終端使用者能夠使用該服務（包含點對多點服務）在網路上接觸或交流內容；透過前項之服務而在網路上向擁有適合接收該內容之設備者提供內容。諸如行動多媒體訊息（MMS）或行動文字訊息（SMS）等均屬之。目前清單所指定者僅限於社群媒體服務[816]。但是，MCI 部長可以經由公報發布命令，撤銷、替換或添加第 4 附表之清單[817]。

其中因涉及隱私之疑義，故規管對象並未擴及至私人人際通訊，但新加坡有注意到「群組」的人數非常眾多[818]，諸多不當的內容亦可透過此方式快速傳散，所造成之結果與非私人人際通訊並無區別，就此，IMDA 將有權對「群組」採取相同的舉措。

2. IMDA 之管制作為

授權主責機關 IMDA 基於確信線上有「極其惡劣之內容」（egregious content）時，可作成命令，命線上通訊傳播服務（目前僅適用社群媒體平臺）在「數小時」（within hours）內刪除該內容[819]；或命線上通訊傳播服務阻斷（block）使用者接取特定來源（例如帳戶、

---

[814] Broadcasting Act 1994, Sec. 45K.
[815] Broadcasting Act 1994, Sec. 45A.
[816] Broadcasting Act 1994, Sec. 45T.
[817] Broadcasting Act 1994, Sec. 2B.
[818] Broadcasting Act 1994, Sec. 2A(3).
[819] Broadcasting Act 1994, Sec. 45H. TelecomNews, *Singapore mandates social media sites to block harmful content sites 'within hours'*, ETTelecom.com (2022/11/09), https://telecom.economictimes.indiatimes.com/news/singapore-mandates-social-media-sites-to-block-harmful-content-sites-within-hours/95409920 (last visited Aug. 1, 2023).

群組或頻道）中之有害內容。甚至得命 IASP 拒絕通訊傳遞以阻斷使用者接取[820]。

而分別收到第 45H 條命令或第 45I 條阻斷命令之線上通訊傳播服務提供者及 IASP 業者均有義務採取所有合理可行之步驟來遵守該命令[821]。不服 IMDA 命令者，可向 MCI 部長提出申訴。

若線上平臺拒絕配合刪除有害內容，IMDA 得處以其認為適宜之任何數額，但最高以 100 萬新加坡幣（約新台幣 2,356 萬元），或可按日連續處罰最高至 10 萬新加坡幣（約新台幣 235 萬元）以下罰金[822]。

而何謂「極其惡劣之內容」，法規中提供進一步的指導，包括宣揚或提倡自殺或自殘、身體暴力或性暴力和恐怖主義之內容、描繪兒童性剝削之內容、在新加坡構成公共健康風險之內容，以及可能導致和歧視之內容，以及涉及新加坡不同的種族和宗教之敵意、仇恨、蔑視或嘲笑之內容[823]。饒是如此，有一些內容仍舊處於難以定義的灰色地帶，就此，IMDA 表示在這種情況下將採取客觀的方法並衡量其呈現的背景。

3. 制定實踐準則

依據第 45L 條之規定，MCI 部長可制定線上實踐準則供受管制之線上通訊傳播服務遵循，且受管制之線上通訊傳播服務之提供者均有義務採取所有合理可行之步驟來遵守該命令[824]。關於 MCI 研擬之實踐準則，詳如後述。

而在 MCI 所制定之實踐準則的限度內，同條規範亦授權 IMDA 得不時發布一個或多個適用於所有受管制之線上通訊傳播服務或相類提供商之線上實踐準則。但是，限制其僅得在遵循某些諮詢程序後，才能發布、修改或撤銷線上實踐準則。

---

820 Broadcasting Act 1994, Sec. 45I. TelecomNews, *id*.
821 Broadcasting Act 1994, Sec. 45J.
822 Broadcasting Act 1994, Sec. 45N.
823 Broadcasting Act 1994, Sec. 45D.
824 Broadcasting Act 1994, Sec. 45M.

有關實踐準則可規定符合或促進第 45A 條之目的，以及下列所有或任何內容（同條第 4 項）：

（1）風險最小化措施

要求線上通訊傳播服務提供者建立和實施適當的系統或流程，以便以 (i) 防止使用者（尤其是不同年齡層之兒童）接近可能對他們造成重大傷害之內容；以及 (ii) 降低和管理其服務內容對新加坡終端使用者(尤其是不同年齡層之兒童)造成危險之風險等方式提供服務。

（2）風險指南

任何就關於有哪些內容會對新加坡終端使用者或特定類型之新加坡終端使用者，存在重大危害的實質性風險之實用指南。

（3）法遵程序

為履行適用於受管制之線上通訊傳播服務提供者之線上實踐準則所定之義務而應遵循的程序，其中可能包括：(i) IMDA 確認服務提供者遵守實踐準則之稽查程序；(ii) 服務提供者（應 IMDA 之要求）而向 IMDA 報告其所採取確保新加坡終端使用者得以安全方式使用服務之資訊；(iii) 對服務提供者之系統性風險進行風險評估，並採取旨在降低這些風險的合理有效措施[825]。

（4）與研究單位合作

要求受管制之線上通訊傳播服務提供者，與合適的專家或經 IMDA 認可之專家進行研究合作，以利 IMDA 掌握就受管制之線上通訊傳播服務的系統性風險及其演變與嚴重程度。

4. 實際案例

起因於新加坡警察部隊（Singapore Police Force, SPF）向 IMDA 示警 Facebook 作為線上共享兒童性剝削製品(child sexual exploitation material, CSEM）內容之一環，且 IMDA 隨即亦發現某個 Facebook 群

[825] Id.

組當中發布包含引導使用者訪問類似內容之超鏈結的貼文，而對於新加坡而言，CSEM 該當《線上安全（其他修正）法》所指涉的「極其惡劣之內容」。

自《廣播電視法》修訂納入線上安全要求以來，IMDA 首次通知社群媒體平臺審查並刪除涉及 CSEM 內容，即要求 Meta 刪除 Facebook 頁面和群組上之相關內容，亦指示新加坡的網際網路服務提供者阻斷接取至 Facebook 相關頁面和群組的網站鏈結，以免該網站上之更多 CSEM 內容繼續向外擴散，而 Meta 亦已配合在 24 小時內將其刪除[826]。

（四）相關實踐準則

對於網路內容之管理，新加坡早先公告《網路行為準則》。其後於 2022 年制定《線上安全（其他修正）法)》後，又著手研擬相關之準則[827]，預許作為有助於提高新加坡之線上安全標準的配套措施，以下說明。

1. 《網路行為準則》

對於網路內容的管理，由於《廣播法》（Broadcasting Act）第 28 章規定 IMDA 得訂定廣播業許可證照之施行規定，並責成 IMDA 確保任何取得許可之廣播服務提供者，於其服務上不得有任何違反公共利益或公共秩序、國家和諧（national harmony）或有損良好品味及體面（good taste or decency）之資訊。

為達到成此任務，IMDA 於 2016 年制定《網際網路實踐準則》（Internet Code of Practice）取代 1996 年新加坡傳播局（Singapore Broadcasting Authority, SBA）發布之實踐準則（Notification no.

[826] IMDA, IMDA notifies Meta of egregious Child Sexual Exploitation content, defined under Singapore's new Online Safety law, found on Facebook, Resources (2023/06/09), https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/imda-notifies-meta-of-egregious-child-sexual-exploitation-content-defined-under-singapores-new-online-safety-law-found-on-facebook (last visited Aug. 1, 2023).

[827] Marian Ho, *New Codes of Practice for Online Safety in Singapore*, Dentons (2022/07/18), https://dentons.rodyk.com/en/insights/alerts/2022/july/18/new-codes-of-practice-for-online-safety-in-singapore (last visited Aug. 1, 2023).

2400/96）。課予受許可者（licensee）相關義務，進而應盡最大努力防止上開資訊透過其服務向新加坡之使用者傳散。

也即，IMDA 通知（notice）所有經許可之網際網路接取服務提供者（Internet Access Service Provider, IASP）、經銷商（resellers）或和網路內容提供者應依其服務性質而負擔《網路行為準則》之規定之相應義務遵守。且網路近用服務業者（Internet Access Service Provider, IASP）在網站內容包含有本準則第 4 條所禁止之內容者，應拒絕網站之近用。

其違反之效果，依《廣播電視法》第 16 條第 3 項之規定，違反該法規定或相關行為準則者，IMDA 對經許可之業者，得處以 2 萬新加坡幣以下之罰鍰，或 2 年以下有期徒刑之制裁。

2. 《線上安全（其他修正）法》之相關準則

MCI 於 2022 年 7 月曾提出《線上安全實踐準則》(Code of Practice for Online Safety, CPOS）、《社群媒體服務內容準則》（Content Code for Social Media Services, CCSMS）兩項準則付公眾諮詢[828]。

（1）《線上安全實踐準則》

MCI 在《線上安全（其他修正）法》通過後提出相關之第一項準則為《線上安全實踐準則》，且已於 2023 年 7 月 18 日通過[829]。。

主要係擬要求指定具有高影響力或高風險之社群媒體平臺，針對色情內容、暴力內容、自殘內容、網路霸凌內容、危害公眾健康內容、兒童性剝削和性虐待內容，以及助長恐怖主義和組織犯罪之內容，制定與實施社群標準及內容審查機制。主動檢測並刪除前開內容，以減少用戶對此類有害內容的接觸，例如在用戶報告時禁止訪問此類內容。

---

[828] Allen & Gledhill, *MCI Seeks Comments on Proposed Code of Practice for Online Safety and Content Code for Social Media Services*, Publications (2022/07/22), https://www.allenandgledhill.com/sg/publication/articles/22084/mci-seeks-comments-on-proposed-code-of-practice-for-online-safety-and-content-code-for-social-media-services (last visited Aug.1, 2023).

[829] IMDA, *IMDA's Online Safety Code comes into effect* (2023/07/17), https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/imdas-online-safety-code-comes-into-effect (last visited Aug. 1, 2023).

此外，亦應為使用者提供工具和選項，以管理使用者個人不想要接收之內容或互動，諸如允許使用者隱藏不想看見的資訊、允許使用者限制與其他使用者之聯繫和互動；以及推送相關安全資訊（例如，幫助熱線和諮詢)搜索高風險內容(例如，與自殘和自殺相關的內容）的使用者等等。

更重要的是，因線上有害內容對兒少、青少等年輕族群影響甚鉅，故指定社群媒體平臺額外針對年輕族群之使用者提供保護措施，包含制定更為嚴格之社群準則，或提供易於接近與理解之安全資訊，為年輕族群及其父母/監護人提供指導，說明如何保護年輕用戶免受有害或不適合年齡的內容和互動之影響。

最後，因社群媒體平臺上創建和共享的內容數量過於龐大，縱使採取保護措施，仍難免有漏網之魚。故而將課以指定的社群媒體服務提供有效之透明度報告，說明其內容審核政策和做法以及其提高用戶安全的措施。並將報告發佈在 IMDA 之官網，以利使用者能夠更為了解如何藉由該服務之作為而減少接觸有害內容之風險。

（2）《社群媒體服務內容準則》

MCI 提出與《線上安全（其他修正）法》相關之第二項準則為《社群媒體服務內容準則》，後續發展仍待追蹤。

此準則旨在處理新加坡之使用者在使用指定社群媒體平臺之服務時，可能會遇到的「嚴重線上危害」，像是鼓勵或支持自殺和自殘、鼓勵或支持性暴力或涉及脅迫或未經同意之性行為、鼓勵對青少年之性虐待、鼓勵未經證實之管制物質或藥品而危及公共衛生及健康、鼓勵或美化恐怖主義之暴力行為而危及公共安全，或是詆毀宗教或種族之內容、負面或過分之比較、汙損或毀壞宗教標誌等內容。

鑑於對此類「極端惡劣」之內容的擔憂，將授權 IMDA，使其得指示任何社群媒體平臺禁止新加坡之使用者觸及該等有害內容；或命社群媒體平臺禁止特定之線上帳號與其他新加坡之使用者進行內容交流和/或互動。

（五）2023 年《線上刑事犯罪危害法》

新加坡有感詐騙、外國干擾、線上賭博與性虐待資訊等線上危害行為層出不窮且形態萬千[830]，新加坡內政部（MHA）認為該等將對新加坡民眾人身安全構成威脅的線上犯罪行為，應透過擴張政府監管之權限，自實體世界延伸至虛擬世界，採取相應措施以有效應對線上犯罪之危害[831]，並順應國際潮流。

因此，新加坡議會於 2023 年 7 月 5 日通過《線上刑事犯罪危害法》（Online Criminal Harms Act 2023）、並於同月簽署後發布，授權政府刪除線上刑事犯罪內容，即允許政府要求個人、企業、線上與網路服務提供者，以及應用程式商店刪除或限制接取其懷疑有犯罪之虞的內容[832]，進而達到保護新加坡民眾受到網路傷害之目的。

雖然如前所述，已於 2022 年通過《線上安全（其他修正）法》，然本法除可涵蓋得進行犯罪活動之所有線上通訊媒介，亦處理包含更為廣泛之惡意網路活動與犯罪行為，包含詐騙、網路釣魚、線上遊戲虛擬寶物（loot boxes）[833]、違法高利貸、違法賭博和毒品等。兩項立法將相輔相成，聯合打擊線上犯罪[834]。

1. 規範對象

本法之規範對象包含個人、指定之線上服務提供者、網際網路服務供應商及應用程式下載平臺。其中有關線上服務提供者，具體而言，如 Facebook、TikTok、WhatsApp 與 WeChat 等均屬之[835]。

---

[830] MHA, Introduction of the Online Criminal Harms Bill, Press Releases (2023/05/08), https://www.mha.gov.sg/mediaroom/press-releases/introduction-of-the-online-criminal-harms-bill/ (last visited Dec. 20, 2023).

[831] David Sun, MHA to introduce new laws to tackle online harms, The Strits Times (2023/05/10), https://www.straitstimes.com/singapore/politics/mha-to-introduce-new-laws-to-tackle-online-harms (last visited Nov. 17, 2023).

[832] Samuel Devaraj, New law passed to remove online content that is criminal or harmful, The Straits Times (2023/07/06), https://www.straitstimes.com/singapore/parliament-passes-bill-that-allows-government-to-remove-online-criminal-content (last visited Nov. 17, 2023).

[833] David Sun, MHA to introduce new laws to tackle online harms, The Straits Times (2023/05/10), https://www.straitstimes.com/singapore/politics/mha-to-introduce-new-laws-to-tackle-online-harms (last visited Nov. 17, 2023).

[834] Samuel Devaraj, *supra* note 832.

[835] Samuel Devaraj, *supra* note 832.

此外，本法有域外適用，不論個人或事業在新加坡境內境外，皆為打擊範圍。

2. 網路犯罪行為

本法管制之特定犯罪、網路犯罪行為類型涵蓋如下：

- 恐怖主義與國家安全（如教唆或資助恐怖主義活動）；
- 破壞種族、宗教或社會階級（classes of the population）之間的和諧；
- 煽動暴力或未遵守法律；
- 洩露政府機密資訊；
- 與毒品或販毒有關之犯罪；
- 非法賭博；
- 非法高利貸；
- 詐騙和惡意網路活動；
- 性相關犯罪（未經同意散布兒童性虐待、偷拍或性愛影片）。

3. 防制措施

政府若有合理理由懷疑利用任何線上服務進行犯罪行為，則授權主管機關（並由部長指定任何公部門之公職人員或公共機構之受僱者擔任指定公務員或授權公務員[836]）得發布第二篇之命令（Part 2 directions）[837]，要求任何個人或事業依命令作為或不作為[838]，此一機制之設計與前述之《2021 年外國干預反制法》相似，根據本法規範之內容與對象[839]，可分為以下類型，：

[836] Online Criminal Harms Act 2023, Sec. 3-5. [hereinafter OCHA] 第 5 條規範可賦予指定公務員或授權公務員全部或部分主管機關之權力或職責。
[837] OCHA, Part2. [hereinafter OCHA]
[838] OCHA, Sec. 6.
[839] OCHA, Sec. 7.

- 停止通訊傳播命令（stop communication direction）[840]：在線上發佈與犯罪相關內容之使用者，於收受停止通訊傳播命令後，須刪除相關內容。
- 中止命令（disabling direction）[841]：要求線上服務提供者（不包括網際網路接取服務或應用程式下載服務）禁止新加坡人民接取其服務中的指定內容(例如貼文或頁面)，包括禁止接取此類資料、任何相同的副本相關資料或任何相關線上位置[842]。
- 帳戶限制命令（account restriction direction）[843]：要求線上服務提供者禁止或限制其服務上的帳戶與新加坡人進行交流，無論是透過終止、暫停或限制與該線上帳戶相關的功能。
- 阻斷接取命令（access blocking direction）[844]：要求網際網路服務供應商阻斷新加坡人接取線上位置。
- 應用程式移除命令（App removal direction）[845]：要求應用程式平臺從其新加坡商店中刪除某個應用程式，以阻止新加坡人進一步下載該應用程式。

[840] OCHA, Sec. 8.
[841] OCHA, Sec. 9.
[842] 第 2 條規定「線上位置」指任何可透過網路接取之網域、網站、網頁、聊天室、頻道、群組、論壇或任何其他位置。
[843] OCHA, Sec. 10.
[844] OCHA, Sec. 11.
[845] OCHA, Sec. 12.

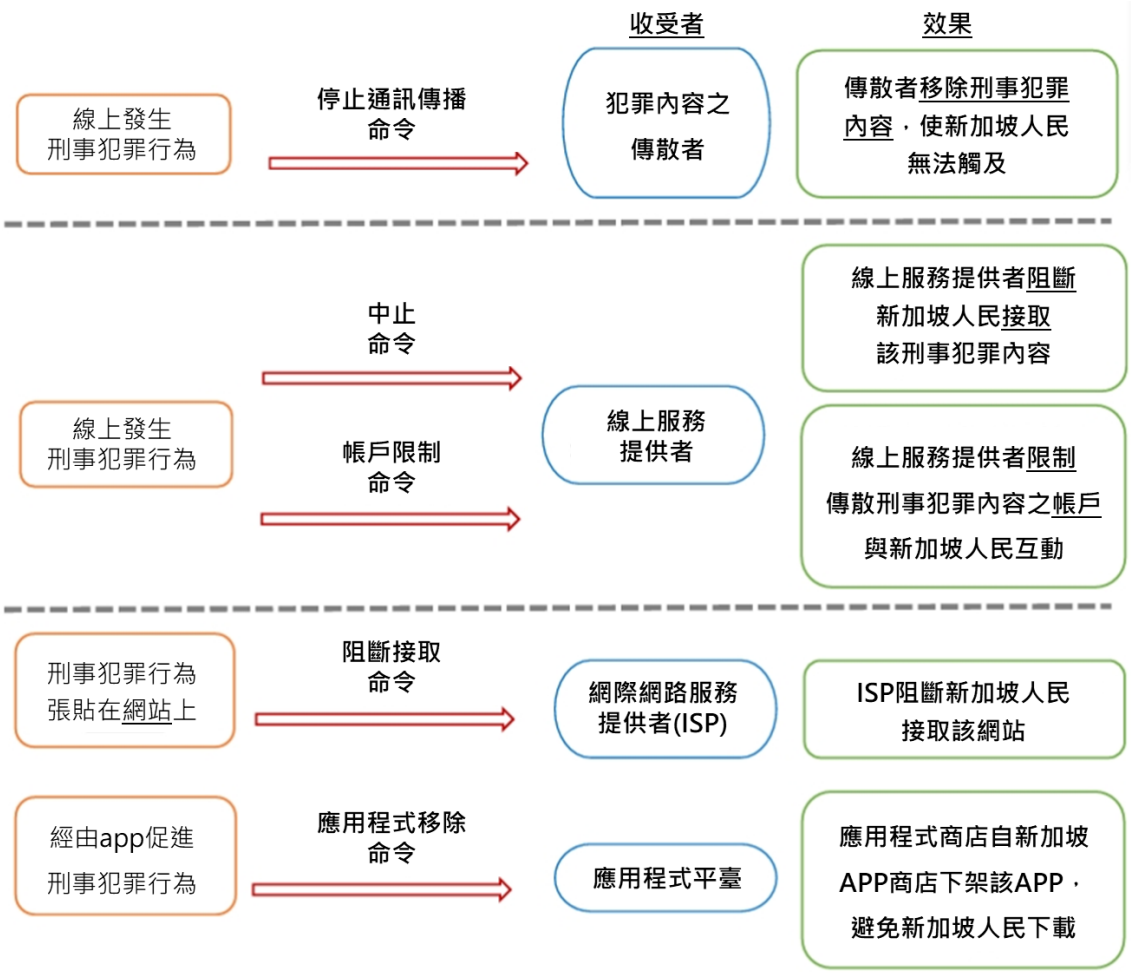


圖 22：《線上刑事犯罪危害法》之命令運作說明

資料來源：MHA[846]

4. 實踐準則

主管機關公告實踐準則（codes of practices），讓指定線上服務提供者遵守相關實踐準則，與警方合作打擊網上犯罪活動，主動偵測可疑情況，並與警方共用資料，減低使用者受騙或受害的風險。

若網上服務提供者未履行實踐準則或命令，警方可進一步發出命令，而使其遵行，否則將可能面對有期徒刑或罰鍰等刑罰。若線上服務提供者或平臺對實踐準則有異議，可以向新加坡內政部提起再議。

[846] MHA, Introduction of the Online Criminal Harms Bill,

5. 上訴機制

政府命令之收受者（Recipients）與該命令所針對之線上行為之發起者，得向審查仲裁庭（Reviewing Tribunal）提出上訴（appeal）。而總統會根據內閣的建議，任命地方法官或治安法官（Magistrate）組成審查仲裁庭，審理相關上訴[847]。且此等上訴程序將被視為司法程序。

三、第三方監督或產業自律機制

新加坡政府明白無法單靠《POFMA》或《線上安全（其他修正）法》遏止線上有害或違法訊息之流竄，基此，MCI 提出新加坡將採取全體社會（whole-of-society）之取徑，並透過 IMDA 高密度之執法權限監管線上之資訊。

所謂「全體社會」路徑，有三大作用方向：其一為以受閱聽眾信任之當地新聞媒體公司為堅實核心，線上為新加坡公民提供權威之資訊來源，應發揮其值得信賴，提供公民訊息與參與。其二為立法，諸如面對前所未聞之 COVID-19 疫情，《POFMA》發揮了重要的功用。

其三則認為應培養「真知灼見之公民」，諸如國家圖書委員會之 S.U.R.E.（Source, Understand, Research, Evaluate）計畫即為是例，透過公共教育幫助公眾辨別真偽，而新加坡政府也在各式平臺上以英語等多種語言發布正確資訊，以減少錯誤資訊之傳散餘地，諸如 gov.sg Whatsapp 官方帳號即以四種語言，共有 120 萬人次之訂閱數；此外，建立強大的事實查核生態系統，除透過事實查核組織間之網路交流與資訊共享外，數位平臺透過與獨立事實查核合作，透過科技與財物支持，共同創造解決之道[848]。

---

[847] OCHA, SecS. 38-44.

[848] Lakeisha Leo, Singapore takes a 'whole-of-society' approach to combat misinformation: Tan Kiat How, CNA (2022/04/29) https://www.channelnewsasia.com/singapore/tan-kiat-how-approach-combat-misinformation-local-news-2656731 (last visited Aug. 1, 2023).

整體而言，新加坡政府為保護新加坡，與人民、私經濟體與公共部門等利害關係人密切合作，致力讓民眾線上環境與現實世界中一樣感到安全[849]。

縱然社群媒體平臺大多有其本身之社群守則，且已積極採取打擊線上有害內容之因應措施[850]，但新加坡政府傾向採取與平臺合作之方式，但由政府佔據主導地位及發揮協調之功用，共同保護所有用戶（尤其是兒童）的線上安全。

四、小結

新加坡為有效集中推動數位發展政策，由 MCI 統籌資通訊與傳播政策發展相關之事項，且由其轄下之 IMDA 執行資通訊與媒體管制及數位發展政策。

新加坡係屬媒體發展之自由相對較為受限的國家，新加坡《廣播電視法》主要係設定新加坡廣電業者之規範框架，具體規範細節則授權由 IMDA 訂定相關實務準則。因此實務上會因為各服務提供者所持有之執照不同而導致所須遵循之具體規範亦不相同。換言之，於新加坡不論傳遞技術為何，包括由無線、有線、衛星與 OTT TV 平臺等任何影視音平臺提供皆屬於廣播電視服務。

諸如 IMDA 已於 2018 年將網路網路視聽服務平臺納管，然僅針對內容設定一般性之監管標準，除於 2018 年 3 月頒布《OTT、VOD 與小眾服務內容準則》（Content Code For Over-The-Top, Video-on-Demand and Niche Services），主要針對與新加坡相關且涉及國家與公共利益、種族與宗教和諧、新聞及其他事實內容、色情產業與對兒少有害之內容進行管制，要求業者負擔防護責任外，並未要求 OTT TV 服務提供者遵循其他實務準則。

再者將數位中介服務平臺或是社群媒體平臺納入線上內容之管

[849] Ministry of Communications and Information, Public Consultation on Enhancing Online Safety for Users in Singapore, https://www.reach.gov.sg/Participate/Public-Consultation/Ministry-of-Communications-and-Information/public-consultation-on-enhancing-online-safety-for-users-in-singapore (last visited Aug. 1, 2023).

[850] IMDA, *supra* note 829.

制體系，從《POFMA》的實踐經驗來看，該法將違法內容定義為「有損公共利益或公共秩序、國家和諧或其他法律禁止之內容」，其構成要件與後續判斷取決於新加坡各政府部門之部長的裁量，似較為主觀、抽象，但其效果卻進一步由 IDMA 命服務提供者阻斷接取服務，讓新加坡之使用者無法近用；到近期透過《線上安全（其他修正）法》之修訂《廣播電視法》等相關法規，及相關之實踐準則，並賦予 IMDA 極大之權限，且對認定「有害或違法」之內容過於廣泛而擁有諸多釋義之空間，恐帶來寒蟬效應的深遠不利影響。

整體觀之，新加坡各法均動輒得由 IMDA 處以罰鍰或有期徒刑之制裁，且無法官保留之設計，恐進一步強化自我審查之效果。雖然仍有設計事後的申訴與司法救濟管道，然其遭受違反基本人權保障的爭議甚多，與我國憲政主義法治國的原則不符，建議後續僅可作為國際案例觀察之參考。

第十二節　綜合歸納與比較

一、違法內容處理之象限圖與電訪概要模式說明

綜上所述，本研究將前開研究國別之法制政策進行不同面向之綜合歸納。其一係以管制措施中之「禁制違法內容廣泛／有限」及「高密度／低密度網際網路內容執法措施」為基準，區別出四個象限，繪製為以下之象限圖（一）。

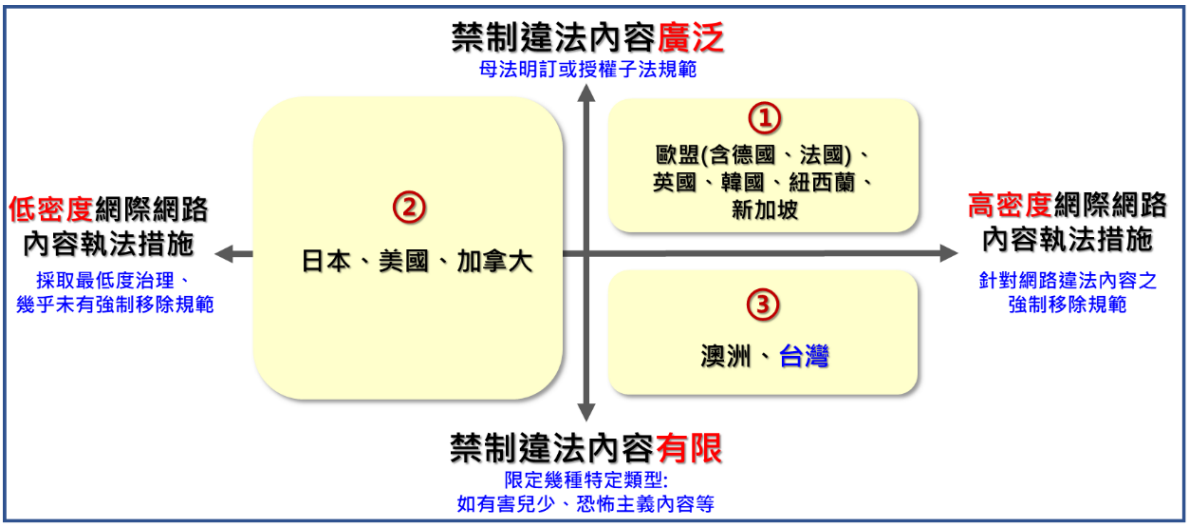


圖 23：世界各國網際網路傳播社會問題之處理模式象限圖（一）
資料來源：本研究自行繪製

關於縱軸，所謂「禁制違法內容廣泛」，係指該國於母法內直接規範對處各類網際網路或數位平臺上之違法內容，如歐盟 2022 年正式通過之《數位服務法》，即將違法內容直接定義為「任何違反歐盟法或內國法之內容或與違法有關之行為」；又如韓國透過寬泛之法律授權，由總統訂定法規命令，將「違反網路倫理」進行文意解釋最大射程範圍之「增築」，而可對處幾乎任何政府判斷應予禁制之內容或資訊。

相對地，「禁制違法內容有限」則指該國立法僅針對有限、特定之網際網路議題進行處理，進而將其定義為違法內容並禁制之。例如澳洲透過《網路安全法》定義兒少性剝削內容、恐怖主義內容等四大類型之違法內容，並僅處理該些違法內容；至若不實訊息，既非規範

之列，當不在規範密度較高之管制之中，而透過其他自律或共管之方式加以治理。又如德國，其《網路執行法》僅規範特定違反刑法之資訊。

橫軸方面，所謂「高密度網際網路內容執法措施」，係指該國法制針對網際網路違法內容設有強制移除等對於使用者言論自由影響較鉅之規範，具體而言又可依其程序是否須先經過法院審議、又或者僅須由行政機關自行為之，而區分為「有法官保留」及「無法官保留」之類型，前者例如德國《網路執行法》，聯邦司法部針對未適切移除違法內容而欲裁罰社群媒體時，須先向波昂行政法院取得先行裁決，始得為之，又如英國《線上安全法》之「接取限制令」，也須由 Ofcom 向法院聲請；後者例如韓國係由 KCSC 審議後，由 KCC 下達處分；澳洲係直接由電子安全專員命移除違法內容。

相對地，「低密度網際網路內容執法措施」則指該國採取低限度之網路治理模式，幾乎沒有透過法律設立網際網路違法內容之強制移除規範，以責任安全港制度或仰賴民間通報組織為治理核心的日本、美國及加拿大即為代表。

日本除了其運行多年的《ISP 責任限制法》外，總務省之專家小組迄今仍認為應維持以行政指導為核心之治理方針。而美國與加拿大則是法制上特別尊重言論自由之國家，除了《通訊端正法》第 230 條外，大抵透過民間通報組織進行相關的治理。不過值得注意的是，近期美國國會與加拿大都有針對數位平臺進行規管、傾向強化平臺問責之法案提出，其後續立法作為值得持續觀察。

另一方面，若進一步從表意者權利保障的角度思考，在維持縱軸「禁制違法內容廣泛／有限」之同時，於橫軸加入「有法官保留／無法官保留」之標準，以此描述各國法制之違法內容移除機制給予司法權判斷之空間大小，則可得出以下之象限圖（二）。

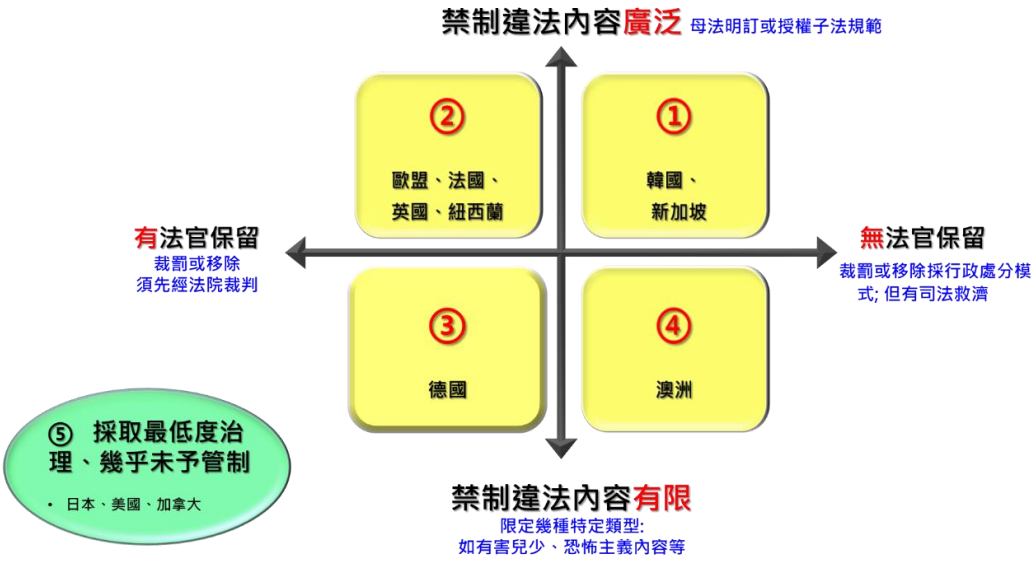


圖 24：世界各國網際網路傳播社會問題之處理模式象限圖（二）
資料來源：本研究自行繪製

所謂「無法官保留」，係指該國政府欲裁罰或移除違法內容，可直接以行政機關之命令或行政處分為之，毋須事先經過法院審議。例如韓國係由 KCSC 審議後，由 KCC 下達處分；或澳洲是直接由電子安全專員命移除之。

所謂「有法官保留」，則係指行政機關認管制主體未適切處置違法，而裁罰或命移除前，應先取得法院之裁判。例如德國《網路執行法》中，聯邦司法部針對未適切移除違法內容而欲裁罰社群媒體時，須先向波昂行政法院取得先行裁決，始得為之。又如英國《線上安全法》中之「接取限制令」，也須由 Ofcom 向法院聲請。再如紐西蘭之制度，共管機構 Netsafe 也無移除或阻斷之實質權力，在通知社群平臺移除而未果時，被害者於向 Netsafe 取得事件摘要後，自行向法院起訴移除或阻斷之。

值得注意者係，若採取此一劃分模式，在實質管制的四個象限外，則有日本、美國、加拿大等未予實質管制，且採取最低度治理之國家。

作為本研究規劃一般大眾電話訪問調查時說明各國法制之基礎，考量電訪所耗費之時間與其完成率息息相關，訪員對於議題之說明宜力求簡要，並降低專業術語之比例，使受訪者易於理解，故本研究擬以象限圖（一）之比較方式，作為電話訪問調查時之說明。

二、共通性議題之處理模式比較研析

另一方面，透過各國法制資料之觀察，本研究也可歸納出「政治不實訊息」、「兒少網路安全」、「網路交易安全」、「網路霸凌」、「使用者權益」等世界主要國家普遍關切之共通性網際網路議題，以下也將就前述各研究國別之政府機關法制政策作為、第三方監督或產業自律機制進行表整如下。

表 12：研究國別就政治不實訊息之處理模式

政治不實訊息		
	政府機關法制政策作為	**第三方監督或產業自律機制**
歐盟	《數位服務法》前言肯認，若服務提供者確實堅守及遵循既有之行為準則，將有可能被視為已採取妥適之風險減輕措施	➢《因應不實訊息實踐準則》 ➢《執委會就強化因應不實訊息實踐準則之指引》 ➢《強化因應不實訊息實踐準則》
德國	➢ NetzDG 設有違法內容移除機制，具體而言，涉及刑法預備危害國家暴力行為罪、外患謠言罪、汙衊宗教與宗教團體罪等行為之內容皆有適用之可能 ➢ NetzDG 廢止後，將透過內國法之革新介接歐盟《數位服務法》	配合歐盟機制，未有特別措施
法國	《2018 年反資訊操縱法》特別規範，選舉期間由緊急審理法官在受理後 48 小時內裁決不實訊息	除配合歐盟機制外，亦以媒體產業自律為主進行事實查核，例如：法新社之 AFP Factuel、《解放報》之 Désintox、《世界報》之 Les Déocoders、《二十分鐘報》之 Fake Off 等
英國	《線上安全法》附表 7 將外國干預列為違法內容態樣之一，並課予服務提供者予以安全管理、受理使用者通知及處理、風險評估等義務	英國政府透過線上國安資訊小組（National Security Online Information Team, NSOIT）關注有關國安與公共安全之內容（尤其是外國勢力故意傳散之不實訊息）

美國	未有特別規範，留待業者自律	業者近年持續推動事實查核、標示不實訊息等相關機制
加拿大	未有特別措施	加拿大文化遺產部「數位公民貢獻計劃」為數家民間組織提供資金，開發識別網路假消息之工具，其中亦包含來自外國政府假訊息之應對工具
澳洲	刻正討論《2023 年通訊法（就打擊不實與錯誤訊息）修正案》，預計賦予 ACMA 對平臺之監理權力，擴大監督非簽署方之網路業者	DIGI 透過《澳洲不實與錯誤訊息實踐準則》，要求簽署方承諾處理其服務上之不實及錯誤訊息
紐西蘭	《有害數位通訊傳播法》之通訊守則要求：數位通訊不得捏造不實指控，且接獲相關申訴時將由 Netsafe 協助處理	《紐西蘭線上安全及危害行為準則》要求簽署方承諾錯誤訊息與不實訊息之傳散，且應提供用戶減輕風險危害之保護措施
日本	未有特別規範，目前政策討論之結果仍傾向業者自律	業者近年持續推動事實查核、標示不實訊息、媒體識讀教育等機制
韓國	《輿論仲裁暨被害救濟等相關法》設有論仲裁委員會，提供救濟管道	➢ 韓國記者協會設有相關規範，得針對記者的不實報導、違法行為進行懲戒 ➢ 平臺業者共同成立之 KISO 設有不實訊息檢舉機制
新加坡	➢《線上虛假內容與操控防止法》 ➢《外國干預反制法》	透過國家圖書委員會之 S.U.R.E.計畫進行媒體識讀公共教育

資料來源：本研究自行整理

表 13：研究國別就兒少網路安全之處理模式

兒少網路安全		
	政府機關法制政策作為	**第三方監督或產業自律機制**
歐盟	《數位服務法》設有共通性之違法內容移除機制，並課予線上平臺義務，就未成年人之隱私、安全保障、資料處理等提供高規格防護措施	未有特別措施
德國	➢ NetzDG 設有違法內容移除機制，具體而言，涉及刑法散布、販賣與持有兒童色情刊物罪之內容有適用可能 ➢ NetzDG 廢止後，將透過內國法之革新介接歐盟《數位服務法》	FSM 作為目前唯一「受認可的受管制之自我管制機構」，可依 NetzDG 審理部分案件
法國	➢《第 2020-936 號家暴受害者保護法》授權主管機關，得要求在網路上散播色情內容者採取防範未成年者接觸的措施。 ➢《設定數位成年人與打擊網路仇恨法》要求線上社群網路服務提供者不得為 15 歲以下的未成年人提供註冊服務，除非其法定代理權之持有者授權	未有特別措施
英國	《線上安全法》針對兒童性剝削與虐待之違法內容、對兒少有害內容等課予服務提供者予以安全管理、受理使用者通知、風險評估及處理等義務	透過網路觀察基金會、西南學習網與兒童網等公益組織組成之「英國網路安全中心」提供協力及通報機制
美國	未有特別規範	未有特別措施

加拿大	➢《網際網路服務提供者強制通報兒少色情內容法》 ➢《網際網路兒少色情通報規則》 ➢刻正審議之「C-36」法案，擬課予數位平臺受理舉報並取下有害內容之責任	加拿大兒童保護中心之「蜘蛛網計畫」透過自動化爬蟲程式主動搜尋網路上公開的兒少性虐待內容，並將偵測到的圖像或影片進行分類，進而向世界各地的資訊儲存服務業者發布移除請求
澳洲	《線上安全法》所規範之線上違法內容亦包含未成年網路霸凌內容，電子安全專員於收到申訴後將啟動調查，並發布通知要求業者移除等處置	未有特別措施
紐西蘭	透過內政部「數位安全小組」處理網路危害之兒童性剝削議題	《紐西蘭線上安全及危害行為準則》要求簽署方承諾減少兒童性剝削與性虐待內容之傳散，且應提供用戶減輕風險危害之保護措施
日本	《青少年網際網路環境整備法》要求 IASP 業者應提供過濾青少年有害內容之服務，並作為家長為青少年申辦行動門號時之參考依據。	未有特別措施
韓國	➢《資通訊網路法》、《資通訊審議規定》設有違法內容移除機制 ➢《兒童暨青少年性保護相關法》 ➢《性暴力犯罪處罰特別法》 ➢兒童暨青少年個人資訊保護基本計畫 ➢2023 年起試行兒童暨青少年之數位遺忘權	平臺業者共同成立之韓國網路自律政策機構」（KISO）

新加坡	➢《線上安全（其他修正）法》針對涉及自殘或性暴力、描繪兒童性剝削等行為之內容設有阻斷機制 ➢《線上刑事犯罪危害法》針對涉及性相關犯罪、詐騙和惡意網路活動、煽動暴力等行為之內容設有阻斷機制	未有特別措施

資料來源：本研究自行整理

表 14：研究國別就網路交易安全之處理模式

網路交易安全		
	政府機關法制政策作為	**第三方監督或產業自律機制**
歐盟	《數位服務法》設有共通性之違法內容移除機制；針對允許使用者與賣家締結通訊交易契約之線上平臺，亦訂有賣家溯源、使用者介面設計要求、賦予使用者對於違法商品知悉權等特別措施	未有特別措施
德國	未有特別規範；刻正透過內國法革新介接歐盟《數位服務法》	未有特別措施
法國	第 2023-451 號《規範商業影響力並打擊社群網路中具影響者之濫用行為之法律》規定，社群網路影響者必須以清晰、易讀或可識別的方式在宣傳圖像或影像上出現，並在促銷過程中標示「廣告」或「商業合作」。	未有特別措施
英國	➢《線上安全法》附表 7 將涉及詐欺、金融服務、槍枝或其他武器等犯罪行為列為違法內容態樣之一，並課予服務提供者予以安全管理、受理使用者通知及處理、風險評估等義務 ➢《線上安全法》針對特定服務提供者設有處理廣告詐騙之累加義務	內政部提出防詐策略（Fraud Strategy），透過公私協力建構防詐生態圈
美國	未有特別規範	未有特別措施
加拿大	未有特別規範	未有特別措施
澳洲	未有特別規範	未有特別措施
紐西蘭	未有特別規範	未有特別措施
日本	未有特別規範	未有特別措施
韓國	未有特別規範	2022 年啟動官民合作之「平臺民間自律機構」，廣泛討論業者之自律規範，內容涵蓋快速因應消費者受害之措施等

新加坡	➢《線上刑事犯罪危害法》針對涉及詐騙等行為之內容設有阻斷機制	未有特別措施

資料來源：本研究自行整理

表 15：研究國別就網路霸凌之處理模式

網路霸凌		
	政府機關法制政策作為	**第三方監督或產業自律機制**
歐盟	《數位服務法》設有共通性之違法內容移除機制	《打擊線上仇恨言論行為準則》
德國	➢ NetzDG 設有違法內容移除機制，具體而言，涉及刑法公然侮辱罪、意圖誹謗罪、妨礙隱私秘密罪等行為之內容皆有適用可能 ➢ NetzDG 廢止後，將透過內國法之革新介接歐盟《數位服務法》	除配合歐盟機制外，FSM 作為目前唯一「受認可的受管制之自我管制機構」，可依 NetzDG 審理部分案件
法國	《2022 年 3 月 2 日第 2022-299 號對抗校園霸凌法》針對「透過反覆發表評論或行為來騷擾他人，其目的或效果是惡化被騷掃擾者之生活條件，從而導致其身心健康發生變化」之行為設有處罰。	除配合歐盟機制外，未有特別措施
英國	《線上安全法》附表 7 將涉及恐嚇、騷擾、跟追、性影像等犯罪行為列為違法內容態樣之一，並課予服務提供者予以安全管理、受理使用者通知及處理、風險評估等義務	透過網路觀察基金會、西南學習網與兒童網等公益組織組成之「英國網路安全中心」提供協力及通報機制
美國	未有特別規範	未有特別措施
加拿大	未有特別規範	未有特別措施
澳洲	《線上安全法》規範之線上違法內容亦包含成年網路暴力內容。電子安全專員於收到相關申訴後將啟動調查，並發布通知要求業者移除等處置	未有特別措施

紐西蘭	《有害數位通訊傳播法》提供受害者快速且有效之補救措施，以減少線上霸凌、數位騷擾、色情報復或其他形式之虐待與恐嚇之影響	《紐西蘭線上安全及危害行為準則》要求簽署方承諾減少網路霸凌或騷擾內容之傳散，且應提供用戶減輕風險危害之保護措施
日本	➢《霸凌防止對策推動法》僅適用於兒童霸凌事件 ➢針對是否應設立移除誹謗、侮辱等內容之規範，目前政策討論結果仍傾向業者自律	未有特別措施
韓國	《資通訊網路法》、《資通訊審議規定》設有違法內容移除機制	平臺業者共同成立之 KISO 訂有仇恨言論自律政策指引等
新加坡	➢《線上安全（其他修正）法》針對涉及歧視、族群仇恨等行為之內容設有阻斷機制 ➢《線上刑事犯罪危害法》針對涉及惡意網路活動、煽動暴力等行為之內容設有阻斷機制	未有特別措施

資料來源：本研究自行整理

表 16：研究國別就使用者權益之處理模式

使用者權益		
	政府機關法制政策作為	第三方監督或產業自律機制
歐盟	《數位服務法》課予服務提供者之各項義務： ➢ 所有網路中介服務提供者皆應提交透明度報告 ➢ 資訊儲存服務提供者應建立「通知即行動」機制 ➢ 線上平臺服務提供者應建立內部及外部權利救濟機制、禁止透過暗黑模式誘導使用者、確保線上廣告透明性等	未有特別措施
德國	➢ NetzDG 課予電子媒體建立申訴窗口、處理違法內容、提供異議機制之義務 ➢ NetzDG 廢止後，將透過內國法之革新介接歐盟《數位服務法》	NetzDG 於特定類型案件委由 FSM 外審之機制，可提供使用者程序保障
法國	刻正審議《數位空間規範與安全法》草案，預計授權設立反詐騙網路安全過濾器，保護使用者免受欺詐性調閱個人資訊或用於惡意目的之金融機構資訊。	經濟部訂有《內容影響者與作者之良好指引指南》
英國	《線上安全法》課予服務提供者建置申訴機制、風險評估、繳交透明度報告等義務	透過《線上安全法》課予第 1 類服務之提供者，就使用者賦權負有疊加義務
美國	未有特別規範	未有特別措施
加拿大	未有特別規範	未有特別措施
澳洲	《線上安全法》設有申訴處理機制，由民眾或受害者向電子安全專員進行線上違法內容之申訴，並由電子安全專員展開	《澳洲不實與錯誤訊息實踐準則》要求簽署方承諾賦予用戶資訊來源的知情權，令使用者更加了解內容來源與提供替代選擇

	調查，再做出處置決定	
紐西蘭	《有害數位通訊傳播法》規定，當 Netsafe 通知社群平臺移除未果時，被害人得於向 Netsafe 取得事件摘要後自行向法院起訴移除或阻斷	《紐西蘭線上安全及危害行為準則》要求簽署方承諾賦予使用者更多控制權，提昇其做成選擇前之知悉權
日本	《服務提供者責任限制法》設有發訊人資訊揭露程序，以供使用者權利救濟	未有特別措施
韓國	2023 年起試行兒童暨青少年之數位遺忘權	2022 年啟動民合作之「平臺民間自律機構」，廣泛討論業者之自律規範，內容涵蓋提昇平臺透明性之措施等
新加坡	未有特別規範	未有特別措施

資料來源：本研究自行整理

第三章　我國網際網路傳播社會問題盤點

為盤點我國網際網路傳播所面臨之主要社會問題，本章節將試圖透過既有調查及文獻之回顧，配合前述國際研析之所得，作為後續規劃一般大眾電話訪問調查、網路調查等工作項目之基礎。

第一節　我國網際網路相關服務之使用情形

一、網際網路之使用比例及頻率

根據通傳會之「111 年通訊傳播市場報告」[851]，我國 16 歲以上民眾中，有使用網路(包含使用社群媒體或即時通訊等)之比例高達 86.3%，沒有使用網路之比例則為 13.7%。

此外，我國民眾最近 3 個月內使用網路之頻率（不論任何地點）以「至少一天一次」比例高達 91.5%，「不是每天使用，但至少一週一次」為 4.7%，「少於一週一次」則為 2.4%。

另一方面，按財團法人台灣網路資訊中心(TWNIC)所作之「2022 台灣網路報告」[852]，我國 18 歲以上最近三個月有上網經驗的民眾為 84.30%。

We are social 與 KEPIOS 合作調查之「DIGITAL 2023: TAIWAN」[853]報告則指出，我國網路使用人口已於 2022 年達到 2,168 萬，占總人口 90.7%，各項調查報告皆可見網際網路在我國之高度普及，其使用已和民眾之日常生活息息相關。

---

[851] 國家通訊傳播委員會，111 年通訊傳播市場報告（2023/01/16），https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=5023&cate=0&keyword=&is_history=0&pages=0&sn_f=48484 （最後瀏覽日：2023 年 8 月 5 日）。

[852] 財團法人台灣網路資訊中心，2022 台灣網路報告，https://report.twnic.tw/2022/ （最後瀏覽日：2023 年 8 月 5 日）。

[853] DATAREPORTAL, DIGITAL 2022: TAIWAN (2023/02/13), https://datareportal.com/reports/digital-2023-taiwan (last visited July 12, 2023).

二、使用網際網路之主要目的

根據通傳會「111 年通訊傳播市場報告」[854]，我國 16 歲以上民眾最近 3 個月內使用網路所從事的活動，比例最高者為「下載圖片/電影/影片/音樂、玩或下載遊戲」比例最高（26%），其次則依序為「參與社群網路」（23.3%）、「撥打網路語音電話」（18.9%）、「觀賞網路電視」（17.5%）、「購買或預訂商品或服務」（14.6%）、「造訪聊天網站、部落格、新聞群組或線上討論」（12.3%）、「使用線上儲存空間存放文件/照片/音樂/影片或其他檔案」（11.1%）、「查詢維基百科、線上百科或學習為目的之網站」（10.8%）、「發送或接收電子郵件」（10.4%）等，其餘活動皆低於 1 成。

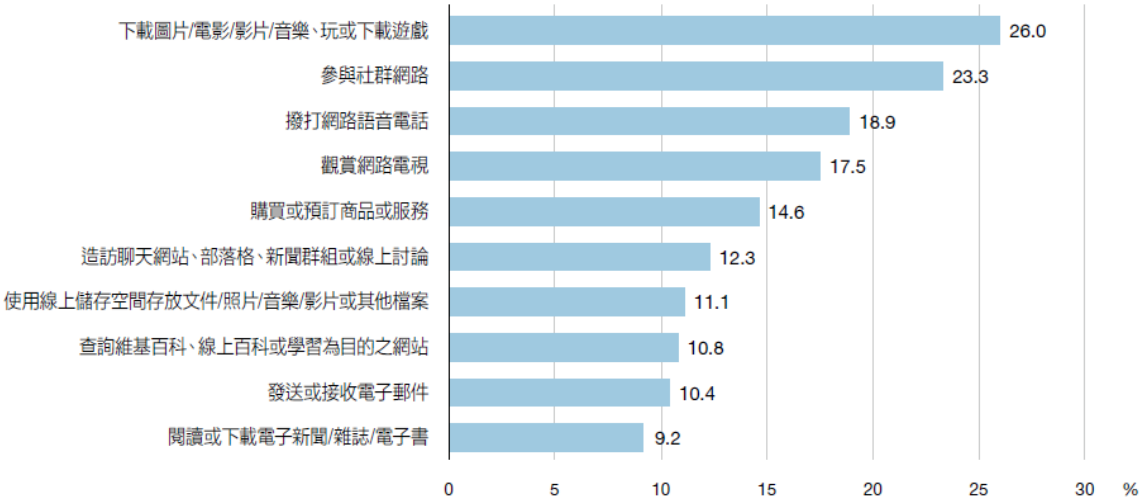


圖3.2.17　民眾最近3個月內使用網路所從事的活動（前十名）
Base：N=1,129，複選（有使用網路者）

圖 25：我國 16 歲以上民眾最近 3 個月內使用網路所從事之活動前十名

資料來源：通傳會[855]

而根據「DIGITAL 2023: TAIWAN」之調查，我國民眾使用網路之主要目的則以「尋找資訊」（61.8%）最高，其次依序為「與親友聯繫」（59.5%）、「觀賞影片、電視劇及電影」（58.5%）、「打發閒暇時間及廣泛瀏覽」（55.1%）、「追蹤新聞與近期事件」（52.9%）、「存取及聆聽音樂」（43.4%）、「財務管理」（42.9%）、「搜尋各種事情的做法」

854 同前註 851。
855 同上註。

（41.3%）、「尋找度假及旅遊景點」（41.2%）、「尋找新構想及靈感」（39.1%）、「遊戲」（38.3%）、「搜尋健康資訊及產品」（37.6%）、「教育及學習相關之活動」（35.9%）、「日常生活規劃」（34.1%），以及「搜尋產品及品牌」（29.9%）[856]。

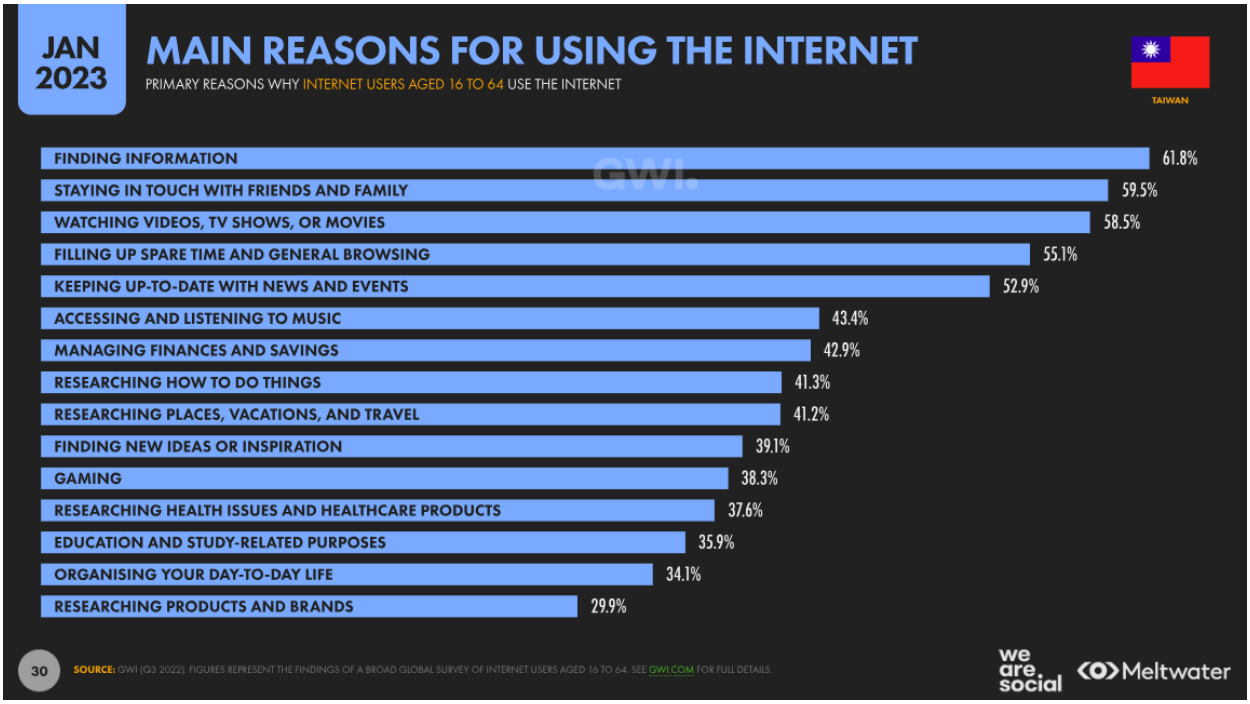


圖 26：我國民眾使用網路之主要目的

資料來源：We are social、KEPIOS[857]

另一方面，按 TWNIC「2022 台灣網路報告」之網路應用服務使用情形調查，我國民眾使用網路應用服務則以「觀看免費網路影音」為最大宗（72.82%），其次則依序為「買東西」（51.30%）、「線上遊戲」（35.76%）、「行動支付」（34.27%）、「餐飲外送服務」（29.70%）、「線上學習」（29.24%）、「觀看付費影音」（26.91%）、「閱讀電子書」（23.56%）、「賣東西」（8.37%）、「線上交友」（7.47%）、「加密貨幣」（2.01%）[858]。

856 同前註 853。

857 同上註。

858 同前註 852。

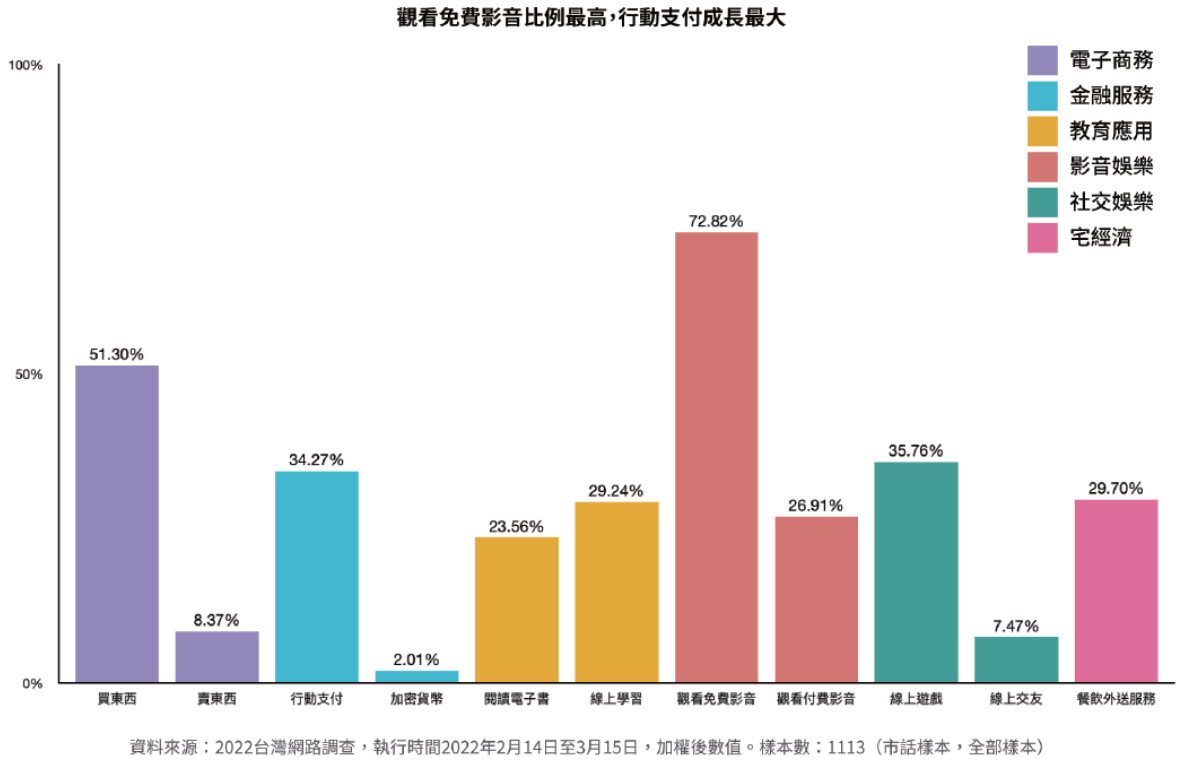


圖 27：我國民眾使用網路應用服務情形

資料來源：TWNIC[859]

整體而言，我國民眾使用網路之主要目的，概以「遊戲或影音娛樂」、「社群人際互動」、「獲取新聞或資訊」、「交易或支付」為重。

859 同上註。

三、最常造訪網站

根據「DIGITAL 2023: TAIWAN」之調查，以 2021 年 12 月至 2022 年 11 月之網站總流量計算，我國民眾最常造訪之網站為 Google.com，平均月流量高達 9.07 億次，其次則為 YouTube（4.39 億次）、Facebook（2.53 億次）、Yahoo.com（2.02 億次）、聯合新聞網（UDN.com，9,770 萬次）、Google.com.tw（9,510 萬次）、Yahoo!News（news.yahoo.com，9,330 萬次）、ETtoday 新聞雲（8,010 萬次）、維基百科（7,070 萬次），以及蝦皮（shopee.tw，6780 萬次）[860]。

而在使用社群平臺與通訊軟體方面，我國民眾高達 89.4%有使用社群平臺與通訊軟體的習慣，其中最常使用的平臺依序則為：LINE（90.7%）、Facebook（85.3%）、Instagram（65.3%）、Facebook Messenger（60.3%）、TikTok（36.0%）、Twitter（33.3%）、WeChat（24.2%）、iMessage（19.5%）、Skype（16.1%）、Telegram（15.7%）、WhatsAPP（15.5%）、LinkedIn（13.4%）、Pinterest（12.9%）、Discord（9.1%），以及 Reddit（7.4%）[861]。

值得一提的是，若進一步按使用者的年齡層細分，根據 TWNIC 的「2022 台灣網路報告」，我國 18 歲至 29 歲民眾使用臉書的比例為 35.89%，40 歲至 49 歲民眾使用臉書的比例則為 78.65%；相較之下，18 歲至 29 歲民眾使用 Instagram 的比例為 55.28%，40 歲至 49 歲民眾使用 Instagram 的比例則為 4.98%，兩者的主力使用者分佈呈現相反的情況，亦顯示了年輕族群近年從 Facebook 轉移至 Instagram 的傾向[862]。

至於台灣人使用社群平臺的原因，據「DIGITAL 2023: TAIWAN」之調查，前五名分別為：與親友保持聯繫（52.5%）、消磨空閒時間（46.1%）、看看大家都在談論些什麼（33.4%）、探索影片等內容（32.7%），以及閱讀新聞時事（25.8%）[863]。

---

[860] 同前註 853。
[861] 同上註。
[862] 同前註 852。
[863] 同前註 853。

四、最常搜尋關鍵字

根據「DIGITAL 2023: TAIWAN」之調查，2022 年 1 月 1 日至 2022 年 12 月 31 日間，我國民眾在 Google 搜尋的前 20 名關鍵字包括天氣、確診、疫苗、匯率等時事；平臺如 PTT、Google、YouTube、FB、Dcard、IG、LINE 等[864]。

而若觀察 Google Trends，2023 年[865]我國快速竄升之新聞議題有：颱風、ChatGPT、世界棒球經典賽、6,000 全民共享普發現金、iPhone 15、以色列、藍白合、亞洲運動會棒球比賽、國際足總女子世界盃、土耳其地震。快速竄升商品「推薦」關鍵字有：旅遊不便險、信用卡、筆電、旅平險、日本網卡、機場接送、中秋禮盒、手機、豬腳、日本租車；快速竄升人物（不含已故人物）則有：黃子佼、炎亞綸、BLACKPINK、賴佩霞、劉文正、NONO、張育成、黃仁勳、大谷翔平、郭台銘[866]。

---

[864] 同上註。

[865] 參考 2022 年快速竄升之議題（不包括單一人物相關）有：烏克蘭、地震、疫情、世足賽、iPhone 14、停電、柬埔寨、國旅補助、動滋券、梨泰院。快速竄升商品「推薦」關鍵字有：血氧機、烘衣機、泳衣、雨衣、防疫險、口罩、發泡錠、雨鞋；快速竄升人物（不包括已故人物）則有：林志穎、裴洛西、林智堅、大 S、高虹安、美輪明宏、具俊曄、強尼戴普、周玉蔻、ØZI。詳見，Google Trends，2022 年度搜尋排行榜—台灣，https://trends.google.com.tw/trends/yis/2022/TW/?hl=zh-TW（最後瀏覽日：2023 年 1 月 13 日）。

[866] Google Trends，2023 年度搜尋排行榜—台灣，https://trends.google.com/trends/yis/2023/TW/?hl=zh-TW（最後瀏覽日：2023 年 1 月 13 日）。

第二節　我國網際網路相關服務之主要問題盤點

根據通傳會「111 年通訊傳播市場報告」，我國 16 歲以上民眾中有 32.5%並沒有對於網路使用的顧慮；顧慮最高者則為「個資外洩／個資被盜用」（16.4%），其次依序為「網路詐騙」（12.5%）、「過多或不適當的廣告銷售」（10.3%）、電腦中毒／駭客入侵（8.9%）、垃圾郵件或釣魚郵件（8.8%）、充斥假新聞或錯誤引導之資訊（7.9%）、兒童接觸到不適宜內容或陌生人（3.7%）[867]。

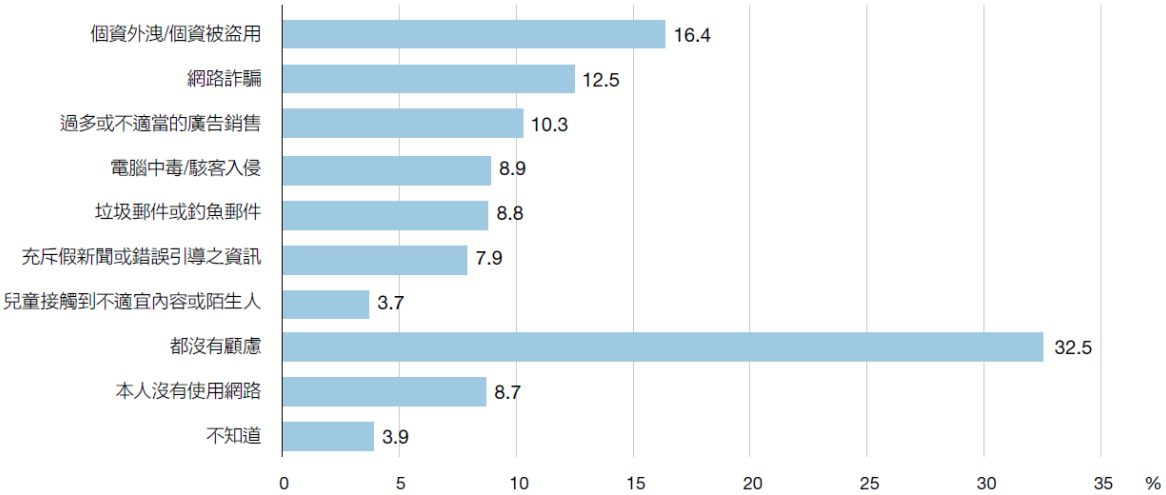


圖3.2.21　使用網路的顧慮（前十名）
Base：N=1,309，複選

圖 28：我國民眾使用網路的顧慮前十名

資料來源：通傳會[868]

除了兒童透過網路接觸到不適宜內容的問題外，網路霸凌亦可能對兒少造成傷害。根據兒童福利聯盟「2021 台灣兒少網路社交焦慮與網路霸凌經驗調查報告」之調查，有超過兩成的兒少曾有遭到網路霸凌的經驗，且有 26.0%的受害者曾經想傷害自己。但在實際遭遇網路霸凌的受害者之中，卻僅有 22.4%會向老師或家長報告，39.8%則只願意向信任的同儕透露。除此之外，調查亦發現有 62.5%的兒少出現疑似「網路社交焦慮」的狀況，網路社交的壓力已是當代社會下不得

867 同前註 851。
868 同上註。

不面對的隱憂[869]。

針對網際網路上的意見交流，TWNIC 的「2022 台灣網路報告」也發現，認為網路上政治相關留言彼此對立之我國民眾高達 40.18%，認為非常對立者亦有 37.47%。此外，多數民眾也認為即時通訊中存在著迴避不同意見的「同溫層」傾向。針對在即時通訊中的公共討論，有 29.09%的民眾只會看到與自己立場大部分相同或完全相同的意見，顯示了此一資訊接收管道存在著「極化」與不實訊息難以消弭的風險。此外，當民眾看到與自己立場不同的意見時，有 78.85%會選擇迴避不予理會，僅 6.83%會選擇正面回覆，此一現象亦與民主社會對於立場不同者相互對話之期待有所落差[870]。

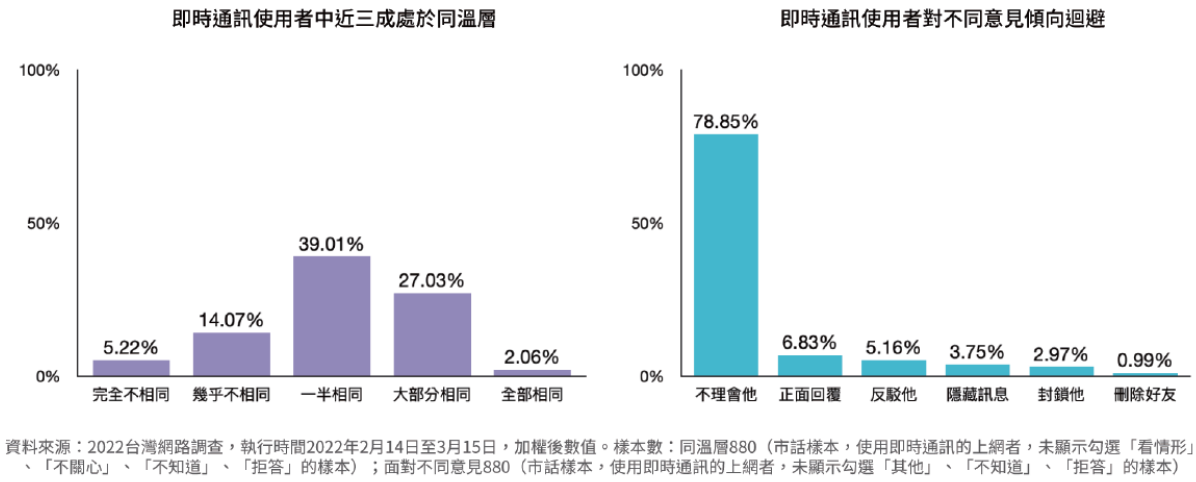


圖 29：我國民眾使用即時通訊軟體時接觸不同意見之情況

資料來源：TWNIC[871]

整體而言，目前我國相關調查所呈現之網際網路相關服務主要問題，或可從「政治不實訊息」、「兒少網路安全」、「網路交易安全」、「網路霸凌」及「使用者權益侵害」五大面向切入，本研究之「我國網際網路傳播社會問題調查」亦將以此作為調查之核心。

---

869 兒童福利聯盟，2021 台灣兒少網路社交焦慮與網路霸凌經驗調查報告(2021/10)，https://www.children.org.tw/publication_research/research_report/2267 （最後瀏覽日：2023 年 8 月 1 日）。

870 同前註 852。

871 同上註。

一、網際網路社會問題過去相關研究分析

本次研究期望能了解目前民眾對於各種網路問題之處理方式與成效有何看法，同時了解未來的公共問責模式與管制網路危害的手段與方法可朝何處前進，因此調查國內外相關網際網路社會問題之研究，以網際網路社會危害、網路政治不實訊息、網路假訊息、網路交易、兒童與少年網路安全、兒童少年網路性剝削、網路霸凌、數位匯流等作為關鍵字，查閱文獻期間為 2010 年至 2023 年間，範圍包含三篇期刊論文及學報、三篇政府研究報告及一篇碩博士論文等，以求能夠研調過往相關資料，參考前人之智慧，並針對現況提出適宜之政策與法制建議。

過往的研究報告大致整理了現狀下的網路危害，包括大數據及演算法資料蒐集問題、個人隱私安全、網路霸凌、不實訊息傳遞、網路交易安全等。本研究案依據這些觀察，大致將網路危害劃分成五大類別，分別為：政治不實訊息、兒少網路安全、網路霸凌、網路交易安全、個人權益侵害。透過過往研究之分析，可發現：

- **現狀下的法規都略有缺失，有待相關單位建立一套更完整的機制，且過往研究案所提出的政策建議範圍較廣泛，但缺乏具體可行的策略建議。**

109 年「因應數位通訊傳播服務發展之規管趨勢與法制革新研析委託研究採購案」指出，現狀下針對「不實訊息」的法規，雖曾提出包含廣電相關等多部法規修正草案，並調修部分法規範，但欠缺系統性整合，且此類法規之構成要件具相當程度之不明確性，判準需要再更加明確。此外，針對「網路霸凌」，雖網路場域中之霸凌行為解釋上亦受到拘束與裁罰，但當前法規仍有待建立一套阻斷傷害之機制[872]。

110 年「數位科技應用發展暨我國匯流法制革新規劃研究委託研究採購案」則指出，針對網路平臺所應負擔的責任與免責標準，可建

[872] 參見王牧寰、徐偉群、陳志宇、鄭嘉逸等，因應數位通訊傳播服務發展之規管趨勢與法制革新研析，國家通訊傳播委員會委託研究成果報告（2021）。

立共通性的平臺問責規範，建立統一的平臺免責標準與程序，提高法律安定性。前述研究案亦針對當時通傳匯流法案提出修法建議，如課予數位通訊傳播中介服務義務規範，或可建立暫時加註警語等警示、應建立使用者救濟機制等對網路平臺課責的相關建議[873]。

另有研究指出，現行網路避風港規則需要被調整和改造，網路內容分享平臺業者尤其是大型、強勢者應當被法律課與一定程度上的主動審查義務或適用較高注意義務。在網路著作權部分，可嘗試透過平臺自治的方式達成與權利人的合作共贏，一同打擊網路著作權侵權行為[874]。

而在兒少網路安全方面，則有研究指出，政府應加強對不法行為的懲罰與數位網路安全的管控，且遏阻網路性暴力犯罪還是需要透過網絡的跨科際合作[875]。

整體而論，上述研究案都點出了現行法規缺少系統性的整合機制，且建議應當加強平臺問責規範或是不法行為的懲罰與網路安全管控，但對於該如何建立這樣的系統性整合機制、且連結平臺問責與不法行為的懲治，並未提出一套具有可行性的建議架構。換言之，具體的解決策略尚未成形。

- **部分研究提及公私協力對於網際網路危害的管制方式與影響層面，但並無詳細針對公私協力之運作模式深入探討。**

在「110 年數位科技應用發展暨我匯流法制革新規劃研究」報告中，針對公私協力合作部分已開始有所著墨，研究了各國有公私合作的案例，並指出政府可建立共同資料庫以促進資源的最大利用。「111 年因應國際數位匯流發展趨勢之法制研究」報告中更大幅度的研究了各國的相關公私協力合作案例。例如英國與獨立的非營利組織「英國電影分級基金會」（British Board of Film Classification, BBFC）合作，

[873] 參見同前註 116。

[874] 參見杜綺晴，網路內容分享平台業者之著作權間接侵權責任—以避風港規則與主動審查義務為中心—，國立臺灣大學法律學研究所碩士論文（2022）。

[875] 廖美蓮，網路性誘拐－兒少影像性剝削實務挑戰，當代社會工作學刊，第 11 期，頁 35-80（2021）。

由非營利組織擔任線上色情年齡驗證之監理機構，由政府賦予該非營利組織發出通知要求封鎖網站的權限。又如法國修法明定各種網路平臺「與公權力合作之義務」[876]。

上開這些案例對於我國網際網路在公私協力上的合作都是良好的參考例子。然，現狀下對於網際網路的公私協力共管機制要如何應用於台灣？民間團體或個人應該扮演何種角色？等問題卻暫時無深入研究。而近幾年來公私協力在台灣愈發成為一合作趨勢，若能透過多方合作來遏止網路危害的發生，對民眾、平臺業者、政府來說也是一大利處。

1. 過往研究案多將責任主體歸責於政府

目前，該如何控管網際網路所產生的危害仍是一個嶄新的議題，各國也正在設立相關的法規去控管這些網路危害，以減少憾事發生。也因此，過往研究案多著墨在政府應該負起什麼責任，又應採取何種行動，如法規面向的建立、設立專責機構等。對於其他主體可採取的相關動作的研究較為稀少，多為促使平臺業者提供透明度報告，或促使其建立自律規範，但對當中的描述則略為稀少。

然而網路社會問題的利害關係人不只政府，若要其他利害關係人配合政府政策，必須瞭解他們的需要、角色與責任。而是故，本研究以宏觀的角度觀察，提出較為完整的網際網路參與活動者關係網絡，並賦予當中的每一位角色一種責任，希望在網際網路的活動中，各方角色可以完善自己應擁有的責任，以期建立一個健康的網路世界。同時，本研究亦認為政府與網路平臺業者作為國家的主體與網路服務的提供者，兩者應主動承擔起較大的責任，並共同合作以面對現今的網路危害。

[876] 同前註 117，頁 161。

二、現有網路社會問題協力機制

（一）公私協力

所謂公私協力，乃是一種跨部門公私組織之間協力式網路關係（collaborative networks）的合作，且這種關係必須注重彼此間的平等互惠關係、協力過程、信任與社會資本[877]。

公私協力能夠成功實行，學者 Trafford 與 Proctor 指出，公私協力成功運作的關鍵因素如下[878]：

1. 規劃：公私協力關係中，雙方應於規劃階段擬訂策略，以確定合夥關係之型態，並以動態觀點引導合夥關係之演進。在此階段，或是簽定契約時，應明確規範各參與者的權利義務與獎懲，防止於執行時因契約不明確而造成各有所本，造成衝突。

2. 開放性：資訊、行為之開放性是建立信任關係的首要之務，唯有在協力過程，參與者具備責任分擔、權利共享之態度，才有互動基礎，在此開放的狀態下，參與者間才能處於相同立足點，避免資訊不對稱的可能。

3. 協調：各組織本身擁有獨特的組織文化與精神，其特有價值觀有時亦會導致合作雙方對立，從而影響公私協力之運作；因此如何協調各參與者，使其暫時放下其自身價值觀，共同為目標努力，是公私協力能否成功之關鍵因素。

4. 領導：基於組織文化不同，再加上政府內各單位常有之本位主義思考，因此領導者如何統合所有參與者，使之能互相合作、妥協，是其領導要務。領導者於協力過程中，應確立目標、建立願景，讓成員能為達成目標而努力。

5. 溝通：良好的溝通能促進參與者間資訊之交換，以減少資訊

---

877 陳敦源、張世杰，公私協力夥伴關係的弔詭，文官制度，第 2 卷第 3 期，頁 17-71（2010）。

878 Sue Trafford & Tony Proctor, *Successful Joint Venture Partnerships: Public-Private Partnerships*, 19 (2) INTERNATIONAL JOURNAL OF PUBLIC SECTOR 117-129 (2006).

不對稱之情形，亦能加強彼此之信任感、互信之夥伴關係，更可培養共享目的與認知。對於良好之溝通，學者JHabermas 認為應建立在可理解性、真實性、真誠性及正當性之基礎上。

曾冠球教授則藉由「臺北市民生活網公私合營專案」的個案研究，闡述原先合作夥伴何以最終淪為「不情願夥伴」，該個案欠缺五大成功關鍵因素[879]：

1. 規劃：廠商與市府在建立合作關係時，雙方沒有明確的契約，導致執行時出現誤解和衝突。市府對於廠商的營運計畫書存在審核機制，但若廠商的計畫不被接受，導致廠商投入的成本無法回收。

2. 開放性：廠商與市府之間的互動基礎並不穩固，存在許多資訊不對稱的情況。市府與廠商的溝通機制不完善，導致彼此之間的信任感下降。

3. 協調：市府與廠商的合作中，因為各自有不同的目標和價值觀，難以達到共同努力的狀態。市府在維護自身利益的同時，對廠商的行為有所干預，使得合作雙方的關係受到影響。

4. 領導：市府在合作中未能有效地統合所有參與者，導致合作夥伴感到被忽略或被當作外部承包商。市府在面對政治風險時，未能有效地平衡各方利益，使得合作方感到不安。

5. 溝通：市府與廠商之間的溝通機制存在不足，導致雙方在執行合作時出現誤解和衝突。廠商在為了避免不必要的政治風險，選擇回避市府的正式審查機制，進而選擇發展最基本的功能，而非提供更多的加值服務。

[879] 曾冠球，為什麼淪為不情願夥伴?—公私夥伴關係失靈個案的制度解釋，臺灣民主季刊，第8卷第4期，頁83-133（2011）。

綜上所述，該事件中的公私協力關係受到多方面的影響，其中包括缺乏明確的規劃、開放性不足、協調困難、領導不當、以及溝通不足等因素，導致合作的結果與原始預期有所偏差。

公私協力已成為當前政府運作的趨勢，因此，政府在公私協力時，應設法注意並具備上述五項關鍵因素，使公私協力的運作達到最大的功效。

（二）iWIN（網路內容防護機構）

iWIN（網路內容防護機構）是我國為應對危害兒童網路安全問題而推動的重要機構。在 2013 年 8 月由行政院依據《兒童及少年福利與權益保障法》第 46 條召集各部會委託「民間」所成立的機構。任務在於維護兒少網路安全環境、推動業者自律、宣導網路正確觀念、以此來監督網路是否出現違反《兒童及少年福利與權益保障法》的不當內容。以下將會著重於介紹 iWIN 的防護例示框架以及 iWIN 與政府及平臺業者之間是如何協力進行。

首先 iWIN 的防護例示框架是其運作的核心。該框架將各種危害大致分為，「色情」、「暴力」、「血腥」、「恐怖」、「有害物品」及「不當內容」六大種類，針對各類型再向下細分項目與呈現類型，並提供以下建議防護措施供業者參考[880]：

- **禁止出現/通知下架：**對於線上不得散布或傳輸之內容，平臺或內容提供業者除在使用者規範載明外，一經發現或檢舉後應於一定時限內自行或要求內容提供者修正或移除內容。
- **年齡驗證：**若線上內容有害兒少身心健康且其情節嚴重者，應採行可驗證年齡身分之會員制或其他安全措施以限制兒少閱聽。
- **阻攔機制：**針對線上內容有害兒少身心健康未達嚴重之程度，每次閱聽前至少提供一次明確阻攔措施，避免兒少接取

[880] 劉昱均，網路治理環境下 Iwin 網路內容防護機制的蛻變與挑戰，NCC NEWS，第 12 卷第 2 期，頁 2（2018）。

或瀏覽，如蓋版過橋頁面或大量空白措施。

- **警示機制**：當線上內容對兒少行為或身心有不良影響之虞，必須至少提供一次內容含兒少不宜之警示。以此讓兒少能夠提前了解並選擇是否閱讀或聽取這些內容，如於內容、標題上加註警語或非蓋版式小視窗過橋等措施。

對於未制定自律機制的網路平臺業者，iWIN 提供防護例示框架作為參考，協助他們制定平臺自律規範，並提出了相關自律準則，包含訂定使用者服務規範、制定平臺內部內容提供規範、提供防護機制、建立申訴管道、提供管道做為機關連繫窗口。同時，iWIN 也提供技術上可行的相應防護措施及申訴處理機制。而一般的網路使用者也能參考 iWIN 的例示框架，檢視內容並在散布或傳送內容前，根據建議採取相應的防護措施，或者配合平臺提供的防護措施。當違反相關規範時，應配合平臺或防護機構之要求進行內容防護或移除[881]。

目前，iWIN 與各利害關係人之間的合作模式主要包括「轉知」和「轉案」兩種機制。在「轉知」方面，當涉及情狀輕微或法律灰色地帶的案件時，iWIN 會先行通知相關業者進行處理。業者自律處理完畢後，需定期提供相關案件清單給相關權責機關。如果權責機關仍認為 iWIN 的處理有問題，可依職權開啟調查並進行裁處；而「轉案」則是針對明確、重大違反法令，或是 iWIN 通知業者處理但業者未有效處理的案件。在這種情況下，iWIN 會立即將案件轉交給相應的權責機關，由權責機關自行進行調查和裁處。簡言之 iWIN 團隊會先了解民眾申訴的訴求及平臺內容是否真的有違反相關法令，如有明確重大違法事宜，iWIN 才會直接轉由各目的事業主管機關進行裁處；若非明確重大違法事宜，iWIN 會先試與平臺業者溝通，並由平臺業者進行相對應的防護措施或內容修正，如持續未有改善，iWIN 才會轉由各目的事業主管機關進行裁處[882]。

[881] 同上註，頁 2-3。
[882] 同上註，頁 5。

表 17：iWIN 申訴機制

iWIN 申訴機制	
未違反例示框架	協助轉知業者知悉。
涉及違反例示框架或相關權責法令	轉業者自律改善，若業者無改善或有改善但仍有反例示框架之虞則交由轉權責機關依法處理。
重大或明確違法無自律空間案件	轉業者處理改善的同時也交由轉權責機關依法處理。

資料來源：本研究自行整理

除此之外，iWIN 針對不同的事件有不同的處理機制，例如：當 iWIN 發現有違反性剝削犯罪嫌疑案件時會先向平臺業者通知，並請求授權 iWIN 協助通報警政單位，網路業者則會經通知後刪除違法訊息，並保存相關證據 90 日，待警政單位調閱。若是兒少性剝削案件會在知悉後內透過 E-Mail 通報地方警政單位，並在一週內補公文。而網路媒介色情案件則會每月彙整定期提供至地方警政單位，最後地方警政單位在依照程序調查資料。

iWIN 也擁有其他與各利害關係人之間的合作，例如在 106 年起與 Facebook 建立直接聯繫窗口，包括建立申訴處理管道以及教育訓練，提升案件處理成效，避免兒少不宜接取內容持續擴散。此外，更有網安防護的相關推廣、宣導活動合作，包含 2017 年 2 月初 Facebook 與臺灣 NGO 網路安全交流座談會，4 月合辦網路安全宣導短片記者發表會，11 月合辦亞太兒少網路安全高峰會，透過緊密的合作與交流，逐步讓 iWIN 的守護兒少上網安全的能力拓展到跨國平臺。iWIN 也舉辦多場「多方利害關係人諮詢會議」，邀請了專家學者 12 位、產業代表 11 位、社會團體 9 位以及政府機關 6 位，共 38 位擔任諮詢會議的代表，確保各領域的利害關係人都能參與並貢獻意見，特別是在網路內容治理和兒童少年網路安全保護方面。透過多元的參與和對話來建立一個共識的框架，避免標準制定和執行方向過於單一，開放式的合作模式有助於確保能更有效的應對網路內容治理和兒童網路安

全的挑戰，符合社會各界的期望[883]。

iWIN 是民眾、業者、與政府三者之間的橋樑，需要能夠將民眾的訴求轉達給業者與政府，盡力滿足民眾的合理要求，還必須了解業界的生態；為能使業者達到民眾與政府的期待，並且協助業者與政府之間建立良好的溝通機制及尋找可執行的方式；也協助政府機關將相關法規宣導給民眾及業者，避免民眾與業者在網路上不小心觸犯法規[884]。同時也發現 iWIN 具備了上所提及的協力關鍵因素，例如提供透明度報告，透過將資訊及行為以開放性的方式來建立其信任關係、面對防制網路兒少安全問題與各業者一起朝向共同的目標努力，並且 iWIN 也與政府及業者建立良好的溝通，促進參與者間資訊之交換，減少資訊不對稱之情形，加強彼此之間信任感、最後達成互信之夥伴關係。然而就目前來說 iWIN 對於網路內容的防治還是偏向危害兒童網路安全為主。而現今網際網路的社會問題十分廣泛，不僅僅只是面對兒少安全問題，不實訊息與網路詐騙已漸漸的危害我國社會安全，侵害的範圍也不斷進一步擴大。因此透過 iWIN 的防治仍然不足，我們仍需要建立一套更良善的機制來去解決其他面向的網際網路社會問題。

觀察現今網際網路社會問題，我們可發現網路治理是為一複雜的動態領域，網路社會不僅隨時間而不斷且快速地變化著，也有許多的利害關係人參與其中。考量到網路治理的複雜程度，以下將介紹多層次治理（multi-level governance）之概念，本研究將透過多層次治理的概念來解析網路治理。

（三）多層次治理

多層次治理之概念最早由 Gary Marks 提出，用來分析與解釋歐盟之間複雜的國家互動與治理模式[885]。而隨著全球化的到來，國家的邊界愈趨模糊，不同區域間的互動也愈趨頻繁。在國家內部，中央政

[883] 同上註，頁 3-4。

[884] 同上註，頁 18。

[885] 參見郝培芝，多層次體系下的歐盟治理模式，中國行政評論，第 15 期第 3 卷，頁 89-116（2006）。

府與地方政府的互動也逐漸多元化，國家權力開始逐漸移轉，大致上可分成上移（moving up）、下移（moving down）及外移（moving out）等三種新的治理型態[886]。

所謂上移，是指國家主權和政府權威部分被國際組織所取代；下移則指國家統治權力部分流向地方政府或都市；外移則指國家透過非營利組織、組織民營化等公私協力的治理方式與第三部門共同治理國家[887]。而多層次治理模式主要可分成三個面向，包含：政策整合（連結不同政策領域，使之產生互動連結）、跨域協調（地方政府、都市等不同層次的治理），及公私夥伴治理（公私部門與民間社會）[888]。

多層次治理的概念現如今被廣泛運用在現今的公共管理上，例如府際關係、跨域治理與公私協力等。簡言之，多層次治理提供一個動態的視野，透過多方利害關係人的參與和合作，去協助現今的政府去治理複雜之政策事務與探討各政策間的互動。

以此視角觀之，由於多層次治理將一複雜的治理問題區分成許多區塊與層次，再透過各層（如區域、功能、部門）進行整合，去解析一複雜的治理問題。如有論文探討綠色城市中的多層次治理模式，其認為綠色城市治理中包含多元政策、多方利害關係人與多層級的治理特性[889]。無獨有偶，辛年豐教授亦從多層次治理的角度出發，探討國土計畫中的治理模式。其認為國土計畫將大範圍的政策治理分層討論，分為全國國土計畫、直轄市、縣（市）國土計畫、都會區計畫與鄉村區計畫等，這將有助於減少權力的過度集中，亦可達到民主原則中透明化的要求，同時也能透過地方與地方間的互相溝通與對話來達到夥伴化精神[890]。亦有論文從多層次治理的途徑討論歐盟個人資料保護治理之變遷。其認為由於歐盟的威權機構的管轄權是分散的，因此在同個議題中，不同階層的治理者皆可發揮影響力，這產生了一個動

886 JON PIERRE & B. GUY PETERS, GOVERNANCE, POLITICS AND THE STATE, p.83-91 (2000).

887 劉坤億，政府課責性與公共治理之探討，研考雙月刊，第 33 卷第 5 期，頁 59-72（2009）。

888 李長晏，區域治理與城市區域發展：公安與食安之探索，中國地方自治月刊（2016）。

889 參見張雅婷，綠色經濟與綠色成長－綠色城市多層次治理模式之初探，社會與區域發展學報，第 6 卷第 2 期，頁 131-171（2021）。

890 參見辛年豐，初探國土計畫的多層次治理，全國律師，第 27 卷第 2 期，頁 45-59（2023）。

態的治理過程，也創造了更多不同的機會開啟政策的機會之窗[891]。

綜上所述，多層次治理可為一動態的治理視野，將複雜的大政策大致分成中央與地方、公部門與私部門、相關利害關係人之影響，或是不同政策間的互動等層級討論。而此一互動過程可廣納多元的討論聲音，減少政府權力集中的情況，也有助於大眾了解動態的政策變動過程。

三、現有網路社會問題研究缺口與待解決問題

總結來看，現今網際網路社會問題日趨嚴重，且影響範圍也日漸擴大。網路上充斥著許多政治不實訊息、網路詐騙等訊息，對於兒童與少年來說，許多不適宜的內容也躍現在兒少面前，若沒有一良好管制措施去限制這些有害內容，將會對我國社會造成許多危害，不僅會破壞社會信任，也會造成社會的混亂。

本研究研析過往研究，提出三項發現：首先，現狀下的法規都略有缺失，有待相關單位建立一套更完整的機制，並提出更具體的執行措施。其次，隨著公私協力機制的成功，在控管網際網路社會危害的方向上，相關單位也可以考慮引進公私協力，與私部門共同管制網際網路社會。最後，網際網路社會危害的不應只是政府的責任，而是全體大眾，包含網路平臺、公民團體、一般大眾的責任。尤其身為提供服務的網路平臺，更應主動承擔起控管危害內容的重大責任。

據此，本研究之研究目的，係瞭解我國網際網路相關服務之使用情形及主要問題，並耙梳各研究國別之具體法制或政策措施、公私協力機制，及促進產業自律之作為等通傳匯流法制整備、行政與司法經驗，以為委託單位提供法制革新建議。

針對上述三項發現，本研究案亦將針對我國網際網路法制案進行深入探討，並透過下列方法回答本研究問題：

---

[891] 參見蔡昀知，歐盟個人資料保護治理之變遷：從《資料保護指令》到《一般資料保護規則》，臺灣大學政治學研究所碩士論文（2019）。

- 研究欲了解我國民眾使用網際網路相關服務之情形為何？衍生哪些個人與社會問題？使用者對於網路傳播之社會影響與風險危害有何種程度之認知？對於各種網路問題之處理成效與處理方式又有何看法？故而本研究將透過兩次民意調查，了解我國民眾對於各種網路問題之處理成效與處理方式之看法。（包含：誰應負責？應如何負責、處理網路問題？）。

- 於研究國際間所採取之應對手段與研究國具體而言採取的法制作為，及推行之第三方監督產業組織自律手段後，試探討目前我國提供服務之主要網際網路傳播相關服務，其公共問責模式之運作方式為何？有無公眾或第三方介入協助強化其問責之可行性？並研析公私協力或第三方監督在我國的可行性與運作方式。

- 針對前項所述，本研究擬依據我國網際網路之整體使用情形、重要議題與相關服務之公共問責模式，提出一適宜之政策與法制建議，試擬出一套政府與網路平臺、第三方機構共同管理的公私協力運作模式。

- 有別於過往，多將責任歸屬於政府，此次研究認為網際網路的安全應由政府與網路平臺共同負責。網路平臺作為提供服務與提供一平臺使民眾交易、討論的主體，對該平臺上發生的網路危害也應有所警覺，並在第一時間做出反應，以杜絕後患。而政府除了需要建立、整理法規並進行統合管理外，也需要教育民眾，提高民眾的媒體識讀能力。最後，民眾更需要提升自我察覺網路危害的能力，不能聽信謠言或盲目跟眾。

為能有效回答研究問題，本研究參考現有網路內容防護機制（即 iWIN）之運作方式，並期望能從中獲得經驗。iWIN 作為民眾、業者、與政府之間的橋樑，扮演著網路社會的維護者，近三年（2020 年至 2022 年）來共計處理了 10,565 件案件，有效協助防護了兒少網路社會安全。

根據前一節所述，iWIN 之協力機制扮演的是「中間人」的角色，對外，先行代替政府接受民眾申訴，iWIN 會了解民眾申訴內容，以及確認該網路平臺是否真有違反例示規則，並透過轉知與轉案目的事業主管機關的方式協助處理相關事件。對內，則會代表民眾，與政府、網路平臺業者進行溝通、協商，以建立更完善的例示規則與網路環境。

iWIN 的成立乃是一成功的協力機制，本研究將融合 iWIN 成功的經驗，提出可協助管制網路危害的協力模型機制，該機制中，有政府、網路平臺、使用者與第三方機構的參與，並將以第三方機構作為中心點，協助各利害關係人進行意見整合與溝通，以求能協助管理網路社會危害內容。

第四章　我國網際網路傳播社會問題調查之設計及調查結果

第一節　社會問題調查研究方法

如前所述，目前網路社會所遭遇到的危害問題大致上可分為「政治不實訊息」、「兒少網路安全」、「網路交易安全」、「網路霸凌」及「使用者權益侵害」五大面向。

首先，政治不實訊息為近年來對網際網路社會造成重大危害的成因之一，台灣社會亦深受其害。有許多真假難辨的不實消息被大眾所流傳，甚至於有些網路新聞業者為求快速量產報導內容，會將網路上的消息，在未經查證的情況下就當作一則新聞播報，這嚴重危害了網路社會的安全。

而隨著網路的普及，有愈來愈多的兒童及少年使用網際網路，若兒童在幼年時期接觸到不安全的網路內容，則會對其身心發展造成一定的負面影響。然而，網路上的內容流傳速度非常快速，亦非常難以控管這些有害內容是否會暴露在兒少的環境中，因此兒少網路安全議題也是近年來政府與民間專業團體所關注的領域。《兒童及少年福利與權益保障法》第 46 條就明訂網際網路平臺提供者需建立內容分級制度、建立自律機制並注意兒少的上網教育安全宣導。此法也為兒少網路安全拉下一道防護網。

同時，網路交易安全、網路霸凌及使用者權益維護亦是各國政府及民眾十分重視的網路議題，尤其是網際網路所擁有的匿名性更是增加了網路霸凌發生的機率。因此，本研究將就上述五大議題進行調查與研究。

本研究區分為四大研究階段，首先，分別針對一般大眾進行電話訪問，調查民眾如何看待網路危害問題，以及這些問題該如何解決。其次，針對平臺業者、公民團體進行面談訪問，以獲得實務上的經驗與政策利害關係人的想法。第三，針對前述研究所獲得的結果，對一般大眾、平臺業者與專家、公民團體進行焦點座談說明會，以聚焦各

團體針對網路危害的想法，並擬定更詳細的解決方案。最後，統整上述所獲得之研究資料，建立出能因應網際網路危害的解決方案。

以下將分別敘述各研究階段之內容與成果。

一、一般大眾電話訪問

（一）問卷設計暨背景說明

本問卷旨在調查民眾之真實想法，預計回答的研究問題為：一、民眾認知到的網路危害有何種？是否有類似經驗？民眾認為這些網路危害的問題有多大？二、面對這些網路危害，民眾認為誰應負起最大責任，並應以何種方式作處理？故一般民眾電訪問卷共分為四大部分。以下說明問卷題目設計之方向及欲得到之解答。問卷設計如下圖所示。

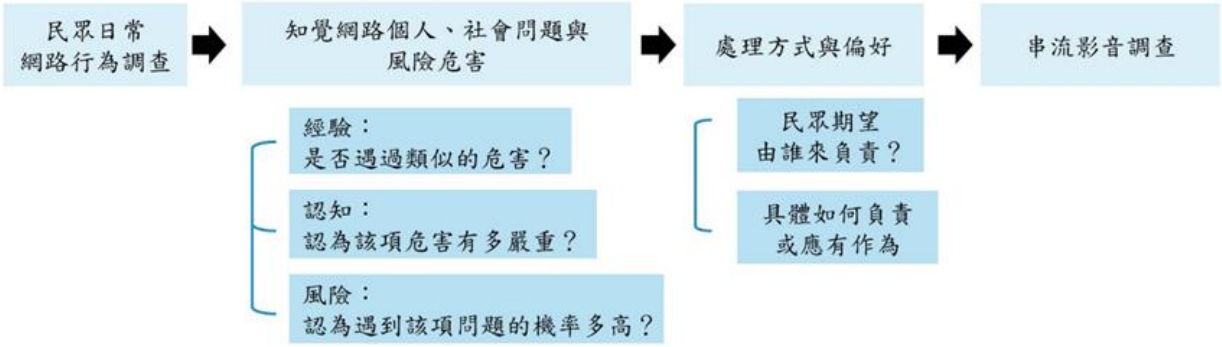


圖 30：一般大眾電訪問卷設計架構

資料來源：本研究自行繪製

1. 第一部分：網路行為與使用平臺

首先，第一部分調查民眾在日常生活中，使用哪些網路平臺、進行何種網路行為，藉以分析民眾行為，及所可能遇到的網路危害問題有哪些。

本研究調查民眾日常可能會使用的平臺，並將網路平臺區分為六項，包含社群平臺、通訊軟體、網路新聞平臺、拍賣及購物平臺、及時下正流行的串流影音服務等。另考量到傳統電視與新興網路服務的

交錯作用，亦調查民眾使用傳統電視服務的次數與比例。

其次，本研究將針對各平臺的使用頻率做調查，以找出該名民眾日常使用哪些網路平臺。根據「110 年網路沉迷研究調查報告」[892]，在工作日或上學日「平均每天上網時間」有網路沉迷傾向者每天平均上網 4.1 小時，無網路沉迷傾向者的平均 2.7 小時。

因此本研究將頻率設為：未滿 1 小時、1～未滿 3 小時、3～未滿 5 小時、5 小時以上及不一定。並將使用超過 3 小時的民眾定義為高網路使用族群。

本研究期望，經由上述調查，本研究預期得知受訪者日常使用過哪些網路平臺，並使用該平臺做何種事情。最後可與受訪者後面針對網路危害行為的認知做連結。

2. 第二部分：知覺網路個人、社會問題與風險危害

第二部分欲調查民眾知覺網路行為會對個人產生之社會和風險的危害認知。參閱我國過往類似調查之結果，可知涉及網際網路之主要危害風險有：政治不實訊息、兒少網路安全、網路交易安全、網路霸凌、使用者權益侵害等五大面向的網路危害。針對這五大危害面向，本研究設置三道題目，分別調查民眾的「經驗」（是否遇過類似的危害？）、「認知」（認為該項危害有多嚴重？）與「風險認知」（認為遇到該項問題的機率多高？）。

經驗是指個人或集體在過去與社會問題相關的事件或情境中所獲得的知識或技能。經驗可以增加或減少個人對於社會問題的敏感度、關注度或參與度。例如，一個曾經遭受網路詐騙的消費者可能比不曾被網路詐騙的人對網路購物更沒有信心，也更可能支持更嚴格的法律或政策。

認知是指個人或集體對於社會問題的理解、評價或判斷。認知可以影響個人對於社會問題的看法、立場或價值觀。例如，一個認為網

[892] 聯合行銷研究股份有限公司，110 年網路沉迷研究調查報告，國家發展委員會委託研究成果報告（2021）。

路世界是一個複雜組成、且因為匿名造成亂象的人，可能更容易認定網路世界有極高的風險，且與他個人的經驗無關。

風險認知是指個人或集體對於社會問題所帶來的潛在危害或不利後果的感知或預期。風險認知可以影響個人對於社會問題的恐懼、憂慮或焦慮程度，也可以影響他們採取預防或應對措施的意願或行動。例如，一個覺得兒少網路問題很嚴重的父母，可能更傾向有更嚴格或更能保護兒少的網路政策，也更可能支持相關的網路管制政策。

然而值得注意的是，認知與風險一般認為關連程度較高，因為問題的認知程度可能影響風險的認知，然而經驗的具備卻不見得與問題認知和風險認知有絕對相關。因為有些問題認知與風險認知程度偏高，恰巧來自於缺乏接觸經驗；因此在學理上，經驗可作為實際問題程度的參考，但問題認知與風險認知則是態度或意向的調查。

3. 第三部分：處理方式與偏好

本研究欲了解針對上述所提及之五大網路危害內容（政治不實訊息、兒少網路安全問題、網路交易問題、網路霸凌及個人權益遭到侵害），民眾內心期望應由誰來負責，並且以何種方式來負責。是故本研究在進行一般民眾電訪問卷的調查時，以各國（如歐盟、法國、英國、美國、日本及新加坡等）相關法規規定作為基礎，根據各國所採行的配套措施與監管密度設計出解決方案，並調查民眾偏好何種解決方案。

首先，本研究將各國相關法規依照監管密度及管制內容劃分成三大象限，分別為：（1）高密度監管搭配管制內容多，如歐盟、新加坡等。（2）高密度監管但管制內容相對少，如澳洲。（3）低密度監管，多為被動處理網路違法內容，或以平臺自律為主，如美國、日本。

其次，依據該象限，我們亦可觀察到國外做法通常將負責主體區分為四項。包含網路使用者自己、網路平臺（如 Facebook、LINE 等）、政府機關、民間組織，或其他。若交由網路使用者自己，及網路平臺來管理者，多為低密度管理的國家，政府偏向被動。若交由政府機關，或有民間組織參與管理者，多為高密度管理的國家，政府角色較為主

動，會擬定法規並介入管理等。

第三，本研究再一開始便區分不同網路危害的樣態，因此各不同網路危害對應到的解方會有所差異，不過大致上依舊是遵循著：政府主動－被動管理（平臺自律）、政府介入程度高－低、有無第三方機構等模式設計問卷選項。以下舉例：

A. 負責主體之界定參照國內外相關經驗如：

- 歐盟《數位服務法》、英國《線上安全法》等以網路平臺為作負責主體，該法規要求社群媒體需繳交透明度報告。
- 歐盟《數位服務法》設置數位服務協調官與歐洲數位服務委員會（European Board for Digital Services），明確監理機構的功能與作用。此是以公權力的角度介入管理網路危害。
- 英國 2019 年「線上危害白皮書」以政府作為負責主體，該白皮書欲下設政府獨立監管機構監管網路危害問題。澳洲《線上安全法》亦同，設立「電子安全專員辦公室」。
- 民間政府組織如：英國非營利組織「英國電影分級基金會」（BBFC）擔任線上色情年齡驗證之監理機構。此外，德國亦有民間政府與政府共同管理的案例。
- 以自由市場競爭為導向的美國，在網路危害問題上，作法仍相對保守，並無太多限制。

B. 政治不實訊息各相關管制辦法參照國內外相關經驗如：

- 英國《線上安全法》明定主管機關可針對不實消息發布警告或處以罰緩等規定。
- 法國《對抗資訊操縱法》賦予法官可以決定該不實訊息是否應刪除的權利。

C. 兒少網路安全各相關管制辦法參照國內外相關經驗如：

- 英國《線上安全法》：主管機關有權課予網路業者網路危害內

容管理義務，如業者必須降低可能危害兒少之內容的出現頻率。

- 澳洲《線上安全法》：主管機關權對業者發出刪除危害兒少健康之內容之通知，要求業者刪除相關違法內容。

D. 個人權益侵害參考規範如：歐盟《數位服務法》。

綜上，本研究依據所觀察到之各國處理相關網路議題之主管機關、政府介入程度，以及處理方式等經驗，擬出適合台灣的參考作為，並將其設計成問卷題目與選項，以電訪形式訪問民眾，藉以蒐集民眾對於網路議題處理方式的態度與想法。並回答如上研究問題：一、民眾認知到的網路危害有何種？是否有類似經驗？民眾認為這些網路危害的問題有多大？二、面對這些網路危害，民眾認為誰應負起最大責任，並應以何種方式作處理？

4. 第四部分：基本資料

最後，第四部分為調查民眾的基本資料。本研究期望，可以透過上述的調查，了解民眾的真實想法，藉以設定解決方向。

為確保問卷設計確實能回答研究問題，本研究於 2023 年 6 月 5 日辦理問卷諮詢會議，邀請相關領域之專家學者針對問卷設計提供專業修正意見，問卷諮詢會議出席之專家學者包括：許詩嫻助理教授（臺灣大學生物產業傳播暨發展學系）、劉嘉薇教授（臺北大學公共行政暨政策學系），以及蘇建州教授（世新大學傳播管理學系）。依會議意見修正後，問卷經委託單位審核後定稿。

（二）訪問對象與調查方式

本研究之電話訪問調查對象為臺灣本島及金門縣、澎湖縣、連江縣 22 個縣市之 18 歲以上民眾，採住宅電話與行動電話併用之雙底冊抽樣調查方式進行。

前測調查於 112 年 6 月 19 日執行。正式調查於 112 年 6 月 30 日至 112 年 7 月 19 日間執行。

本案以電腦輔助電話訪問系統（Computer Assisted Telephone Interviewing System,以下簡稱 CATI 系統）進行市話及手機調查，CATI 電話調查系統使得民意調查更具效率與精確性，其將資料處理過程與電話訪問進行結合，除省去傳統的資料輸入時間，也透過 CATI 系統的作用，事先將調查內容進行邏輯性的安排，避免訪員錯誤的訪問程序，或者受訪者提供不適當的回答，造成後續資料檢誤的困難。

電話追蹤的部分，訪問對象一旦確定後絕對不替換，需以電話追蹤的方式至少打 3 次，找到指定的受訪者完成訪問，若該戶拒訪或無合格受訪者時，CATI 系統將產生相同區域之替代樣本戶電話，再行撥號，直到訪談成功，以維持樣本結構不變，確保樣本代表性。

（三）抽樣、執行方式與樣本代表性檢定

問卷採分層隨機抽樣，同步執行住宅電話調查與手機調查，住宅電話與手機調查抽樣比例為 1:1，有效樣本數應至少達 1,100 份（信心水準〔confidence level〕至少 95%，抽樣誤差不超過±3%）。

市話、手機雙底冊資料合併處理步驟方面，採用國發會「雙底冊電話調查估計」搭配加權處理方式辦理，資料合併處理過程先計算完訪樣本的唯市話族、市話手機兩者都用、唯手機族三類的比例，以 x、y、z 分別表示雙底冊電話調查產生的樣本估計值，x＋y＋z＝100%。x 是「只有使用住宅電話且沒有使用行動電話者」的估計，y 是對「住宅電話與行動電話都有使用者」的估計，z 是「只有使用行動電話且沒有使用住宅電話者」的估計。住宅電話訪問結果得到「只有使用住宅電話且沒有使用行動電話者」的樣本數 n1，「住宅電話與行動電話都有使用者」的樣本數 n2，手機調查結果得到「住宅電話與行動電話都有使用者」的樣本數 n3，「只有使用行動電話且沒有使用住宅電話者」的樣本數 n4，公式推導如下：

令 $n1/(n1+n2)=a$，即 a 表示「只有使用住宅電話且沒有使用行動電話者」占「使用住宅電話者」之比例。如此則 $x/(x+y)= a$，即 a 等於「只有使用住宅電話且沒有使用行動電話者的估計值」除以「使用住宅電話者的估計值」。

在 a 不等於 1 的情況下，推導出 x=ax+ay，(1-a)x=ay，x=(a/(1-a))y

同理令 n4/(n3+n4)=b，z/(y+z)= b

則在 b 不等於 1 的情況下，推導出 z=by+bz，(1-b)z=by，y=((1-b)/b)z。

x +y +z =100%

(a/(1-a))y+y+z=1，

(a/(1-a))((1-b)/b)z + ((1-b)/b)z + z=1，*

*((1 - ab) / (b - ab))*z = 1，*

因此可以透過雙底冊電話調查結果的 a 和 b 得到三個估計：

z=((b - ab) / (1 - ab))，y=((1-b)/b)z，x=(a/(1-a))y。

即依據 x（唯住宅電話比例）、y（兩者都使用比例）、z（唯行動電話比例）進行併檔。

本研究進行市話與手機雙底冊調查，依據國發會市話手機加權方式進行電話使用行為進行資料合併，透過解聯立方式計算出唯市話族（2.85%）、市話手機兩者都用（48.95%）、唯手機族（48.20%）的比例，完成資料合併後，再依據人口統計資料，進行樣本代表性檢定，本案依據內政部戶政司公布 2023 年 5 月人口資料為檢定依據，分別針對有效樣本的性別、年齡、縣市與母體結構進行卡方檢定。

檢定結果發現有效樣本在「性別」、「年齡」、「縣市」與母體結構有顯著差異。針對調查樣本進一步運用「多變數反覆加權法」（raking）的事後加權處理方式，針對所需檢定的變項，逐項進行加權調整，直至樣本結構與母體結構無顯著差異，才停止加權，加權後檢定結果呈現樣本結構與母體結構並無顯著差異（如下表所示）。

表 18：一般民眾調查樣本檢定結果

		母體	加權前樣本			加權後樣本		
		百分比	人數	百分比	檢定結果	人數	百分比	檢定結果
性別	男性	48.95%	727	55.88%	χ^2=24.99 $p < 0.05$ 顯著差異	637	48.95%	χ^2=0.000 $p > 0.05$
	女性	51.05%	574	44.12%		664	51.05%	
	合計	100.0%	1,301	100.0%		1,301	100.0%	
年齡	18~29 歲	16.80%	156	11.99%	χ^2=15.15 $p < 0.05$ 顯著差異	217	16.68%	χ^2=0.000 $p > 0.05$
	30~39 歲	16.35%	212	16.30%		212	16.30%	
	40~49 歲	19.39%	270	20.75%		251	19.29%	
	50~59 歲	17.78%	285	21.91%		231	17.76%	
	60~69 歲	16.32%	225	17.29%		212	16.30%	
	70 歲及以上	13.36%	148	11.38%		173	13.30%	
	拒答	-	5	0.38%		5	0.38%	
	合計	100.0%	1,301	100.0%		1,301	100.0%	

說明：此處加權前百分比與加權後百分比為扣除未填答者之計算結果。

資料來源：本研究自行整理

表 19：調查樣本分佈檢定結果（依縣市）

		母體	加權前樣本			加權後樣本		
		百分比	人數	百分比	檢定結果	人數	百分比	檢定結果
縣市	新北市	17.36%	195	14.99%	χ^2=154.26 $p < 0.05$ 顯著差異	225	17.27%	χ^2=0.052 $p > 0.05$
	臺北市	10.69%	125	9.61%		139	10.65%	
	桃園市	9.60%	107	8.22%		125	9.59%	
	臺中市	11.89%	135	10.38%		154	11.82%	
	臺南市	8.01%	90	6.92%		104	8.02%	
	高雄市	11.83%	132	10.15%		154	11.82%	
	宜蘭縣	1.94%	30	2.31%		26	1.97%	
	新竹縣	2.39%	30	2.31%		31	2.37%	
	苗栗縣	2.30%	30	2.31%		30	2.30%	
	彰化縣	5.31%	58	4.46%		70	5.35%	
	南投縣	2.09%	30	2.31%		28	2.13%	
	雲林縣	2.88%	32	2.46%		38	2.92%	
	嘉義縣	2.17%	30	2.31%		28	2.19%	
	屏東縣	3.50%	37	2.84%		46	3.54%	
	臺東縣	0.92%	30	2.31%		12	0.93%	
	花蓮縣	1.38%	30	2.31%		18	1.39%	
	澎湖縣	0.47%	30	2.31%		6	0.48%	
	基隆市	1.60%	30	2.31%		21	1.60%	
	新竹市	1.84%	30	2.31%		24	1.82%	
	嘉義市	1.12%	30	2.31%		15	1.13%	
	金門縣	0.64%	30	2.31%		9	0.66%	
	連江縣	0.06%	30	2.31%		1	0.06%	
	合計	100.0%	1,301	100.0%		1,301	100.0%	

說明：此處加權前百分比與加權後百分比為扣除未填答者之計算結果。

資料來源：本研究自行整理

（四）接觸紀錄

本研究之「住宅電話調查」共撥號 17,055 筆，其中成功樣本為 654 份，占總撥出電話的 3.8%。另有 8,724 通無人接聽（占 51.2%）等，詳細撥號資料如下表。

表 20：住宅電話調查訪問接觸結果

項目	次數	有接通電話百分比	總撥出電話百分比
完成訪問	654	10.4%	3.8%
拒訪_太忙沒時間	1,011	16.0%	5.9%
拒訪_對這個主題沒興趣或不清楚	1,403	22.2%	8.2%
拒訪_已經受過類似訪問	2	0.0%	0.0%
拒訪_覺得被侵犯個人隱私反對電話調查	34	0.5%	0.2%
配額已滿	104	1.6%	0.6%
其他時段約訪	-	0.0%	0.0%
中止訪問_非住宅電話	1,134	18.0%	6.6%
中止訪問_無合格受訪者	106	1.7%	0.6%
中止訪問_因受訪者心理／生理因素無法進行訪問	73	1.2%	0.4%
中止訪問_語言不通（如原住民、外語等）無法進行訪問	20	0.3%	0.1%
中止訪問_原因不明、什麼都沒說就掛電話	1,775	28.1%	10.1%
小計	6,316	100.0%	37.0%

資料來源：本研究自行整理

表 21：住宅電話調查訪問接觸結果（續）

項目	次數	未接通電話百分比	總撥出電話百分比
無人接聽	8,724	81.2%	51.2%
空號	837	7.8%	4.9%
忙線	391	3.6%	2.3%
傳真機	750	7.0%	4.4%
住宅答錄機	18	0.2%	0.1%
電話故障	15	0.1%	0.1%
暫停使用	3	0.0%	0.0%
勿干擾	1	0.0%	0.0%
小計	10,739	100.0%	63.0%
合計	17,055	100.0%	100.0%

資料來源：本研究自行整理

本研究的「手機電話調查」共撥號 21,469 筆，其中成功樣本為 647 份，佔總撥出電話的 3.0%。另有 11,559 通無人接聽（佔 53.8%）等，詳細撥號資料如下表。

表 22：手機電話調查訪問接觸結果

項目	次數	有接通電話百分比	總撥出電話百分比
完成訪問	647	8.8%	3.0%
拒訪_太忙沒時間	1,828	24.8%	8.5%
拒訪_對這個主題沒興趣或不清楚	1,098	14.9%	5.4%
拒訪_已經受過類似訪問	4	0.1%	0.0%
拒訪_覺得被侵犯個人隱私反對電話調查	41	0.6%	0.2%
配額已滿	1,509	20.4%	7.0%
其他時段約訪	-	0.0%	0.0%
中止訪問_非個人手機	353	4.8%	1.6%
中止訪問_無合格受訪者	90	1.2%	0.4%
中止訪問_因受訪者心理／生理因素無法進行訪問	29	0.4%	0.1%
中止訪問_語言不通（如原住民、外語等）無法進行訪問	14	0.2%	0.1%
中止訪問_原因不明、什麼都沒說就掛電話	1,768	24.0%	8.2%
小計	7,381	100%	34.4%

資料來源：本研究自行整理

表 23：手機電話調查訪問接觸結果（續）

項目	次數	未接通電話百分比	總撥出電話百分比
無人接聽	11,559	82.0%	53.8%
空號	1,228	8.7%	5.7%
忙線	796	5.7%	3.7%
傳真機	14	0.1%	0.1%
住宅答錄機	108	0.8%	0.5%
電話故障	17	0.1%	0.1%
暫停使用	331	2.3%	1.5%
勿干擾	35	0.2%	0.2%
小計	14,088	100.0%	65.6%
合計	21,469	100.0%	100.0%

資料來源：本研究自行整理

（五）分析方法

本案針對各項調查主題，視各題目的類型與特性，採取下列統計分析方法：

1. 百分比分析

用以瞭解受訪樣本之基本特性、認知、評價、滿意狀況之分配狀況，主要功能為針對分類性變數進行整體分析之用。例如：各題項及基本資料之分析。透過計算各項意見表達態度或意見的百分比，可推估各因素的分布情形及重要性。

2. 交叉分析與卡方檢定

針對各題項與受訪樣本之基本資料所進行的統計方法。藉由兩個變項間次數的交叉列聯表，來檢視受訪者基本背景變項與各題項間是否存在顯著的差異性。若交叉表的卡方機率值小於顯著水準（0.05）時，才認定兩變數間並非獨立。

3. 平均數與變異數分析

探索兩變項間關係時，若為等距尺度資料進行平均數比較時，可考慮使用變異數分析。變異數分析係將總變異數分解為組間變異、組內變異兩個來源，其分析原理即在求取組間及組內變異的比例，如果組間變異明顯大於組內變異數，則顯示各組的平均數中，至少有兩組以上具有顯著差異，如果無顯著差異，則各組的平均數亦無顯著不同。

二、公民團體面訪

本研究挑選關切網際網路社會問題相關議題之公民團體進行面訪，類型涵蓋人權倡議、公民傳播權益推動、匯流趨勢研究、消費者權益保障、兒少權益保障之團體。依據受訪者的距離與實體面訪的可行性，以實體面訪為主，但部分安排線上會議訪談。

面訪對象代號說明可見下表：

表 24：本研究公民團體面訪名單

代號	團體類型	辦理情形
A1	關注人權議題及相關法律倡議	7/11 面訪
C1	促進媒體自律、保障公民傳播權益	7/21 面訪
D1、D2	國際匯流趨勢、台灣匯流發展研究	7/24 面訪
H1	消費者權益保障推動	8/1 線上會議
I1	兒少權益保障推動	8/4 線上會議

資料來源：本研究自行整理

面訪問卷之設計結構共分為四大部分：

首先，第一部分為調查網路社會問題與風險認知。本研究綜合過往文獻，梳理出五大網際網路網路危害，包含：政治不實訊息、網路霸凌、兒少網路安全問題、網路交易安全問題及使用者權益侵害（使用者權益被限制）。本研究將在第一部分調查公民團體以自身角度出發，針對上述五大危害做「嚴重程度」之排序，及其認為網路平臺使用者可能會遇到這些問題的「機會」排序。

第二部分將針對前述公民團體所作之排序，調查他們認為該網路問題之負責主體應為誰，以及應如何解決。在此部分，本研究將「負責主體」區分為五塊，分別為：網路使用者自己、網路平臺、政府機關、民間專業組織與其他。例如：從公民團體的角度來看，您覺得在網路平臺上的「網路霸凌」問題，誰應當負「最大的責任」，並出面處理？

在處理面向上，本研究將調查公民團體認為，在這五大網路危害中，政府、網路平臺／業者，及民間組織應扮演何種角色？應有何種作為？

第三部分將詢問受訪者，是否有問卷未提及，但仍重要的網路議題，以及政府應該如何解決該項網路議題。

最後，第四部分將針對串流影音產業現況，詢問公民團體的看法。包含：現狀下串流影音產業「目前面臨最迫切」的議題為何？如盜版問題、境內／外同業競爭、消費者爭議、兒少保護、個資保護、身心障礙者權利保護等。其次，在這些問題上，該如何解決？又政府扮演何種角色？

同時，本研究亦探討，串流影音服務應採取何種機制落實身障人士權利保障、兒少保護？他們應採取何種機制處理有害內容？如業者是否應採取分級制度等。

除此之外，近年來，受到歐盟限制串流影音業者必須投資當地影視作品 30%的法規影響，我國國內也興起相當的社會音量，要求要設立相關投資標準。故，本研究亦針對國內串流影音業者的服務作為，及有關本土影視作品之相關議題設立相關問題，用以了解公民團體的看法。最後則是訪問受訪者針對串流影音業者是否應實施登記制問題的相關看法。

三、網際網路傳播相關服務業者面訪

本研究挑選民眾使用習慣較為相關之網際網路平臺業者進行面訪。依據受訪者的距離與實體面訪的可行性，以實體面訪為主，部分則安排線上會議。訪談詳細訪問名單可見下表：

表 25：本研究網際網路傳播相關服務業者面訪名單

面訪對象代號	提供之服務類型	辦理情形
OTT TV 產業協會	B1	7/17 面訪
OTT TV 產業協會	E1	7/25 面訪
網路平臺	F1	7/28 線上會議
網路平臺、OTT TV	G1、G2	7/31 線上會議
網路平臺、OTT TV	J1、J2、J3	8/1 線上會議

資料來源：本研究自行整理

面訪問卷設計結構共分為四大部分：

首先，第一部分為調查網路社會問題與風險認知。本研究綜合過往文獻，梳理出五大網際網路網路危害，包含：政治不實訊息、網路霸凌、兒少網路安全問題、網路交易安全問題及使用者權益侵害（使用者權益被限制）。本研究將在第一部分調查平臺業者以自身角度出發，針對上述五大危害做「嚴重程度」之排序，及其認為網路平臺使用者可能會遇到這些問題的「機會」排序。

本研究將面訪主軸聚焦在與平臺業者共同談討「具體而言，應該如何處理這些網路危害？各利害關係人的角色為何？」並請教該平臺是否有針對相關網路危害做出防護措施？是如何做的？有遇到什麼困難嗎？等，研究預期將透過面訪來獲得業界的實務經驗，以此作為參考解方之一。

因此，第二部分將針對前述業者所作之排序，調查他們認為該網路問題之負責主體應為誰，以及應如何解決。在此部分，本研究將「負責主體」區分為五塊，分別為：網路使用者自己、網路平臺、政府機

關、民間專業組織與其他。例如：從業者的角度來看，您覺得在網路平臺上的「網路霸凌」問題，誰應當負「最大的責任」，並出面處理？

在處理面向上，本研究將調查業者認為，在這五大網路危害中，政府、網路平臺／業者，及民間組織應扮演何種角色？應有何種作為？

第三部分將詢問受訪者，是否有問卷未提及，但仍重要的網路議題，以及政府應該如何解決該項網路議題。

最後，第四部分將針對串流影音產業現況，詢問業者的看法。包含：現狀下串流影音產業「目前面臨最迫切」的議題為何？如盜版問題、境內／外同業競爭、消費者爭議、兒少保護、個資保護、身心障礙者權利保護等。其次，在這些問題上，該如何解決？又政府扮演何種角色？

同時，本研究亦探討，串流影音服務應採取何種機制落實身障人士權利保障、兒少保護？他們應採取何種機制處理有害內容？如業者是否應採取分級制度等。

除此之外，近來受到歐盟限制串流影音業者必須投資當地影視作品30%的法規影響，我國國內也興起相當的社會音量，要求要設立相關投資標準。故，本研究亦針對國內串流影音業者的服務作為，及有關本土影視作品之相關議題設立相關問題，用以了解業者的看法。最後則訪問受訪者針對串流影音業者是否應實施登記制的看法。

四、焦點團體座談

本研究另外辦理焦點團體訪談，共同就問卷與面訪之調查結果，交叉分析深入探討原因及因應之道。依照利害關係人類別，分為：

1. **一般民眾場次：**每場邀請 10 位不同職業、年齡層、性別之民眾參與，共舉辦 3 場，分別於 112 年 8 月 2 日、8 月 4 日、8 月 10 日辦理。出席者之招募主要係透過以下兩種方式進行，一為針對先前曾接受過電話訪問之民眾，篩選居住地區位於台北市者再次進行電話接觸，詢問其參與座談會之初步意願，並依據各場座談會性別、年齡、職業的數量配置進行邀約；二為列出座談會與會者在性別、年齡、職業之需求數量，發布招募訊息，讓有興趣參與的民眾報名，再對報名的民眾進行篩選及電話接觸以確認最後參與座談會的民眾名單。

2. **公民團體與學者專家場次：**邀請長期關心網際網路社會問題之公民團體代表，以及法律、傳播、公共行政等相關領域之學者專家，共舉辦 1 場，於 112 年 8 月 11 日辦理。

3. **網際網路傳播相關服務業者場次：**邀請網際網路傳播相關之平臺業者，共舉辦 1 場，於 112 年 8 月 14 日辦理。

每一場次之名單與座談題綱可見下表。

表 26：一般民眾場次（8/2）出席民眾名單

代號	年齡	性別	職業
K1	20-29 歲	男	行銷企劃
K2		男	餐飲業
K3		男	待業
K4		男	運動員
K5		女	護理師
K6		女	護理師
K7	30-39 歲	男	攝影師
K8	40-49 歲	女	會計
K9		男	攝影師
K10	50-59 歲	女	自由業

資料來源：本研究自行整理

表 27：一般民眾場次（8/4）出席民眾名單

代號	年齡	性別	職業
L1	18-19 歲	男	學生
L2	30-39 歲	男	行銷企劃
L3		男	業務
L4		女	服務業
L5		男	旅館業人員
L6	40-49 歲	女	助理
L7		女	國小老師
L8	50-59 歲	女	生管
L9		女	自由業
L10	60-69 歲	女	家庭主婦

資料來源：本研究自行整理

表 28：一般民眾場次（8/10）出席民眾名單

代號	年齡	性別	職業
M1	20-29 歲	男	數位遊戲工程師
M2		女	保險
M3		女	保險
M4	30-39 歲	男	銷售員
M5		男	保險業
M6		女	餐飲業
M7		男	學生
M8	40-49 歲	女	飯店服務業
M9	50-59 歲	女	會計
M10		女	會計

資料來源：本研究自行整理

表 29：公民團體場及學者場次（8/11）出席名單

代號	所屬單位	職稱
N1	法律學系	副教授
N2	公共行政學系	教授
N3	法律學系	教授
N4	法律學系	副教授
N5	兒少權益團體	常務理事
N6	媒體教育團體	董事長
N7	匯流研究團體	秘書長
N8	事實查核組織	執行長

資料來源：本研究自行整理

表 30：網際網路傳播相關服務業者場次（8/14）出席名單

代號	業者提供之服務類型	職稱
O	網路平臺、OTT TV	政府事務及公共政策協理
O2	即時訊息服務、OTT TV	副理
O3		資深總監
O4	網路論壇	公關總監
O5	網路論壇	法律顧問
O6	產業協會	組長

資料來源：本研究自行整理

表 31：一般民眾場次討論題綱

討論階段	討論題綱
第一階段	**一、 網路平臺使用習慣** 請簡單介紹自己的職業、網路平臺使用習慣。最近一個月內有使用哪些網路平臺服務（如視訊分享平臺 YouTube、社群媒體 Facebook、通訊軟體 LINE、網路論壇 PTT、網路新聞平臺 Yahoo 新聞、拍賣網站）？平均一天大約花多少時間使用？ **二、 網路上可能的社會問題** 1. 從您網路平臺使用的生活經驗來看，您覺得網路上哪些問題最困擾您？是網路平臺業者必須要重視的？（如網路詐騙或交易糾紛、色情或暴力的內容、站方隨便刪留言或帳號停權、政治類的不實訊息、網路霸凌、個資外洩……等） 2. （承上）如果是政府機關必須首要重視的網路問題，您的答案會有不同嗎？ 3. 您會期待網路平臺業者做些什麼來減少網路上的社會問題？政府機關又必須做些什麼？您覺得有沒有哪些民間專業組織可以幫助網路平臺業者或政府機關減少社會問題？

	三、 傳統電視新聞與網路新聞的互動 1. 請問您有沒有看過電視新聞報導網友在網路上（如PTT、FB）的留言或反應？您覺得這種新聞正確或公正嗎？這樣算是事實查證嗎？您對於這種電視新聞有何想法？ 2. 請問您有沒有看過電視台官方網站或電視台製作的網路新聞？這種網路新聞在標題或內容上，跟原本的電視新聞有何不同？
第二階段	**一、 網路平臺的角色** 1. 您覺得讓網路平臺業者擔任網路世界秩序的維護者，是恰當的嗎？政府機關是否更應該擔起這個責任？ 2. 您覺得網路平臺業者有能力擔任網路世界秩序的維護者嗎？政府機關是否更具備這樣的能力？ **二、 民間專業組織的角色** 您覺得產業公會作為民間專業組織擔任網路世界的整合者，是恰當的嗎？您會期待其他民間組織擔起這個責任嗎？ **三、 政府機關的角色** 1. 您覺得讓政府機關擔任資源的提供者與協助者，是恰當的嗎？您會期待政府機關做更多嗎？ 2. 您覺得讓政府機關擔任資源的網路問題的防護者，是恰當的嗎？您會認為這樣政府機關太被動了嗎？ **四、 網路使用者的期待與信任** 1. 從您作為網路使用者的角度來看，您期待網路世界的管理，如何兼顧使用者的個人權益，又同時維護網路秩序呢？ 2. 您信任這個網路秩序的建立，能由網路平臺業者和其產業公會協調、成形嗎？ 3. 您是否還有認為不合理、或有疑問之處呢？

資料來源：本研究自行整理

表 32：公民團體場及學者、網際網路傳播相關服務業者場次討論提綱

討論題綱
一、 網際網路現行的社會問題牽涉到管理成本、可行性、彈性，以及權利的限制與風險衡平問題，您覺得怎樣的治理方式比較能兼顧各種需要？政府機關、業者、產業公會等分別應該扮演什麼角色？ 二、 （承上）請問在網際網路社會問題的處理上，政府機關應該是主事者？還是協助者？ 1. 主事者：主導所有相關政策、管制法規的制訂，並將審查、懲處（違法內容張貼者）、救濟等相關業務交由分散或特定主管機關辦理。 2. 協助者：協助業者盤點當前相關法規、協助/督導業者整合出產業自制規範、提供業者所需要的資源與支援（含資金與技術）；平臺內容的管理交由業者以產業自制規範自律。 三、 若我們期待政府機關在必要的時候可以整合跨機關的資源(例如業務主管機關、警察機關、產業公會、業者)，這樣的政府機關應該在哪一個組織層級？是分散的還是單一的？ 四、 公民監督是網路治理理論中非常重視的環節，政府、民間專業組織或數位平臺業者如何引入或擁抱更多的民眾的聲音，形成可運作的公私協力模式？ **五、** 研究團隊將於會議中提出針對我國民眾電訪問卷的統計結果，觀察並討論民眾對於各種違法或具傷害性的網路活動的處置意向。同時，除了問卷調查，政府針對網路治理的政策擬定過程，應如何強化與民眾及產業界的溝通？

資料來源：本研究自行整理

第二節　一般大眾電話訪問調查結果

本案欲透過民眾之電話訪問瞭解民眾日常網路行為、衍生之社會問題風險與危害、網路及電視交互作用下之傳播效果，以及對於問題處理之看法與建議。

由於電訪調查經代表性分析之後，有效樣本在「性別」、「年齡」、「縣市」與母體結構有顯著差異，因此樣本經過加權處理。以下分析若無特殊說明，主要以「加權後」的樣本為主。

一、日常網路行為：網路行為與使用平臺

（一）社群媒體平臺

近一個月內有使用社群平臺，如 Facebook、Instagram、YouTube、PTT 等的民眾，加權後的樣本有 925 位，計有 71.1%的民眾近一個月內有使用過社群平臺，超過半數（50%）。而其中，每天使用 1~3 小時社群平臺的民眾為最多數（加權後計有 45.3%），社群平臺重度使用者（每天平均上網超過 4.1 小時者，此處以超過 5 小時計）有 12.4%（加權後計有 13.4%）。

詳細次數統計表如下。

表 33：民眾使用社群媒體平臺的頻率

近一個月內有使用：				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
有使用	917	70.5%	925	71.1%
沒有使用	384	29.5%	376	28.9%
合計	1,301	100.0%	1,301	100.0%
一天使用之時間：				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
未滿 1 小時	163	17.8%	162	17.5%
1～未滿 3 小時	427	46.6%	419	45.3%
3～未滿 5 小時	153	16.7%	167	18.1%
5 小時以上	114	12.4%	124	13.4%
不一定	57	6.2%	46	5.0%
不知道／拒答	3	0.3%	6	0.7%
合計	917	100.0%	925	100.0%

資料來源：本研究自行整理

（二）通訊軟體

近一個月內有使用通訊軟體，如 LINE、Messenger、Discord 等的民眾，有 1,161 位（加權後計有 89.1%），有高達近九成的近一個月內有使用過社群平臺。

而其中，每天使用 1~3 小時通訊軟體的民眾為最多數（加權後計有 38.6%），通訊軟體重度使用者（每天平均上網超過 4.1 小時者，此處以超過 5 小時計）約有 15%（加權後計有 16.8%）。

詳細次數統計表如下。

表 34：民眾使用通訊媒體平臺的頻率

近一個月內有使用：				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
有使用	1,161	89.2%	1,160	89.1%
沒有使用	140	10.8%	141	10.9%
合計	1,301	100.0%	1,301	100.0%
一天使用之時間：				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
未滿 1 小時	307	26.4%	281	24.2%
1～未滿 3 小時	446	38.4%	448	38.6%
3～未滿 5 小時	126	10.9%	137	11.8%
5 小時以上	181	15.6%	195	16.8%
不一定	93	8.0%	89	7.7%
不知道／拒答	8	0.7%	9	0.8%
合計	1,161	100.0%	1,160	100.0%

資料來源：本研究自行整理

（三）網路新聞平臺

近一個月內有使用網路新聞平臺，如 Yahoo 新聞、LINE TODAY 等的民眾，有 622 位，加權後計有 47.8%。近一個月內有使用與沒使用網路新聞平臺的民眾約一半一半，但仍以沒使用者居多（52.2%）。

其中，每天使用未滿 1 小時網路新聞平臺的民眾為最多數（加權後計有 50.4%），網路新聞平臺重度使用者（每天平均上網超過 4.1 小時者，此處以超過 5 小時計）加權後計有 2.3%。

詳細次數統計表如下。

表 35：民眾使用網路新聞媒體平臺的頻率

近一個月內有使用：				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
有使用	622	47.8%	622	47.8%
沒有使用	679	52.2%	679	52.2%
合計	1,301	100.0%	1,301	100.0%
一天使用之時間：				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
未滿 1 小時	304	48.9%	313	50.4%
1～未滿 3 小時	254	40.8%	244	39.3%
3～未滿 5 小時	22	3.5%	21	3.5%
5 小時以上	15	2.4%	14	2.3%
不一定	20	3.2%	19	3.1%
不知道／拒答	7	1.1%	9	1.5%
合計	622	100.0%	622	100.0%

資料來源：本研究自行整理

（四）拍賣、購物平臺

近一個月內有使用拍賣、購物平臺，如 Yahoo 拍賣、蝦皮購物、露天、淘寶等的民眾，有 516 位，加權後計有 39.7%。近一個月內沒有使用拍賣、購物平臺的民眾（加權後計有 59.1%）略高於有使用拍賣平臺的民眾。

其中，每天使用未滿 1 小時拍賣、購物平臺的民眾為最多數（加權後計有 69.2%），拍賣、購物平臺重度使用者（每天平均上網超過 4.1 小時者，此處以超過 5 小時計）加權後計有 1.1%。

詳細次數統計表如下。

表 36：民眾使用拍賣、購物平臺的頻率

近一個月內有使用：				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
有使用	516	39.7%	532	40.9%
沒有使用	785	60.3%	769	59.1%
合計	1,301	100.0%	1,301	100.0%
一天使用之時間：				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
未滿 1 小時	354	68.6%	368	69.2%
1～未滿 3 小時	90	17.4%	94	17.8%
3～未滿 5 小時	10	1.9%	15	2.8%
5 小時以上	6	1.2%	6	1.1%
不一定	54	10.5%	46	8.6%
不知道／拒答	2	0.4%	3	0.5%
合計	516	100.0%	532	100.0%

資料來源：本研究自行整理

（五）串流影音服務

近一個月內有使用串流影音平臺，如 Netflix、愛奇藝、MyVideo 等的民眾，有 348 位，加權後計有 29.7%。近一個月內沒有使用串流影音平臺的民眾（加權後計有 70.3%）高於有使用串流影音平臺的民眾四成左右。

其中，每天使用 1～未滿 3 小時串流影音平臺的民眾為最多數（加權後計有 54.5%），串流影音平臺重度使用者（每天平均上網超過 4.1 小時者，此處以超過 5 小時計）加權後計有 4.1%。

詳細次數統計表如下。

表 37：民眾使用串流影音服務的頻率

近一個月內有使用：				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
有使用	348	26.7%	387	29.7%
沒有使用	953	73.3%	914	70.3%
合計	1,301	100.0%	1,301	100.0%
一天使用之時間：				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
未滿 1 小時	86	24.7%	87	22.4%
1～未滿 3 小時	189	54.3%	211	54.5%
3～未滿 5 小時	40	11.5%	53	13.7%
5 小時以上	12	3.4%	16	4.1%
不一定	20	5.7%	19	5.0%
不知道／拒答	1	0.3%	1	0.3%
合計	348	100.0%	387	100.0%

資料來源：本研究自行整理

（六）傳統電視

近一個月內有使用傳統電視，如有線電視、中華電信 MOD、無線電視等的民眾，有 807 位，加權後計有 56.5%。近一個月內有使用傳統電視的民眾（加權後計有 56.5%）略高於沒有使用傳統電視的民眾（加權後計有 43.5%）。

其中，每天使用 1～未滿 3 小時傳統電視的民眾為最多數（加權後計有 46.2%），傳統電視平臺重度使用者（每天平均上網超過 4.1 小時者，此處以超過 5 小時計）加權後計有 8.5%。

詳細次數統計表如下。

表 38：民眾使用傳統電視的頻率

近一個月內有使用：				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
有使用	807	62.0%	735	56.5%
沒有使用	494	38.0%	566	43.5%
合計	1,301	100.0%	1,301	100.0%
一天使用之時間：				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
未滿 1 小時	166	20.6%	172	23.4%
1～未滿 3 小時	396	49.1%	340	46.2%
3～未滿 5 小時	128	15.9%	114	15.5%
5 小時以上	69	8.6%	63	8.5%
不一定	45	5.6%	44	5.9%
不知道／拒答	3	0.4%	3	0.4%
合計	807	100.0%	735	100.0%

資料來源：本研究自行整理

（七）綜合分析

從下表可看出網路、傳統電視的使用者有年齡上的差異。只使用網路的對象以 49 歲以下的民眾居多，只使用傳統電視的民眾則多為 60 歲以上，兩種都用的則以 40 歲至 59 歲這個年齡區間居多。

其他網路平臺使用大多也以 59 歲以下的族群為主。這個年齡交叉分析可知，我國民眾的網際網路平臺使用基本上 59 歲以下的行為模式差異不大，但通訊軟體的使用（例如 LINE）幾乎所有的年齡層的使用比例都相當高。高齡者較少接觸的平臺，是網路交易平臺以及網路新聞平臺。

表 39：網路、傳統電視使用與使用者年齡之交叉分析

年齡	只用網路	只用傳統電視	兩種都用	總計
18-29 歲	12	0	142	154
30-39 歲	28	2	180	210
40-49 歲	14	2	252	268
50-59 歲	9	5	264	278
60-69 歲	4	25	182	211
70 歲以上	0	35	97	132
總計	67	69	1,117	1,253

資料來源：本研究自行整理

表 40：社群媒體平臺與年齡交叉分析

年齡	沒有使用	有使用	總計
18-29 歲	8	209	217
30-39 歲	17	195	212
40-49 歲	44	208	251
50-59 歲	65	165	231
60-69 歲	118	94	212
70 歲以上	124	49	173
總計	376	920	1,296

資料來源：本研究自行整理

表 41：通訊軟體與年齡交叉分析

年齡	沒有使用	有使用	總計
18-29 歲	4	213	217
30-39 歲	8	204	212
40-49 歲	9	242	251
50-59 歲	14	217	231
60-69 歲	39	172	212
70 歲以上	67	106	173
總計	141	1155	1,296

資料來源：本研究自行整理

表 42：網路新聞平臺與年齡交叉分析

年齡	沒有使用	有使用	總計
18-29 歲	124	93	217
30-39 歲	104	108	212
40-49 歲	96	156	251
50-59 歲	96	135	231
60-69 歲	119	92	212
70 歲以上	138	35	173
總計	677	619	1,296

資料來源：本研究自行整理

表 43：網路購物平臺與年齡交叉分析

年齡	沒有使用	有使用	總計
18-29 歲	100	117	217
30-39 歲	75	137	212
40-49 歲	117	135	251
50-59 歲	145	86	231
60-69 歲	172	40	212
70 歲以上	159	14	173
總計	768	528	1,296

資料來源：本研究自行整理

二、衍生之個人及社會問題，以及其風險與危害之認知

本研究透過文獻檢閱先行鎖定了五大類網路衍生之社會問題，並以這五類問題為主進行網路調查，瞭解民眾對於這五類問題的「經驗」（是否遇過類似的危害？）、「問題程度認知」（認為該項危害有多嚴重？），以及「風險認知」（認為遇到該項問題的機率多高？）。相關統計如下所示。

（一）政治不實訊息

在政治不實訊息題組部分，加權後共計有 62.9％的民眾曾經在網路上接觸過政治相關的不實訊息。其次，有超過八成（84.6％）的民眾認為網路平臺上與政治相關的訊息很多都難以辨識真假。第三，有 86.9％的民眾認為政治上的不實訊息影響了每個人的判斷。第四，有 69％的民眾曾經看過電視新聞將擷取自網路平臺的訊息作為新聞加以報導。

最後，有 27.8％的民眾認為，電視新聞在報導擷取自網路平臺的訊息前，有做到多方的事實查核；65％的民眾則持不同意見，認為電視新聞在擷取網路平臺訊息並作成報導時，並沒有確實做到多方的事實查核。

上述結果顯示，民眾對於網路上發生之政治不實訊息多有所感，也認為其影響了每個人的判斷，是在經驗上、問題以及風險認知上都嚴重的問題類型。

表 44：民眾針對政治不實訊息的經驗、風險與危害認知

	我不曾在網路平臺上看到與政治相關的不實訊息				網路平臺上與政治相關的訊息很多都難以辨識真假				政治上的不實訊息影響了每個人的判斷			
	加權前		加權後		加權前		加權後		加權前		加權後	
	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比
非常同意	122	10.2%	117	9.8%	728	56.0%	714	54.9%	745	57.3%	750	57.7%
有點同意	226	19.0%	231	19.4%	380	29.2%	387	29.7%	400	30.7%	380	29.2%
有點不同意	316	26.5%	319	26.8%	95	7.3%	87	6.7%	76	5.8%	84	6.5%
非常不同意	434	36.4%	430	36.1%	47	3.6%	55	4.3%	42	3.2%	47	3.6%
不知道/無法回答	94	7.9%	94	7.9%	51	3.9%	58	4.4%	38	2.9%	39	3.0%
合計	1,192	100.0%	1,190	100.0%	1,301	100.0%	1,301	100.0%	1,301	100.0%	1,301	100.0%

資料來源：本研究自行整理

表 45：（續）民眾針對政治不實訊息的經驗、風險與危害認知

	我曾經看過電視新聞將擷取自網路平臺的訊息作為新聞報導				我認為電視新聞在報導擷取自網路平臺的訊息前，有做到多方的事實查核			
	加權前		加權後		加權前		加權後	
	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比
非常同意	489	37.6%	520	40.0%	128	9.8%	122	9.4%
有點同意	418	32.1%	378	29.0%	237	18.2%	239	18.4%
有點不同意	164	12.6%	156	12.0%	436	33.5%	423	32.5%
非常不同意	125	9.6%	128	9.9%	409	31.4%	422	32.5%
不知道/無法回答	105	8.1%	119	9.1%	91	7.0%	94	7.2%
合計	1,301	100.0%	1,301	100.0%	1,301	100.0%	1,301	100.0%

資料來源：本研究自行整理

（二）兒少網路安全

在兒少網路安全題組部分，有 54.6%的民眾家裡的未成年人曾有在網路平臺上接觸到色情或暴力內容的經驗。

相對地，有 78%的民眾認同網路平臺對於未成年人來說是很危險的環境，87.5%的民眾則認為未成年人在網路平臺上接觸到色情或暴力內容的機率很高。而且值得注意的是，兩個題目得到的意見強度都偏高，分別有 51.7%及 63.3%的受訪者選擇了強度最強的「非常同意」。

透過前述結果可知，在兒少網路安全的問題上，除了民眾的經驗本身已經超過半數，其經驗與問題及風險認知間也存在著相當顯著的差距。可以推斷，由於社會大眾普遍將兒少網路安全視為風險容受度低的嚴肅問題，其真實發生的後果難以承受，因此可以透過受訪者的回答觀察到問題認知與風險感受明顯高於經驗程度的現象。

表 46：民眾針對兒少網路安全的經驗、風險與危害認知

	家裡的未成年人曾經在網路平臺上接觸到色情或暴力內容				網路平臺對於未成年人來說是很危險的環境				未成年人在網路平臺上接觸到色情或暴力內容的機率很高			
	加權前		加權後		加權前		加權後		加權前		加權後	
	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比
非常同意	361	27.7%	337	25.9%	689	53.0%	672	51.7%	841	64.6%	824	63.3%
有點同意	355	27.3%	374	28.7%	346	26.6%	343	26.3%	317	24.4%	315	24.2%
有點不同意	153	11.8%	156	12.0%	156	12.0%	167	12.8%	72	5.5%	82	6.3%
非常不同意	214	16.4%	215	16.5%	86	6.6%	97	7.4%	43	3.3%	49	3.7%
不知道/無法回答	218	16.8%	219	16.8%	24	1.8%	22	1.7%	28	2.2%	32	2.4%
合計	1,301	100.0%	1,301	100.0%	1,301	100.0%	1,301	100.0%	1,301	100.0%	1,301	100.0%

資料來源：本研究自行整理

（三）網路交易安全

在網路交易安全題組部分，有 59.4％的民眾曾有在網路平臺上購物但卻被店家欺騙的經驗。其次，有 62.1％的民眾認為使用網路平臺進行消費買賣非常危險。最後，有 72％的民眾認為使用網路平臺交易被騙的機會很高，高於不這麼認為的 26.3％。

這個結果顯示，民眾對於網路交易安全多有所感，也認為確實有一定程度的交易風險，是在經驗上、問題以及風險認知上都嚴重的問題類型。但值得注意的是，雖然同意問題存在的比例頗高，但以強度來看的話，以最高強度回答問題的比例相較於其他問題類型來的低。

表 47：民眾針對網路交易安全的經驗、風險與危害認知

	我曾經在網路平臺上購物被賣家/店家欺騙				我認為使用網路平臺進行消費買賣非常危險				使用網路平臺交易被騙的機會很高			
	加權前		加權後		加權前		加權後		加權前		加權後	
	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比
非常同意	387	32.5%	386	32.4%	361	27.7%	357	27.4%	491	37.7%	467	35.9%
有點同意	324	27.2%	321	27.0%	469	36.0%	451	34.7%	469	36.0%	469	36.1%
有點不同意	237	19.9%	240	20.2%	349	26.8%	350	26.9%	253	19.4%	263	20.2%
非常不同意	163	13.7%	171	14.4%	94	7.2%	112	8.6%	68	5.2%	79	6.1%
不知道/無法回答	81	6.8%	72	6.1%	28	2.2%	32	2.5%	20	1.5%	23	1.8%
合計	1,192	100.0%	1,190	100.0%	1,301	100.0%	1,301	100.0%	1,301	100.0%	1,301	100.0%

資料來源：本研究自行整理

（四）網路霸凌

在網路霸凌題組部分，有 35.5%的人曾有被網路霸凌的經驗，而有 56.7%的人未曾被網路霸凌過。但有高達八成六（86.1%）的人認為網路平臺使霸凌行為更加嚴重，同時，不這麼認為的人只有 10.9%。最後，亦有 87.5%的人認為網路平臺的出現使現代人遭受霸凌的機會變高了。

這個結果顯示，網路霸凌是另一個風險容受程度低的問題類型。因此雖然實際經驗的民眾比例不高，但多數人已經認同這是個嚴重的社會問題，且網路平臺讓遭受霸凌的機會變高。

表 48：民眾針對網路霸凌的經驗、風險與危害認知

	我曾經有被網路霸凌的經驗（例：人身攻擊、肉搜）				網路平臺讓霸凌行為變得更嚴重				因為有網路平臺，現代人遭受霸凌的機會變高了			
	加權前		加權後		加權前		加權後		加權前		加權後	
	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比
非常同意	198	16.6%	203	17.1%	795	61.1%	796	61.2%	781	60.0%	773	59.4%
有點同意	243	20.4%	219	18.4%	344	26.4%	324	24.9%	379	29.1%	365	28.1%
有點不同意	309	25.9%	293	24.6%	72	5.5%	82	6.3%	68	5.2%	82	6.3%
非常不同意	349	29.3%	382	32.1%	52	4.0%	60	4.6%	43	3.3%	47	3.6%
不知道/無法回答	93	7.8%	93	7.8%	38	2.9%	38	3.0%	30	2.3%	34	2.6%
合計	1,192	100.0%	1,190	100.0%	1,301	100.0%	1,301	100.0%	1,301	100.0%	1,301	100.0%

資料來源：本研究自行整理

（五）使用者權益

在使用者權益題組部分，有 35.4%的人曾有在網路平臺上的言論被管理員刪除的經驗。值得注意的是，有 66.5%的人認為為了維護網路安全，政府或網路平臺有權力刪除不適當的言論是合理的，但也有 78.8%的人認為政府或網路平臺對不安全言論的管制會讓個人權益被侵害的可能性變高。

因此，政府或網路平臺在管制不安全或不適當的言論時，其中的力道拿捏需要非常注意。

表 49：民眾針對使用者權益的經驗、風險與危害認知

	我曾經有在網路平臺上的言論被管理員刪除的經驗				為了維護網路安全，我認為政府或網路平臺有權力刪除不適當的言論是合理的				政府或網路平臺對不安全言論的管制會讓個人權益被侵害的可能性變高			
	加權前		加權後		加權前		加權後		加權前		加權後	
	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比
非常同意	159	13.3%	142	12.0%	534	41.0%	505	38.8%	488	37.5%	491	37.7%
有點同意	288	24.2%	278	23.4%	355	27.3%	360	27.7%	532	40.9%	535	41.1%
有點不同意	298	25.0%	292	24.5%	172	13.2%	184	14.1%	144	11.1%	141	10.9%
非常不同意	323	27.1%	353	29.7%	199	15.3%	205	15.8%	87	6.7%	79	6.1%
不知道/無法回答	124	10.4%	124	10.4%	41	3.2%	47	3.6%	50	3.8%	55	4.2%
合計	1,192	100.0%	1,190	100.0%	1,301	100.0%	1,301	100.0%	1,301	100.0%	1,301	100.0%

資料來源：本研究自行整理

（六）綜合分析

前述的百分比可以看出民眾對於各類問題嚴重程度的認知，但從各類問題實際所獲得的分數平均，可以看出不同問題的強度。

本研究將每一個問題問項重新編碼，分數愈高代表嚴重程度愈高，依此計算每一個問題的認知強度，結果如下表。

表 50：問題強度分析

問題類型		樣本數	平均數	標準差	最小值	最大值
政治不實訊息	經驗	1,098	2.97	1.02	1	4
	問題程度認知	1,250	3.43	0.79	1	4
	風險認知	1,263	3.46	0.75	1	4
兒少網路安全	經驗	1,083	2.80	1.11	1	4
	問題程度認知	1,277	3.28	0.92	1	4
	風險認知	1,273	3.54	0.75	1	4
網路交易安全	經驗	1,111	2.84	1.06	1	4
	問題程度認知	1,273	2.86	0.91	1	4
	風險認知	1,281	3.08	0.89	1	4
網路霸凌	經驗	1,099	2.26	1.09	1	4
	問題程度認知	1,263	3.49	0.78	1	4
	風險認知	1,271	3.49	0.75	1	4
使用者權益	經驗	1,068	2.26	1.05	1	4
	問題程度認知	1,260	2.97	1.09	1	4
	風險認知	1,251	3.14	0.87	1	4

資料來源：本研究自行整理

從平均數來看，政治不實訊息、兒少網路安全、網路霸凌的問題認知與風險認知平均數都接近或是超過 3.3 分（滿分 4 分），是屬於嚴重群。網路交易安全以及使用者權益問題的問題認知與風險認知平均數則是在 3.0 附近或低於 3.0，在這五類問題中屬於問題強度較低的兩類問題。

從標準差來看，標準差愈小代表民眾在此題的共識程度愈高。政治不實訊息、兒少網路安全、網路霸凌同樣是標準差較小的三種問題，而網路交易安全以及使用者權益問題的標準差較其他三種問題高，表示共識程度略低。

從這個結果來看，政治不實訊息、兒少網路安全問題，以及網路霸凌問題，是三項具有較高社會共識且問題較為嚴重的三類問題。

三、網路及電視交互作用影響下之效果

本研究為了瞭解民眾使用網路與電視之交互行為對網際網路平臺衍生之社會問題可能有不同的認知，特別進行分析。本研究首先將民眾依照其網際網路與傳統電視使用行為分群：只使用網路（意指過去一個月內未曾使用傳統電視）、只使用傳統電視（意指過去一個月內未曾使用網際網路平臺），以及兩者皆使用（意指過去一個月內曾經使用網際網路平臺，亦曾使用傳統電視）。這三群的樣本人數分佈請見下表。

根據調查結果顯示，有 51.42％的受訪者在過去一個月內曾經使用網際網路平臺，亦曾使用傳統電視；只使用網際網路平臺的民眾有 43.51％，已接近半數；但只使用傳統電視的民眾僅有 5.8％。這個結果顯示，網路已經成為民眾日常生活的重要工具。

表 51：網際網路平臺使用模式（只使用網路、只使用傳統電視，或兩者都用）

使用情形	人數	比例（加權後）
只用網路	566	43.51%
只用傳統電視	66	5.08%
兩種都用	669	51.42%
總計	1,301	100%

資料來源：本研究自行整理

為了瞭解網路與傳統電視的使用行為是否對網際網路傳播社會問題以及風險認知有差異，本研究將第二部分「對網際網路傳播社會問題的認知」等相關題項與「對網際網路傳播社會問題的風險」等相關題項進行加總[893]，獲得「網際網路認知分數」，並以此分數針對三種不同的網際網路使用情形進行變異數分析（ANOVA）。

表 52：網際網路傳播社會問題「認知」之變異數分析（ANOVA）

使用情形	問題認知平均分數	標準差	分組人數
只用網路	31.92	4.63	492
只用傳統	33.59	5.53	34
兩種都用	33.02	4.55	612
總計	32.56	4.65	1,137

資料來源：本研究自行整理

有使用網路平臺的民眾對於網際網路社會問題嚴重程度的認知是三組中最低，只使用傳統電視的民眾對於網際網路傳播社會問題的認知為三組最高。進一步做 ANOVA 的後設檢定，發現只使用網路平臺的民眾對於網際網路社會問題的認知顯著較其他兩組低。

表 53：網際網路社會問題「經驗」之 t 檢定

使用情形	人數	平均數	標準誤	標準差	[95% conf.	interval]
只用網路	515	13.23	0.13	3.05	12.97	13.50
兩種都用	318	13.39	0.17	2.95	13.06	13.71
全體	833	13.29	0.10	3.01	13.09	13.50
diff		-0.15	0.21		-0.58	0.27
						t=0.72（p>0.05）

資料來源：本研究自行整理

[893] 該題組共分為「對政治不實訊息」、「網路霸凌」、「兒少網路安全問題」、「網路交易安全問題」，以及「個人權益侵害問題」之認知與風險，共 10 題。經過 Cronbach’s alpha 信度測試，alpha 值為 0.71，信度值為高，表示該題組測量之問題面向相同，因此可進行加總，並以加總所產生之新變數作後續分析。

本研究另外針對實際經驗網際網路社會問題的程度與網際網路平臺使用情形的差異進行分析。本研究發現，只使用網路平臺和同時使用網路平臺與傳統電視遇到網際網路社會問題的平均數 t 檢定未達顯著標準，表示兩群民眾實際經驗網際網路社會問題的程度沒有顯著差異。換言之，同時使用傳統電視和網際網路並不會加深、加重民眾對於網際網路傳播社會問題的感知，相反的，完全不使用網際網路平臺的民眾更容易認為網際網路平臺存在嚴重的社會問題。

四、民眾偏好的網路問題處理方式

（一）政治不實訊息

在政治不實訊息方面，民眾認為政府及網路平臺是主要的負責主體。加權後計有 61.3％的民眾認為「政府」應出面負責。第二高的是 20.9％的民眾認為是網路平臺該出面負責。

而在解決方法上，選擇由平臺管理員出面負責的民眾中有 50.9％的民眾認為網路上若流傳政治不實訊息，平臺管理員應主動巡視、判斷並處置。另，認為網路平臺應負起最大責任並出面解決的民眾中，有 40.2％的民眾認為網路平臺應要主動判斷並加註警語或降低排序。

認為該由政府出面負責解決政治不實訊息的民眾中，有 38.2％及 28.2％的民眾認為政府應派出單一／業務主管機關來判斷是否為不實訊息並決定是否阻斷、移除或裁罰。

面對政治不實訊息，民眾認為應出面負責的行為人及其應有之行為調查統計如下表。

表 54：面對政治不實訊息，民眾認為應出面負責者

您覺得在網路平臺上的「政治不實訊息」問題，誰應當負「最大的責任」，並出面處理？（複選）				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
網路使用者自己	177	13.6%	191	14.7%
網路平臺（例：FB、LINE 等）	260	20.0%	272	20.9%
政府機關	830	63.8%	797	61.3%
民間專業組織（例：台灣事實查核中心）	66	5.1%	73	5.6%
不知道/拒答	236	18.1%	245	18.8%
合計	1,301	100.0%	1,301	100.0%

資料來源：本研究自行整理

表 55：民眾認為網路使用者面對「政治不實訊息」的應有作為

您覺得網路使用者面對「政治不實訊息」的問題該如何處理？（單選）				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
自行提升對不實訊息的判斷能力	94	53.1%	101	52.7%
交由事實查核網站或 LINE 官方帳號	65	36.7%	70	36.7%
不必在意不實訊息的問題	13	7.3%	13	6.7%
不知道/拒答	5	2.8%	8	3.9%
合計	177	100.0%	191	100.0%

資料來源：本研究自行整理

表 56：民眾認為網路平臺管理員面對「政治不實訊息」的應有作為

您覺得網路平臺粉專管理員面對「政治不實訊息」的問題該如何處理？（單選）				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
由各粉專管理員 主動巡視、判斷並處置	139	53.5%	138	50.9%
由各粉專管理員 依投訴判斷並處置	111	42.7%	124	45.5%
不知道/拒答	10	3.8%	10	3.6%
合計	260	100.0%	272	100.0%

資料來源：本研究自行整理

表 57：民眾認為網路平臺面對「政治不實訊息」的應有作為

您覺得網路平臺面對「政治不實訊息」的問題該如何處理？				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
主動判斷 並加註警語或降低排序	102	39.2%	109	40.2%
主動判斷並移除	106	40.8%	102	37.6%
依投訴判斷 並加註警語或降低排序	26	10.0%	31	11.5%
依投訴判斷並移除	14	5.4%	18	6.5%
不知道/拒答	12	4.6%	11	4.1%
合計	260	100.0%	272	100.0%

資料來源：本研究自行整理

表 58：民眾認為政府面對「政治不實訊息」的應有作為

您覺得政府面對「政治不實訊息」的問題「最應該」如何處理？				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
由單一主管機關判斷是否為不實訊息並決定是否阻斷、移除或裁罰	335	40.4%	305	38.2%
由業務主管機關判斷是否為不實訊息並決定是否阻斷、移除或裁罰	238	28.7%	225	28.2%
由法院判斷是否為不實訊息並決定是否阻斷、移除或裁罰	197	23.7%	207	26.0%
不知道/拒答	60	7.2%	61	7.6%
合計	830	100.0%	797	100.0%

資料來源：本研究自行整理

表 59：民眾認為民間組織面對「政治不實訊息」的應有作為

您覺得民間組織面對「政治不實訊息」的問題該如何處理？				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
由民間專業組織針對違規者提出警告，並公布名單	4	6.1%	5	6.4%
由民間專業組織針對違規者通報平臺或主管機關	15	22.7%	17	23.7%
由民間專業組織要求平臺提供第三方認證的透明度報告	23	34.8%	26	35.3%
由民間專業組織向提供不實訊息（假新聞）的平臺進行裁罰	22	33.3%	23	31.7%
不知道/拒答	2	3.0%	2	2.8%
合計	66	100.0%	73	100.0%

資料來源：本研究自行整理

（二）兒少網路安全

在兒少網路安全方面，民眾認為政府及網路平臺是主要的負責主體。加權後計有 50.9%的民眾認為「政府」應出面負責。第二高的是 34.9%的民眾認為是網路平臺該出面負責。

而在解決方法上，認為網路平臺應負起最大責任並出面解決的民眾中，有 63.0%的民眾認為網路上若發生有害兒少網路安全的內容，網路平臺應要主動判斷並移除。

至於認為應由政府出面解決的民眾中，有 49.2%認為政府應派出單一主管機關判斷是否為兒少網路安全問題並決定是否阻斷、移除或裁罰。

面對兒少網路安全，民眾認為應出面負責的行為人及其應有之行為調查統計如下表。

表 60：面對兒少網路安全，民眾認為應出面負責者

您覺得在網路平臺上的「兒少網路安全」問題，誰應當負「最大的責任」，並出面處理？（複選）				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
網路使用者自己／父母／長輩	264	20.3%	271	20.8%
網路平臺 （例：FB、LINE 等）	446	34.3%	454	34.9%
政府機關	719	55.3%	662	50.9%
民間專業組織 （例：台灣事實查核中心）	31	2.4%	36	2.8%
不知道/拒答	184	14.1%	212	16.3%
合計	1,301	100.0%	1,301	100.0%

資料來源：本研究自行整理

表 61：民眾認為網路使用者面對「兒少網路安全」問題的應有作為

您覺得網路使用者面對「兒少網路安全」的問題該如何處理？				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
監控家中兒少網路平臺使用情形	65	24.6%	67	24.8%
主動學習辨識和協助兒少過濾危險的網路內容	192	72.7%	197	72.8%
不知道/拒答	7	2.7%	7	2.5%
合計	264	100.0%	271	100.0%

資料來源：本研究自行整理

表 62：民眾認為粉專管理員面對「兒少網路安全」問題的應有作為

您覺得粉專管理員面對「兒少網路安全」的問題該如何處理？				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
由各粉專管理員主動巡視、判斷並處置會危害兒少的網路內容	304	68.2%	308	67.9%
由各粉專管理員依投訴判斷並處置會危害兒少的網路內容	127	28.5%	129	28.4%
不知道/拒答	15	3.4%	17	3.7%
合計	446	100.0%	454	100.0%

資料來源：本研究自行整理

表 63：民眾認為網路平臺面對「兒少網路安全」問題的應有作為

您覺得網路平臺面對「兒少網路安全」的問題該如何處理？				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
主動判斷並加註警語或降低排序	114	25.6%	126	27.7%
主動判斷並移除	293	65.7%	286	63.0%
依投訴判斷並加註警語或降低排序	17	3.8%	20	4.4%
依投訴判斷並移除	11	2.5%	12	2.6%
不知道/拒答	11	2.5%	11	2.3%
合計	446	100.0%	454	100.0%

資料來源：本研究自行整理

表 64：民眾認為政府面對「兒少網路安全」問題的應有作為

您覺得政府面對「兒少網路安全」的問題「最應該」該如何處理？				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
由單一主管機關判斷是否為兒少網路安全問題並決定是否阻斷、移除或裁罰	362	50.3%	326	49.2%
由業務主管機關判斷是否為兒少網路安全問題並決定是否阻斷、移除或裁罰	191	26.6%	170	25.6%
由法院判斷是否為兒少網路安全問題並決定是否阻斷、移除或裁罰	130	18.1%	130	19.7%
不知道/拒答	36	5.0%	36	5.5%
合計	719	100.0%	662	100.0%

資料來源：本研究自行整理

表 65：民眾認為民間組織面對「兒少網路安全」問題的應有作為

您覺得民間組織面對「兒少網路安全」的問題該如何處理？				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
由民間專業組織針對違規者提出警告，並公布名單	6	19.4%	8	20.7%
由民間專業組織針對違規者通報平臺或主管機關	5	16.1%	7	18.0%
由民間專業組織要求平臺提供第三方認證的透明度報告	10	32.3%	13	36.3%
由民間專業組織向提供兒少網路安全問題的平臺進行裁罰	8	25.8%	8	21.2%
不知道/拒答	2	6.5%	1	3.8%
合計	31	100.0%	36	100.0%

資料來源：本研究自行整理

（三）網路交易安全

在網路交易安全方面，民眾認為政府及網路平臺是主要的負責主體。加權後計有 44.6%的民眾認為「網路平臺」應出面負責。第二高的是 41.6%的民眾認為是政府該出面負責。

而在解決方法上，認為網路平臺應負起最大責任並出面解決的民眾中，有 59.1%的民眾認為網路上若有危害網路交易安全的內容，網路平臺應要主動判斷並移除。

至於認為政府應出面解決網路交易安全問題的民眾中，有 42.9%的民眾認為政府應派出單一主管機關來判斷是否具有網路交易安全的風險，並決定是否阻斷、移除或裁罰。

面對網路交易安全，民眾認為應出面負責的行為人及其應有之行為調查統計如下表。

表 66：面對網路交易安全，民眾認為應出面負責者

您覺得在網路平臺上的「網路交易安全」問題，誰應當負「最大的責任」，並出面處理？（複選）				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
網路使用者自己	180	13.8%	168	12.9%
網路平臺 （例：FB、LINE 等）	570	43.8%	580	44.6%
政府機關	555	42.7%	541	41.6%
民間專業組織 （例：台灣事實查核中心）	76	5.8%	65	5.0%
不知道/拒答	184	14.1%	196	15.1%
合計	1,301	100.0%	1,301	100.0%

資料來源：本研究自行整理

表 67：民眾認為網路使用者面對「網路交易安全」問題的應有作為

您覺得網路使用者面對「網路交易安全」的問題該如何處理？				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
提升自己辨識網路詐騙、釣魚網站等的判斷能力，並提醒自己網路上的交易都具有風險，購物前務必三思	144	80.0%	135	80.4%
不要在網路平臺上購物	36	20.0%	33	19.6%
合計	180	100.0%	168	100.0%

資料來源：本研究自行整理

表 68：民眾認為粉專管理員面對「網路交易安全」問題的應有作為

您覺得網路平臺粉專管理員面對「網路交易安全」的問題該如何處理？				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
由各粉專管理員主動巡視、判斷並處置	348	61.1%	340	58.6%
由各粉專管理員依投訴判斷並處置	202	35.4%	218	37.6%
不知道/拒答	20	3.5%	22	3.7%
合計	570	100.0%	580	100.0%

資料來源：本研究自行整理

表 69：民眾認為網路平臺面對「網路交易安全」問題的應有作為

您覺得網路平臺面對「網路交易安全」的問題該如何處理？				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
主動判斷並加註警語或降低排序	165	28.9%	159	27.4%
主動判斷並移除	330	57.9%	343	59.1%
依投訴判斷並加註警語或降低排序	23	4.0%	25	4.3%
依投訴判斷並移除	30	5.3%	36	6.2%
不知道/拒答	22	3.9%	18	3.0%
合計	570	100.0%	580	100.0%

資料來源：本研究自行整理

表 70：民眾認為政府面對「網路交易安全」問題的應有作為

您覺得政府面對「網路交易安全」的問題該如何處理？				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
由單一主管機關判斷是否具有網路交易安全的風險，並決定是否阻斷、移除或裁罰	238	42.9%	231	42.6%
由業務主管機關判斷是否具有網路交易安全的風險並決定是否阻斷、移除或裁罰	166	29.9%	151	27.9%
由法院判斷是否具有網路交易安全的風險並決定是否阻斷、移除或裁罰	117	21.1%	126	23.2%
不知道/拒答	34	6.1%	34	6.3%
合計	555	100.0%	541	100.0%

資料來源：本研究自行整理

表 71：民眾認為民間組織面對「兒少網路安全」問題的應有作為

您覺得民間組織面對「網路交易安全」的問題該如何處理？				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
由民間專業組織針對違規者提出警告，並公布名單	17	22.4%	15	23.1%
由民間專業組織針對違規者通報平臺或主管機關	24	31.6%	22	34.4%
由民間專業組織向未處理好網路交易安全問題的平臺進行裁罰	33	43.4%	26	40.5%
不知道/拒答	2	2.6%	1	2.1%
合計	76	100.0%	65	100.0%

資料來源：本研究自行整理

（四）網路霸凌

在網路霸凌方面，民眾認為政府及網路平臺是主要的負責主體。加權後計有 49.9%的民眾認為「政府」應出面負責。第二高的是 33.2%的民眾認為是網路平臺該出面負責。

而在解決方法上，認為網路平臺應負起最大責任並出面解決的民眾中，有 61.6%的民眾認為網路上若有網路霸凌發生，網路平臺應要主動判斷並移除。

至於認為政府應負起最大責任並出面解決網路霸凌問題的民眾中，有 37.2%的民眾認為政府應派出單一主管機關判斷是否為網路霸凌問題並決定是否阻斷、移除或裁罰。

面對網路霸凌，民眾認為應出面負責的行為人及其應有之行為調查統計如下表。

表 72：面對網路霸凌，民眾認為應出面負責者

您覺得在網路平臺上的「網路霸凌」問題，誰應當負「最大的責任」，並出面處理？				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
網路使用者自己／父母／長輩	137	10.5%	147	11.3%
網路平臺 （例：FB、LINE 等）	410	31.5%	432	33.2%
政府機關	695	53.4%	649	49.9%
民間專業組織 （例：台灣事實查核中心）	23	1.8%	27	2.0%
不知道/拒答	246	18.9%	268	20.6%
合計	1,301	100.0%	1,301	100.0%

資料來源：本研究自行整理

表 73：民眾認為網路使用者面對「網路霸凌」問題的應有作為

您覺得網路使用者面對「網路霸凌」的問題該如何處理？				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
自行提升對網路霸凌的認知與辨別能力，並提醒自己不製造、不跟隨、不傳播、不被影響	125	91.2%	135	91.3%
不必在意網路霸凌的問題	9	6.6%	9	6.3%
不知道/拒答	3	2.2%	4	2.4%
合計	137	100.0%	147	100.0%

資料來源：本研究自行整理

表 74：民眾認為網路平臺粉專管理員面對「網路交易安全」問題的應有作為

您覺得網路平臺粉專管理員面對「網路霸凌」的問題該如何處理？				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
由各粉專管理員主動巡視、判斷並處置	265	64.6%	282	65.2%
由各粉專管理員依投訴判斷並處置	137	33.4%	144	33.4%
不知道/拒答	8	2.0%	6	1.4%
合計	410	100.0%	432	100.0%

資料來源：本研究自行整理

表 75：民眾認為網路平臺面對「網路霸凌」問題的應有作為

您覺得網路平臺面對「網路霸凌」的問題該如何處理？？				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
主動判斷並加註警語或降低排序	108	26.3%	113	26.1%
主動判斷並移除	252	61.5%	266	61.6%
依投訴判斷並加註警語或降低排序	13	3.2%	11	2.5%
依投訴判斷並移除	28	6.8%	35	8.1%
不知道/拒答	9	2.2%	8	1.8%
合計	410	100.0%	432	100.0%

資料來源：本研究自行整理

表 76：民眾認為政府面對「網路霸凌」問題的應有作為

您覺得政府面對「網路霸凌」的問題該如何處理？				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
由單一主管機關判斷是否為網路霸凌問題並決定是否阻斷、移除或裁罰	267	38.4%	240	37.2%
由業務主管機關判斷是否為網路霸凌問題並決定是否阻斷、移除或裁罰	185	26.6%	167	25.9%
由法院判斷是否為網路霸凌問題並決定是否阻斷、移除或裁罰	214	30.8%	216	33.4%
不知道/拒答	29	4.2%	23	3.6%
合計	695	100.0%	646	100.0%

資料來源：本研究自行整理

表 77：民眾認為民間組織面對「網路霸凌」問題的應有作為

您覺得民間組織面對「網路霸凌」的問題該如何處理？				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
由民間專業組織針對違規者提出警告，並公布名單	6	26.1%	7	25.9%
由民間專業組織針對違規者通報平臺或主管機關	2	8.7%	3	11.8%
由民間專業組織要求平臺提供第三方認證的透明度報告	4	17.4%	5	19.2%
由民間專業組織向提供網路霸凌問題的平臺進行裁罰	11	47.8%	11	43.1%
合計	23	100.0%	27	100.0%

資料來源：本研究自行整理

（五）使用者權益

在使用者權益方面，民眾認為若使用者權益受到限制，可透過平臺所建立之內部異議機制進行申訴（35.1%）。其次，可透過向業務主管機關申訴，由業務主管機關負責處理相關紛爭（25.1%）。

另外，也有 20.4%的民眾認為可透過訴訟，由法院判定使用者權益是否有被限制。

面對使用者權益受侵害，民眾認為可維護權利的方式調查統計如下表。

表 78：在使用者權益上，民眾認為可維護權利的方式

您覺得當使用者被限制時（例如：平臺處理違規事情有誤），應以何種方式來進行申訴或維護權利？（例如：民眾張貼在社群平臺上之貼文無故被移除、移除理由不合理，或帳號被停權卻未被告知任何理由）				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
透過平臺所建立之內部異議機制進行申訴	461	35.4%	456	35.1%
向業務主管機關申訴，由業務主管機關負責處理相關紛爭	336	25.8%	327	25.1%
由民間專業組織，處理相關紛爭	140	10.8%	137	10.5%
透過訴訟，由法院判定使用者權益是否有被限制	268	20.6%	265	20.4%
不知道/拒答	96	7.4%	116	8.9%
合計	1,301	100.0%	1,301	100.0%

資料來源：本研究自行整理

（六）擴充題－串流影音服務

針對使用串流影音服務時之消費爭議經驗，在近一個月內有使用串流影音服務的民眾中，有 90.5%的民眾未曾有過消費爭議，2.4%的民眾則表示不知道／拒答。其餘民眾遭遇之爭議類型依比例高低為：「退訂」(3.4%)、「續訂」(2.3%)、「無法聯繫上客服」(1.7%)、「服務不穩定或無預警中斷」(1.1%)，以及「信用卡資料外洩」(0.6%)。

由此顯示，過往主管機關於擬定串流影音服務政策時所強調的「消費者保護議題」，在當前未立「專法」的情形下，平臺業者普遍透過《消費者保護法》體系之規制及產業自律之努力，已甚少（不到 10%）發生消保爭議。

當然，這不代表政府不應持續透過制度減少消費爭議之發生；但這約 10%之消費爭議數據，也並不表示這些爭議最後沒有透過業者的自願性讓步（如購買單片 VOD 或訂閱包月制服務卻無觀看紀錄，聯繫業者後允為退費）、或《消費者保護法》體系（如經消保官處理）獲得圓滿的解決。進一步的數據，或許本研究可以透過之後的「網路調查」加以探索。

而在曾經遭遇過串流影音服務消費爭議之民眾中，多數人認為「無法聯繫上客服」是最需要解決的爭議類型(32.4%)，其餘則為「續訂」(23.5%)、「退訂」(12.6%)、「服務不穩定或無預警中斷」(11.0%)，以及信用卡資料外洩(3.5%)。另有 17.0%表示不知道／拒答。

另一方面，針對政府在此議題可著力之處，在近一個月內有使用串流影音服務的民眾中，多數認為政府最需要採取之措施為「立法課予服務提供者相關義務」，例如要求業者公告服務使用條款(43.3%)，以及「設立單一窗口，作為處理串流影音服務消費爭議的專責機構」(43.1%)，其次為「透過該產業的公協會轉介，以業者自律之方式處理」(8.6%)。

表 79：民眾使用串流影音服務時之消費爭議經驗

在使用串流影音服務時，您是否曾經遭遇過消費爭議？【複選題】				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
退訂（例如：介面上找不到退訂功能，須致電客服處理）	9	2.6%	13	3.4%
續訂（例如：無法更換付費方案，或自動續訂時被重複扣款）	7	2.0%	9	2.3%
服務不穩定或無預警中斷	2	0.6%	4	1.1%
信用卡資料外洩	2	0.6%	2	0.6%
無法聯繫上客服	6	1.7%	6	1.7%
未曾有過消費爭議	320	92.0%	350	90.5%
不知道/拒答	7	2.0%	9	2.4%
合計	348	100.0%	387	100.0%

資料來源：本研究自行整理

表 80：曾有串流影音服務消費爭議經驗之民眾認為最需解決之爭議類型

承上題，在您回答的消費爭議類型中，您認為最需要解決的是？				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
退訂（例如：介面上找不到退訂功能，須致電客服處理）	3	14.3%	3	12.6%
續訂（例如：無法更換付費方案，或自動續訂時被重複扣款）	6	28.6%	6	23.5%
服務不穩定或無預警中斷	1	4.8%	3	11.0%
信用卡資料外洩	1	4.8%	1	3.5%
無法聯繫上客服	7	33.3%	9	32.4%
不知道/拒答	3	14.3%	5	17.0%
合計	21	100.0%	27	100.0%

資料來源：本研究自行整理

表 81：民眾認為政府面對流影音服務消費爭議最需要採取之措施

您認為政府面對「串流影音服務的消費爭議」最需要採取的措施為何？（先不提示，回答不出來再一口氣提示選項 01-03）				
	加權前		加權後	
	樣本數	百分比	樣本數	百分比
立法課予服務提供者相關義務（例如：要求業者公告服務使用條款）	154	44.3%	167	43.3%
設立單一窗口，作為處理串流影音服務消費爭議的專責機構	141	40.5%	167	43.1%
透過該產業的公協會轉介，以業者自律之方式處理	34	9.8%	33	8.6%
不知道/拒答	19	5.5%	20	5.1%
合計	348	100.0%	387	100.0%

資料來源：本研究自行整理

（七）民眾偏好的整體發現

綜上所述，在本研究觀察到的網路危害中，多數民眾傾向由「政府」及「網路平臺」來作為負責主體，出面解決相關問題。同時，民眾也期待政府及網路平臺能主動並積極地調查是否有政治不實訊息，或有兒少網路安全、網路交易安全、網路霸凌、使用者權益受侵害等地問題，希望以此來維護網路安全。

然而，民意調查上的「多數」不代表就是公共政策的最佳選擇，僅是在提供給民眾的民調選項中，民眾的直覺選擇。舉例來說，在政治不實訊息這個問題類別中，認為「應該要由政府出面處理的占了 61.3%，而且這 61.3%的人當中又有 38.2%的人希望由單一主管機關判斷是否要阻斷、移除或裁罰」，這是一個絕對多數，然而若直接把這樣的答案解讀為「民眾就是希望政府出面，因此政府一定要由單一主管機關出面主導並解決問題」，可能過度簡化這個民調的結果。

搭配其他網際網路社會問題民眾偏好出面解決問題的對象來看，雖然偏好政府出面解決的比例為多，但偏好平臺與業者出面的比例亦不小，整體來說並未有顯著的社會共識。此外，電話民調因為題目題型、數量的限制，並未能針對政府與業者、平臺能負責的方式進一步調查，因此要將此結果簡化成一定要由單一主管機關出面主導並解決問題，並不適當。

電訪結果由政府出面占多數，可能暗示著民眾對政府擁有更強大資源和權力，能夠更有效地解決網路問題的期待。此外，民眾可能認為政府應該在網路治理中發揮更積極的角色，但並不一定排除其他利益相關者的參與和作用。因此，雖然多數民眾希望政府出面主導，但這並不意味著他們不支持其他機構或組織參與解決問題，而是認為政府在其中扮演著核心和關鍵的角色。因此，政府在滿足民眾期望的同時，也應該與其他利益相關者密切合作，以制定全面、有效的網路治理策略。

如進一步依照問題的類型討論，政治不實訊息、兒少網路安全問題、網路霸凌問題是民眾希望主要由政府機關出面處理比例較高的問題類型。這三個問題類型剛好屬於本研究歸納為「問題強度高」的問題類型。因此本研究認為較為合適的解讀方式是：當問題強度高，民眾期待政府能介入，民眾希望看到政府能有所做為。但至於政府該如何作為，尚待進一步討論。

至於「問題強度低」的問題類型，例如網路交易安全以及使用者權益保障，從電訪民調的結果來看，民眾將這樣的責任歸咎於網路平臺的比例較高，也希望網路平臺能夠以「主動巡視」的方式介入管理。這樣的結果顯示，我國的民眾對於問題解決方式的偏好相當直接，民眾期望找到一個負責的對象，並期待這個對象直接以具體的手段解決問題。

電訪的調查結果提供本案兩個主要的訊息：

（1）網路社會問題需要有明確的負責對象：民眾認為政治不實訊息、兒少網路安全問題、網路霸凌問題等三項屬於「問題強度高」的類型，希望政府有所做為。網路交易安全問題、使用者權益保障問題等二項屬於「問題強度低」的類型，但也希望由網路平臺以主動巡視的方式解決問題。

（2）應該負責的對象應當如何負責，尚須進一步研議。電訪的結果因為問卷調查的限制，僅能呈現概略的偏好，但實際解決辦法需要相當多的細節，是電話訪問的結果無法概括的。因此更多面向的研究資料與多方的對話是找到解決辦法的關鍵。

基於上述整體發現，本研究將試圖提出一套解決網路社會問題的整合機制，並在第四章節中，透過公民團體與業者的訪談，以及多場焦點座談的資料，持續探究在這個多利害關係人的網際網路社會問題當中，各利害關係人可以扮演的角色。

五、各利害關係人角色分析

本研究透過前期的文獻資料分析，將與網際網路社會問題有關之利害關係人分為：平臺業者、政府機關、公民團體與民間專業組織，以及使用者個人。從一般民眾的電訪結果可知，民眾認為要解決網際網路社會問題，主要的角色應該在政府機關和平臺業者身上，本研究另外透過與公民團體和業者的訪談，以及多場的焦點團體，希望能夠找到更多的可能性以及獲知更詳細的細節。

以下，本研究將從訪談以及焦點座談的資料，分析各種利害關係人在網際網路社會問題的處理當中可扮演的角色。

（一）平臺業者

網路平臺，無論是社群媒體、通訊軟體、或是拍賣平臺等，都提供了一個使網路使用者互相交流的管道，由此也延伸出許多網路危害。

1. 平臺業者的角色：依訪談及電訪結果

本研究根據訪談紀錄及電訪問卷之結果，試整理以下三種在處理網路危害議題上，平臺業者所需扮演的角色：

（1）整合需求

在進行網際網路治理時，平臺作為一個中介角色，除了處理各方的需求和利益外，自身也具備一系列特定需求和目標。為了有效表達這些需求，平臺應採取多種方式。首先，透明溝通是非常重要的，平臺應與相關利益相關者，包括政府、企業、公民社會組織等，建立透明的溝通管道，以表達自身的需求和立場。

我們也會去看使用者的回應，因為我們站上有很多檢舉或是可以跟客服溝通的管道。所以大家會把用戶的這些 feedback 收進來，然後去看說，我們是不是在哪些營運上要去做調整，所以它同時是有很多的，怎麼講，很多的組成，那像我自己，我們公司是沒有直接做 GR 單位，但是譬如說像我是 PR，GR、IR 等等一起做。所以我們也會去參加，像 iWIN 他

們會有一些，多方利害關係人的會議，然後他們就會給我們很多建議。譬如說NGO 會說，我們覺得應該怎麼樣，那我們確實都會把這些帶回來，然後去調整我們的站規。像之前有一個類似是數位女力，就是比較女性的組織，它就覺得說，如果我們刪掉了跟兒少權益相關的文章，我們必須應該要註明，它覺得這樣會比較好，不要只寫其它。它覺得寫出來，這樣其它用戶就會知道說，因為這一個文章內容，侵害了兒少的權益，所以它被刪除了，那它某種程度上也具有教育意涵。所以說那這個也蠻好的，所以我們就因為這樣，特別去新增了一個「刪除文章的原因」。所以我想要說的是說，這個來源是很多面向的，我們不見得是一個會議中就完全決定的，是從很多的來源，然後共同再去修改我們的一個政策。(F1)

透過多次的溝通，平臺能夠與其他利益相關者建立更深入的共識，消除可能存在的誤解，並找到更符合各方利益的解決方案。同時，重複表達需求可以提高平臺需求的重要性和優先性。在長期的溝通過程中，可能會有新的議題出現，或者政策和法規發生變化，多次表達需求可以使平臺及時調整立場，並符合不斷變化的環境。整體而言，多次表達需求有助於確保平臺的聲音被聽取和尊重，並能夠更有效地參與網際網路治理過程，建構推動更好的環境和推動整體共同發展。

（2）形成自律規範

網路業者建立自律公約可以避免過度立法、增加業者的自主性，並將業者自律作為業務發展的一部分。這樣的公約有助於提高網路平臺業者對於社會責任感，同時建立更可靠的用戶體驗。

首先平臺業者自律公約的原則與內容，平臺業者在建立自律公約時應依循一些基本原則，包含透明度報告、消費者保護與服務提供。網路平臺業者必須清楚的告知用戶其使用條款、隱私政策和相關規定，讓用戶能夠清楚理解平臺的運作方式。此外，資訊保護也是不可忽視的一環，業者需要確保用戶資料的安全和隱私不受侵犯。保障用戶權益是自律公約的核心，網路平臺業者應該建立有效的投訴機制和

澄清程序，以處理用戶的投訴和疑慮。

其次，業者在制定自律公約與執行的過程十分關鍵，建立自律公約必須是以多方參與的方式來進行。在制定過程中，業者應與用戶、學界和相關政府機構進行積極溝通和合作，也可與民間專業組織討論相關自律公約規範的內容，以獲得多元的意見。也需進一步思考未來業者對公約的執行，業者的自律措施是否有效實施，以及適時的提出改進建議。隨著科技和社會環境的不斷變化，自律公約也應不斷進行修訂和更新，以確保其持續適用。

最後，對於平臺業者建立自律公約後的效果評估與修訂也相當重要，必須建立評估機制來檢視其實施效果。透過追蹤投訴數量的變化、用戶滿意度調查等，來瞭解自律公約對平臺和用戶的影響。平臺業者也刻透過定期討論社會上發生的一些個案來擬定相關策略，建立相關解決機制，並且根據評估結果，業者及時修訂和改進自律公約，以使其能夠更好地適應不斷變化的網路環境，並繼續保護用戶的權益。

綜上所述，建立網路平臺業者自律公約不僅僅只是保護用戶的權益，更可維護業者信譽的關鍵一環。透過明確的原則和內容，以及多方參與的制定過程，可以確保自律公約的有效實施和適應性。藉由民間專業組之來監督自律公約執行與建議，並持續評估和修訂公約，網路平臺業者將更加成為社會負責任的角色，同時為用戶提供更安全、可靠的網路環境。

（3）對使用者負責，並落實消費者保護

在處理網路危害內容上，平臺業者除了需表達自身需求，和形成自律規範外，最重要的就是要落實消費者保護，對廣大的網路使用者負責。

平臺業者對消費者所需負的責任又可分為「直接責任」與「間接責任」兩種：直接責任指，平臺業者在提供服務時，因自己的行為造成他人的權利受到侵害或損失，則平臺必須負直接侵權責任。而間接責任則指，平臺使用者或他人的行為造成第三方的權利受到侵害或損

失，雖平臺業者本身並無從事侵權行為，但仍需負起責任的型態[894]。

2. 平臺業者的角色：本研究建議

承上，根據「直接責任」與「間接責任」兩種責任型態，本研究認為，網路平臺業者所扮演的角色為：

（1）形成自律規約

在管理網路危害的議題上，政府的責任是建立完善的管理框架、對平臺課予責任，而平臺業者的責任是依照框架形成自律規約，並落實執行。至於此一框架的具體內容，則可說是平臺業者的自律規約，可由平臺業者共同組成之產業公會或值得信賴之協力組織協調各平臺業者、公民團體、政府機關等相關利害關係人共同協議而成。

舉例而言，在焦點座談民眾場中曾有民眾提及，現階段應先建立出一套網路基準法，並可參考《勞動基準法》的管理模式，將所應該管理的網路問題、該出手解決的網路危害，或是業者該做到的消費者保護權益救濟措施，都寫進去管理辦法中。將底線畫好之後，留與平臺業者自行訂定管理辦法，交給主管機關備查，再由政府及民眾作為監督執行。換言之，政府作為把關者，平臺作為管理者。若是平臺業者沒有做到管理辦法提及的事項，那麼政府就會出手介入，同時，民眾也可以去檢舉平臺違反管理辦法。

> *就是應該就是說就像勞基法，他們有一個規定說，你就是要給勞工什麼什麼，然後發下去，給各個企業的人資，你就是要做這樣，如果你沒有做到，下面的人就可以去告你。對，他政府就要出手，所以最主要還是政府要去把關。（M8）*

> *政府會立勞動基準法，然後公司會制定自己的工作規則，政府核可公司內部的工作規則，那如果推到網路上就變成政府立一個網路基準法，然後想要創造平臺的人設定自己平臺*

[894] 參見張淑美，網路服務業者之侵權責任–以著作權侵權為中心，交通大學科技法律研究所碩士論文（2006）。

的內部規則到政府去做核備，然後完成以後這個平臺才能設立，這個平臺的使用者就有點像受僱這個平臺的工作員，然後當他被這個工作做裁罰的時候，可能有個第三方的，在勞動基準法上它是一個勞檢單位，那這邊可能就是網路檢查單位，你可以去那邊做申訴，如果對於平臺的裁罰你覺得不滿意的話，可能就會有一個類似第三方的東西，它其實是兩個類似的概念並存，只是一個是放在勞動法令上，一個是放在網路法令上。(M5)

可能就是政府要用一個法，就像勞基法一樣，他就是說，你一定要做到這些這些弄出去，他公會也是去幫忙做執行。就是有點算是政府是老大，公會是老二。OK，他老二去弄，老二弄了不行之後，老大就要出手了。(M8)

只是這樣一個網路基準法的模式，在政策形成初期就應該廣納業者以及各方民眾、公民團體的意見，因為什麼問題應該被納入歸管、每一個問題的底線在哪裡，依然必須要所有利害關係人的共識。

至於自律規約的內容，可以包含平臺對於假帳號的控管、完整的平臺使用規範（訪談記錄：A、F），以及與政府聯防配合的方式等（訪談紀錄：H、G）。上述內容僅為可以考慮的規約內容，至於實際的細節應由業者自行訂定產生。

（2）與各方利害關係人共同協力

單一的平臺業者難以形成網路的完整秩序，必須靠多數的平臺業者、政府機關、公民團體、各方使用者共同研議；同時，因為網路的科技、環境變遷速度快，業者所形成之自律規約必須在一定的機制底下定期的研討修正、滾動式發展。

值得注意的是，研究調查發現，不論是平臺業者，或是民間專業組織，都十分認同 iWIN 在兒少方面所建立的機制，並認為這一套機制是大家都可依循、遵守，並擴大使用的。

在兒少這個領域其實 iWIN 的框架，其實算是行之有年，而且運作也好，然後其實我覺得我們在透過這機制的時候我們其實還滿好的去表達說我們能做到的事情是哪些，然後我們限制是哪些，讓實務上觀察到的問題有哪一些，所以我們其實有比較好的交流機制，然後就結論上來說我覺得兒少這題各方不管是政府，或是民間或產業都滿信賴這機制，所以我也覺得可能在思考類似問題的時候 maybe iWIN 是一個可以接近的一個 model，就是它是真的有效的一個自律而且是有實現就是讓不同的利害關係人都有機會在裡面有交流的機會，那我覺得這個是需要參考的。（G1）

因為 iWIN 的機制提供了平臺之間與政府機關、家長、使用者、各公民團體等相關利害關係人定期對話的機制，平臺業者多肯定這樣的對話機會是一個平等、協力、為一個目標共同努力的對話空間，頗能形成共識、產生協力。因此 iWIN 的模式應當考慮擴大成一般模式，將其他網際網路問題的處理納入，找到業者、政府、民眾都能接受的網路協力治理模式。

綜上，平臺業者身為一個提供服務的商家，落實使用者保護機制，並對使用者負責是平臺必不可躲的責任，而在這些網路危害問題上，也並非是平臺業者一人孤身戰鬥，政府與民間專業團體能給予適時的協助與支持。本研究期望能透過建立三方合作模式，來減少網路危害。

（二）民間專業組織與公民團體

隨著網際網路的迅速發展和普及，針對這五大網路社會議題中，民間專業組織和公民團體可以在緩解網路風險方面發揮關鍵作用。本研究認為民間專業組織和公民團體在應對網際網路風險方面可以扮演一個合作，提供助力的角色。透過民間專業組織來補足政府與平臺業者的不足，並且可以進一步的協調、整合業者，形成網路秩序，建立相關的自律機制。

本研究將從五大不同網路社會危害出發，並詳述民間專業組織和公民團體可扮演的角色如下：

首先，民間專業組織和公民團體在網際網路社會問題中可以發揮著重要的監督與倡導角色。透過民間專業組織可以關注並監督平臺業者的行為，確保其遵守相關規範。並且可以針對本研究中的五大社會問題提出倡議，促使相關平臺業者加強自律，保護用戶的權益。

其次，民間專業組織和公民團體能夠在教育與宣傳方面發揮積極作用。透過各種多元的教育宣導，向公眾傳遞有關網路使用風險的資訊，教導民眾能建立主動學習、辨識危險、遵守規範的能力。

媒體素養公民教育去讓這個民眾的這個使用的認知提高、閱讀的認知提高，然後發送訊息的時候他能夠知道，他的行為對行為本身的這個理解的能力也提高。所以，就公民素養的能力，這個基金會一直在推。(C1)

例如在政治不實訊息的問題上提供民眾辨識訊息的真偽與近一步的去教育民眾如何去辨識，或者避免成為網路詐騙的受害者。除此之外，透過媒體素養公民教育提高民眾在對於網路暴力和仇恨言論、發送訊息等行為之認知。讓民眾不光單單只會辨識訊息而已，當民眾的媒體素養與資訊素養都有所成長時即能降低各項網路社會問題的產生。

再者，民間專業組織和公民團體可以與平臺業者以及政府來進行合作，以平臺業者來說，民間專業組織和公民團體可以針對各項不同的社會問題來給予平臺建議，受訪對象指出像現行 iWIN 的機制對於解決兒少網路安全問題已行之有年，這讓平臺在處理相關問題時會帶來很大的幫助。

我記得 iWIN 他們自己是因為他們跟很多業者有認識，然後他們另外一邊又是政府，所以變成他們的力量很大。那他們自己好像有做一個例示表，就是他們去詳細講說，兒童不宜的內容有哪些？（A1）

或者對於私人訊息傳送這類平臺業者難以介入的部分，民間專業組織可提供第三方的查核機制，運用在不同社會問題的專業性來彌補業者的不足。

此外，民間專業組織在政策制定方面與協助平臺建立自律公約也能扮演關鍵角色。民間專業組織可以積極參與與政府、產業和學術界的對話，就網際網路社會問題提出建議與政策意見。這些意見對於建立更有效的監管機制、建立良好網路環境和保護用戶權益至關重要。而平臺在建立相關自律公約時民間專業組織也能提出相關建議，以利業者的自律公約能更加完善，最終達到協助業者形成、整合產業秩序。

除了這些方面之外，受訪者也指出其實我國的民間專業組織已相當豐富，民間專業組織總期望能在網路社會問題上出一份心力，但往往會遇到心有餘而力不足的情況。

> *我會覺得民間專業組織自己的資源不夠，所以有時候需要靠政府把它列為一個議題多給一些資源，讓民間專業組織去從社會學、心理學這個角度去多培養就是說政府要給一些資源，資源這邊都可以給民間專業組織、可以去弄，它們要有一些這樣的單位，我覺得是有一些單位是有在做，但是常常看到民間的這個組織就很可惜資源不足（D1）*

民間專業組織的資源往往較為缺乏，不管是資金或者是技術上，這仍然需要更多資源的挹注，才能使民間專業團體發揮最大的作用。

總結來說，民間專業團體在網際網路社會問題中扮演著多重角色。民間專業團體可同時兼具監督與倡導平臺業者的行為，教育公眾保護自身權益，促進網路社會中的對話與理解，並提供相關政策制定建議，為建立更健康、安全和公正的網路空間做出了重要貢獻。這些努力都有助於實現一個更繁榮、平等且和諧的數位社會。

（三）政府機關

政府機關在消除相關網路社會危害亦扮演重要角色。本研究認為政府在這五大網路社會議題中，最重要的角色是扮演一個「規則的建立者」，將各類相關規範進行統合、整理，建立起一套具有整合性的法規，使各網路業者能在此大框架中受到相應的規範；民間機構能在此大框架中與公部門、私部門進行相應的合作與整合。最後，此一框架若建立起來，亦能使網路使用者受到相應的保護。

而本研究將政府機關區分為「主管機關」（如：數位發展部或NCC）；「協力機關」（如衛福部、內政部、金管會等各相關部會或地方政府），及「法院」。以下本研究將由五大不同網路社會危害出發，並詳述政府可扮演的角色如下：

1. 主管機關

（1）盤點現行法規，建立起相關法律架構，並課予平臺相關責任

本研究觀察現狀下五大網路社會問題，包含政治不實訊息、網路霸凌、兒少網路安全、網路交易安全及使用者權益被限制等，發現現階段並沒有一個能統管網路危害的單一法律，也尚無相關的法制框架出現，這使得相關的業者、民間組織與團體及民眾在遇到相關問題時，容易變成無頭蒼蠅，不曉得該向哪求助。受訪對象台灣線上影視產會就指出，台灣盜版產業難以消除的原因，就是因為沒有「法」。

那過去幾年我們一直在跟政府、警調單位一直在打盜版，但是盜版很難打，因為沒有，就是說沒有法律（B1）

此外，在法制的角度上，也都偏向各機關獨立立法的「分散式立法」。而分散式立法造成的副作用卻無法根治這些網路危害問題。首先，分散式立法容易讓各機關的立法互相打架，這反過頭來又使得業者遵從也不是，不遵從也不是。其次，過多且複雜的法律難以讓民眾了解。第三，為因應網路問題而倉促推行的法律並未經過業者和全體社會的充分討論，易形成弊端和灰色空間，業者在執行上有窒礙難行的問題。

舉例而言，有關兒少網路相關的影視分級制度，在傳統電視上有較為統一的標準與仔細的審查，但在串流影音平臺上，卻沒有一個較為統一的標準。產生此種問題的原因有二，其一，為年齡分級標準不一：例如，Netflix 的年齡分級為：7+、13+、16+與 18+，而同類型的業者 Disney+年齡分級卻是 G、PG、12+、15+與 18+。兒童福利聯盟文教基金會同樣指出，現在的分級太亂，以至於民眾很難知道該如何參考這樣的分級制度。其二，除了不同的年齡分級外，各媒體對影視作品的分級標準也不一，絕大多數的業者會依據影視作品製作當地的年齡標準來作為引入台灣時的年齡分級判斷依據，但有些國家審查較為寬鬆，有些國家審查較為嚴格，這也產生了有時候是歸類在「兒童可以觀賞」的節目其實不適合讓兒童來觀賞。尤有甚者，在業者時常為了追求「快速上架」而不會去仔細審查這樣的年齡分類適不適宜。

無一個統一的年齡分級標準也變相導致兒童時常接觸到許多不適合的節目，而家長亦會不知道該如何幫助兒童選擇較安全的節目，誠如兒童福利聯盟文教基金會所言：

> *就是我不是說它的節目一定要被審查，而是有一點不知道說他們現在這樣就是家長要怎麼幫兒少比較安全的選節目。（I1）*

> *那我們要不要至少先給家長一個可以參考的分級？（I1）*

本研究認為，無論是打詐、打假、兒少保護等問題，之所以在執行階段讓業者無所適從，主要的原因就在於現行的相關法規錯落在不同業務主管機關所主管之不同規範當中，且未曾盤點讓業者知悉。這樣的情況讓業者疲於在各種突然出現、或突然認知到某法規必須要遵照配合、或突然意會到某法規的解讀可能與過去的認知不同的窘境。

資訊過於繁複、管道過於多樣的情況，容易使得業者在不同的主管機關之間疲於回應，削減其真正花氣力處理平臺管理問題的資源。因此盤點現有法規，應該是做到法規制度整合的第一步。

（2）政府應扮演背後支撐者的角色，提供平臺或民間組織經濟或技術支援

值得注意的是，受訪者亦指出了現今民間團體與平臺業者會受到資源和技術的限制，時常落於「空有理想，但卻無法實現」的處境中。故在解決相關網路社會危害議題上，除了整合現有規範並制定相關法律規管框架外，相關行為者如平臺業者、民間專業團體是否有能力可以確實執行框架下所擬定的配套措施，亦是很重要的一環。

部分民間專業組織期望可以在解決網路社會危害上出一分力，但受到資金和資源限制，不是沒有資金去支撐他們運作相關的規範，就是技術上沒辦法協助產出一套配套機制。這大大地限制了民間專業團體和平臺業者能發揮的空間。林淑馨教授也指出[895]，一旦政府想採用公私協力的方式來解決相關社會問題，能夠確實評估協力者的資源承接能力也是重要項目之一。

而由於政府是掌握最多資源的行為者，故本研究認為，在解決相關網路危害問題上，可以提供較多的資源協助，包含經濟資源、技術資源、法律諮詢等。誠如業者所言，政府應該採取積極的作法，並提供技術支援，使危害難以發生。

> *積極的做法應該是讓他們（盜版產業）根本沒辦法供應出來，所以像這種積極和消極都不是業者可以做的，一定都只能透過政府來協助，然後就我所知應該是有希望可以透過電信業者來幫忙，因為他們有這個技術可以去禁止，技術上應該也做得到。(E1）*

> *對啊，就是資金或是說，你說像工程師等等。那其實有時候，譬如說現在看到有一些單位，它也許預算很夠，它自己有一個小組，那它把它的這些 know how share 出來給業者，那我們的工程師很快接觸他們。我覺得那整個流程就會蠻順暢的。(F1）*

[895] 參見林淑馨，公共管理，巨流圖書公司，增訂二版（2017）。

本研究認為，若政府在建構完善治理框架之下，還能提供給平臺業者及民間專業團體各種背後的協助，妥善扮演好「協力者」的角色，在教育面上亦推動媒體識讀教育，教導民眾如何「識假、破假、抑假、懲假」，那麼台灣在治理網路危害的議題上，必會有所突破。

（3）推行「媒體識讀」教育，使民眾更能辨識危害

民眾有能力能夠自行判斷可能的風險，並且替自己避開危險，是多數受訪者、甚至出席焦點團體座談的民眾，都一致表達的必要。例如台灣匯流學會指出，台灣政府已經在不實訊息防制上提出四大面向的教育，即「識假、破假、抑假、懲假」，這四大方向的配套措施也非常齊全，政府應繼續推動，教育民眾。

> *然後是「識假」，是要去長期去推動的，教育部去推動對不實訊息的資訊素養。還有「防假」，所以就跟第三方的機制去配合，像那個事實查核機制，都是要靠政府的支援配套。（D1）*

唯有政府同時在教育面教育民眾學習辨識這些網路危害，方能將每一塊齒輪都安裝到正確的位置上，使防制網路危害這項大工程能不停地運轉。

教育民眾在網際網路社會問題的防護扮演重要角色，其中一個重要原因是因為民眾和平臺都不希望、也認為不應該有太強而有力的公權力介入審查，甚至有太過強勢的管制措施。民眾也相信許多的審查或管制都緩不濟急，多數等到危害已經發生了才有公權力能夠介入，因此避免傷害最關鍵的部分，還是必須建立民眾的媒體素養、資訊素養，才能在根本上避免網路使用者誤入網路陷阱。

（4）執行公權力，對於違法行為進行懲處

執行公權力，對違法行為進行懲處，這是只有政府能做的事。舉例來說，查緝經營假帳號的業者、追查散佈不雅照片的個人或業者、查緝在網路上販賣不實商品、追查網路詐騙等等，都是只有政府才具備的權限。

此外，還有 OTT TV 業者關注的盜版問題。OTT TV 產業受訪者亦明確指出，盜版產業在台灣非常興盛。根據 2021 年警察機關查緝侵害智慧財產權成果指出，2020 年盜版產業在台灣一年的產值就可高達新台幣 181.44 億元，且隨著數位科技的快速流動，盜版產業也開始將手觸碰到 OTT 影音串流服務中。若我們放任盜版產業繼續興盛，對台灣的文創、影視業而言，必然會造成一大衝擊。盜版雖然便宜，但它是不尊重正版的表現，無法對影視環境造成良好的正面影響，因此，追查盜版產業是現今政府應努力的方向。然而，盜版的追查並非易事，許多民間組織雖致力於消除台灣境內的盜版產業，但苦於沒有公權力和政府資料，無法獲得盜版產業的相關資訊。

比方說：真正發現一個盜版的源頭，這種禁止一定是政府才能做的。（E1）

上述受訪者就明確指出，能杜絕盜版產業源頭的就是政府，因此本研究認為，政府應拿出自身所擁有的公權力，透過強制的手段來落實盜版產業的追查和審核，以維護影視和文創產業的市場。

此外，與盜版產業同樣也日益猖狂的是網路詐騙問題，又稱為網路交易安全問題。

網路詐騙防不勝防，乃因其具有隱匿性、迅速性、全球性、多樣性，且網路詐騙的成本極低，獲利卻極高[896]。申言之，網路的無國界及迅速傳達使得詐騙集團能在短暫的時間內用極低的成本大量投注詐騙廣告，雖然不一定是人人都會上當，但只要有一人上當，所得利潤就相當可觀。

此外，隨著時空的發展，詐騙集團的詐騙手法也愈來愈多樣。警政署統計部指出，2023 年 1 月至 5 月網路犯罪以「詐欺」占 39.65%居首，且較去年同期增長 10.47%[897]，再依據警政署進一步統計同年

[896] 參見鄧煌發，虛擬世界陷阱多－淺談預防兒少網路詐騙之道，師友月刊，第 495 期，頁 34-39（2008）。

[897] 內政部警政署，警政統計通報，112 年第 28 週（2023/07/12），https://www.npa.gov.tw/ch/app/data/list?module=wg057&id=2218（最後瀏覽日：2023 年 8 月 17 日）。

1 月至 10 月之詐欺類型與被害年齡比對分析，未滿 18 歲以「假網路拍賣（購物）最多」、18 歲至 29 歲以「解除分期付款詐欺（ATM）」最多，30 歲以上則以「投資詐欺」最多，甚至投資詐欺較上年同期增加 3,784（漲幅 71.42%）[898]，足以見證網路詐欺的氾濫。無獨有偶，網路平臺業者同樣指出，現階段有些詐騙集團很狡猾，不會用很直白的口語叫民眾匯錢給他，反而會利用「送書」、「教育」、「分享」等方式誘騙你加他好友，再一步步誘拐民眾。

根據本研究之一般民眾電話訪問調查，有高達 59.4%的受訪民眾曾有在網路平臺上購物被賣家或店家欺騙的經驗。考量到如何找出加害者、進而追回財產損失與受害者的權益救濟息息相關，本研究認為，在此議題上，政府應利用公權力的力量，擔起追查加害者的角色。

> *在個資這部分其實政府我選它原因是說，我覺得在個資法執法或是基層的部分，可能也可以部分去防止這個交易後詐騙的狀況。……政府機關對於這一些業者本身，他是不是有追尋個資就是應該要去做相關的調查。（A1）*

而政府能做的事情也遠不止於調查盜版和追查詐騙者，政府同時也應減少不實訊息的出現機率。如業者所言，台灣政府應該要去調查散佈不實訊息背後的操作者，因為這是平臺業者無法調查的。

> *我們覺得它應該要由政府，因為它要有一些調查權，譬如說誰是口碑公司？或是誰是業主？譬如以我們平臺是沒有辦法去做這一層的調查。（F1）*

綜上，研究認為，在詐騙集團猖狂且極易隱藏真實身分的情況下，政府應在前端教育民眾，並與業者和民間專業團體合作，減少網路詐騙的發生，並擔當起在後端追查、捕獲詐騙集團的角色，使網路交易環境能更加健全。

---

[898] 內政部警政署，警政統計通報，112 年第 50 週（2023/12/13），https://www.npa.gov.tw/ch/app/data/list?module=wg057&id=2218（最後瀏覽日：2024 年 1 月 11 日）。

（5）留意管制幅度，不宜緊繃

承接上述，在調查過程中，本研究亦發現，現階段的網際網路平臺業者普遍支持要有一套相關規範，來管理如盜版、業者登記及兒少保護與使用者權利等相關問題；但各業者亦表達希望是由政府授權業者自律，而非用一套法規命令將所有的管理措施綁死，反而限制產業發展。舉例來說，OTT TV 業者反應，不希望政府對於內容產製、投資於台灣本土影視作品的比例等管太多。業者指出，現階段是 OTT TV 產業開始蓬勃發展的時候，政府在前頭確實應建立一套基準框架，去規管不守規矩的業者，但若在後端規管太多，反而會抹消這項產業的競爭力及背後的產值。

OTT 還太早，不表示說以後沒有法律來管，還是讓它先跑，現在管太多了，後面就真的就出不來了。(B1）

值得注意的是，多數受訪者都非常認同現階段的法律需要建立「業者登記制」，特別是針對這些境外業者。這主要是為了在發生爭議時，能在台灣找到負責的人，包含可以使政府追查盜版來源，或是在發生消費者爭議時，能找到對應的處理窗口。誠如消費者文教基金會所言，站在消費者的角度來看，這樣的登記制度是一定要的。

那消費爭議發生了之後，一定要找到窗口、一定要找到對口來處理。所以會覺得應該要登記。(H1）

剛剛說的國外公司，公司法 371 條要登記，它有登記了，所以合法正版都有機房可以合法使用，盜版有沒有？盜版就不給他，那盜版要來登記，好，那你就有人頭了，那到時候我知道你是盜版我可不可以抓你？就可以抓你，對不對？(B1）

由此來看，政府應積極推動業者登記制的設立，要使得這些境外業者在進入台灣時，能夠負擔起相對應的責任，這才能使政府有效控管網路所造成的危害。

2. 協力機關

此處的協力機關係指各業務主管機關，可以是各部會以及各層級地方政府。以目前的制度環境來看，網際網路社會問題所牽涉的相關法規錯落於各主管機關所主管之法律，尚難整合盤點。即便完成盤點，未來亦可能因為新興問題或問題的變化使得不同的業務主管機關必須協同主管機關共擬對策。

因此各業務主管機關與各地方政府在此必須扮演協力角色：

- 協助盤點主管法規，是否有網際網路社會問題相關或網路平臺業者必須協力配合的條文。
- 定期與主管機關、跨部會代表進行協力會議，交換網際網路相關之問題，滾動式調整需要的協力模式。

整體而言，在解決五大網路危害中，各業務主管機關應確保雙方目的相同，重視與合作者的資訊流通問題，並致力於增加雙方的互信、互惠關係。最後，脫離本位主義思考，傾聽業者及民眾的說法，切勿只是站在學術的象牙塔中制定規管框架，而沒有實際將真實業界中所發生的情況中納入考量。

3. 法院

法院在所有參與者中，扮演「最後防護者」的角色。雖然法院一直是站在被動審理案件的立場，但這也代表若有相關網路危害事件，法院必須扮演起妥善審理的角色，將案件分別依據現有法律規管框架，進行完整的審查並給予專業的判斷。

然而，現狀下法院的審查時常需要耗費許多時間，不論是針對盜版產業的審查，或是業者有無侵犯到使用者個人權益的審查，都需要耗上數年的時間，當中所需花費的金額也是十分龐大。因此，如何有效縮短審查過程中所需消耗的人力、物力及金錢、時間，就是法院需要去思考的。

整體而言，法院在政府體系中，雖處於被動姿態，但卻是每個案件最後的守護者，法院必須以公正的第三人角色，給予出專業的判斷。

4. 政府的協力角色

（1）進行公私協力時，應注意與協力者的「信任」和「透明」問題

現今，政府與私部門、民間專業組織合作的「公私協力」愈來愈興盛。所謂公私協力，乃是一種跨部門公私組織之間協力式網路關係（collaborative networks）的合作，且這種關係必須注重彼此間的平等互惠關係、協力過程、信任與社會資本（陳敦源、張世杰，2010）。

本研究認為，在解決網路社會危害上，政府可以扮演整合、支撐、給予資源的角色，但此外，我們仍需與平臺業者、民間專業組織進行合作，除了是提高民眾的媒體素養能力，教育民眾如何主動辨識這些危險，並不傳播相關不實訊息或詐騙訊息外，也應在前端與平臺合作，攔下不實訊息、有害兒少內容，或是一頁式詐騙訊息等。而民間專業組織更能協助政府整合業者與民眾意見，扮演一個傳達民意的角色，也扮演一個支撐政府運作的角色。

因此，為了能順利達成本研究所建立的框架運作，公私協力是必不可少的一環。本研究認為，政府在合作過程中，有以下三點需要特別注意：

A. 應與合作夥伴維持平等的關係，不應過於強調主、客關係。若過於強調主從關係，則會使私部門的彈性、效率和多元等特性難以發揮。

B. 暢通溝通管道，使訊息能不斷交流，並提高雙方互信程度，方能使合作順利進行。誠如受訪者表示：

我覺得政府如果要跟任何，就是比方說，平臺或者是民間組織合作，我覺得前提是它一定全部都是要透明。（A1）

C. 增加利害關係人的參與。林淑馨教授指出[899]，公私協力的成功要件之一就是增加利害關係人的參與。政府應推動民眾和相關利害關係人參與，否則若只有少數幾個利益團體參與，

[899] 同前註 895。

則將來可能面臨到他人不願或無法配合的情況，這反而會阻礙協力的推動。誠如受訪者 C1 所言：

政府的角色不一定是代理，不一定是執行說哪樣的行為是不能操作的，而是可能要至少要扮演一個像是平臺的，它也要用平臺的思維來進行網際網路的治理，也要多方利害關係人來可能開個會，然後我們就是定期可能檢討這段時間內社會上發生的一些個案的態樣，時間一久的話資料庫就會建立起來，建立起來之後未來再發生一樣的事情就會有依據可以循，我們也知道怎麼處理。(C1)

簡言之，公私協力的確是現今的趨勢之一，但在合作過程中，政府仍應注重和合作夥伴的地位，並致力於增加彼此的信任程度，同時維持溝通管道的暢通，如此一來方能動用多方關係，將網路所造成的危害縮到最小。

（2）傾聽業者、民眾想法

除了政府與平臺業者、民間專業團體間要維持信任與溝通的暢通外，本研究亦認為，政府在研議法律框架的時候，需要注重與傾聽業者與民眾的想法，將業者在實務操作上會遇到的困難考慮進去，而非是一意孤行的設立法律框架。

我覺得那就是在不違法的狀況之下，其實可能政府它要花更多時間去理解今天平臺它的信念是什麼？它想要做什麼事情？然後協助我們。(F1)

換言之，各政府機關在研議法律框架的時候，關鍵並非將框架建構得相當完善，而是從業者的需求、民眾的想法出發，作為一個協助者的角色。

（3）各業務主管機關應彼此協調、整合

最後，由於政府行政機關十分龐大，在同一項議題中，可能會牽涉到許多機關，亦可能有共同管轄的情況發生。誠如台灣人權促進會所言，各業務主管機關彼此間應先行調和，整合彼此資訊與資源，方能將法規完善的建立起來。

其實這應該是政府之間彼此協調可以做什麼事情，但當然它可能需要跨部會，因為可能來開會的部會代表是真的不知道自己的機關這麼大，有哪些法律在做什麼事情，所以他會覺得不關我的事。(A1)

簡言之，唯有政府先行整合好彼此間的資源與確立共有目標，才能使平臺業者及民間專業組織能有一個可以依循的框架，並且能清楚明白若他們需要幫助，政府可以提供何種資源或技術的協助？本研究亦期望，各政府部門能打破組織與組織間的藩籬，脫離本位主義的思考，將目的共同放在解決網路危害問題上。

5. 小結

綜上分析，本研究歸納出政府在可扮演的角色有以下兩點：(1)整合現有資源，負責協調並建立出規管網路危害的框架；(2)發揮政府公權力，積極執法，介入一般業者與公民團體難以深入的領域，追查詐欺犯與盜版業者，協助整頓網路世界的環境。

在建立出相關規管框架後，政府也應課予平臺相對應的責任，例如監督平臺提供「透明度報告書」等，使政府、民間專業團體、民眾都能共同監督平臺業者。

要課予責任，比如說：我們現在原來網路中介服務法提出來的透明度報告非常好，在那個十五條、十六條、二十九條那一邊透明度報告，而且是一層一層來。(D1)

與此同時，政府也應注意自身的公平、公開、公正性，並隨時保持著開放的思想，透過召集利害關係人，舉行會議，共同研擬出一套

可行的規管框架與規管方針。待框架出來後，再由相關業者或民間專業團體負責執行，而政府則在背後負責技術與資金的支援。

本研究期望，能夠過這樣的一個分工合作模式，建構出台灣自身的網路管理法則。

（四）民眾

隨著數位科技及網際網路的快速發展，網際網路傳播不再僅限於傳遞訊息，更成為了解民眾關注議題，促成社會共識的重要途徑。在這樣的背景下，民眾身為網路世界的使用者，扮演著關鍵的角色，對於網際網路生態的健康發展有著至關重要的作用。本研究認為民眾除了行為上遵守規範之外，可以藉由擔任以下角色，強化整體社會的資訊素養與媒體素養：

首先，民眾可以擔任「主動查證者」的角色。面對海量的資訊，民眾可以主動運用媒體識讀及查證能力，去確認訊息的真實性和可靠性。透過查證來源、尋求多方證據，以及分辨內容是否具有偏見或操縱性，民眾能夠避免相信不實消息，並避免傳播。

> *我們用戶把訊息去報到這個官方帳號之後，我們會把這個後台給傳在就是事實查核組織上，所以它們可以根據這個彙報結果再去決定它們可能哪些訊息是可以處理、可以查核，然後把它們查核結果上傳上去之後再回給用戶。（G1）*

其次，民眾也能成為「批判性思考者」，藉由對媒體報導的內容進行深入思考與評估。應對資訊具備批判性的眼光，質疑訊息的立場、動機以及可能存在的隱含偏見。這樣的思考模式能幫助民眾更全面地了解議題，避免被狹隘的觀點所影響，促進對多元觀點的接納與尊重。在進行網路交易的同時，也能辨識是否為釣魚網站，避免受騙，保障自身的交易安全。

這相關的不實訊息，可能要能夠辨識以外，他還要能夠不傳播，或者是不傳播還要能夠去說明，就有人要傳播的時候，他要能夠告訴別人說：為什麼這是一個不實訊息。（C1）

這需要民眾不斷地學習和增進自己的媒體素養和查證能力，並積極參與資訊教育的推廣。同時，共同支持事實查核機構的工作，維護公共資訊的準確性和可靠性。

另外，民眾也在社交媒體平臺上發揮著「訊息分享者」的角色。當民眾發現可靠的資訊和來源時，他們能夠主動分享給身邊的人或社群，這將有助於阻止不實消息的傳播，並提供更多人可以查證的資料。同時，對於兒少不宜或是涵蓋霸凌言論的內容，民眾也可以擔任守門員的角色，進一步提升網路安全性。

以網路平臺上的「兒少網路安全」問題為例，民眾可以擔任起重要的角色，特別是對於年紀較小的孩子，當他們在接觸網際網路時，由於家長無法始終陪伴在旁，孩子可能暴露在網路內容的風險中。

網路平臺上的「兒少網路安全」問題確實是一個值得關注的重要議題。在這方面，家長和使用者應該負起最大的責任，並積極出面處理這個問題。特別是對於年紀較小的孩子，當他們在使用這些 3C（電腦、手機、平板）的產品時，由於家長無法始終陪伴在旁，孩子可能暴露在網路內容的風險中。（F1）

民眾可以建立家庭網路過濾系統，封鎖不適宜兒童觀看的網站和內容。同時，設立家庭網路使用規範，告知孩子應該遵守哪些網路使用原則，進行充分的網路教育，向孩子解釋網路的潛在危險，教導他們避免點擊不明連結、不公開個人資料等基本的網路安全知識。

此外，民眾還可以成為「積極溝通者」，運用有效的溝通方式與他人討論資訊和議題。這包括尊重對方的立場、耐心聆聽對方的觀點，並以理性和客觀的態度進行討論。透過積極的溝通，民眾有機會分享各自對議題的看法，從而促進理解、凝聚共識，並達成社會共同目標。

網路使用者自己當然就是除了媒體識讀、查證能力，跟我覺得也滿重要的是「親友關係」，我知道有滿多社群他們是在做親友關係的互動，就是怎麼跟家人、怎麼跟長輩聊聊我們看到的這些訊息，而不只是去指出這是錯誤的。就是你怎麼不查，就是這不是一個有效的互動跟溝通。(A1)

如果發現親友相信了假消息，不立刻與他們辯論，這可能會引發爭吵，讓情況更加惡化。可以嘗試找尋共通點，並且分享一些可靠的事實查核網站，讓親友可以在未來具備自行查證訊息的能力。

總體來說，民眾在數位時代扮演了多重角色，這些角色彼此相輔相成，共同構築了一個健康、開放且充滿信任的資訊生態系。透過自身行為的自律，主動查證、批判性思考、訊息分享和積極溝通，民眾能夠提高媒體識讀水準，更加敏銳地理解社會議題，並共同推動社會向更進步的方向發展，真正培養數位民主的韌性。

第三節 綜合觀察

針對電訪、網路問卷及焦點團體座談會的主要發現，本研究綜合觀察如下：

一、電話訪問

（一）多數民眾都有受到五大網路危害的經驗

在調查民眾的使用經驗中，主要調查民眾是否有遇過相關的網路危害。調查結果顯示，在政治不實訊息上，有 62.9%的民眾曾在網路平臺上看到與政治相關的不實訊息。而有 54.6%的民眾家裡的未成年人曾經在網路平臺上接觸到色情或暴力內容。有 59.4%的民眾曾被網路詐騙過。值得注意的是，雖然僅有 35.5%的民眾有過被網路霸凌的經驗，但有 59.4%的民眾認為網路平臺的出現讓網路霸凌的發生率更為高漲。

通傳會「112 年通訊傳播市場報告」之調查也呈現出相似之結果。我國民眾遭遇電話詐騙或網路詐騙情形，超過 6 成有遇過電話詐騙或網路詐騙，對於「網路詐騙」的疑慮，占比也自 106 年的 48.4%躍升至 112 年的 69.9%[900]，民眾對於「充斥假新聞或錯誤引導之資訊」之顧慮，比例亦大致呈逐年增加趨勢，自 106 年的 13.8%增加至 112 年的 40.5%[901]。這些結果都顯示，五大網路危害的發生機率甚高。

（二）在各項危害上，民眾皆希望政府能出面處理

電訪問卷中將主要負責對象分成：民眾自己、網路平臺、政府機關及民間專業組織四塊。其中各項危害中，受訪者皆表示希望政府能夠出面處理這些危害，這表示在處理網路相關議題上，民眾仍對政府抱有一定的信賴，且希望政府能夠出面解決。

---

[900] 國家通訊傳播委員會，112 年通訊傳播市場報告（2023 年 12 月 28 日），頁 136-137，https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=5023&cate=0&keyword=&is_history=0&pages=0&sn_f=49716（最後瀏覽日：2023 年 12 月 30 日）

[901] 同前註。

（三）民間專業組織可從旁提供協助

民間專業組織在社會上扮演重要的協助者角色，可以幫助政府完善社會保護網，使大眾能夠享受更好的社會。而在網路議題上，民間專業團體亦可提供政府專業的協助。例如行之有年的 iWIN 網路內容防護機構可提供有關兒少網路使用安全的專業協助。在此次電訪調查中，雖民眾主要認為應由網路平臺及政府出面處理，但亦有部分民眾認為可由民間專業團體負責處理這些網路議題。在「政治不實訊息」及「網路交易安全」的題組上，皆有超過 5%的民眾認為可以交給民間專業團體負責處理該項問題。而在「使用者權益」的題組上，有 10.8%的民眾認為可交由民間專業團體來處理紛爭。

二、公民團體及業者面訪

面訪係依據電訪問卷所得之結果進一步延伸諮詢專家及業者、公民團體，調查結果可總結為以下幾點：

（一）業者需整合自身需求並形成自律規範，與各方利害關係人共同協力

網路平臺業者作為提供網路服務的業者，必然與建構網路安全一事息息相關，因此建構一套自律規範亦是平臺業者的重大責任。作為提供服務者，網路業者應先整合自身需求以形成自律規範，明確指出希望政府的管制幅度落於何處，如此一來方可減少雙方的資訊不對等或期望落差。同時，業者也可和各方利害關係人合作，提升民眾的媒體識讀素養，或共同打擊網路上的非法行為。

（二）政府機關亟需進行法規及資源整合，並適時給與平臺業者技術或經濟的支援

要想管制龐大的網路，並使危害受到控管，法規的限制十分重要。而現階段相關的法律卻四散在各處，這給業者和民眾帶來一定的困擾，業者要遵守現有法規，需清楚了解相關法規有哪些；而民眾亦需知道若自己的權益受損，可以尋求哪些管道的協助，因此整合法規十分重

要。

此外，由於部分網路平臺較小，可動用的資源與技術較少，有時會受到一定的限制，因此在保護民眾使用網路安全的情況下，政府可以給予小平臺一定的技術或經濟支持，使小平臺也能跟上大平臺的腳步。

（三）應善用民間專業組織的力量，減輕政府管制負擔

民間專業組織在社會上扮演重要角色，其在網際網路社會問題中可以發揮著重要的監督與倡導角色，監督平台業者是否有良善運作，或是提供不實訊息的澄清（如台灣事實查核中心會協助進行公共事務相關訊息之事實查核）。於大眾而言，亦可教育民眾媒體識讀，使民眾擁有辨識假消息的能力。此外，民間專業組織在特定領域上的專業知識和技術更是政府應該善加利用的，民間專業組織可作為一「中間人」，與政府和平臺業者進行溝通。政府可與民間專業組織進行合作，減輕負擔。

（四）民眾的媒體素養能力必須提升

網路上的消息真假難辨，詐騙訊息層出不窮。民眾身為網路的使用者，自身的媒體素養能力對於建構良好的網路秩序就顯得格外重要。民眾應要有足夠的能力去辨別真偽，能夠識假與防假。除了政府應在教育端教育民眾外，平臺業者與民間專業組織都應出一份力。但除此之外更重要的是民眾自身必須與時俱進，不斷學習如何辨識假訊息與詐騙、霸凌資訊，不讓自己在網路世界中隨波逐流。

三、焦點團體座談

電訪與面訪之調查，發現民間專業組織在建構網路秩序上扮演重要角色，不僅可教育民眾，也可協助政府進行監督的工作，因此焦點團體座談會著重詢問民間專業機構可扮演的角色與其功能。調查結果主要為：

（一）可引進第三方機構，協助建立與維護網路秩序

網路秩序之建立與維護非一朝一夕就可完成，若完全交由政府來建立與維護會大幅增加政府的負擔，政府不一定有足夠的行政量能可完成如此龐大的任務。故，可引進民間專業組織的協助，或可建立一第三方機構，協助維護網路秩序。而一個跳脫政府與網路平臺的第三方機構對民眾而言，亦是一個公正、多元聲音的代表，避免單一立場的偏頗問題（訪談記錄 K5、M5）。

此外，亦有學者認為，在建立網路秩序一事上，政府同時是主事者，也是協力者。我們不應過度給予政府主事的權力，否則容易有無限上綱的事情發生，政府應是先建立一框架，框架內部的事情才由政府出面處理，同時與民間團體共同扮演協力者的角色，去共同負責網路安全問題，如此一來可限縮政府權力，以防政府權力過大（訪談記錄 N4）。

（二）平臺業者應率先管制網路違法行為，責任不可推卸

平臺業者提供服務，有時會藉由販賣廣告以獲取收益，在此情況下，平臺就負有責任，需要查核廣告真偽（訪談記錄 L7）。平臺業者應建立自律規約並遵守之，而民間專業團體則可與民眾共同監督平臺業者是否有遵守該自律規約。

（三）政府應保持公平、公正、公開的態度與各方進行協力合作

為使協力合作順利運行，政府在與各方進行公私合作時，應保持彼此的資訊公開透明，傾聽民間專業組織與業者的想法，同時留意彼此間的地位是「對等」的合作者，而非「不對等」的雇傭關係。政府需要傾聽業者和民間團體的想法並參考其意見，切勿讓合作的場所變成一言堂。

四、「協力模式」作為最大公約數

根據電訪、面訪與焦點團體之調查結果，本研究發現，儘管電訪結果中多數民眾希望網路問題由政府出面解決，但面訪與焦點團體的各方意見並非將政府置於第一線。電訪、面訪和焦點團體的結果看似衝突，但實則合理。電訪的問卷設計受限於訪談時間、問題不能夠太複雜等的限制，未能於題目中詳述政府出面解決的方式與選項，故民眾在選擇上會受到一些限制，因此在眾多利害關係人中，民眾很容易選出最顯而易見的選項：政府；但在該題目中並未能測得民眾希望政府以何種形式／角色出面處理問題。

面訪與焦點團體訪談，本研究進一步針對由政府出面解決的方式探詢適合的治理模式，綜合面訪與焦點團體訪談之調查結果，本研究發現政府出面解決最合適的方式，是架構適合業者、公民團體等相關利害關係人共同參與的協力環境。政府先以立法的方式架構適合的治理環境，並賦予各個利害關係人相映的權利義務。業者因為是平臺的實際經營者，與使用者/民眾的關係有直接的交易關係，因此最適合做為第一線的執行者；同時，業者因為平臺性質的不同、規模的不同差異頗大，能適用的規則各異，因此若依照平臺需求發展部同的治理規範最具可行性。公民團體的角色代表多元利益，能彰顯社會不同層面的需求，也能平衡平臺與政府在治理過程當中權力過大的問題。綜合上述發現，本研究認為協力治理模式符合電訪結果民眾希望政府出面的期待，又能兼顧權力制衡與可行性

因此本研究後續將以具備權力限制特色的協力治理模式做為後續研究的基礎。

第五章　國內主要網際網路傳播相關服務公共問責模式研析

本研究依照一般大眾電話訪問調查、公民團體訪談、業者訪談、學者專家訪談，以及五場焦點座談的結果，初步產出一個網際網路傳播社會問題的協力治理模式；期望能夠透過相關利害關係人的協力參與，降低、解決網際網路的社會問題，並瞭解該治理模式的適用程度。

本研究另外針對網際網路的使用者，進行網路問卷調查；亦邀請學者專家、網路平臺業者以及相關團體，進行專家諮詢會議。透過網路問卷調查以及專家諮詢會議，確認本研究設計的模型的可行性與問題解決能力。

本章第一節說明一般大眾網路問卷調查的設計、執行與結果。

第一節 一般大眾網路問卷調查

一、網路調查摘要

（一）研究方法

本研究執行至少 300 份網路調查，蒐集網路使用者對於社會調查結果及網際網路傳播相關服務問責模式之相關意見。填答者必須具有至少 3 種平臺之會員資格，且在近一個月內曾使用過該平臺。

（二）執行平臺

本研究以典通股份有限公司獨家開發之 EZChoice 行動 APP 為執行平臺。EZChoice 會員人數達 10 萬餘人，且從會員資料庫可區辨會員性別、年齡、是否為唯手機族等關鍵要項，可作為網路調查抽樣規劃之依據。使用 EZChoice 為調查執行平臺優勢有二，其一為 EZChoice 行動 APP 調查之會員登錄成為會員或使用平臺前，須以實名登入註冊為會員，並以手機帳戶進行認證、綁定身分，加上填寫完問卷後也會再利用基本資料反覆驗證會員資料的正確性，成功的克服網路調查多重身分、填卷真實性質疑。

其二為 EZChoice 會員係參考國家發展委員會之「108 年個人/家戶數位機會調查」，依照與我國行動族結構分布進行招募，因此具有母體代表性，且其母體結構的涵蓋率已經達 75%以上。

二、問卷設計暨背景說明

本研究在期中執行的電訪問卷中，主要調查一般大眾針對五大網路危害與其主要負責對象，及相關的解決方式構想。

下表為本研究將期中電訪問卷第二部分（知覺網路個人、社會問題與風險危害）每一個問題問項重新編碼所得之結果，分數愈高代表嚴重程度愈高，依此計算每一個問題的認知強度。

表 82：網路問題強度分析

問題類型		樣本數	平均數	標準差	最小值	最大值
政治不實訊息	經驗	1,098	2.97	1.02	1	4
	問題程度認知	1,250	3.43	0.79	1	4
	風險認知	1,263	3.46	0.75	1	4
兒少網路安全	經驗	1,083	2.80	1.11	1	4
	問題程度認知	1,277	3.28	0.92	1	4
	風險認知	1,273	3.54	0.75	1	4
網路交易安全	經驗	1,111	2.84	1.06	1	4
	問題程度認知	1,273	2.86	0.91	1	4
	風險認知	1,281	3.08	0.89	1	4
網路霸凌	經驗	1,099	2.26	1.09	1	4
	問題程度認知	1,263	3.49	0.78	1	4
	風險認知	1,271	3.49	0.75	1	4
使用者權益	經驗	1,068	2.26	1.05	1	4
	問題程度認知	1,260	2.97	1.09	1	4
	風險認知	1,251	3.14	0.87	1	4

資料來源：本研究自行整理

從結果來看，面對五大網路危害，過半數民眾都有受害的經驗，也認知到這些網路危害有一定的風險和問題。其中，政治不實訊息、兒少網路安全問題，以及網路霸凌問題，是三項具有較高社會共識且問題較為嚴重的三類問題。

此外，民眾多數認為政府與網路平臺需要負起最大的責任，各項所得結果請參考下表。因此，針對現狀下網際網路傳播所會導致的社會危害現象，本研究擬提出一套可以約束網路危害問題產生的協力治理模型。

表 83：網路調查民眾認為在各類網路危害中應負最大責任者之主體

您覺得在網路平臺上的網路危害問題，誰應當負「最大的責任」，並出面處理？（各危害分別詢問，並取結果中的前兩名。）		
	政府機關	網路平臺
政治不實訊息	61.3%	20.3%
兒少網路安全	50.9%	34.9%
網路交易安全	41.6%	44.6%
網路霸凌	49.9%	33.2%
使用者權益	25.1%	35.1%

資料來源：本研究自行整理

為能更了解民眾對於治理模式的看法，研究團隊在研究後半部進行網路問卷調查，期望可以更深入的了解民眾希望如何處理、管制這些網路危害。預計回答的問題有：一、民眾認為現狀下的網路危害應如何管制？該由誰來管制？管制強度為何？二、針對本研究提出的協力治理模型，民眾有何看法？

在問卷設計上，本次網路問卷共分成四大部分。第一部分調查民眾的網路行為與有使用的平臺。第二部分將調查民眾針對網際網路社會問題治理結構所應該有的態樣，包含對於管制違法內容的寬鬆程度與處理範圍、行政與司法機關兩者間的權利相衡等。

再者，本研究特別提出一套處理網際網路違法問題的協力治理模型，此機制參與者有：政府、網路平臺、第三方組織與民眾。故研究團隊亦將詢問民眾對於不同角色間的互動關係的滿意程度與想法。第三部分將調查民眾使用串流影音服務的頻率與所遇到的問題。第四部分則為受訪者基本資料調查。

問卷設計如下圖所示。

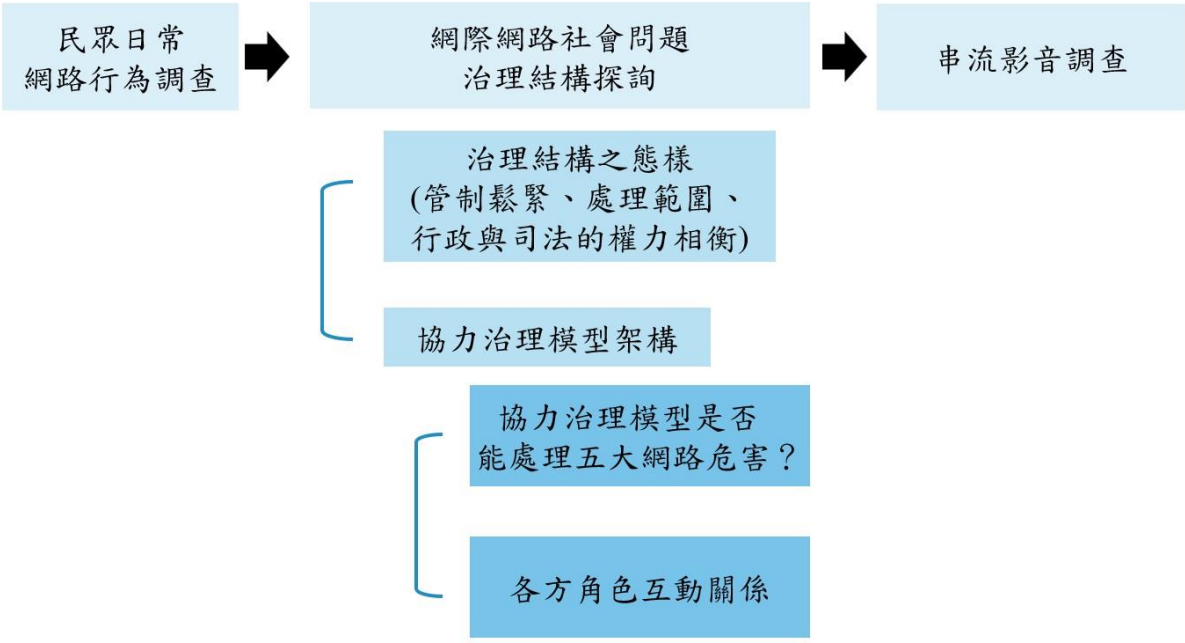


圖 31：一般大眾網路問卷設計架構

資料來源：本研究自行整理

本研究將網路平臺先劃分成六類，因此問卷設計上也分成六類平臺：社群網站（例如：Facebook、Instagram）、影音分享平臺（例如：YouTube、TikTok）、網路論壇（例如：批踢踢實業坊、DCard）、通訊軟體（例如：LINE、Messenger、Discord）、網路新聞平臺（例如：Yahoo 新聞、LINE TODAY），以及拍賣、購物平臺（例如：Yahoo 拍賣、蝦皮購物、露天市集、淘寶）。

（一）網路行為與使用調查

第一部分的調查分為三大面向，包括：一、民眾使用各類型網路平臺的頻率；二、民眾針對網路平臺所訂定出的使用者條款滿意程度的認知面向，以及三、使用者條款帶來的感受面向。

使用面向延續電訪問卷，採用「110 年網路沉迷研究調查報告」[902]，所界定出的「網路沉迷者」平均每天上網時間的時數，我們將民眾使用網路的頻率設為：未滿 1 小時、1～未滿 3 小時、3～未滿 5 小時、5 小時以上及不一定。並將使用超過三小時的民眾定義為「高網路使用族群」。

認知面向的題組則為使用者是否曾閱讀過平臺的服務及使用者條款？若閱讀過，對其內容瞭解程度有多高？感受面向的題組則詢問民眾是否滿意現狀下網路平臺所訂立的使用者服務條款？感到不滿意的理由為何？特別重要的是，由於網路危害有諸多面向，依據不同面向網路平臺亦有可能有不同的規範去規制其平臺上的違規內容，因此本研究在感受面向上，將依五大網路危害（政治不實訊息、兒少網路安全、網路霸凌、網路交易安全、個人權益侵害）分別詢問民眾對服務條款訂定的滿意程度。

本研究期望透過第一部分的調查，了解到民眾使用這些網路平臺的頻率，以及現狀下網路平臺針對五大危害所訂定出的使用者條款是否讓民眾感到滿意？有哪些地方是可修改或精進的方向？又或是有哪些網路危害的使用者條款特別需要改善。

[902] 同前註 876。

（二）網際網路社會問題治理結構探詢

第二部分本研究期望調查民眾針對網際網路社會問題治理結構所應該有的態樣，因此分成兩階段進行調查。第一階段依據先前研究已提出的象限架構分別詢問民眾對於治理模式的偏好。第二階段則提出研究團隊制定的管理框架，詢問民眾對管理方式的滿意度及想法。

在第一階段治理模式偏好的調查中，研究團隊希望調查出民眾偏好的管制程度到哪？因此我們將依據管制程度及處理範圍，與行政、司法間的權力關係作為主軸詢問民眾的看法。

首先，會調查移除網路上的違法資訊或內容的寬鬆–嚴格程度：1 為最寬鬆，以網路平臺業者為主，透過自律方式將違法資訊或內容移除；10 為最嚴格，以行政機關或司法機關（法院）為主，依據法令強制將違法資訊或內容移除。

其次，調查移除機制所處理的範圍：1 為最有限，僅將處理重點放在詐騙、兒少保護等社會重視的違法類型，且配合不同事件類型，分別建立對應的移除機制；10 為最廣泛，無論觸犯的是《刑法》、《民法》或政府各級機關訂定的行政法規，所有的「違法」資訊或內容都必須處理，且應建立一套一體適用的移除機制。

第三，調查在管理網路上的違法資訊或內容中，行政機關與司法機關這兩者的權限大小：1 為行政機關擁有最大權限，行政機關可自行決定裁罰或移除，法院只提供事後的司法救濟；10 為司法機關擁有最大權限，裁罰或移除必須先行經過法院的裁判決定。

統整上述三題調查，我們可以初步界定出網際網路危害的管制程度應在何處。

接著，在第二階段中，本研究提出一協力治理模型，分別由政府、網路平臺業者與第三方機構共同完成的協力模式。在此協力治理模型中，由政府與第三方機構協力，整合各方意見，建立各網路平臺共通的自律框架，再由各網路平臺依照自律框架，訂定平臺的自律規則，並照章執行，做為平臺與其使用者的自律依據。

而倘若使用者（即民眾）發現平臺有違反自律規則，應先向平臺進行申訴；若申訴未果，可向第三方機構投訴，機構受理投訴後若確認平臺違反自律規則，或其自律規則違反共通性自律框架，將通報政府相關業務主管機關進行裁罰。

在此協力治理模型中，第三方機構指稱一獨立的、非政府的第三方的服務機構。一般有三種組成模式：A. 由相關業者組成的商業團體（公會）或協會，如中華民國無店面零售商業同業公會、台北市電腦商業同業公會、台灣網路暨電子商務產業發展協會。B. 由多方團體或個人共同組成，如財團法人中華民國消費者文教基金會（消基會）、台灣事實查核教育基金會（事實查核中心）、台灣展翅協會。 C.由政府捐助成立之財團法人，如財團法人資訊工業策進會（資策會）。

在此階段的調查中，本研究欲解答兩個問題：第一，以五大網路危害作為框架，民眾認為在此項網路危害中，該協力治理模型是否適合？各角色有無需要加強的部分？若有，該角色可做何種事？研究團隊將依據電訪問卷第三部分—各網路危害中，民眾的處理方式與偏好之所得結果進行問卷選項的設計。各角色所可做的事情為電訪問卷所得結果之「前兩項」最多人選擇的項目。（舉例而言，在「政治不實訊息」中，民眾認為「網路平臺」應該處理的方式前兩名為：主動判斷並加註警語或降低排序（40.2%）、主動判斷並移除（37.6%）。

另外，由於電訪問卷希望能深入了解民眾認為政府應該透過誰來管制相關問題，因此在「政府作為」此題組中，將業務機關區分為「單一業務機關」與「業務主管機關」和「法院」。而此次網路問卷希望可了解行政機關與司法機關間的權限劃分問題，因此統一調整問卷選項成「單一業務機關」與「法院」，方便結果蒐集。

第二，研究團隊欲了解民眾對於此協力模式中第三方機構與其他角色間的互動關係的認同程度，以及第三方機構可做的事情。包含：第三方機構與政府間的互動、第三方機構與網路平臺間的互動、第三方機構與民眾間的互動。同時，特別針對第三方機構的不同組成方式，調查民眾在此協力模式下，偏好的第三方機構組成模式。

透過此題組的詢問，有望能調查出在此協力模式中，民眾對第三方機構的看法，與民眾認為第三方機構是否有能力可以解決相關的網際網路危害問題。並輔以前部分的調查結果，去劃分出在這協力模式中，誰的角色或功能需要加強。本研究期望透過第二部分兩階段的詢問，探詢出符合民眾期望，且也適合台灣的網際網路治理模式。

第三部分為串流影音服務題組，主要調查民眾的使用經驗，與其認為何種問題最需要被解決，政府需要採取何種措施？最後一部分為個人資料調查。

綜上所述，透過本問卷前兩部分的調查，研究預計可取得一定資料，藉以回答研究問題：一、民眾認為現狀下的網路危害應如何管制？該由誰來管制？管制強度為何？二、針對本研究提出的協力治理模型，民眾有何看法？應該如何改善？

第二節　一般大眾網路問卷調查結果

一、日常行為：網路行為與使用平臺調查

（一）各網路平臺使用狀況

針對民眾網路使用行為，本研究分成六大網路平臺及有線電視進行調查。分別為：社群平臺、影音分享平臺、網路論壇、通訊軟體、網路新聞平臺、拍賣及購物平臺與有線電視。

近一個月內有使用社群平臺，如 Facebook、Instagram、YouTube、PTT 等的民眾，樣本有 298 位，計有 99.3%的民眾近一個月內有使用過社群平臺，超過半數（50%）。而其中，每天使用 1～未滿 3 小時社群平臺的民眾為最多數（40.6%），社群平臺重度使用者（每天平均上網超過 4.1 小時者，此處以超過 5 小時計）有 11.1%。

詳細次數統計表如下。

表 84：近一個月內有使用社群平臺的民眾與使用時間

問項	選項	樣本數	百分比
承上，請問您近一個月內是否有使用這些您註冊為會員的社群網站（例如：Facebook、Instagram）？	有使用	298	99.3
	沒有使用	2	0.7
	總計	300	100.0
請問您平均一天使用這些社群網站的時間約為幾小時？	未滿 1 小時	74	24.8
	1～未滿 3 小時	121	40.6
	3～未滿 5 小時	58	19.5
	5 小時以上	33	11.1
	不一定	12	4.0
	不知道/拒答	0	0.0
	總計	298	100.0

資料來源：本研究自行整理

近一個月內有使用影音分享平臺（例如：YouTube、TikTok）的民眾，樣本有 259 位，計有 97.0%的民眾近一個月內有使用過影音分享平臺，超過半數（50%）。

其中，每天使用 1～未滿 3 小時影音分享平臺的民眾為最多數（52.1%），影音分享平臺重度使用者（每天平均上網超過 4.1 小時者，此處以超過 5 小時計）有 7.7%。

詳細次數統計表如下。

表 85：近一個月內有使用影音分享平臺之民眾與使用時間

問項	選項	樣本數	百分比
請問您近一個月內是否有使用這些您註冊為會員的影音分享平臺（例如：YouTube、TikTok）？	有使用	259	97.0
	沒有使用	8	3.0
	總計	267	100.0
請問您平均一天使用這些影音分享平臺的時間約為幾小時？	未滿 1 小時	49	18.9
	1～未滿 3 小時	135	52.1
	3～未滿 5 小時	44	17.0
	5 小時以上	20	7.7
	不一定	11	4.2
	不知道/拒答	0	0.0
	總計	259	100.0

資料來源：本研究自行整理

近一個月內有使用網路論壇（例如：批踢踢實業坊、DCard）的民眾，樣本有 172 位，計有 92.5%的民眾近一個月內有使用過網路論壇，超過半數（50%）。

其中，每天使用 1～3 未滿小時網路論壇的民眾為最多數（43.6%），網路論壇重度使用者（每天平均上網超過 4.1 小時者，此處以超過 5 小時計）有 4.7%。

詳細次數統計表如下。

表 86：近一個月內有使用網路論壇的民眾與使用時間

問項	選項	樣本數	百分比
請問您近一個月內是否有使用這些您註冊為會員的網路論壇（例如：批踢踢實業坊、DCard）？	有使用	172	92.5
	沒有使用	14	7.5
	總計	186	100.0
請問您平均一天使用這些網路論壇的時間約為幾小時？	未滿 1 小時	69	40.1
	1～未滿 3 小時	75	43.6
	3～未滿 5 小時	15	8.7
	5 小時以上	8	4.7
	不一定	5	2.9
	不知道/拒答	0	0.0
	總計	172	100.0

資料來源：本研究自行整理

近一個月內有使用通訊軟體（例如：LINE、Messenger、Discord）的民眾，樣本有 301 位，計有 99.3%的民眾近一個月內有使用過通訊軟體，超過半數（50%）。

其中，每天使用 5 小時以上通訊軟體的民眾為最多數（29.6%），此為通訊軟體重度使用者（每天平均上網超過 4.1 小時者，此處以超過 5 小時計）。次多數者為每天使用 3～未滿 5 小時通訊軟體使用者（25.6%）。

詳細次數統計表如下。

表 87：近一個月內有使用通訊軟體的民眾與使用時間

問項	選項	樣本數	百分比
請問您近一個月內是否有使用這些您註冊為會員的通訊軟體（例如：LINE、Messenger、Discord）？	有使用	301	99.3
	沒有使用	2	0.7
	總計	303	100.0
請問您平均一天使用這些通訊軟體的時間約為幾小時？	未滿 1 小時	34	11.3
	1～未滿 3 小時	86	28.6
	3～未滿 5 小時	77	25.6
	5 小時以上	89	29.6
	不一定	15	5.0
	不知道/拒答	0	0.0
	總計	301	100.0

資料來源：本研究自行整理

近一個月內有使用網路新聞平臺（例如：Yahoo 新聞、LINE TODAY）的民眾，樣本有 201 位，計有 92.2%的民眾近一個月內有使用過網路新聞平臺，超過半數（50%）。

其中，每天使用 1～未滿 3 小時網路新聞平臺的民眾為最多數（29.4%），網路新聞平臺重度使用者(每天平均上網超過 4.1 小時者，此處以超過 5 小時計）有 2.0%。

詳細次數統計表如下。

表 88：近一個月內有使用網路新聞平臺的民眾與使用時間

問項	選項	樣本數	百分比
承上，請問您近一個月內是否有使用這些您註冊為會員的網路新聞平臺（例如：Yahoo 新聞、LINE TODAY）	有使用	201	92.2
	沒有使用	17	7.8
	總計	218	100.0
請問您平均一天使用這些網路新聞平臺的時間約為幾小時？	未滿 1 小時	114	56.7
	1～未滿 3 小時	59	29.4
	3～未滿 5 小時	15	7.5
	5 小時以上	4	2.0
	不一定	9	4.5
	不知道/拒答	0	0.0
	總計	201	100.0

資料來源：本研究自行整理

近一個月內有使用拍賣、購物平臺（例如：Yahoo 拍賣、蝦皮購物、露天市集、淘寶）的民眾，樣本有 281 位，計有 97.6%的民眾近一個月內有使用過拍賣、購物平臺，超過半數（50%）。

其中，每天使用 1～未滿 3 小時拍賣、購物平臺的民眾為最多數（38.4%），拍賣、購物平臺重度使用者（每天平均上網超過 4.1 小時者，此處以超過 5 小時計）有 6.4%。

詳細次數統計表如下。

表 89：近一個月內有使用拍賣、購物平臺的民眾與使用時間

問項	選項	樣本數	百分比
請問您近一個月內是否有使用這些您註冊為會員的拍賣、購物平臺（例如：Yahoo 拍賣、蝦皮購物、露天市集、淘寶）	有使用	281	97.6
	沒有使用	7	2.4
	總計	288	100.0
請問您平均一天使用這些拍賣、購物平臺的時間約為幾小時？	未滿 1 小時	113	40.2
	1～未滿 3 小時	108	38.4
	3～未滿 5 小時	21	7.5
	5 小時以上	18	6.4
	不一定	21	7.5
	不知道/拒答	0	0.0
	總計	281	100.0

資料來源：本研究自行整理

近一個月內有使用傳統電視（例如：有線電視〔第四台〕、MOD、無線電視）的民眾，樣本有 202 位，計有 66.2%的民眾近一個月內有使用傳統電視，超過半數（50%）。

其中，每天使用 1～未滿 3 小時傳統電視的民眾為最多數（45.5%），拍賣、傳統電視重度使用者（每天平均使用超過 4.1 小時者，此處以超過 5 小時計）有 7.4%。

詳細次數統計表如下。

表 90：近一個月內有使用傳統電視的民眾與使用時間

問項	選項	樣本數	百分比
請問您近一個月內是否有使用傳統電視（例如：有線電視〔第四台〕、MOD、無線電視）？	有使用	202	66.2
	沒有使用	103	33.8
	總計	305	100.0
請問您平均一天使用傳統電視的時間約為幾小時？	未滿 1 小時	64	31.7
	1～未滿 3 小時	92	45.5
	3～未滿 5 小時	24	11.9
	5 小時以上	15	7.4
	不一定	7	3.5
	不知道/拒答	0	0.0
	總計	202	100.0

資料來源：本研究自行整理

從上述結果來看，民眾使用各類型平臺的時間幾乎為 1~未滿 3 小時。而社群軟體、影音分享平臺與通訊軟體的重度使用者相較其他類別上偏多，本研究認為，這情況應與平臺之性質有關。社群軟體與通訊軟體為民眾用來交流、互動的日常軟體，使用時間長為正常，而網路上影片時間通常較長，民眾觀看一、兩部影片就會花費 30 分鐘至一小時，因此使用的時間也會較長。

（二）使用者對於各平臺服務及使用者條款之滿意度

針對各平臺所設立之使用者條款之民眾滿意程度調查，本研究分為有閱讀使用者條款組，以及沒有閱讀使用者條款組。有閱讀組使用者條款組會再往下細分成：清楚瞭解相關內容、大致瞭解內容、有仔細閱讀，但對內容不太瞭解、有瀏覽過，但沒有仔細閱讀內容，以及拒答等五類。

在社群平臺中，有閱讀使用者條款者占該分類的 57.4%，沒有閱讀者為 38.9%；在影音分享平臺中，有閱讀使用者條款者占該分類的 55.6%，沒有閱讀者為 40.9%；在網路論壇中，有閱讀使用者條款者占該分類的 50.6%，沒有閱讀者為 43.6%；在通訊軟體中，有閱讀使用者條款者占該分類的 55.1%，沒有閱讀者為 40.9%；在網路新聞平臺中，有閱讀使用者條款者占該分類的 44.8%，沒有閱讀者為 48.8%；在拍賣及購物平臺中，有閱讀使用者條款者占該分類的 57.3%，沒有閱讀者為 40.6%。統計調查如表 91 所示。

這個結果告訴我們，在使用該平臺時，有過半數的民眾會先閱讀該平臺的使用者條款。惟在網路新聞平臺上，沒有閱讀使用者條款的民眾大於有閱讀使用者條款的民眾，本研究認為，這是源自於網路新聞平臺的特性。民眾使用網路新聞平臺來閱讀網路新聞，其目的是在「閱讀該新聞」，進而獲得資訊，且多數是透過新聞連結點進去使用，很少有機會能去閱讀到其使用者條款。然在其他類型平臺上，如社群軟體、拍賣和購物平臺等，由於會牽涉到民眾的相關資訊，或有被禁言、無法交易等的問題，因此民眾會特地閱讀相關的使用者條款。

表 91：民眾閱讀平臺服務與使用者條款分布

	社群網站		影音分享平臺		網路論壇		通訊軟體		網路新聞平臺		拍賣、購物平臺	
	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比	樣本數	百分比
有，曾經閱讀過	171	57.4	144	55.6	87	50.6	166	55.1	90	44.8	161	57.3
無，不曾閱讀過	116	38.9	106	40.9	75	43.6	123	40.9	98	48.8	114	40.6
不知道有服務及使用者條款	11	3.7	9	3.5	10	5.8	12	4.0	13	6.5	6	2.1
拒答	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
總計	298	100.0	259	100.0	172	100.0	301	100.0	201	100.0	161	100.0

資料來源：本研究自行整理

此外，針對上述「有閱讀使用者條款」的民眾，本研究將調查他們的了解程度落在何處，並劃分成五項指標：清楚瞭解相關內容、大致瞭解內容、有仔細閱讀，但對內容不太瞭解、有瀏覽過，但沒有仔細閱讀內容，以及拒答。依平臺區分，相關統計圖表如下圖所示。

下圖結果告訴我們，有閱讀過使用者條款的民眾，針對使用者條款的瞭解程度中，除影音分享平臺之外，其他平臺上有瞭解相關內容（含大致瞭解相關內容與清楚瞭解相關內容）者都超過五成。

另外，各平臺也有約二到四成的民眾是「有瀏覽過，但沒有仔細閱讀相關內容」者，選擇此選項的民眾，對於相關的使用者條款可能不甚瞭解。

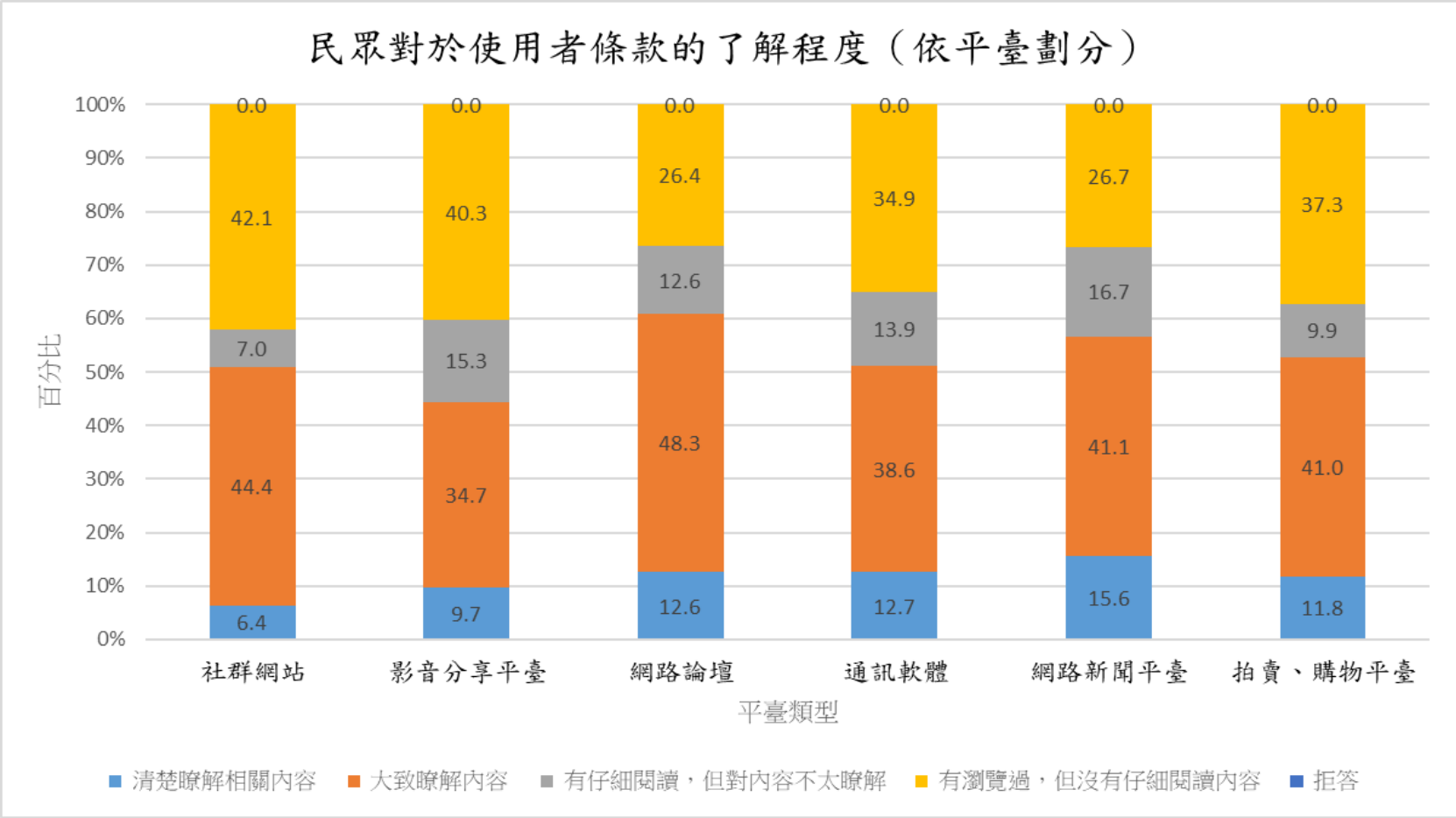


圖 32：民眾對與使用者條款之了解程度

資料來源：本研究自行整理

二、使用者對於平臺各項措施之滿意度

第一部分第二階段之調查將網路上的危害大致分成五大類，包括：政治不實訊息、兒少網路安全、網路霸凌、網路交易安全、個人權益侵害。針對此類網路危害，本研究調查民眾對於網路平臺對於五大危害的處理方式與其使用者條款之滿意程度。

就網路平臺針對「政治不實訊息」訂定的使用者條款，選擇「非常滿意」者，與「有點滿意」者合計達 49.18%，選擇「非常不滿意」者，與「有點不滿意」者，合計達 28.85%。在此選項上，多數民眾皆滿意平臺為「政治不實訊息」所訂定的使用者條款。

其中，表示不滿意的民眾認為，雖然有設立機制，但不實訊息還是很猖獗，不實訊息沒能有效阻斷；有部分民眾則認為，處罰太輕，無法有效遏止不實訊息。

調查統計如下表。

表 92：對「政治不實訊息」所訂定的使用者條款之滿意度

問項	選項	樣本數	百分比
針對「政治不實訊息」所訂定的使用者條款。	非常滿意	73	23.9
	有點滿意	77	25.2
	有點不滿意	68	22.3
	非常不滿意	20	6.6
	不知道/無法回答	67	22.0
	總計	305	100.0

資料來源：本研究自行整理

就網路平臺針對「兒少網路安全」所訂定的刪除機制（例如刪除腥羶色內容），選擇「非常滿意」者，與「有點滿意」者合計達 70.81％，選擇「非常不滿意」者，與「有點不滿意」者，合計達 18.7％。這個結果顯示，超過七成民眾皆滿意平臺為「兒少網路安全」所訂定的刪除機制（例如刪除腥羶色內容）。

其中，表示不滿意的民眾認為，刪除機制並無有效防護兒少網路安全，應可以更加積極來防護兒少網路安全。亦有部分民眾認為，限制不夠嚴謹、罰則太輕。

調查統計如下表。

表 93：對「兒少網路安全」所訂定的刪除機制之滿意度

問項	選項	樣本數	百分比
針對「兒少網路安全」所訂定的刪除機制（例如刪除腥羶色內容）。	非常滿意	113	37.0
	有點滿意	103	33.8
	有點不滿意	41	13.4
	非常不滿意	16	5.2
	不知道/無法回答	32	10.5
	總計	305	100.0

資料來源：本研究自行整理

就網路平臺針對「網路交易安全」所訂定的防詐機制（例如通報及先行下架商品），選擇「非常滿意」者，與「有點滿意」者合計達67.2%；選擇「非常不滿意」者，與「有點不滿意」者，合計達29.6%。這個結果顯示，超過半數民眾皆滿意網路平臺為「網路交易安全」所訂定的防詐機制（例如通報及先行下架商品）。

其中，表示不滿意的民眾認為，網路詐騙仍層出不窮，審查及判定標準並不周全。

調查統計如下表。

表 94：對「網路交易安全」所訂定的防詐機制之滿意度

問項	選項	樣本數	百分比
針對「網路交易安全」所訂定的防詐機制（例如通報及先行下架商品）	非常滿意	109	35.7
	有點滿意	96	31.5
	有點不滿意	45	14.8
	非常不滿意	37	12.1
	不知道/無法回答	18	5.9
	總計	305	100.0

資料來源：本研究自行整理

就網路平臺針對「網路霸凌」所訂定的防護機制（例如暫時關閉留言功能），選擇「非常滿意」者，與「有點滿意」者合計達 67.21%，選擇「非常不滿意」者，與「有點不滿意」者，合計達 22.3%。這個結果顯示，超過半數民眾皆滿意網路平臺為「網路霸凌」所訂定的防護機制（例如暫時關閉留言功能）。

其中，表示不滿意的民眾認為，網路霸凌沒有效處理及減少，仍然很嚴重。

調查統計如下表。

表 95：對「網路霸凌」所訂定的防護機制之滿意度

問項	選項	樣本數	百分比
針對「網路霸凌」所訂定的防護機制（例如暫時關閉留言功能）。	非常滿意	108	35.4
	有點滿意	97	31.8
	有點不滿意	39	12.8
	非常不滿意	29	9.5
	不知道/無法回答	32	10.5
	總計	305	100.0

資料來源：本研究自行整理

就網路平臺針對「個人權益」所訂定的使用者申訴與審查機制，選擇「非常滿意」者，與「有點滿意」者合計達 70.81%，選擇「非常不滿意」者，與「有點不滿意」者，合計達 16.7%。這個結果顯示，超過半數民眾皆滿意網路平臺為「網路霸凌」所訂定的防護機制（例如暫時關閉留言功能）。

其中，表示不滿意的民眾認為，網路平臺的處理速度和回應很糟糕，效率差。

調查統計如下表。

表 96：對「個人權益」所訂定的使用者申訴與審查機制之滿意度

問項	選項	樣本數	百分比
針對「個人權益」所訂定的使用者申訴與審查機制。	非常滿意	106	34.8
	有點滿意	110	36.1
	有點不滿意	42	13.8
	非常不滿意	9	3.0
	不知道/無法回答	38	12.5
	總計	305	100.0

資料來源：本研究自行整理

三、民眾對違法內容移除機制之偏好

網路問卷的第二部分係進行網際網路社會問題治理結構探詢，調查民眾針對網際網路社會問題治理結構所應該有的態樣。在此部份上，問卷將依據三種態樣進行調查：1. 依據管制程度鬆緊度；2. 依據處理範圍；3. 依據行政與司法間的權力關係。研究將依據此三態樣，分析出民眾希望有的治理結構。

首先，關於網路上的違法資訊或內容的寬鬆－嚴格程度：1 為最寬鬆，以網路平臺業者為主，透過自律方式將違法資訊或內容移除；10 為最嚴格，以行政機關或司法機關（法院）為主，依據法令強制將違法資訊或內容移除。

共計有 87.9%的民眾選擇嚴格者（即尺度選擇大於等於 6 者），在這之中，最多人與次多人選擇的尺度為 8（27.2%）與 7（21.0%）；共計有 5.2%的民眾選擇寬鬆者（即尺度選擇小於等於 4 者）；此外，有 6.9%的民眾選擇中立（即尺度選擇 5 者）。

統計資料如下表所示。

表 97：民眾對於網路上違法資訊或內容的移除強度分布

問題	尺度	樣本數	百分比
面對網路上的違法資訊或內容，如果由您設計一套移除機制，請問您較傾向以怎樣的強度進行處理？	1	0	0.0
	2	1	0.3
	3	6	2.0
	4	9	3.0
	5	21	6.9
	6	34	11.1
	7	64	21.0
	8	83	27.2
	9	58	19.0
	10	29	9.5
	總計	305	100.0

資料來源：本研究自行整理

其次，調查移除機制所處理的範圍：1 為最有限，僅將處理重點放在詐騙、兒少保護等社會重視的違法類型，且配合不同事件類型，分別建立對應的移除機制；10 為最廣泛，無論觸犯的是刑法、民法或政府各級機關訂定的行政法規，所有的「違法」資訊或內容都必須處理，且應建立一套一體適用的移除機制。

共計有 81.3%的民眾選擇廣泛者（即尺度選擇大於等於 6 者），在這之中，最多人與次多人選擇的尺度為 7（23.0%）與 8（28.5%）；共計有 11.5%的民眾選擇寬鬆者（即尺度選擇小於等於 4 者）；此外，有 7.2%的民眾選擇中立（即尺度選擇 5 者）。

統計資料如下表所示。

表 98：民眾對於網路上違法資訊或內容的移除範圍分布

問題	尺度	樣本數	百分比
如果要決定這套移除機制所處理的範圍，請問您較傾向哪種做法？	1	0	0.0
	2	5	1.6
	3	10	3.3
	4	20	6.6
	5	22	7.2
	6	25	8.2
	7	87	28.5
	8	70	23.0
	9	40	13.1
	10	26	8.5
	總計	305	100.0

資料來源：本研究自行整理

第三，調查在管理網路上的違法資訊或內容中，行政機關與司法機關這兩者的權限大小：1 行政機關擁有最大權限，行政機關可自行決定裁罰或移除，法院只提供事後的司法救濟；10 為司法機關擁有最大權限，裁罰或移除必須先行經過法院的裁判決定。

共計有 80.7%的民眾選擇嚴格者（即尺度選擇大於等於 6 者），在這之中，最多人與次多人選擇的尺度為 7（27.9%）與 8（26.6%）；共計有 7.5%的民眾選擇寬鬆者（即尺度選擇小於等於 4 者）；此外，有 11.8%的民眾選擇中立（即尺度選擇 5 者）。

統計資料如下表所示。

表 99：民眾認為行政機關與司法機關對於違法資訊或內容處理機制之權限分布

問題	尺度	樣本數	百分比
如果由行政機關與司法機關共同管理網路上的違法資訊或內容，請問在這套管理機制中，您較傾向如何分配兩者的權限大小？	1	1	0.3
	2	3	1.0
	3	9	3.0
	4	10	3.3
	5	36	11.8
	6	31	10.2
	7	85	27.9
	8	81	26.6
	9	29	9.5
	10	20	6.6
	總計	305	100.0

資料來源：本研究自行整理

透過上述三題調查，我們可以初步界定民眾所偏好的網際網路危害的管制態樣為：偏好移除機制範圍廣泛且嚴格，移除方式由行政機關或司法機關依據法令強制將違法資訊或內容移除，同時以法官保留作為保障機制。

往下將三種光譜劃分成兩種圖形進行分析。其一為：移除範圍與法官保留；其二為移除強度與移除範圍。

首先，將光譜結構中移除機制範圍作為 x 軸，法官保留強度作為 y 軸，進行人群的劃分。第一象限為選擇移除範圍廣（強度 6~10）且高度法官保留（強度 6~10）者；第二象限為選擇移除範圍窄（強度 1~5）但高度法官保留（強度 6~10）者；第三象限為選擇移除範圍窄（強度 1~5）但低度法官保留（強度 1~5）者；第四象限為選擇移除範圍廣（強度 6~10）但低度法官保留（強度 1~5）者。依此象限區分，繪製出的圖表如下：

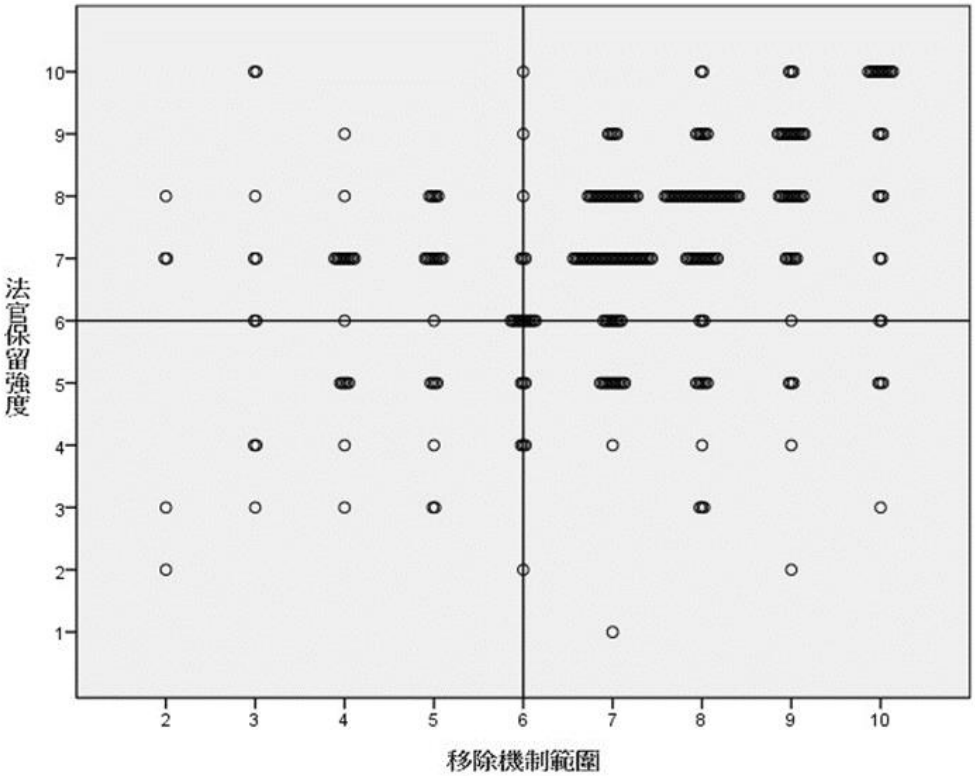


圖 33：移除機制範圍與法官保留象限分析
資料來源：本研究自行整理

統計數據如下表所示：

表 100：移除機制範圍與法官保留強度結構象限表

結構光譜	樣本數	保留	強度
第一象限	225	6～10	6～10
第二象限	20	6～10	1～5
第三象限	16	1～5	1～5
第四象限	44	1～5	6～10

資料來源：本研究自行整理

其次，若將光譜結構中移除機制強度作為 x 軸，移除範圍作為 y 軸，進行人群的劃分。第一象限為選擇高強度移除機制（強度 6~10）且移除範圍廣（強度 6~10）者；第二象限為選擇低強度移除機制（強度 1~5）但移除範圍廣（強度 6~10）者；第三象限為選擇低強度移除機制（強度 1~5）但移除範圍窄（強度 1~5）者；第四象限為選擇高強度移除機制（強度 6~10）但移除範圍窄（強度 1~5）者。依此象限區分，繪製出的圖表如下：

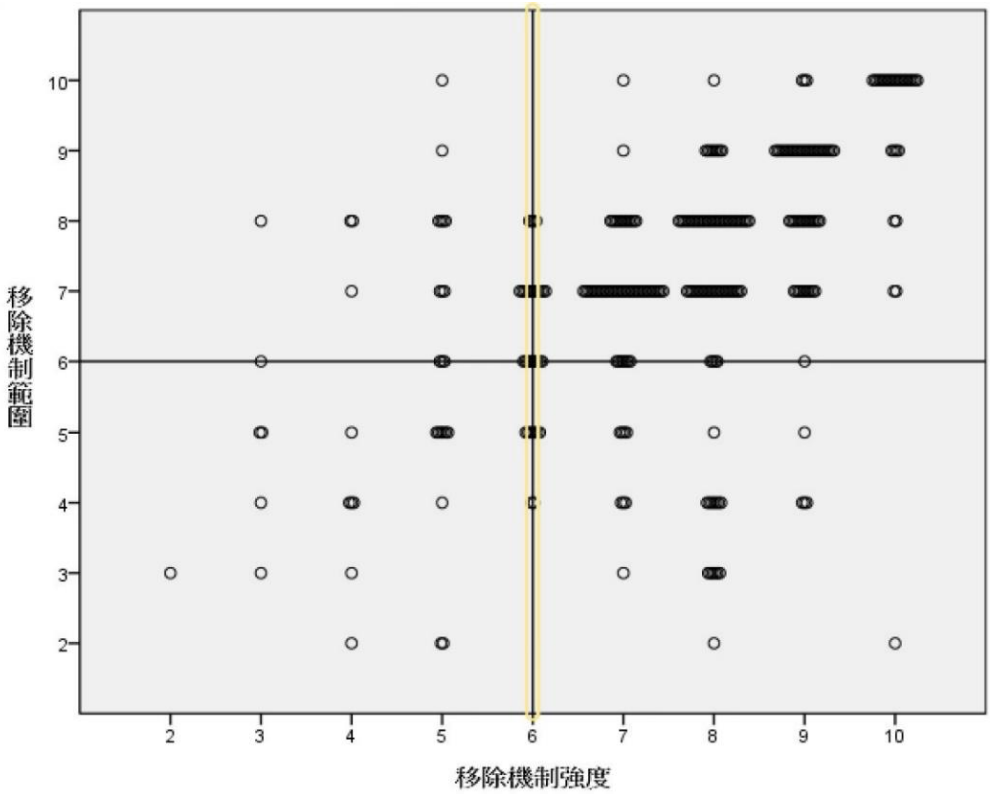


圖 34：移除強度與移除範圍象限分析

資料來源：本研究自行整理

統計數據如下表所示：

表 101：除機制範圍與移除機制強度結構象限表

結構光譜	樣本數	保留	強度
第一象限	231	6～10	6～10
第二象限	16	6～10	1～5
第三象限	20	1～5	1～5
第四象限	38	1～5	6～10

資料來源：本研究自行整理

四、第三方協力治理模型

為了建立網際網路社會秩序，本研究基於一般民眾電訪調查及焦點團體座談諮詢學者專家、業者及公民團體所得之前期研究成果，提出涵納第三方機構、政府與業者的協力治理模式，期望能解決網際網路社會問題。

在此一協力治理模式中，由政府與第三方機構協力，整合各方意見，建立各網路平臺共通的自律框架，再由各網路平臺依照自律框架，訂定平臺的自律規則，並照章執行，做為平臺與其使用者的自律依據。而倘若使用者發現平臺有違反自律規則，應先向平臺進行申訴；若申訴未果，可向第三方機構投訴，機構受理投訴後若確認平臺違反自律規則，或其自律規則違反共通性自律框架，將通報政府相關業務主管機關進行裁罰。

如下圖所示：

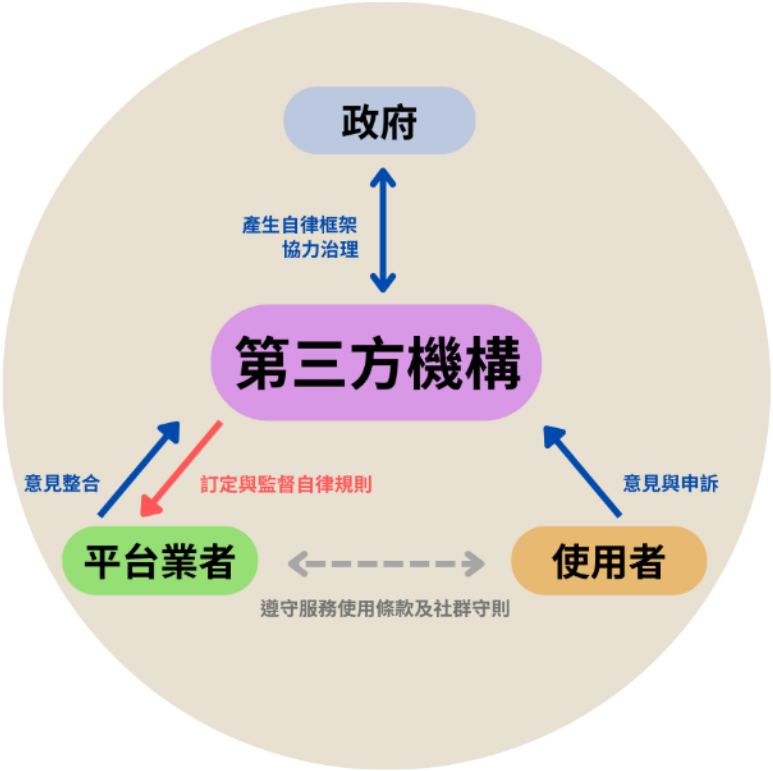


圖 35：第三方協力治理模型架構圖
資料來源：本研究自行整理

（一）民眾對協力治理模型的認同度

第二部份第二階段依據協力治理模型的態樣，分別針對五大問題危害進行民意調查。

總體來看，民眾普遍同意（非常同意與有點同意合併觀之，皆超過八成民眾同意）：在各網路危害上，此治理架構能處理相關的網路危害。同時，民眾也同意該協力治理模型的各角色都被賦予了最適當的責任。

進一步詢問民眾認為協力模型中的角色何者可以再加強責任，則在各類型網路危害中，民眾認為網路平臺應被賦予更多責任，其次是政府，最後是第三方機構。

以數據觀之，皆有超過四成的民眾認為「網路平臺」應被賦予更多責任。在政治不實訊息、兒少網路安全與網路交易安全中，有超過三成的民眾認為「政府」應被賦予更多的責任。

在兒少網路安全、網路交易安全與網路霸凌中，有超過一成五的民眾認為「第三方機構」應被賦予更多的責任。

民眾相關結果如下表所示。

表 102：民眾對協力治理模型之認同度

同意程度	治理結構是否能處理各類型網路危害？（單位：%）				
	政治不實訊息	兒少網路安全	網路交易安全	網路霸凌	個人權益保障
非常同意	25.2	36.7	38.7	40.0	37.7
有點同意	56.4	48.9	48.9	44.6	45.6
有點不同意	9.8	9.5	8.2	7.9	9.5
非常不同意	3.0	1.3	1.0	3.3	3.0
不知道/無法回答	5.6	3.6	3.3	4.3	4.3
總計	100.0	100.0	100.0	100.0	100.0

資料來源：本研究自行整理

表 103：民眾對協力治理模型之認同度（續）

同意程度	治理架構中的各個角色是否被賦予了最適切的責任？（單位：%）				
	政治不實訊息	兒少網路安全	網路交易安全	網路霸凌	個人權益保障
非常同意	29.8	40.0	42.6	40.0	41.0
有點同意	57.0	48.2	47.9	47.9	43.6
有點不同意	6.9	7.2	6.6	6.9	9.8
非常不同意	1.6	0.7	0.3	1.0	1.3
不知道/無法回答	4.6	3.9	2.6	4.3	4.3
總計	100.0	100.0	100.0	100.0	100.0

資料來源：本研究自行整理

表 104：民眾對協力治理模型之認同度（續）

同意程度	我認為架構中的角色，應該被賦予更多的責任，該角色為何？（單位：%）			
	政治不實訊息	兒少網路安全	網路交易安全	網路霸凌
政府	32.2	41.5	37.1	29.0
網路平臺	41.1	42.1	44.6	53.0
第三方機構	26.6	16.4	18.3	18.0
總計	100.0	100.0	100.0	100.0

資料來源：本研究自行整理

往下分析，民眾認為在各網路危害中，應被賦予更多責任的角色可以做何種事情？

以下依據網路問題劃分並做敘述，相關結果如下所示：

1. 在政治不實訊息的問題上，認為政府應被賦予更多責任的民眾（32.2%）中，有 50.7%民眾認為應該由單一主管機關判斷是否為政治不實訊息並決定是否阻斷、移除或裁罰。認為網路平臺應被賦予更多責任的民眾（41.1%）中，有 59.1%民眾認為網路平臺應主動判斷並加註警語或降低排序。認為第三方機構應被賦予更多責任的民眾（26.6%）中，有 63.2%民眾認為第三方機構可要求平臺提供第三方機構認證的透明度報告。

2. 在網路兒少安全的問題上，認為政府應被賦予更多責任的民眾（41.5%）中，有 52.6%民眾認為應該由法院判斷是否危害兒少網路安全並決定是否阻斷、移除或裁罰。認為網路平臺應被賦予更多責任的民眾（42.1%）中，有 50.6%民眾認為網路平臺應主動判斷並加註警語或降低排序。認為第三方機構應被賦予更多責任的民眾（16.4%）中，有 56.7%民眾認為第三方機構可向危害兒少網路安全問題的網路平臺進行裁罰。

3. 在網路交易安全的問題上，認為政府應被賦予更多責任的民眾（37.1%）中，有 50.8%民眾認為應該由單一主管機關判斷是否具有網路交易安全的風險，並決定是否阻斷、移除或裁罰。認為

網路平臺應被賦予更多責任的民眾（44.6%）中，有 53.8%民眾認為網路平臺應主動判斷並移除。認為第三方機構應被賦予更多責任的民眾（18.3%）中，有 59.4%民眾認為第三方機構可針對違規者通報網路平臺或主管機關。

4. 在網路霸凌的問題上，認為政府應被賦予更多責任的民眾（29.0%）當中，有 50.9%民眾認為應該由法院判斷是否為網路霸凌問題並決定是否阻斷、移除或裁罰。認為網路平臺應被賦予更多責任的民眾（53.0%）中，有 54.6%民眾認為平臺應主動判斷並移除。認為第三方機構應被賦予更多責任的民眾（18.0%）中，有 63.6%民眾認為第三方機構可向未妥善管理網路霸凌問題的平臺提出警告，並公布名單。

表 105：民眾認為應被賦予更多責任的角色可做的事情

	我認為被賦予責任的角色，可以做的事情為：(單位：%)							
	政治不實訊息		兒少網路安全		網路交易安全		網路霸凌	
	選項	百分比	選項	百分比	選項	百分比	選項	百分比
政府	由單一主管機關判斷是否為政治不實訊息並決定是否阻斷、移除或裁罰。	50.7	由單一主管機關判斷是否危害兒少網路安全並決定是否阻斷、移除或裁罰。	47.4	由單一主管機關判斷是否具有網路交易安全的風險，並決定是否阻斷、移除或裁罰。	50.8	由單一主管機關判斷是否為網路霸凌問題，並決定是否阻斷、移除或裁罰。	49.1
	由法院判斷是否為政治不實訊息並決定是否阻斷、移除或裁罰。	49.3	由法院判斷是否危害兒少網路安全並決定是否阻斷、移除或裁罰。	52.6	由法院判斷是否具有網路交易安全的風險並決定是否阻斷、移除或裁罰。	49.2	由法院判斷是否為網路霸凌問題並決定是否阻斷、移除或裁罰。	50.9
	總計	100.0	總計	100.0	總計	100.0	總計	100.0
	選項	百分比	選項	百分比	選項	百分比	選項	百分比
網路平臺	主動判斷並加註警語或降低排序。	59.1	主動判斷並加註警語或降低排序。	50.6	主動判斷並加註警語或降低排序。	46.2	主動判斷並加註警語或降低排序。	45.4
	主動判斷並移除。	40.9	主動判斷並移除。	49.4	主動判斷並移除。	53.8	主動判斷並移除。	54.6
	總計	100.0	總計	100.0	總計	100.0	總計	100.0

	選項	百分比	選項	百分比	選項	百分比	選項	百分比
第三方機構	要求平臺提供第三方機構認證的透明度報告。	63.2	要求平臺提供第三方機構認證的透明度報告。	43.3	針對違規者通報平臺或主管機關。	59.4	向未妥善管理網路霸凌問題的平臺提出警告，並公布名單。	63.6
	向傳播政治不實訊息的平臺進行裁罰。	36.8	向危害兒少網路安全問題的平臺進行裁罰。	56.7	向未處理好網路交易安全問題的平臺進行裁罰。	40.6	向未妥善管理網路霸凌問題的平臺進行裁罰。	36.4
	總計	100.0	總計	100.0	總計	100.0	總計	100.0

資料來源：本研究自行整理

（二）第三方機構與其他角色的互動關係

本研究提出的協力治理模型中，第三方機構扮演尤為重要的角色。從民眾的角度出發，調查發現有 46.2%的民眾認為第三方機構應由多方團體或個人共同組成。在此模式下的第三方機構有如：財團法人中華民國消費者文教基金會（消基會）、台灣事實查核教育基金會（事實查核中心）、台灣展翅協會等。

詳細統計資訊如下表。

表 106：民眾偏好的第三方機構組成結構

	次數分配	百分比
由相關業者組成（註解 A 模式）的第三方機構	104	34.1
由多方團體或個人組成（註解 B 模式）的第三方機構	141	46.2
由政府捐助成立的財團法人（註解 C 模式）擔任第三方機構	60	19.7
總計	305	100.0

資料來源：本研究自行整理

另外，第三方機構與協力治理模型中各角色的互動關係亦會影響協力如何進行、協力的完成度，並會對協力模式能否順利運作有極大的影響。故以下將調查民眾如何看待第三方機構與各角色（包含：政府、平臺業者與使用者）之互動關係。

1. 第三方機構與政府間的互動關係

在第三方機構與政府的互動過程中，會由兩者進行雙向的溝通，討論並產生適合的網路自律框架，並由第三方機構協助政府治理網路平臺。

據此，從調查結果來看（將有點同意與非常同意合併為同意），92.1%的民眾肯定第三方機構有能力能與政府協力訂定平臺自律框架，也88.8%的民眾認為第三方機構有能力判斷平臺是否違反政府訂定的

共通性自律框架，同時有 88.1%的民眾同意第三方機構所做的判斷會是公正客觀的。最後，有 83.9%的民眾認為由第三方機構比政府更適合出面判斷平臺是否違規。這結果告訴我們，民眾認同第三方機構的存在，也認可其與政府間的互動關係。

詳細統計資訊如下表。

表 107：民眾對於第三方機構與政府之互動關係的看法

問項	同意程度	樣本數	百分比
我認為第三方機構有能力與政府協力訂定平臺自律框架	非常同意	108	35.4
	有點同意	173	56.7
	有點不同意	17	5.6
	非常不同意	4	1.3
	不知道/無法回答	3	1.0
	總計	305	100.0
我認為第三方機構有能力判斷平臺是否違反政府訂定的共通性自律框架。	非常同意	101	33.1
	有點同意	170	55.7
	有點不同意	27	8.9
	非常不同意	3	1.0
	不知道/無法回答	4	1.3
	總計	305	100.0
我認為由第三方機構出面判斷平臺是否違規是公正的。	非常同意	101	33.1
	有點同意	168	55.1
	有點不同意	29	9.5
	非常不同意	2	0.7
	不知道/無法回答	5	1.6
	總計	305	100.0
我認為第三方機構比政府更適合判斷平臺是否違規。	非常同意	101	33.1
	有點同意	155	50.8
	有點不同意	28	9.2
	非常不同意	2	0.7
	不知道/無法回答	19	6.2
	總計	305	100.0

資料來源：本研究自行整理

2. 第三方機構與網路平臺間的互動關係

在第三方機構與網路平臺的互動過程中，平臺業者會將業者意見整合給第三方機構，而第三方機構則會協助其訂定自律規則，並監督平臺業者的自律規則實施狀況。

據此，從調查結果來看（將有點同意與非常同意合併為同意），有92.7%的民眾認為第三方機構有能力判斷平臺是否違反平臺自訂的自律規則，90.8%的民眾肯定第三方機構有協助平臺進行意見整合的能力，87.8%的民眾認為第三方機構比政府更適合整合網路平臺的意見。這結果告訴我們，民眾認同第三方機構的存在，能有助於協助判斷平臺是否違反自律規則，並且協助整合平臺意見。

詳細統計資訊如下表。

表 108：民眾對於第三方機構與網路平臺之互動關係的看法

問項	同意程度	樣本數	百分比
我認為第三方機構有能力判斷平臺是否違反平臺自訂的自律規則。	非常同意	94	30.8
	有點同意	189	62.0
	有點不同意	18	5.9
	非常不同意	2	0.7
	不知道/無法回答	2	0.7
	總計	305	100.0
第三方機構能夠協助平臺進行意見整合。	非常同意	102	33.4
	有點同意	175	57.4
	有點不同意	18	5.9
	非常不同意	5	1.6
	不知道/無法回答	5	1.6
	總計	305	100.0
我認為第三方機構比政府更適合整合網路平臺的意見。	非常同意	106	34.8
	有點同意	162	53.1
	有點不同意	26	8.5
	非常不同意	0	0.0
	不知道/無法回答	11	3.6
	總計	305	100.0

資料來源：本研究自行整理

3. 第三方機構與使用者間的互動關係

在第三方機構與使用者的互動過程中，使用者若遇到相關問題，但自網路平臺申訴無果後，可向第三方機構進行意見反映與申訴，而第三方機構則會協助民眾爭取權益。

據此，從調查結果來看（將有點同意與非常同意合併為同意），有96.3%的民眾在向平臺申訴無果後，願意向第三方機構申訴，86.2%的民眾認為向第三方機構申訴，比向政府機關申訴更能有效解決在網路平臺遭遇到的問題，87.5%的民眾認為若將意見告訴第三方機構，能有效改善整體網路的使用環境。

這結果告訴我們，民眾認同第三方機構的存在，能成為民眾在使用網路的後盾，協助民眾改善整體網路使用環境。值得注意的是，在狀告法院或向第三方機構申訴的選擇中，有 66.8%的民眾認為直接狀告法院，比向第三方機構申訴更能有效解決在網路平臺遭遇到的問題，此題應與第四部份光譜題及民眾對協力模式下權責分配的態度進行合併觀察。

前面已分析大多數民眾皆認同本研究的協力模式設計，故綜合觀之，民眾在此期待的可能只是一個確定能夠得到解答的申訴機構，而法院在民眾心中確實扮演一個最高的申訴機構，因此在第三方機構尚未出現前，民眾傾向於選擇已知的結果。但這並不代表民眾不認同第三方機構，亦不代表民眾不願意向第三方機構進行申訴。

詳細統計資訊如下表。

表 109：民眾對於第三方機構與使用者之互動關係的看法

問項	同意程度	樣本數	百分比
當我向平臺申訴未果時，我願意向第三方機構提出進一步申訴。	非常同意	141	46.2
	有點同意	153	50.2
	有點不同意	5	1.6
	非常不同意	4	1.3
	不知道/無法回答	2	0.7
	總計	305	100.0
我認為向第三方機構申訴，比向政府機關申訴更能有效解決我在網路平臺遭遇到的問題。	非常同意	118	38.7
	有點同意	145	47.5
	有點不同意	24	7.9
	非常不同意	4	1.3
	不知道/無法回答	14	4.6
	總計	305	100.0
我認為直接狀告法院，比向第三方機構申訴更能有效解決我在網路平臺遭遇到的問題。	非常同意	98	32.1
	有點同意	106	34.8
	有點不同意	64	21.0
	非常不同意	18	5.9
	不知道/無法回答	19	6.2
	總計	305	100.0
我認為將我的意見告訴第三方機構，能有效改善整體網路平臺的使用環境。	非常同意	106	34.8
	有點同意	161	52.8
	有點不同意	23	7.5
	非常不同意	4	1.3
	不知道/無法回答	11	3.6
	總計	305	100.0

資料來源：本研究自行整理

五、線上串流影音服務擴充題

線上串流影音服務題共有五題。其中有 21.3%的民眾在近一個月內曾使用盜版網站（如楓林網及小鴨影音等）觀看串流影音。此外，57.8%的民眾使用時間為一小時以上，未滿三小時。在調查民眾使用串流影音服務時，所曾經遭遇過消費爭議問題中，有超過六成的民眾未曾有過消費爭議，而有 18.1%的民眾遇到的消費爭議是服務不穩定或無預警被中斷服務，次高的是續訂問題（13.7%），次則是退訂問題（12.9%）。

另外，民眾認為最需要解決的消費爭議事件是服務不穩定或無預警中斷（32.6%），其次是續訂問題（21.1%），再次則是退訂問題（16.8%）。最後，民眾認為政府面對「串流影音服務的消費爭議」最需要採取的措施中，有 55.7%的民眾認為應立法課予服務提供者相關義務（例如：要求業者公告服務使用條款，包含消費者保護措施、服務中斷賠償或隱私政策等），而選擇透過該產業的公協會轉介，以業者自律之方式處理的民眾則有 4.6%。詳細統計資訊如下表。

表 110：民眾使用串流影音平臺之統計

串流影音平臺	樣本數	百分比	串流影音平臺	樣本數	百分比
Netflix	125	41.0%	MyVideo	16	5.2%
Disney+	59	19.3%	Hami Video	13	4.3%
Amazon Prime	4	1.3%	KKTV	11	3.6%
Catchplay+	4	1.3%	LiTV	18	5.9%
HBO GO	6	2.0%	GagaOOLala	1	0.3%
HBO MAX	5	1.6%	四季線上	3	1.0%
Hulu	1	0.3%	公視+	19	6.2%
Apple TV+	6	2.0%	楓林網	31	10.2%
LINE TV	103	33.8%	小鴨影音	34	11.1%
愛奇藝	57	18.7%	其他（請說明）	2	0.7%
巴哈姆特動畫瘋	39	12.8%	沒有使用	56	18.4%
總計		樣本數		百分比	
		305		100.0%	

資料來源：本研究自行整理

表 111：民眾使用串流影音平臺的平均時間

時間	樣本數	百分比
未滿 1 小時	54	21.7%
1～未滿 3 小時	144	57.8%
3～未滿 5 小時	28	11.2%
5 小時以上	12	4.8%
不一定	11	4.4%
不知道／拒答	0	0.0%
總計	249	100.0%

資料來源：本研究自行整理

表 112：民眾使用串流影音平臺時所曾遭遇的消費爭議

問項	樣本數	百分比
退訂（例如：介面上找不到退訂功能，須致電客服處理）	32	12.9%
續訂（例如：無法更換付費方案，或自動續訂時被重複扣款）	34	13.7%
服務不穩定或無預警中斷	45	18.1%
信用卡資料外洩	20	8.0%
無法聯繫上客服	25	10.0%
其他（請說明）	1	0.4%
未曾有過消費爭議	154	61.8%
總計	249	100.0%

資料來源：本研究自行整理

表 113：民眾認為消費爭議中最需要被解決的問題

問項	樣本數	百分比
退訂（例如：介面上找不到退訂功能，須致電客服處理）	16	16.8%
續訂（例如：無法更換付費方案，或自動續訂時被重複扣款）	20	21.1%
服務不穩定或無預警中斷	31	32.6%
信用卡資料外洩	15	15.8%
無法聯繫上客服	12	12.6%
其他（請說明）	1	1.1%
總計	95	100.0%

資料來源：本研究自行整理

表 114：民眾認為政府面對「串流影音服務的消費爭議」最需要採取的措施

問項	樣本數	百分比
立法課予服務提供者相關義務（例如：要求業者公告服務使用條款，包含消費者保護措施、服務中斷賠償或隱私政策等）	170	55.7%
設立單一窗口，作為處理串流影音服務消費爭議的專責機構	121	39.7%
透過該產業的公協會轉介，以業者自律之方式處理	14	4.6%
其他（請說明）	0	0.0%
總計	305	100.0%

資料來源：本研究自行整理

觀察上述結果，可以發現在線上串流影音服務上，儘管目前多數民眾未曾有過消費爭議，但政府及平臺仍需要特別注意關於服務穩定程度與訂閱服務相關的問題，並研議出較好的服務措施。

六、綜合分析

本研究進一步將該階段題組與前階段光譜題組合併分析，x 軸為移除機制強度，y 軸為法官保留強度，共將人群分成四象限。

（一）強度偏好與協力模型認同交叉分析

本研究透過四象限卡方分析探索強度偏好與協力模型認同之間的關聯。結果顯示，對於高移除強度與高移除範圍的認同者，或是認同法官保留與高移除強度的受訪者，對協力模式的認同程度明顯較高。相對地，當兩者偏好不一致或都較低時，對於協力模式的接受程度並無明確趨勢。

這樣的結果意味著，本研究提出的協力模式，其核心特點和要求，更接近於對網路社會問題處理具有嚴格標準的受訪者的期待。對於大部分的民眾而言，這或許代表協力模式所帶來的治理機制，實際上是一種更為嚴謹和全面的方法。此外，這也強調了自律架構內容在整個協力模式中的重要性。

從光譜題的分析中，我們可以觀察到大多數受訪者的偏好都集中在第一象限，顯示他們對於移除的強度和範圍都持有相當嚴格的態度。因此，政府在制定相關政策時，必須明確地定義自律架構的範疇，並給予網路平臺和第三方適當的授權，確保其有足夠的能力來有效執行移除違規內容的任務。

在這樣的協力模式中，第三方機構的角色尤為關鍵。他們不僅在協助偵查違規平臺上扮演著重要角色，還需要在接到民眾的投訴後進行初步的調查。因此，政府應該賦予第三方適當的權限和資源，使他們能夠更有效地執行這些職責，包括要求網路平臺提供透明度報告或在必要時公開警告和名單。

（二）使用者條款理解程度與協力模型認同交叉分析

分析過程中，旨在探討民眾對於使用者條款的理解程度與其對協力模型的認同度之間的可能關聯性。首先，本研究對參與者進行了分群，區分出對使用者條款有高度理解的群體和理解程度較低的群體。接著，我們進行了交叉分析，將這兩群體在協力模型認同度上的得分進行對比。

在分析結果中，我們發現高度理解使用者條款的民眾在協力模型的認同度上並未明顯優於理解程度較低的民眾。換句話說，儘管某些參與者對使用者條款有較深入的了解，但這並未直接轉化為對協力模型的更高認同度。

這樣的結果提供了一個重要的啟示：儘管使用者條款的理解程度是影響協力模型認同的可能因素，但它不是唯一或最主要的因素。其他如個人價值觀、文化背景、使用經驗等多種因素可能同樣影響著人們對協力模型的認同度。

總結而言，儘管我們在初步的假設中預期存在某種關聯，但實際的研究結果顯示，使用者條款的理解程度與協力模型認同度之間並無明確的相關性。

（三）第三方機構組成與協力模型認同交叉分析

分析過程中，旨在探討第三方機構的組成模式與協力模型認同度之間的可能關聯性。在研究樣本中，第三方機構的組成主要包括三種形式：商業團體（如公會）、由多方團體或個人共同組成的組織（如基金會），以及由政府捐助成立的財團法人。透過 ANOVA 交叉分析，我們期望能夠確定這些不同組成模式的第三方機構是否與協力模型認同度存在顯著差異。

然而，研究結果顯示，無論是哪種組成模式的第三方機構，其與協力模型認同度之間的差異均未達到統計上的顯著性。這意味著，在考慮第三方機構的組成模式與協力模型認同度之間的關聯時，其他未被考慮的因素或變數可能也對結果產生影響。

此結果提供了一個重要的觀點，即第三方機構的組成模式本身可能不是影響協力模型認同度的主要因素。未來的研究可以進一步探討其他可能的變數，以更為全面地理解和解釋協力模型認同度的形成和變化。

（四）小結

本研究透過多種交叉分析方法探索了協力模型認同度與其相關因素之間的關聯性。首先，對於高度認同高移除強度與高移除範圍的受訪者，或是認同法官保留與高移除強度的受訪者，對協力模式的認同程度明顯較高。這顯示出，大部分的民眾對於網路社會問題的處理有著嚴格的標準，而協力模型可能提供了一種相對較為全面和嚴謹的解決方案。

然而，本研究也發現，儘管高度理解使用者條款的民眾對於協力模型的認同度可能有所期待，但實際的結果卻未顯示明確的相關性。這暗示著，協力模型的認同度可能受到多種因素的影響，而不僅僅是使用者條款的理解程度。

此外，第三方機構的組成模式與協力模型認同度之間似乎沒有顯著的關聯性，指出了在探討協力模型認同度的因素時，需要考慮到更多可能的變數和因素。

交叉分析為我們提供了對於協力模型認同度的深入洞察，並指出了其背後可能的影響因素。為了提升民眾的認同度，在協力治理架構上還需進一步探討其他潛在的因素。

第三節　諮詢座談會辦理成果

基於一般大眾電訪問卷及網路問卷、專家學者與業者、公民團體、焦點團體座談會之面訪結果，本研究於 112 年 12 月 15 日舉行「網際網路傳播社會調查暨法制政策架構」諮詢座談會。

相關出席名單如下：

表 115：「網際網路傳播社會調查暨法制政策架構」諮詢座談會出席名單

姓名	單位
尤騰毅	城邦媒體出版集團法務主任
盧恩廣	Google 政府事務及公共政策部經理 *會後書面意見
王天岑	禾倣顧問服務有限公司總經理（Google 代表）
劉昱均	台北市電腦商業同業公會資安法律組組長
林孟楠	中原大學財經法律學系副教授
廖洲棚	空中大學公共行政學系副教授
劉定基	政治大學法律系副教授
羅慧雯	世新大學傳播管理學系助理教授
陳敦源	政治大學公共行政學系教授　*會後個別訪談

資料來源：本研究自行整理

諮詢座談會主要想探討：一，對於網路調查問卷的解讀結果，是否有可以精進之處？二，本研究所提出之協力治理模型中，是否有可改善或調整的空間？三，為了順利運行此協力治理模型，跨部會間該如何整合？其角色應該如何被設計？四，有關自律框架的設定，應朝哪個方向前進？相關完整題綱如下：

表 116：「網際網路傳播社會調查暨法制政策架構」諮詢座談會討論題綱

討論題綱
一、本研究基於世界主要國家之網路政策歸納，透過網路調查探詢民眾對於違法內容處理模式之意向，發現：多數民眾對於網路社會問題的處理模式呈現出處理強度高（由行政或司法機關依法令強制移除違法資訊）、處理範圍廣泛（建立所有違法內容一體適用之移除機制），以及高度法官保留（裁罰或移除須先行經過法院判決）之偏好。另一方面，針對網路治理結構之探詢，多數民眾則傾向課予平臺業者更高的責任，兩者之解讀應如何調和？整體而言，研究團隊對於問卷調查結果的判讀又是否有其他可精進之處？ 二、為解決網際網路社會問題，建立符合當代社會需求之公共問責模式，本研究提出涵蓋政府、平臺及第三方機構之「協力治理模式」，而此一模式亦在網路調查中受到偏好傾向較嚴格的多數民眾認同。整體而言，此一模式是否還有改善或調整的空間？ 三、在本研究提出的協力治理模式下，跨部會間的法規制度應如何進行整合？以國家通訊傳播委員會為例，其對內與各部會之決策、資源協力、意見反饋模式，以及對外與第三方與業者、民眾溝通時需扮演的角色與任務應如何設計？ 四、承上，在本研究提出的協力治理模式下，自律架構的規範方向與內容框架應秉持怎樣的原則建立？其具體內容應如何設計為宜？

資料來源：本研究自行整理

以下針對討論題綱逐一分析座談結果。

一、網路調查問卷之解讀結果探討

首先，關於網路調查結果的解讀，與會的專家學者多數認為民眾的意見僅能做為決策的參考，不適合做為決策的依據。與會專家此言主要考量研究問題的性質以及問卷調查手法的限制。舉例來說，有學者認為，本研究所欲解決的問題已經到達了「憲法層次」，不適合透過民意調查做為政策決策的依據。

有做民意調查或者是網路調查，可以知道一些民眾的想法，但是對於比較管制層面的問題，或憲法層面的議題，這個調查我覺得參考就好。畢竟問題其實很多，即使盡力去解釋，還是會有一些溝通上面的誤差。(劉定基副教授)

從學者的言談中得知，並非所有的議題都適合透過民意調查進行。當然我們可以從民意調查當中知道民眾的意向，但是民眾的意向並非所有政策問題都需要先優先考量的指導原則。該學者認為「憲法層次」的議題，就不是以民眾的意向為依歸的問題類型。這類型的問題仍然應該回歸到「應然」的制度設計或法律層次的討論。

除了問題層次過高，可能不適合使用民意調查之外，亦有學者指出本研究透過線上平臺發放問卷，可能導致樣本的自我選擇（self-selected）。

EZChoice 我也用過，是自願受訪者的樣本，雖然母體在選擇上面，可能可以用「事後加權」的方式去處理，但是因為是給予填答者誘因進來填，再加上題目的前提是在問違反了這些情況，所以我覺得這個可能是我們要小心的地方。如果我們直接用調查結果來解讀民眾特別偏好高強度的管制模式，在判讀上面就要非常小心。(廖洲棚副教授)

意思是，因為是受訪者自願選擇參加的樣本，本身可能就有偏誤，即便可用事後加權的方式使其接近母體，但本身的偏誤並無法靠這樣的方式消除。因此該學者認為，在統計結果的解讀上必須要非常小心。

例如，在光譜題當中民眾多數選擇偏好高強度、範圍廣、高法官保留的嚴格模式，但實際上高強度的管制是不是真的就是民眾最偏好的，也許答案並不能這麼絕對。

二、協力治理模型之調整建議

歸納專家座談針對本研究所提出之協力治理模型的意見，大概可以分成二點：

（一）第三方機構的組成與運作是關鍵

由於第三方機構是本研究所設計的協力治理模式的核心，其組成與運作會是該模式成敗的關鍵。因此席間有多位學者關心其組成以及運作的問題。包含了第三方機構由誰經營？由誰組成？是單一機關經營，還是以聯盟的方式組成？如果是聯盟，業者、公協會、政府機關是否有席次比例的設計？這些問題的答案都關係到這個機制的運作是否能平衡，並產生公信力。

假如有聯盟的話，其實更大的重點是，誰會加入？比例是什麼？業者那麼多、公協會那麼多、政府機關那麼多，席次比例應該會是什麼？一旦這件事情可以稍微抓住平衡，我相信運作機制不見得不可行，各界可能不見得滿意，但反對程度也不見得那麼高。(劉昱均組長）

除了第三方機構的組成、席次比例問題，運作的問題也需要提前考量。若第三方機構像個聯盟，聯盟內成員眾多，要整合意見也相當不容易，或許可以考慮內部以分組的方式進行決策。即便如此，可能運作起來都需要時間適應，因此應該不要要求一次到位，需以漸進的方式逐步推動。

如果要讓聯盟並不是只是溝通的角色，因為裡面會有很多的利害關係人，決策效率不好，所以聯盟向下應該要再有個別的分組，因議題、因要討論政策，比如說自律框架，集市

中心的自律框架跟影音平臺的自律框架，跟社群平臺的自律框架，我覺得應該會不一樣吧？總不能要這五十幾個人，共同一起討論這些的自律框架。可以分小組進行，小組裡面有業者也有專家學者，也有民間代表，也有政府機關，這都是可以的。如果假設真的要這麼做，我覺得副理應該很快就變白頭髮，是困難的，但是可行的。選擇這個做發展方向的話，不需要一步到位。所有的政策發展都是從 model，大家覺得不錯，再慢慢的擴大。不要一開始做超大聯盟，然後要分十幾個組。把最重要的問題先拿下來。（劉昱均組長）

從與會專家學者的角度來看，他們雖然認同以第三方機構為核心的協力治理機制是可行的、有解決問題能力的，但他們認為前提必須是第三方機構的組成與運作具備代表性、公平、漸進、互信等原則。唯有制度設計能讓第三方機構在組成上與運作上達到具備代表性、公平、漸進、互信，圍繞在第三方機構的協力治理模式才能成為網際網路社會問題的解決方案。

（二）必須思考行為者之間的權力制衡

席間學者提到，協力模式在名詞的意向上給人進步的感覺，因此民眾在不瞭解其內涵與細節的情況下很容易表達支持，但實際上有許多的案例成效不高，或是無法貫徹。

有一個可能性就是大家很常聽到公私協力、協力治理，所以看到這個就會覺得應該是好的進步，但是要做起來其實很難，民眾可能就沒有想到。例如之前跟政治大學公共行政學系學系的老師們做過公民審議方式的立法，我給法律的地方提供了一些建議。如果提出來這個，大家也都會很喜歡，但是，第一個，成本非常高，實際上成效其實不高。看過的一個就是數位身份證，另一個就是健保，後來都不了了之了。所以我有點擔心這個架構實際上運作的情況是不是好。第三個的問題，跨部會之間的法規整合，前提就假設要接受現狀，各部

會各自在立法，所以需要來整合一下。(劉定基副教授)

案例成效不高或無法貫徹的原因，可能就來自於協力治理模式是否能夠有效達成行為者之間的權力相互制衡。

席間另有學者說明，網際網路社會問題的治理已經來到了憲政層級；因其關係到一般人民的基本權利保障，以及行政部門的權限。當行政部門因為各種原因必須要將網際網路社會問題的治理權限外包（協力也是一種外包），原主管的行政機關與被外包出去的民間協力組織之間的關係就必須要謹慎設計。

在此有兩個主要的關係必須討論：人民權利保障的責任歸屬，以及權力如何制衡。

學者陳敦源認為，協力治理模式的關鍵不完全只有「信任」(trust)，還有「權力」(power) 問題；信任與權力這兩個元素就像是孿生雙塔一樣，同時並存，也同時關係著治理機制運作的成敗[903]。信任的產生來自於權力的節制，而權力是否能有效的節制，就來自於制度設計是否能清楚界定權力的範圍。權力範圍的界定可以透過行為者能影響或掌握的資源來討論，例如：人事任命、預算來源、席次比例等。

應該是說還是要回到那個 constitutional level，然後往下看這個機制裡面比較關鍵的，應該就是這個第三方機構跟政府的這個關係，而且這政府一定是行政部門。所以你這樣談的時候他一定有缺陷，因為他已經 moving away from 我們本來的 check and balance，甚至有很多時候人家會講說你這樣幹是為什麼，因為一方面讓民眾對你有信心，另外一方面逃避立法院監督，所以反而是反過來說那這個 operation 你還要看公視，公視那邊也要跟他學一點，因為公視有一個什麼什麼政黨，他就乾脆把政黨看成是 landscape，所以在那個第三方機構裡面就用政黨比例代表，那這個到底好不好我不知道，可是他也是一個 solution 對不對，你不要否認說好像把他丟

[903] Ran, B., & Qi, H. (2019). The entangled twins: Power and trust in collaborative governance. Administration & Society, 51(4), 607–636

到外面來之後就沒有政治性了，就用粉紅泡泡把這些事情都處理了，我覺得沒有那麼簡單。(陳敦源教授)

另有學者亦提及第三方機構自我監督的問題，呼應了權力必須被節制的重要性。該位學者強調的是第三方機構的獨立性必須被保護，因此其預算來源、人事組成都是重要關鍵。政府的手是否對人與財有影響的權力、是否應該要有「獨立董事」的概念、該用什麼樣的制度設計確保第三方機構的獨立性，這些都是重要必須考量、解決的問題。

不同管制程度的政策設計思維要配合網路媒體的特性來發展。比如說，在管制思維上，應該要往「聯防」的概念來發展。也就是說，原來業者也不希望品牌變成是犯罪的溫床，那我如何去形成聯防機制？讓業者跟政府來合作，政策工具要引導成「聯防」這個概念去做發展。對於不願意配合聯防的業者，我們應該要有一些規範，來要求它一定要配合我們去做聯合管制。第二個，對於鼓勵第三方機構自我監督，就是說以比較公正客觀的立場來監督平臺業者的經營方式，看看有沒有按照它所宣稱的自律模式在執行，政策工具設計的核心，應該是要確保第三方機構的獨立性。舉例來講，我可不可以讓平臺業者來捐贈，然後設置聯盟機構？或者是說，機構組織要「獨立董事」的概念放在這裡，獨立董事應該要具有什麼樣的資格，讓它可以發揮公正第三者的立場？再鼓勵業者確實落實自律條件。(廖洲棚副教授)

從上述學者的意見可知，第三方機構的獨立性、第三方機構與政府的關係、政府對於第三方機構的權力節制，將會是協力治理模式的重點。目標是要能透過權力的相互節制、制衡，讓第三方機構的獨立性夠高，才能產生足夠的信任，維護協力模式的運作與平衡。

同樣地，也有業者代表呼籲，若欲將違法內容調控的權力賦予第三方機構，理想中的治理框架應透過清楚明確的法規授權，使第三方機構獨立於政府機關的控制。

第三方治理機構應享有結構獨立，以此降低其成為政治俘虜（political capture）的可能性。應該讓所有利害關係人都對該機構治理決定的客觀與透明充滿信心（盧恩廣政府事務及公共政策部經理）。

三、跨部會法規制度之整合建議

本研究所設計的協力治理模式，包含政府內部的協力；期待政策主管機關能夠協調各業務主管機關盤點相關法規，並定期整合。該項協力任務需要跨部會之間的合作，業者亦表達相關法規整合的必要：

如果在政府在這方面要做管制，我們一定是會配合的。不過要事先讓我們知道，我們要遵守哪些規定？然後希望多跟我們溝通，而不是說法令出來，或者說看到協力框架，叫我們開始自律，但是我們其實都不知道內容。（尤騰毅法務主任）

在推動的這方面，可以從各個法令去做，業者就會慢慢地適應，而不是一下就說要遵守這個框架，媒體人、出版人可能就會有比較大的反彈。（尤騰毅法務主任）

除了法規有必要整合，治理的層次也需要思考。「多層次治理」將不同的問題類型，依照嚴重程度、重要程度等進行分類，並依照類型的不同設計不同層次的治理模式。席間其中一位學者建議，網際網路社會問題的治理模式，可採取多層次治理的概念，依照問題的嚴重程度分為：放任機制、鼓勵機制、管制機制等三個層次。

我有提出「多層次治理」的概念，就是配合這三個程度，有不同治理機制的設計。任其發生的機制設計，目標是讓它有健全的網路平臺的市場。第二個，就是鼓勵它發生的機制設計，目標是要讓網路平臺的透明度增加，讓業者承諾要做的事情確實有做到，以便使用者能夠做出比較好的選擇。第三個層次，就是「高強度管制」的層次，必須要在介入管制之前，因為個別的主管機關，法令有不同公共利益的任務，應該

要在訂定法規之前，就充分的溝通。在管制作為上面，充分的跟業者去做一些討論。我們訂定之後才用這個方式去做實施。政府角色最重要的，就是最後拿到這一項。其它的部分，可能我們就看情況，從經濟的優異輔助，到我們只要看著就好，我們不要管那麼多事情，這樣不同程度的思維。(廖洲棚副教授)

第一層的放任考量大部分的網際網路活動都是沒有問題的，需要自由空間、需要保障權益，因此在這個層次之下應該採取自由的機制設計，任由其依照市場機制發展。

第二層是鼓勵平臺業者以維護網際網路秩序為目標，鼓勵其採取任何有助於整體網路環境健全的措施，例如增加透明度、確實自律等。第三層次是高強度管制，但這涉及不同業務法規的溝通，而這也是政府必須介入最多的一部分。

換言之，政府在第一層與第二層都不需要介入太多，應該在必須要高強度管制的部分扮演較多角色即可。

四、自律框架之設定建議

關於自律框架的內容與範圍，有幾點必須討論：採取單一立法或分散式立法，以及如何考量不同行為者之間的權力與權限。

關於單一立法或分散式立法的問題，席間有專家建議，應該要以整體思考，而不是分散式的思考：

關於自律框架範圍，建議考慮整體法規的自律框架，不要在現行的法規討論自律框架，會徒勞無功，或者是讓專業團體負擔過度的責任。(劉定基副教授)

分散式思考的問題就是現狀的問題，本研究所進行的深度訪談，許多業者所表達的意見與專家諮詢會議當中的意見相似：現狀之下由於法規散落在各主管機關的主管法規中，沒有人說的準必須遵守的項目、範圍、內容究竟為何；經常等到有需求了、有狀況了，才有主管

機關跳出來說哪些法條有關，但往往讓業者無所適從。因此，單一式的立法有助於自律框架的落實。

再者，該自律框架的立法也必須言明主管機關、第三方機構的權力範圍與限制。必須考量權力節制、權力制衡等機制的設計，避免動搖協力模式必須有的信任。

它必須要立一個法要限制它自己在什麼狀況下不可以指定裡面的人啊，或者說不要抽它的預算啊，或者說動員下面的人把它幹掉啊，或什麼等等。(陳敦源教授)

這個機構呢，你如果自己守不住，你現在是某一個政黨它要求你要照它的意思去 manipulate 那個資料，你如果一開始就這樣搞的話，搞到後來漸漸的這個 trust 也一樣沒有，就是你不要說大家對政府的，對這個的 trust 也沒有，所以就沒有意義了。所以現在的問題應該是說在需要行使 power 的狀況下，怎麼同時維繫這個第三方機構的 trust，這件事情反而比較重要。(陳敦源教授)

這第三方機構要如何一直在變的這個環境裡面保持中立，而且保持它的專業，包括它的人啊它的什麼。(陳敦源教授)

綜合專家的意見，該自律框架的設計必須把握幾點重要原則：

- 最好採取單一式立法，藉此減少業者自律的成本。
- 自律框架的立法必須考量第三機構的組成、運作，與監督。
- 第三機構與主管行政機關之間的權力制衡。

第四節　問責模式研析

本研究透過電話民調、深度訪談、網路民調、焦點座談等方式研議合適的網路社會問題問責模式。從電話民意調查、深度訪談與焦點座談中的分析結果，收斂出以協力模式為主軸的治理模型，並透過網路民調與專家座談確認該協力治理模式的可行性。

本節首先綜整各種研究方法關於問責模式的主要發現，並於本節第二部分描述「協力治理模式」的雛形。

一、關於問責模式的主要發現

（一）從民意調查而來的協力模式的接受度

本研究在電話民調中得出了政府機關受到民眾高度期待的結果，但從深度訪談、民眾焦點座談、網路民調、專家諮詢會議當中，皆得到政府的權力必須在網路治理中被有效限制的建議。綜合這些資料，本研究認為電訪民調中民眾希望政府做為主要負責對象的結論應當理解為民眾希望政府能夠有所作為，但這樣的作為不一定是由政府親自介入執行網路社會的相關管制。

民眾對於協力模式的接受度可從網路問卷的分析中得知。本研究於網路問卷發現：

- **協力模式的接受度：**那些偏好高移除強度結合高移除範圍或高法官保留的受訪者，對於本研究的協力模式表現出較高的認同度。
- **模式的多元性：**不同的偏好組合（例如，高強度但低範圍的受訪者）並不表示對於協力模式的反對，而是顯示了民眾對於問題處理方式的多樣性看法。

從以上發現可得知，多數民眾對於網路問題的處理期望反映在他們對協力模式的支持上。但是，要實施這樣的協力模式，必須考慮到各方的權責分配和實際操作方式。

從民眾對「法官保留」的偏好，以及對本研究所提出的治理模式的認同，本研究認為，民眾對於解決方案的偏好是相當「工具導向」的；意思是，只要解決方式能有效解決網際網路社會問題，同時能夠讓民眾免於權益被侵害、無言論自由傷害的副作用，民眾即認同此一制度的設計。這點從網路問卷關於協力治理模式的認同程度相關問題當中可得到驗證。與協力治理模式有關的意見調查中，民眾在各個問項的認同程度幾乎都接近或超過九成，顯見民眾對於協力治理模式是支持的。

然而，協力治理模式與法官保留原則是衝突的，這些衝突偏好的表達可能有幾點原因：

- 民眾對於議題的理解程度有限，且無法考量各種模式必須負擔的成本問題。
- 民眾對於議題的理解是表面的、工具性的，並非整合的。因此他們面對不同問題，無法具體思考整體資訊或前因後果，僅能依照題項做片段的回答，因此容易出現邏輯上的不一致。
- 關於網際網路社會問題的治理，因為議題層次過高（如同多位學者所言，已來到憲政層次）因此不適合用民意調查的方式探詢解決方案。

考量從民調的結果參酌於網際網路社會問題的解決方案有其限制，本研究認為，我們從電話民調與網路民調能夠獲得的訊息主要有二：

- 民眾對於網際網路社會問題感受深刻，而且希望問題能被快速、有效地解決。
- 由於民眾在問題解決模式上的偏好不一，因此多元多軌模式（納入不同行為者、依照問題態樣的差異採取不同的措施）可納入考慮。

由於從民意調查所得之的訊息有限，因此本研究後續的機制設計，將以質化類型的資料為主。

（三）公民團體、業者、學者訪談、焦點團體座談及專家諮詢會議結果分析

綜合質化資料的分析結果(包含本研究前半段的10場公民團體、業者、學者深度訪談以及5場焦點團體座談，以及後半段的專家諮詢會議)，本研究認為，網際網路社會問題解決機制的設計，必須包含「2必須，2不能」：

1. 「必須」考量業者/平臺性質差異

業者之間有大有小、有境內有境外、有學術有營利、有論壇式的有私訊式的，不同的業者或平臺依照性質的不同，有資源、技術、適用的管理模式的差異，且難以一概而論。例如業者規模的大小與資源的多寡有關，資源的多寡與技術可行性有關，因此並非每一家業者都可以使用高科技管理平臺訊息的流通。

又例如，論壇式的與私訊式的平臺需要的管理模式也有非常大的區別；論壇式的訊息開放，業者可以透過AI科技偵測具有風險的訊息，但私訊式的平臺業者則無法讀取用戶的私人訊息，因此技術的介入有其限制。境內、境外的業者其適用的法律、能被管制的強度、願意配合的程度有非常大的差別；學術平臺與營利行的平臺業者不但在資源上有差別，其經營理念也有差別。考量網路業者的樣態、性質的差異，很難採用一體適用的統一規範限制業者/平臺的經營管理。

2. 「必須」減少業者法遵的成本

網路的世界是現實世界的延伸，也因為如此，網路世界可能產生的問題範圍廣大。過去因為這個理由，我國採用分散式立法的方式，將網路社會問題可能涉及的法律規範分散在各業務主管機關的主管法規中。這種模式雖然成功地將網路世界視為現實世界的延伸，但卻增加了網路世界管理的困難，因為業者法遵的成本相當高。他們很難盤點所有與網路世界相關的法律，甚至法條之間規範的重疊也因為條文多如牛毛甚難盤點而難以避免。當業者法遵的成本過高，網路世界秩序的維繫難度就會增加，其治理就會更加困難。因此單一式的立法，

將網路社會問題的治理統一設計，能適度減少業者的法遵成本。

3. 「不能」採取行政主管機關由上而下的管制模式

由於業者性質差異問題，以及執行管制終究必須要回到業者身上執行，完全的由上而下的管制模式使得第一線執行的業者缺乏裁量空間，也缺乏依照業者性質調整的彈性空間。

強度過高、過度集中的管制措施必然會因為無法適應所有的問題態樣而導致可行性過低而失敗。

4. 「不能」忽視協力治理模式的權力制衡問題

若採取協力治理模式，必須兼顧權力制衡的問題。協力的本質是信任，但網際網路社會問題的治理涉及基本權利(言論自由)的保障，以及管制權力的節制，因此若協力機制的設計無法顧及權力制衡問題，可能導致信任無法產生，進而造就協力模式的失敗。

本研究將根據上述四項主要結論，發展建議的協力治理模式與建議的執行步驟。

二、協力治理模式

本研究依照分析的結果設計了網際網路傳播社會問題的協力治理模式（如下圖）。該模式的主要行為者包含了政府、第三方機構、平臺業者，以及使用者（民眾），每一個行為者都有主要扮演的角色。本研究先由下而上說明各行為者在此協力治理模式中應當扮演的角色，再進一步介紹協力治理模式的機制設計。

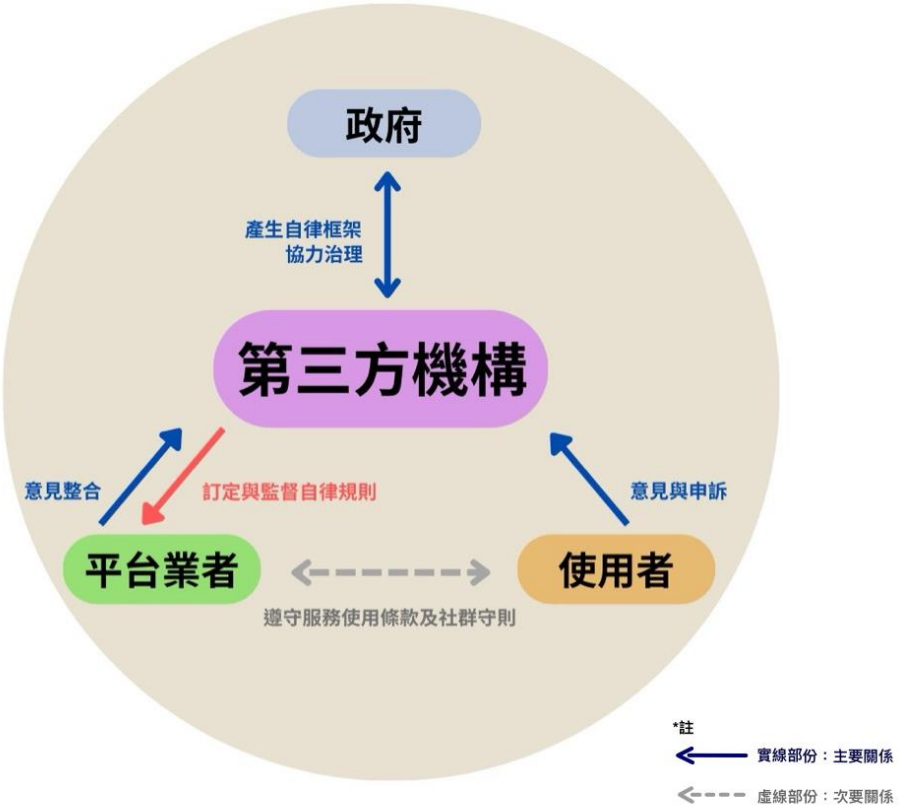


圖 36：本研究提出之協力治理模式架構圖
資料來源：本研究自行整理

（一）行為者在此協力治理模式中應當扮演的角色

1. 第三方機構：治理結構核心協調者

第三方機構位於模型的最核心，表示協力模式將以第三方機構為關鍵角色。第三方機構必須扮演協力模式的中介者，一方面整合平臺與民眾的需求與期待，與政府主管機關協力制訂自律框架，另一方面監督平臺確實依照自律框架執行自律規則，並回應民眾的申訴。考量第三方機構必須整合政府、平臺與民眾的需求，第三方的組成有幾個必須注意的原則：

（1）**獨立性**：由於第三方機構管理、監督的內容涉及言論自由與訊息傳播，已經來到了憲政層級的權力平衡與權利保障問題，因此確保其運作不受其他力量的干擾相當重要。

（2）**財源穩定**：確保獨立性的其中一個重要關鍵就是財源獨立且穩定。

（3）**人事獨立**：人事獨立是另一個確保第三方機構具備獨立性的原則。

（4）**透明課責**：除了在關鍵的人與財上面能夠穩定獨立，第三方機構的績效、產出也必須公開透明。因此定期公開透明度報告等執行成果，是必要的。

2. 政府：以立法方式建立治理框架，限制、定義權利義務範圍

政府機關雖然也是維護網際網路社會秩序的關鍵角色，但必須避免成為高權、控制角色，而是必須扮演平臺業者的協力者、民眾素養提升的教育者，以及權益侵害的防護者。各方協力角色的權力義務範圍，需透過立法作框架式的定義。

所謂框架式的定義，意指該立法內容並非直接規範具體的違法內容，亦非提供業者統一遵循的具體規則，而是要求業者必須依照其平臺特性，自行訂定自律規則，並賦予第三方機構整合各平臺規則、監督平臺自律執行成果，並針對平臺違反自律規則的嚴重程度

進行判斷，並做初步懲處或將情節嚴重者移交主管機關。

換言之，政府的立法僅是確認政府主管機關、第三方機構、平臺業者各自的權力義務範圍，平臺管理網路相關社會問題的具體規範必須由第三方機構協調各平臺業者後產生。政府在這個治理框架中的角色，主要為「授權」，推動這個治理框架的立法過程，並確保所有行為者在這個框架中各自節制權力、扮演好自己的角色。

3. 業者：維護網路秩序的執行者

本研究調查發現，業者應該是網際網路社會問題解決的關鍵角色。原因有如下：

（1）業者是網際網路社會的環境建構者，有留住使用者的生存動機。雖然業者多是以營利為目的（部分為非營利，例如PTT），但正如同所有的組織都有存續壓力一樣，平臺業者並不希望自己因為無法管理網際網路傳播社會問題而失去正當性、失去使用者的青睞。換言之，平臺業者作為網路社會的環境建構者，為了其組織存廢的本能，有維護網際網路社會秩序的誘因。

（2）網際網路治理需要彈性、對平臺的瞭解，以及對環境變化的快速感知能力。光是有維護網際網路社會秩序的誘因還不夠，要主要由業者擔起責任，或交由業者「當責」，關鍵之處還是「沒有其他人比平臺業者更瞭解該如何管理平臺」。

（3）網際網路平臺並不是一個一元化的個體，平臺的樣態依據提供服務內容的差異各有不同的特色。平臺所面對的問題樣態、資源各異，但他們能做的就是用不同的方式維持平臺的秩序。

（4）網路社會問題變化快速，管理方式需具備彈性。網際網路平臺所面臨的挑戰與社會問題的演變有關，而這些社會問題就如同詐騙集團的手法不斷推陳出新一樣，無法用單一

方式、手段一招半式平天下，因此管理的手法必須滾動式調整，甚至需要不斷試錯。這種必須與環境高強度互動的管理環境，不適宜由政府透過法規命令的方式進行管制，反應的速度會趕不上問題變化的速度。因此由在第一線的平臺直接面對、調整管理方式，才是管理網路問題的方法。

綜上所述，平臺業者是具有維持平臺秩序誘因，同時具備、也是唯一具備實際管理平臺能力，並能保持管理彈性的角色。未來網際網路治理政策的發展，應該朝向協助網路平臺完善其管理能力的方向努力。

4. 使用者（民眾）：自我權益的保護者

多數的業者、公民團體，甚至是民眾的焦點座談的多位民眾都提到了使用者本身媒體識讀與數位素養的關鍵地位。民眾本身的媒體識讀能力與數位素養無關政府或平臺管理能力與管理效能的高低，而是整個網際網路的社會秩序還是必須由一個一個的網路公民來打造。因此，具備足夠的媒體識讀能力，使民眾成為自我權益的保護者，是確保個人不容易受到傷害的不二法門。

民眾的角色可以分為兩個層次：

（1）媒體識讀能力是為了自保

美國加州媒體識讀中心（Center for Media Literacy，CML）認為媒體識讀教育有五個核心要點（Share, Thoman & Jolls, 2005）：

- 所有媒體訊息都是經過精心構建的；
- 媒體訊息是基於創意語言及其內在規則所構築的；
- 相同訊息可能因不同人而產生不同的理解；
- 媒體背後隱含著特定的價值觀和觀點；
- 多數媒體訊息的製作目的是為了追求獲利或權力

瞭解這五個核心要點，民眾對於網路上訊息與文字能更有判讀的

能力，對於詐騙、不實訊息、甚至是不友善的霸凌語言，能較有抵抗能力。

（2）數位素養是為了成為網路公民

民眾光有對於網路各種不實訊息、傷害言論、詐騙廣告的抵抗能力還不夠，作為使用者自己也必須要有能夠在網路上以合宜的行為與人互動的基本素養，這就是數位素養。

數位素養包含數位工具的運用、數位環境的思考，以及瞭解在數位環境下的規範[904]。換言之，當民眾具備數位素養，便能夠使用適宜的方式在網際網路平臺與人互動，也能夠謹守網際網路世界當中的各種規範，如同網際網路世界當中的公民，能夠共同維繫、維持網際網路世界中的秩序。

（二）協力治理模式的制度設計

綜合上述的各項研究發現，本研究設計協力治理模式的制度，提供未來政策立法的參考：

1. 採用單一式立法，建立網路社會的治理「框架」

依照本研究的分析，目前由於相關規範錯落於不同主管機關的主管法規中，增加業者配合管制的成本，亦增加管理失敗的可能。因此本研究建議，未來若研議修法，應採單一式立法，透過單一式立法建立自律框架。然本研究所言之單一式立法，並非將具體的管制規範直接寫入法條，而是透過單一式立法建立網路社會的治理「框架」，具體的規範內容應由平臺業者自行訂定。

單一式立法治理框架應以架構各行為者在此治理模式當中的責任義務與權力範圍為主，其內容應該包括：關於政府（主管機關）的責任義務與權力限制、關於第三方機構的組成、責任義務與權力限制、關於業者的責任義務與權力限制、關於權利侵害的救濟管道。以下分

[904] *See generally* DAVID BAWDEN, ORIGINS AND CONCEPTS OF DIGITAL LITERACY (2008).

別說明。

2. 關於政府的責任與權力限制

本研究經由訪談與問卷調查發現，民眾對於網際網路傳播社會問題的治理，最擔心的就是政府對於言論自由的控制過於嚴苛，侵害了基本的人權，限制資訊傳播的自由。然而網際網路的治理，勢必有公權力的介入，因此政府的角色必須具體，同時必須節制。

因此，治理框架的立法必須明訂政府主管行政機關的責任範圍與權力限制。包含：

（1）主管機關對第三方機構的指導或監督，僅限於法律授權範圍，例如僅能檢視第三方機構是否有行使其職權、檢驗其透明度報告，但不可對其管理上的決策進行審查（例如：平臺違規案件的審查與決議）。

（2）若主管機關已經授權第三方機構監督、管理平臺業者，則政府不應越過第三方機構干預平臺業者的監督與管理。

（3）政府是否對於第三方機構有預算與人事權。若考量第三方機構的運作不易，必須由政府的預算支應，則預算額度、給付方式應有固定額度/公式與管道模式且不受政府行政部門監督。

以上為治理框架關於政府責任與權力限制的立法建議，該權力限制應該至少包含關於政府對第三方機構的監督範圍、預算與人事的影響範圍。

3. 關於第三方機構的組成與責任與權力限制

第三方機構是治理結構的核心，治理框架的立法應當著重第三方機構成員的組成與比例，以及政府對其授權的範圍。

（1）業者自律框架的內容，應由第三方機構整合業者與多方團體或個人代表決定。

（2）第三方機構對平臺業者的監管權限，在框架規範的範圍內應該要充分授權。第三方機構應有足夠的權限可以檢視平臺的自律規則、實際管理制度、透明度報告，

（3）第三方機構要有完整的權限能判定平臺是否有違反自律規則，並有完整的權限能決定該項違規是否符合裁罰要件。

（4）應具體敘明第三方機構是否被授權能對違反自律規則的平臺開罰。

（5）第三方機構的組成，依照本研究的調查，建議以委員會的方式依照比例包含業者代表、公民團體代表、民眾代表、專家學者代表。業者代表比例應有限制，例如可規範業者代表不能過半，或不能超過三分之二。

（6）第三方機構應定期召開代表會議。

（7）第三方機構應定期公開透明度報告，完整公開期間內的運作情形（包含預算與人事變動）、對業者監管的結果、審查結果等。

（8）得考慮另外設置第三方機構的監理單位。由不同的公民團體、民眾代表、學者專家組成，監督第三方機構的運作、決策與績效。

以上僅針對第三方機構之基本組成、運作與權力限制進行建議。至於更詳細的制度設計，未來應進行進一步研究。

4. 關於業者的責任與權力限制

業者是治理架構當中主要執行平臺規範的行為者，因此關於業者的權限與責任必須在治理架構中明確規範。

（5）明訂業者必須列入自律規範的項目。例如要求平臺業者必須針對政治不實訊息、兒少安全問題、網路霸凌、網路交易安全、消費者權益保障等指定的問題面向，逐一提出管理措施與規約。

（6）明訂業者能採取的管制規範範圍，例如帳號停權、回覆停權、分享停權等。

（7）明訂業者違反規約的處置與罰則。例如：未能產出有效規約、不同程度違反規約的條件與罰則。

（8）明訂業者與使用者權益遭受侵害時的救濟管道。

5. 關於救濟管道

本研究發現，民眾對於網際網路社會問題的治理，最害怕的就是個人權利遭受侵害。然而只要有任何管制措施介入，權利侵害的問題幾乎無從避免，因此明確的救濟管道必須成為制度設計的一環。在這個治理架構當中可能產生救濟需求的環節包括：

（1）使用者遭受業者侵權

（2）業者遭受第三方機構侵權

（3）第三方機構被政府機關侵權

（4）民眾被政府機關侵權

這些可能需要救濟的環節，應有逐級而上的救濟管道，包含：第三方機構、各級法院等。應該依照第三方機構與各級法院可審理的層級逐一規範。

第六章　綜合觀察與政策建議

第一節　本研究研析重點回顧暨政策評估檢討

在提出本研究之法制政策建議之前，謹再次回顧本研究之各個研究重點。要之，以考量要素來分類，包括國際平臺問責法制的發展、國內在嘗試倡議《數位中介服務法》草案後的近況，以及辦理民眾意見調查和專家諮詢會議之精要。以下分述之。

一、國際平臺問責法制持續演進

（一）有關高密度網際網路內容執法措施

從近年國際間的法制趨勢觀之，除仍處於立法倡議期的美國、加拿大與日本，韓國、紐西蘭、歐盟及其會員國、英國及新加坡，已先後建立對應廣泛違法內容的高密度網際網路內容執法措施。

其中，以韓國和甫通過新法的新加坡最為特殊，因該二國於網際網路執法時，並無事前的法官保留制度，也即行政機關得透過行政處分先行移除或阻斷各類違法內容。就行政運用面來說，可說是打擊範圍最廣、效率最高的類型；但若考量國際間較高標準的人權典範，不宜貿然效法。

而紐西蘭、歐盟及其會員國與英國之立法，雖然可對應廣泛之違法內容，但若涉及移除或阻斷各類違法內容，則有法官保留制度，必須先取得法院的裁判，行政機關並無直接移除的權限。

至於澳洲則與我國最相似，介於前兩類國家群之間。其近期作用法之立法雖授權行政機關無法官保留移除或阻斷違法內容的權限，但僅得針對法律所明訂、有限的違法內容，目前並未擴及更廣泛的違法內容類型。

（二）有關課與數位平臺之義務類型

若以義務別數量加以觀察，較近期的立法之立法技術與提供的管制工具較為多元多樣，其中，以歐盟及英國的最新立法最為龐大，後者之法典甚至更勝前者。本研究試圖以以下圖表，將英國《線上安全法》與我國（參考歐盟《數位服務法》初版草案之）《數位中介服務法》草案所課與的義務進行比較：

規範對象 / 義務規範	英國線上安全法(OSA)		數位中介服務法草案(2022)	
	U2U服務(第1類) (包含即時通訊軟體)	搜尋服務(第2A類)	連線服務	線上平臺服務
違法內容之風險評估	O	O	X	O 第33條 (限指定線上平臺服務)
違法內容之安全	O	O	X	O 第34條 (限指定線上平臺服務)
兒童風險評估	O	O	X	O 第33條 (限指定線上平臺服務)
保護兒童之安全	O	O	X	O 第34條 (限指定線上平臺服務)
使用者賦權及評估	O	X	X	
保護民主重要性及新聞出版/工作者之內容	O	X	X	
受理使用者通知	O	O	X	O 第22條、第23條
申訴處理程序	O	O	X	O 第24條
訴外爭端解決機制	O	X	X	O 第25條
認證舉報者	X		X	O 第26條

圖 37：英國 OSA 與我國《數位中介服務法》草案課與義務比較圖(1)

資料來源：本研究繪製整理

規範對象 義務類型	英國線上安全法(OSA)		數位中介服務法草案(2022)	
	U2U服務(第1類)	搜尋服務(第2A類)	連線服務	線上平臺服務
維護言論自由、隱私	O	O	O 第33條 (限指定線上平臺服務)	
留存使用記錄及檢視	O	O	X	
有害兒少身心內容之接取評估	O	O	X	O 第33條 (限指定線上平臺服務)
處理廣告詐騙廣告	O	O	Δ 第9條、第12條 (加速移除之安全港，非義務)	Δ 第11、12條(加速移除之安全港，非義務)、第27條
賣方溯源	X		X	O 第28條
使用者年齡驗證	O	X	X	
向政府舉報CSEA內容	O	O	X	
服務使用條款義務	O	X	O 第15條	O 第15條、第27條
揭露已故兒童使用服務之資訊	O		X	
透明性報告	O		O 第16條	O 第16條、第29條
繳納規費	O		X	
資訊揭露及指定代理人	X		O 第13條至第14條	O 第13條至第14條

圖 38：英國 OSA 與我國《數位中介服務法》草案課與義務比較圖(2)

資料來源：本研究繪製整理

除了大型法典的立法模式外，澳洲具共管特色的制度亦頗值得參考。誠如前開介紹，澳洲的《線上安全法》將管制分為三階段。首先，第一種是「基礎期望」，也即由行政機關制訂安全使用、法定違法內容處置、設置通知與申訴機制、資訊揭露與保存、諮詢及與 eSafety 合作等各類期望，並要求業者據以訂定「強制性產業行為準則」（mandatory codes）；主管機關 eSafety 並可要求業者針對其行為準則何以達成該期望提出說明報告。

第二種則是「共管」，也即由產業公協會「由下而上」(bottom-up）發展前述之「強制性產業行為準則」。eSafety 得命業者遵守該行為準則；同法並授權 eSafety 有核准各產業行為準則之權限，換而言之，eSafety 除在產業行為準則草擬過程中與產業公協會密切合作外，更有以未提出適當措施為由而不予核准，或於產業公協會無法訂出合於「基礎期望」的行為準則之場合，由 eSafety 經公眾諮詢等程序代為定之的權限，以迫使產業公協會制訂合宜行為準則。

第三種是「正式監管」，也即授權 eSafety 以行政處分移除法定違法內容或連結。

二、數位中介服務法草案倡議中止後之立法行動

由於《數位中介服務法》草案的公布引發了產業界、新聞媒體與民眾的強烈反對聲浪，故在僅僅一個半月後的八月中，行政院旋即宣布中止數位中介服務法草案之倡議。此後各界皆要求主責機關應強化與產業界及民眾溝通後，再行思索法制政策取向。

而由於冀希的違法內容共通處理機制推展受挫，各部會則開啟了分散式立法的進程[905]。而由於各部會處理違法資訊的態度各異，若行政院並未有專責小組統合立法經驗，最終可能會發展成多樣化的處理程序。例如衛生福利部等部會所主責的「性暴力犯罪防制四法」，即在 2023 年初完成立法。針對所涉之違法內容移除或限制接取程序，採取擴大版的「行政通知—移除」模式。

此外，金融監督管理委員會鑑於《數位中介服務法》草案倡議的停滯，也推動了《證券投資信託及顧問法》的修法，立法院並於 2023 年 5 月通過修正條文。根據新法第 70 條之 1，非相關特許的持照人不得於網路刊播招攬廣告，刊播人亦必須揭露其資訊，知悉有違法刊播情事之網際網路平臺提供者、網際網路應用服務提供者、網際網路接取服務提供者或其他網路傳播媒體業者，即應移除該廣告或限制其接取。

又，中央選舉委員會為了避免利用深偽（deepfake）技術的不實訊息干擾選舉，也提出修正草案，立法院並於 2023 年 5 月修正《公職人員選舉罷免法》及《總統副總統選舉罷免法》。根據其新規定，候選人得向警察機關申請鑑識網際網路刊播其本人之深度偽造聲音及影像，並據以要求網際網路平臺提供者或網際網路應用服務提供者移除該內容或限制其接取。

---

[905] 例如，金管會主委於立答詢時，針對《證券投資信託及顧問法》修正草案，即表示：「*…像是英國有訂定類似於台灣曾推的《數位中介服務法》，既有法源也有處分依據，但後來台灣的《數位中介服務法》暫緩了，因此才退而求其次，表達出宣示的態度…*」，顯見《數位中介服務法》草案與各部會走向分散式立法有直接的關係。參見葉佳華，〈遏止投資詐騙廣告　金管會修訂《投信投顧法》　沒有罰責恐怕淪為宣示性條文〉，《信傳媒》，2023/5/3，https://www.cmmedia.com.tw/home/articles/39894（最後瀏覽日：2023/12/1）。

三、未來可能的立法嘗試之挑戰

相較於歐美各國或亞洲的日韓，臺灣針對網際網路的治理規範的探討仍處於萌芽期，實務上長期以來以自律或低度管制為主流，甚至缺乏著作權法以外之責任安全港規範。而《數位中介服務法》草案參考已踐行《電子商務指令》等網際網路規範逾二十年、且歷經多次大規模檢討的歐盟最新法律草案，則不啻為一蛙跳式的立法策略，確實應負擔更多的說理責任。

而學界也陸續傳出不同意見，除了認為諸多違憲之虞的全面批判者之外，亦有許多學者認為朝「平臺責任」的立法方向是正確的，草案中部分條文亦有正面、積極的意義，惟數個法條及細節仍有需要調整之處[906]。整體而論，學者間也未呈現具體共識。

同時，民眾也則習慣此「自由」的網際網路空間，對如何管制等國際趨勢並不熟悉，同樣缺乏共識。過去，不同部會確實有針對不同領域的網際網路內容監理提出若干立法或修正草案，但品質良莠不齊，且普遍缺乏與民眾的政策溝通，致使引發大規模批判的事例時有所聞，導致民眾更容易對於任何言論自由緊縮的倡議採取抗拒之態度。

加諸，主責機關公布《數位中介服務法》草案後，各種對於條文內容的誤解、誤導訊息（misinformation）、陰謀論等甚囂塵上；在社會紛擾之下，行政體系決定中止倡議，則是扼殺了後續各界深入的理性溝通之機會，相當可惜。

由是，針對此一涉及業者眾多、管制規範複雜，且產業界與民眾都不熟悉的議題，應該要選擇正確的時間點，花上更長的期程來瞭解產業並行政策說服。尤其，數位中介服務提供者的管制是數位轉型的重要議題，但不會只有 NCC 一個部會需要推動數位轉型，整體行政部門、產業界與民眾都應該共同參與。甚至，《數位中介服務法》草案中創設的「資訊限制令」也涉及司法程序，且可預期應需要投入更

[906] 例如，黃銘輝教授即認為草案中的「資訊限制令」在某些構成要件上有違憲的疑慮。參見陳洧農，〈數位法制再精進：累積韌性籌碼〉，《卓越新聞電子報》，2023/2/9，https://www.feja.org.tw/68730（最後瀏覽日：2023/12/1）。

多司法資源，則倡議過程都更應該與司法體系有更多互動。

四、本研究民眾意見調查與政策建議之關係

本研究之針對民眾意見之調查概可分為電話訪問、焦點座談及網路調查三大階段。

首先於第一階段，本研究透過電訪問卷之方式得知，多數民眾都有受到「五大網路危害」的經驗，因此可確認該五大網路危害係我國網路社會一普遍存在的弊病。而我國民眾因對於政府仍有一定程度的依賴與信賴，因此也希望政府能積極地出面解決網路危害，並同時也認為平臺業者也應出面處理；但同時，也有部分的民眾認為可由民間專業團體負責處理這些網路危害。

第二階段，則更進一步依照電訪之結果，聚焦並再確認民眾的意見。多場焦點座談的結果，民眾大抵認為，網路社會與網路世界相當複雜，完全依靠政府可能無法完遂任務，且也不希望政府的手直接深入進行監控，以彰言論自由，因此可引進一個各自獨立於政府和平臺業者的公正、容納多元意見的第三方機構，協助建立與維護網路秩序。再者，本研究也再次確認，民眾認為平臺業者既於其營運的平臺上透過廣告等機制牟利，則即應有相當的責任監督其平臺上的活動，確保其合法。繼而，在民眾既期待政府出面處理網路危害議題，卻又擔心政府「洪水猛獸」的過度限制或侵害權利可能性下，本研究認為，透過第三方機構的協力治理模式，是一條兼顧權力制衡與可行性的方案。

第三階段，本研究基於第二階段的結論，重繪網路問卷，希望網路民眾就治理模式的各項細節表示意見。就此，得出網路民眾對協力模式意向的結論如次：

- 移除違法內容：對移除強度和範圍都持相當嚴格的態度，故政府於擘畫法制時，須給予平臺業者和第三方機構適當且明確的授權，確保其具備足夠的能力有效執行移除違法內容。
- 公私協力機制：第三方機構的角色可協助監督違規平臺、接

獲民眾投訴後行初步調查，故政府應該賦予第三方機構適當的權限和資源，包括要求網路平臺提供透明性報告，或在必要時公開警告和名單，以遂任務之達成。

- 第三方機構的組成模式本身可能不是影響協力模型認同度的主要因素。

五、本研究專家諮詢座談會與政策建議之關係

本研究於辦理之末，邀請專家學者與會，對本研究提出政策等建言，其結論概如次：

- 第三方機構的組成與運作是關鍵：從 iWIN 第一線角度觀察，如何取得業界與民眾的信賴，是第三方機構能否成功的重要因素，故組成如何具代表性、公平、漸進、互信、多元，而終可產生公信力，至關重要。同時，可以內部分組之方式進行決策。
- 協力模式是一種治理權限外包：因此組織、權限及（與政府間的）獨立性必須以法律嚴謹設計、並確保。
- 行政部門應協調各業務主管機關盤點相關法規，並定期整合：現狀之下由於法規散落在各作用法及其法規中，應遵守的項目、範圍、內容常以「滾動式調整」的面容演進，經常是事件發生或有政府管理端的需求時，會無預警地被增加前所未有的義務性要求，讓業者無所適從。故此有賴行政部門間跨部會之通力合作，更必須由更高層次的行政單位加以統合，逐步邁向單一立法框架，以減少業者法遵成本。

第二節　法制政策建議

本研究依據我國網際網路傳播社會問題調查、國際資料耙梳所得，並綜合上開盤點之審酌因素，提出網際網路平臺社會治理協作模式，作為改善網際網路平臺社會秩序之政策建議。

該協作模式以網路平臺業者擔當主要責任者，政府機關作為協力者，公民團體作為監督者，民眾作為參與者、使用者。這些多方的利害關係人，共同以「網路治理跨界協力聯盟」為中心，採取目前 iWIN 的模式，進行對話與共治。

以下，謹提出本研究之具體法制政策建議。

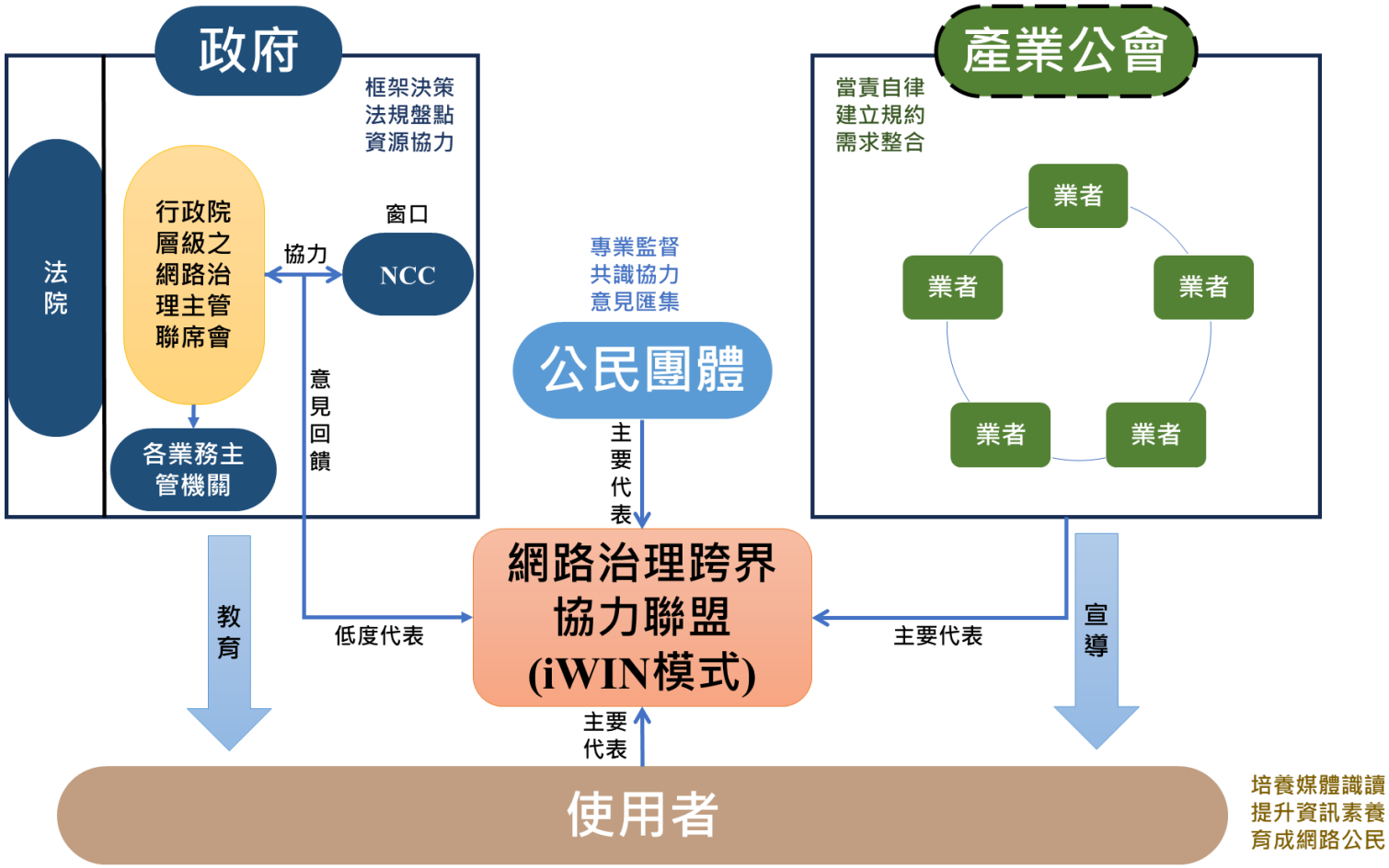


圖 39：網際網路社會治理協作模式

資料來源：本研究自行繪製

一、短期建議：揉合行政體系能量，適切對應分散式立法

（一）對內整合：建立行政院層級之跨部會會報

考量現實層面，以當前學界、民間、以及國會意見分歧的態勢而言，要在短時間內推動並討論出一部各方皆首肯且具有高度共識的集中式立法，難度相當高。因此短期內比較務實的取向，仍是由各部會針對具嚴重性、急迫性及重要性之所管網際網路活動事項加以立法，即分散式立法。

惟分散式立法時至今日已陸續出現業者的不滿聲浪。誠如本研究前開調查所得，目前網際網路平臺可能涉及的法律規範錯落於各部會、各地方政府主管之法規中，而且許多的規範來自於現實世界秩序當中的擴大適用或解釋。雖然網路世界和現實世界無法完全切割，但法規命令系統的錯落確實為多間平臺業者難以配合政府、形成秩序的關鍵因素。尤其，各部會的立法成果差異頗大，構成要件也顯不相同，欲達管制目的所採用的手段更是寬嚴不一，已造成業者法遵上的成本增加及困難。因此，**首先，政府機關應該進行對內的法規盤點與資源整合。**

其次，政府機關需要建立跨部會會報，係因為網際網路的問題並不會依著部會的業務分類分門別類出現，可能同個問題同時牽涉到數個部會的業務；也由於是必須由跨部會協力解決的問題，出席的人選必須是在會議上有決策權力者，使該會議確實具備整合資源、做成決策的能力，會議的層級必須到行政院層級，落實跨域治理。

跨部會會報的任務，除了主管之間的網路治理相關業務協調，最主要的任務是形成網路治理的框架性規範。這個框架性規範決定該如何讓網路業者「當責」，以及什麼是網路社會的底線、政府在什麼情況之下必須以公權力介入。

以政治不實訊息這個問題類型為例，框架性規範的範圍即是「課予平臺處理不實訊息的責任，要求各平臺提出管理辦法備查；若有危害社會秩序、國家安全程度之犯罪行為，平臺必須配合檢調調查」。但至於哪些問題類型必須列入框架性規範，建議主管機關先行累積社

會共識之後，交由跨部會會報決議。

基此，本研究建議由行政院出面成立具「設置要點」的跨部會會報，先揉合行政體系能量，對各部會的分散式立法或立法規劃、以及業界之反饋進行體例的統整與收斂；再針對執法實情、司法機關及業界與民眾反應，加以滾動式調整。待漸形成較成熟、穩定的作法後，再加以歸納並草撰集中式立法草案。

（二）NCC 應有之取向

於前開過程中，本研究所蒐集到的學者意見大抵認為，由於 NCC 的獨立機關及合議制性格，其並不適合擔任跨部會協調的主責部會，仍適合由行政院院本部的高度橫向協調各部會。

不過，新修《國家通訊傳播委員會組織法》第 3 條第 1 款明訂通傳會的職掌包括：「通訊傳播監理及**網際網路傳播政策之訂定、法令之訂定、擬訂、修正、廢止及執行**。」根據其立法說明第 1 點：「網際網路服務快速發展下，**建立多方利害關係人參與、自律、他律之機制；並協調各部會依其權責處理非法內容機制**。」可見立法者對通傳會瞭解、掌握各部會有關平臺問責等處理非法內容機制之需求，仍有相當之期待。基此，NCC 在行政院層級之跨部會會報運作中的角色，至少仍是持續觀察各部會法制政策及執法的發展；並就以此基礎視其可能性及需要性，研議包括處理非法內容之共通機制等可行的集中式立法策略。

（三）對業者、公民團體維持對話、聆聽、共識創建

改善、解決網際網路社會問題不是靠政府由上到下的管制能夠完成的任務；相反的網路社會問題的治理是一個政府必須最小化的協力模式。協力模式最關鍵的是利害關係人彼此之間能夠創建共同目的、相互信任，因此政府機關必須先做這個創建共識的協力者。

共識的創見有幾個可以參考的起點：

- 兒少網路安全已經是共識
- 消費者保護是業者的天職

從兒福聯盟的訪談以及消基會的訪談記錄中可知，他們分別將所有的網路問題都看做兒少網路安全問題（I，L49-54）以及消費者權益保障問題（H1）。換言之，網路社會問題可以用兒少安全以及消費者保護進行包裝，作為和業者創建共識的起點，說服業者共同來打造一個安全、值得信賴的網路環境。iWIN 之所以成功，也是因為這個平臺的信服力來自於社會共識（E-Q，L618-621）。

iWIN 之所以可以創建共識，原因在於那是一個能夠讓業者、公民團體、民眾代表充分表達意見、對等溝通的平臺。因此政府機關面對業者、面對公民團體必須維持對話、聆聽、理解的態度，才能在最後凝聚共識。

（四）對民眾持續教育

對民眾持續教育，是政府機關、公民團體、平臺業者都希望持續努力的任務。許多平臺業者已經認知到，提升網路使用者的素質與能力，是改善網路社會問題的根本之道。因此政府的資源協力，一部分應該用來鼓勵業者和公民團體持續對民眾進行媒體識讀、數位素養教育，另一部分用來配合國民教育從小紮根。

總結來說，網際網路社會問題的解決，不是單一利害關係人的獨力責任，這是一個複雜的協力關係。政府作為這個協力關係的協力者（coordinator），必須打造良好的對話環境、給予充分的資源、創建信賴的共識，持續互助互信、資訊共享，才能讓這個協力模式發揮完整的治理功能。

二、中長期建議：仍有必要走向集中式立法，建構穩定法制

（一）集中式立法之新草案法制框架

在傳播與溝通活動大量聚集於數位中介服務的當下，正如《數位中介服務法》草案那短暫的公眾諮詢程序中所獲得之反饋，對於資訊限制令及暫時加註警示處分以外的課與義務之批判較少，顯示各界也認同臺灣仍需要一部整合的平臺問責的法律。

因此，作為臺灣第一部針對各類網際網路服務的管制立法嘗試，《數位中介服務法》草案並不完美，但仍足以成為後續公民社會深入檢討及重啟倡議的素材。

在整體立法應有的取向上，由於臺灣市場的規模不若其他大型經濟體，故在針對具有網際網路跨境特徵之數位中介服務的規範上應避免特立獨行，而與大型經濟體之實定法行管制對接（regulatory alignment）。也即大抵上跟隨其法制思維與架構，不僅降低大型數位中介服務者法遵成本，亦降低其退出臺灣市場的風險。

而針對層級化之義務，本研究則建議採取「定礎與加建」（cornerstone-and-addition）的立法策略。也即儘速針對各種數位中介服務建立一套普通法（*lex generalis*）之規範，而針對特殊種類的平臺（例如即時通訊軟體或視訊分享平臺）、或特殊的違法資訊（如影響兒少身心發展之內容或選舉期間的不實訊息），則另以部門硬法（sectoral hard-law）作為特別法（*lex specialis*），予以追加或排除規範。尤其，針對違法資訊之移除或限制接取程序，由於涉及言論自由之限制，仍應以法官保留為設計原則，行政移除模式作為例外。

而「資訊限制令」的部分，雖然各界評論意見較多，但本研究仍認為，專為網際網路內容之執法設計一套「禁制令」（injunction）制度（或稱令狀主義）仍有必要。畢竟，雖數位平臺上傳播及複製的速度極快，根本不可能創造「無菌空間」，但另一方面，數位平臺業者在後台的管理技術及功能也同時在進步，政府應扮演透過法制政策推手的角色，持續為數位平臺業者創造誘因或反誘因，以配合社會需求，

僅針對「立即且明顯」並具相當嚴重性的違法內容加以處置。此部分從國際經驗看來，數位平臺業者並不是做不到，即使是跨國的大型業者，只是需要政府展現立法及執法的決心與魄力，以及投入人力與時間溝通磨合。

（二）新草案課與平臺義務項目之取捨

從本研究前開民眾及業者及公民團體之調查中仍可得知，規範數位中介服務提供者之適切基本法制框架仍有必要，但由於各方意見不一，故折衷之計，仍得以《數位中介服務法》草案為基礎，基於各界意見之「最大公約數」的思維，從刪減有爭議性規範的角度出發，倡議《數位中介服務法》草案的後續版本。

從前開各國法制經驗的耙梳中可得知，如歐盟、甚至英國般鉅細靡遺的大型立法，不僅需要從長計議，過程中出現的爭議之大，也可見一斑。尤其，歐盟和英國立法完竣以來，可謂是「徒法不足以自行」的最佳典範。要之，由於母法的義務種類眾多，制訂後的子法規模龐雜，耗時甚鉅；先行實施的義務中，以歐盟《數位服務法》透明性報告為例，出現了歐盟執委會規範及指引不夠細緻，導致業者對於法律文字理解歧異，其格式與臚列之數據也質與量落差也非常大，導致後續比較、對照的困難[907]。這在在顯示，大型立法於立法後亦可能產生之執行難點。

由是，僅規範重點的課與義務條文，進一步減少業者法遵成本，是一條可行性較高的途徑。具體而言，本研究根據前開歸納，建議可以從下列五項較無爭議的義務為基礎出發，視各界討論情形再向上增加：

- 建立並揭露通知及行動機制

[907] *See* Gabby Miller, *First Transparency Reports Under Digital Services Act Are Difficult to Compare*, TECH POLICY PRESS, Nov 23, 2023, https://www.techpolicy.press/first-transparency-reports-under-digital-services-act-are-difficult-to-compare/?fbclid=IwAR2tN5XluAvBofHp_PdsbmklVtxJFtSiyg3y9ABB2h3r1lqV3eqKnGGD0E8 (last visited Feb. 10, 2024).

- 制訂並揭露內容調控之處理標準
- 建立並揭露完善之內容調控制度與人員
- 儘速告知通知人及被通知人處理結果
- 透明性報告

要之，各項義務細節性規範不可能規範於母法之中，立法後仍必須制訂相關法規命令或指引。但為求更能貼近數位平臺業者的聲音及導入外部監督能量，並且避免高權過度干預，本研究建議採取澳洲法之結構，由法律明訂業者自行組織產業組織或第三方專責機構，真正「由下而上」地制訂「強制性」產業行為準則；法律亦必須授權政府做最後法遵控制的權限，也即，其一、該強制性產業行為準則必須符合政府（經公眾諮詢）的基本期待，若有空泛、不完整等不適合之處，政府應保留命產業組織或第三方機構再議，或直接由政府訂定之權限；其二、業者必須遵守該強制性產業行為準則，否則政府仍保留裁罰之可能，以資擔保法遵。

此外，歐盟《數位服務法》法制細緻規劃也值得參考。也即，歐盟雖然建立諸多「自願性行為準則」，貌似業者自由參加，不受政府拘束。但《數位服務法》於前言中明言，可將加入自願性行為準則作為整體風險評估後的「風險減緩措施」；且若業者不具正當理由拒絕加入自願性行為準則，則可作為違法認定的審酌要素之一。種種跡象皆顯示，與其說是「自願性行為準則」，其透過《數位服務法》明確的法制接點，已有將「自願性行為準則」成為一部分法規命令或指引之態勢。

（三）新草案所涉違法內容範疇之界定

從本研究網路調查的民意基礎中得知，民眾對違法內容移除機制之偏好，在「移除範圍」的結果相當明顯，其結構光譜皆聚焦在「廣泛的違法內容」，也即根據網路問卷中的定義：「無論觸犯的是刑法、民法或政府各級機關訂定的行政法規，所有的『違法』資訊或內容都

必須處理，且應建立一套一體適用的移除機制[908]」。

基此，若依民意取向，則新草案就所涉違法內容範疇之規劃，似乎應朝向參考歐盟、英國或紐西蘭等國。不過於此，除可參考本研究先前提及的澳洲模式外，建議再混搭英國模式，也即，可於草案中明訂或授權主管機關以公告之方式，將違法內容加以類型化，區分為最嚴格可透過法官保留加以移除或阻斷之「最嚴重違犯」；次嚴重但必須透過強制性產業行為準則（如建立「通知及行動」機制）迅速對處之「重要違犯」；以及雖違法但並未具有急迫性之「一般違犯」，此類僅需透過「基本期望」要求業者以自律處理，並授權主管機關命業者提出說明報告即可。

（四）對外協力：以 iWIN 模式建立協力聯盟或專責機構

本研究所提出協作模式的核心便是此協力聯盟。多數業者以及公民團體在訪談中提到，既然目前已經有了一個 iWIN 模式受到各界的信任與重視，認為應當仿造這樣的模式，建立協力聯盟。由政府委託一具有社會公信力的協會組織作為發起人，以建構穩定和諧的網路社會秩序作為號召，邀請平臺業者、民眾（可以含一般使用者、家長代表等）、公民團體、政府主管機關共同作為聯盟成員。

1. 提供各界對話平臺、促進共識形成

目前 iWIN 的運作模式提供了各界平等、實質對話的機會與空間，平臺也願意在 iWIN 的架構下配合建立對兒少安全的網路環境。同時，這個平臺定期開會、定期做業者培訓，提供滾動式修正、持續溝通的管道，且多年來運作順暢，受到各界肯定。

網際網路社會問題的治理最需要的就是平等地交流、實質地對話，以及滾動式地與時俱進。因此仿照 iWIN 模式提供對話平臺，是主管機關能做的協力的第一步。

[908] 光譜另一端「有限」的違法內容的定義則為「僅將處理重點放在詐騙、兒少保護等社會重視的違法類型，且配合不同事件類型，分別建立對應的移除機制」。

但本研究也必須提醒，iWIN 模式有其限制，要之，iWIN 模式之成功，根基於其係處理放諸四海皆準、且相對容易判斷之有害兒少身心健康內容等，則對於其他難以判斷、爭議性大、眾說紛紜或後真相（post-truth）之不實訊息、誹謗、公然侮辱等違法內容，其適切性確實存在疑慮。

不過，誠如本研究前述，不妨可嘗試以 iWIN 模式為基礎，在此類第三方協力聯盟或專責機構中，向下進行分組，以不同的多方利害關係人組成，各自倡議適切的處理模式，而非依違法內容議題分散至不同組織，對主管機關協力治理而言，將有實質單一窗口之功。

2. 政府低度代表，將意見帶回整合資源

這樣的聯盟政府機關的代表必須最小化，其任務是在這個對話平臺中蒐集各界意見，回到政府的跨部會主管聯席會中找資源及支援。換言之，若國家通訊傳播委員會作為主管機關，在這個協力模式當中扮演的是一個協力者（coordinator）以及窗口，任務是瞭解需求、整合資源、建立框架。

3. 立法授權並保障其組織獨立性為必要

承前述，本研究建議集中式立法後的法規命令及指引，應由該第三方協力聯盟或專責機構加以溝通、中介、統合。首先，本研究透過質性及量性的研究，發現業者幾乎全數希望採取「由下而上」的方式建立第三方專責機構，而不希望該第三方專責機構係由政府所成立並具有主導性。基此，政府應最大程度傾聽業者之意見，畢竟，從各國的經驗觀之，網際網路政策的妥善執行，有賴於業者的配合。

職是，本研究建議，該第三方專責機構之運作模式應透過立法明訂；其組成模式，可能不適合由政府捐助成立、或由政府編列預算委託特定組織為之，否則都與業者的期望有所落差。因此，能走的途徑，似乎僅剩下兩種。其一，由業者自行成立「單一的」產業公會，以「實質單一窗口」的模式對接主責部會；其二，雖由政府捐助成立、或由政府編列預算委託特定組織，但政府必須創造該第三方專責機構的「獨立性」，也即徹底退出、不插手於董事會或相類重要成員的派任。

換而言之，政府的角色就是，在組織成立時將章程等制度完善建立，盡可能地保障其財務暨人事獨立性，後續則完全交由業界或民間自治，此才能徹底得到業界及民眾的信賴。

至於該第三方專責機構之組成，本研究則建議由本國業者、於我國設立分公司之國際業者及未於我國設立分公司但我國使用人數或年營業額達一定標準之國際業者，以及專家學者暨使用者代表加入、組成之。

參考資料

一、書籍

王牧寰、林家暘、陳譽文主持，數位科技應用發展暨我國匯流法制革新規劃研究，國家通訊傳播委員會委託研究成果報告（2021）。

林淑馨，公共管理，巨流圖書公司，增訂二版（2017）。

陳志宇、林家暘、吳秦雯、江耀國、王牧寰主持，因應國際數位匯流發展趨勢之法制研究，國家通訊傳播委員會委託研究成果報告（2022）。

Bawden, D. (2008). Origins and Concepts of Digital Literacy. NY: Peter Lang.

Liesching, in: Paschke/Berlit/Meyer/Kröner (Hrsg.), Hamburger Kommentar Gesamtes Medienrecht, 4. Aufl., 2021, 71. Abschnitt, Rn. 24.

Dazu auch vgl. Grünwald/Nüßing, Vom NetzDG zum DSA: Wachablösung beim Kampf gegen Hate Speech, MMR 2021, 283, S. 284.

Kraul/Schmidt, Plattformregulierung 2.0 – Digital Services Act und Digital Markets Act als Herausforderung für die Compliance-Organisation, CCZ 2023, 177, S. 177 f.

二、期刊

范傑臣，從多國網路內容管制政策談台灣網路規範努力方向，資訊社會研究，頁 207-208（2002）。

趙英基（조영기，音譯），數位性犯罪發文根絕了嗎？事前處置義務的現況與限制（디지털 성범죄 게시물은 근절되고 있나? - 사전조치 의무의 현황과 한계），KISO JOURNAL，第 50 期，頁 2-6（2023）。

金賢真（김현경，音譯），數位未來社會與自律規範（디지털 미래사회와 자율규제），KISO JOURNAL，第 49 期，頁 62-65（2022）。

李貞嬋（이정념，音譯），KISO 制定「仇恨言論自律政策指引」的意義與考量（KISO <혐오표현 자율정책 가이드라인>의 제정 의의와 몇 가지 고려사항），KISO JOURNAL，第 51 期，頁 2-5（2023）。

DIRECTORATE-GENERAL FOR THE INFORMATION SOCIETY AND MEDIA (EUROPEAN COMMISSION), EU STUDY ON THE LEGAL ANALYSIS OF A SINGLE MARKET FOR THE INFORMATION SOCIETY: NEW RULES FOR A NEW AGE? (2014).

Ross Anderson & Sam Gilbert (with a preface from Diane Coyle), *The Online Safety Bill: Policy Brief*, University of Cambridge & Bennett Institute for Public Policy Cambridge (2022).

Tschorr, Meldepflicht von illegalen Inhalten an staatlichen Stellen – Digital Services Act versus Netzwerkdurchsetzungsgesetz, MMR 2022, 1053, S. 1056 f.

三、其他

國家通訊傳播委員會，111 年通訊傳播市場報告（2023/01/16），https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=5023&cate=0&keyword=&is_history=0&pages=0&sn_f=48484。

財團法人台灣網路資訊中心，2022 台灣網路報告，https://report.twnic.tw/2022/。

兒童福利聯盟，2021 台灣兒少網路社交焦慮與網路霸凌經驗調查報告(2021/10)，https://www.children.org.tw/publication_research/research_report/2267。

簡恆宇，社群平臺質疑「反假新聞法」箝制言論自由《華盛頓郵報》：新加坡藉疫情測試法規成效，風傳媒（2020/03/18），https://reurl.cc/o7ELj3。

林偉傑，李顯揚貼文不實 接到更正指示，聯合早報（2023/07/25），https://www.zaobao.com.sg/realtime/singapore/story20230725-1417196?close=true。

Chomkins，史上最嚴假新聞法案上路，新加坡對「分享者」加重兩倍刑罰、最高監禁 10 年，數位時代（2019/10/24），https://www.bnext.com.tw/article/55206/singapore-fake-news-protection-from-falsehoods-manipulation-act。

KISO 自律規制白皮書（KISO 자율규제백서） Vol.2（2013-2015），頁 23，KISO，https://www.kiso.or.kr/kiso%ec%86%8c%ea%b0%9c/%ea%b8%b0%ea%b5%ac%ec%86%8c%ea%b0%9c/%ec%9e%90%ec%9c%a8%ea%b7%9c%ec%a0%9c%eb%b0%b1%ec%84%9c/。

鄉新聞，아동·청소년 3 명 중 1 명 “SNS 서 낯선 사람이 대화 요구（2020.12.13），https://www.khan.co.kr/national/national-general/article/202012132056005。

ZDNETKorea，정부，디지털플랫폼정부 국민체감 선도프로젝트

사업 (2023/06/08) 착수 https://zdnet.co.kr/view/?no=20230608112042。

ACCC, *Digital platforms inquiry - final report, June 2019*, https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf.

ACCC, *Digital platform services inquiry 2020-2025 - Project overview*, https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-2025.

ACCC, *Digital platforms services inquiry - Interim report 6: Report on social media services*, Mar. 2023, https://www.accc.gov.au/system/files/Digital%20platforms%20services%20inquiry%20-%20Interim%20report%206%20-%20Report%20on%20social%20media%20services_0.pdf.

ACMA, *Online misinformation and news quality in Australia: Position paper to guide code development*, https://www.acma.gov.au/online-misinformation-and-news-quality-australia-position-paper-guide-code-development.

ACMA, *Misinformation and news quality on digital platforms in Australia—A position paper to guide code development*, June 2020, https://www.acma.gov.au/sites/default/files/2020-06/Misinformation%20and%20news%20quality%20position%20paper.pdf.

ACMA, *A report to government on the adequacy of digital platforms' disinformation and news quality measures*, June 2021, https://www.acma.gov.au/sites/default/files/2021-11/Adequacy%20of%20digital%20platforms%20disinformation%20and%20news%20quality%20measures.pdf.

Australia Government, *New ACMA powers to combat misinformation and*

disinformation, https://www.infrastructure.gov.au/have-your-say/new-acma-powers-combat-misinformation-and-disinformation.

ACMA, *Online Misinformaiton*, (last updated 2023/07/25), https://www.acma.gov.au/online-misinformation#our-role.

Australian Government, *Online Safety Act 2021*, https://www.legislation.gov.au/Details/C2022C00052.

AMTA, BSA, CA, CESA, DIGI & IGEA, REQUEST FOR REGISTRATION OF ONLINE SAFETY CODES, Mar. 2023, https://onlinesafety.org.au/wp-content/uploads/2023/04/230331_Request-for-registration-of-revised-Codes_FINAL.pdf.

AMTA, BSA, CA, CESA, DIGI & IGEA, Online Safety Codes, https://onlinesafety.org.au/.

Aotearoa New Zealand Code of Practice for Online Safety and Harms, (2022/07/25), https://nztech.org.nz/wp-content/uploads/sites/8/2022/07/FINAL-NZ-Code-of-Practice-for-Online-Safety-and-Harms-25-July-2022.pdf.

Allen & Gledhill, *MCI Seeks Comments on Proposed Code of Practice for Online Safety and Content Code for Social Media Services*, Publications (2022/07/22), https://www.allenandgledhill.com/sg/publication/articles/22084/mci-seeks-comments-on-proposed-code-of-practice-for-online-safety-and-content-code-for-social-media-services.

TelecomNews, *Singapore mandates social media sites to block harmful content sites 'within hours'*, ETTelecom.com (2022/11/09), https://telecom.economictimes.indiatimes.com/news/singapore-mandates-social-media-sites-to-block-harmful-content-sites-within-hours/95409920.

Cybertip!ca, *Child Sexual Abuse: Project Arachnid*, https://cybertip.ca/en/child-sexual-abuse/project-arachnid/.

DATAREPORTAL, DIGITAL 2022: TAIWAN (2023/2/13), https://datareportal.com/reports/digital-2023-taiwan.

Dan Milmo, *Rohingya sue Facebook for £150bn over Myanmar genocide*, The Guardian (2021/12/06), https://www.theguardian.com/technology/2021/dec/06/rohingya-sue-facebook-myanmar-genocide-us-uk-legal-action-social-media-violence.

AFP in Yangon, *Myanmar's genocide against Rohingya not over, says rights group*, The Guardian (2020/11/23), https://www.theguardian.com/world/2020/nov/23/myanmar-is-still-committing-genocide-against-rohingya-says-rights-group.

Die Medienanstalten, *Viedo Trends 2022*, abrufbar unter: https://www.die-medienanstalten.de/fileadmin/user_upload/die_medienanstalten/Publikationen/Digibericht_Video/2022_Video_Trends/Video_Trends_2022.pdf.

Die Medienanstalten, *Vielfaltsbericht 2022 der Medienanstalten*, abrufbar unter: https://www.die-medienanstalten.de/fileadmin/user_upload/die_medienanstalten/Publikationen/Vielfaltsbericht/Vielfaltsbericht_2022_DMA_final_WEB.pdf.

DIGI, *Australian Code of Practice on Disinformation and Misinformation*, Dec. 22, 2022, https://digi.org.au/wp-content/uploads/2022/12/Australian-Code-of-Practice-on-Disinformation-and-Misinformation-FINAL-_-December-22-2022.docx.pdf.

DIGI, Australian Code of Practice on Disinformation and Misinformation, Feb. 22, 2021, https://digi.org.au/wp-content/uploads/2022/12/Australian-Code-of-Practice-on-Disinformation-and-Misinformation-FINAL-PDF-Feb-22-2021.pdf.

DIGI, DISINFORMATION CODE, https://digi.org.au/disinformation-code/.

DIGI, GOVERNANCE OF THE CODE, https://digi.org.au/disinformation-code/governance/.

DIGI, *Australian Code of Practice on Disinformation and Misinfromation*, Dec. 22, 2022, https://digi.org.au/wp-content/uploads/2022/12/Australian-Code-of-Practice-on-Disinformation-and-Misinformation-FINAL-_-December-22-2022.docx.pdf.

DIGI, 2022 CODE REVIEW, https://digi.org.au/disinformation-code/code-review/.

Dartmouth College, *Singapore's Fake News Law: For or Against Democracy?*, Democratic Erosion (2022/05/27), https://www.democratic-erosion.com/2022/05/27/singapores-fake-news-law-for-or-against-democracy/.

European Union, *Types of legislation*, https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en.

European Commission, *Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines* (2023/4/25), https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413.

EURACTIV, *Amazon joins Zalando in challenging very large online platform designation* (2023/7/11), https://www.euractiv.com/section/platforms/news/amazon-joins-zalando-in-challenging-very-large-online-platform-designation/.

Exposure Draft Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023, https://www.infrastructure.gov.au/sites/default/files/documents/communications-legislation-amendment-combatting-misinformation-and-disinformation-bill2023-june2023.pdf.

eSafetyCommissioner, *Online Safety Act 2021-Fact sheet*, Updated: January 2022, https://www.esafety.gov.au/sites/default/files/2022-02/OSA%20fact%20sheet%20updated.pdf.

eSafetyCommissioner, *Learn about the Online Safety Act*, https://www.esafety.gov.au/newsroom/whats-on/online-safety-act.

eSafetyCommissioner, *Our structure*, https://www.esafety.gov.au/about-us/who-we-are/our-structure.

eSafetyCommissioer, *Basic Online Safety Expectations*, https://www.esafety.gov.au/sites/default/files/2022-07/Basic%20Online%20Safety%20Expectations%20Table%20one%20-%20Summary%20of%20the%20Expectations%20%281%29.pdf.

eSafeCommissioner, *Basic Online Safety Expectations-reasonable steps*, https://www.esafety.gov.au/industry/basic-online-safety-expectations.

eSafetyCommisssioner, *eSafety issues first Basic Online Safety Expectations notices*, https://www.esafety.gov.au/sites/default/files/2022-08/Basic%20Online%20Safety%20Expectations%20first%20notices_0.pdf.

eSafetyCommisssioner, *Basic Online Safety Expectations-Summary of industry responses to the first mandatory transparency notices*, December 2022, https://www.esafety.gov.au/sites/default/files/2022-12/BOSE%20transparency%20report%20Dec%202022.pdf.

eSafetyCommisssioner, *Responses to transparency notices-Online service*

providers are required to report on how they are implementing the Basic Online Safety Expectations set out by the Australian Government, https://www.esafety.gov.au/industry/basic-online-safety-expectations/responses-to-transparency-notices.

eSafetyCommissioner, *Development of industry codes under the Online Safety Act-Position Paper*, September 2021, https://www.esafety.gov.au/sites/default/files/2021-09/eSafety%20Industry%20Codes%20Position%20Paper.pdf.

Eileen Yu, *Singapore can now order social media sites to block access, as 'online safety' law kicks in*, ZDNET (2023/01/31), https://www.zdnet.com/article/singapore-can-now-order-social-media-sites-to-block-access-as-online-safety-law-kicks-in/.

FSM, *Tätigkeitsbericht 03/2022 – 03/2023*, abrufbar unter: https://www.fsm.de/files/2023/05/20230517_fsm-taetigkeitsbericht-netzdg-selbstregulierung.pdf.

FSM, *Entscheidung v. 23.05.2023 - NetzDG 0442023*, abrufbar unter: https://www.fsm.de/files/2023/06/netzdg0442023_voe.pdf.

FSM, *Entscheidung v. 11.05.2023 - NetzDG 0442023*, abrufbar unter: https://www.fsm.de/files/2023/06/netzdg0432023_voe.pdf.

GOV.UK, *Department for Science, Innovation & Technology*, About US, https://www.gov.uk/government/organisations/department-for-science-innovation-and-technology/about.

GOV.UK, *Making Government Deliver for the British People*, Policy Paper (2023/02/07), https://www.gov.uk/government/publications/making-government-deliver-for-the-british-people/making-government-deliver-for-the-british-people-html?_cldee=M5321QKQK01ii5V_yXGdskZuH-AI-o0Hve6nzTGsfFFdNoa1pwkfbNki7vN4OcaK&recipientid=contact-

eda20ad0fe864d5bab07e9ad0e7c4bd3-a8333ba040ff4aed9683cb549d81dae6&esid=bdd69c2a-28a9-ed11-aad1-000d3adea432.

GOV.UK, *Online Harms White Paper*, Consultation Outcome (2019/04/08), https://www.gov.uk/government/consultations/online-harms-white-paper.

GOV.UK, *Draft Online Safety Bill*, Regulation (2021/05/12), https://www.gov.uk/government/publications/draft-online-safety-bill.

GOV.UK, *A guide to the Online Safety Bill*, Guidance (2022/12/16), https://www.gov.uk/guidance/a-guide-to-the-online-safety-bill.

GOV.UK, *Year 2 Online Media Literacy Action Plan (2022/23)*, Policy Paper (2022/04/16), https://www.gov.uk/government/publications/year-2-online-media-literacy-action-plan-202223.

Government of Canada, *The Government's Commitment to Address Online Safety*, (2023/01/31), https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html.

Government of Canada, *What We Heard: The Government's Proposed Approach to Address Harmful Content Online*, (2022/02/03), https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/what-we-heard.html.

Gov.sg, *Corrections and clarifications regarding falsehoods posted by Mr Brad Bowyer: Misleading and false statements were made by Brad Bowyer on Temasek and GIC* (2019/11/24), https://www.gov.sg/article/factually-clarifications-on-falsehoods-posted-by-mr-brad-bowyer.

Holznagel, *Das DSA ist fertig – Neunummerierung, Inkrafttreten, Behördezuständigkeit und Zukunft des NetzDG & Co.*, abrufbar unter:

https://www.cr-online.de/blog/2022/11/04/der-dsa-ist-fertig-neunummerierung-inkrafttreten-behoerdenzustaendigkeit-und-zukunft-des-netzdg-co.

House of Commons, Digital, Culture, Media & Sport Committee, *Disinformation and 'fake news': Interim Report: Government Response to the Committee's Fifth Report of Session 2017–19* (Oct. 17, 2018), *available at* https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1630/1630.pdf.

Hamilton Spectator, *Canadian Government Says It's Considering Regulating Facebook and Other Social Media Giants* (2019/4/9), https://www.thespec.com/news/canada/canadian-government-says-its-considering-regulating-facebook-and-other-social-media-giants/article_212ed47d-6927-5f39-a2ea-4a9c2cfff8bb.html?.

Internet Watch Foundation, *Who we are*, https://www.iwf.org.uk/about-us/who-we-are/.

Internet Watch Foundation, *Our history*, https://www.iwf.org.uk/about-us/why-we-exist/our-history/.

IMDA, *About IMDA*, https://www.imda.gov.sg/Who-We-Are/about-imda.

IMDA, *Regulations and Licensing Listing*, Acts and Regulations, https://www.imda.gov.sg/regulations-and-licensing-listing/acts-and-regulations.

IMDA, *About IMDA*, Our Team, https://www.imda.gov.sg/about-imda/who-we-are/our-team.

IMDA, *Regulations and Licensing Listing*, Internet, https://www.imda.gov.sg/regulations-and-licensing-listing/content-standards-and-classification/standards-and-classification/internet.

IMDA, *Singapore has a three-prong approach to Internet content*

regulation, Internet Content Regulation, Internet Content Regulation (2022/10/26), https://www.imda.gov.sg/Infocomm-regulation-and-guides/infocomm-regulation/internet-content-regulation.

Ian Seiderman, *RE: Protection from Online Falsehoods and Manipulation Bill 2019*, International Commission of Jurists (ICJ) (2019/04/12), *available at* https://www.icj.org/wp-content/uploads/2019/04/Singapore-online-regulation-bill-letter-advocacy-open-letter-2019-ENG.pdf.

International Commission of Jurists, *Singapore: ICJ calls on government to repeal or substantially amend the POFMA, two years after it entered into force*, ICJ (2021/04/10), https://www.icj.org/singapore-icj-calls-on-government-to-repeal-or-substantially-amend-the-pofma-two-years-after-it-entered-into-force/.

IMDA, *IMDA notifies Meta of egregious Child Sexual Exploitation content, defined under Singapore's new Online Safety law, found on Facebook*, Resources (2023/06/09), https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/imda-notifies-meta-of-egregious-child-sexual-exploitation-content-defined-under-singapores-new-online-safety-law-found-on-facebook.

IMDA, *IMDA's Online Safety Code comes into effect* (2023/07/17), https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/imdas-online-safety-code-comes-into-effect.

Netzpolitik, *Meta muss keine Widerspruchsmöglichkeit anbieten*, abrufbar unter: https://netzpolitik.org/2023/netzdg-reform-ungueltig-meta-muss-keine-widerspruchsmoeglichkeit-anbieten.

Kahl/Lippert, *Warum nan das NetzDG doch noch braucht*, abrufbar unter: https://www.lto.de/recht/hintergruende/h/netzdg-das-zustellungsbevollmaechtigter-inland-rechtsschutz-internetnutzer-

plattformhaftung.

Kathleen, *SPH and Mediacorp remain silent on criticisms and concerns by various statements published by different groups on POFMA*, TQC (2019/04/30), https://www.theonlinecitizen.com/2019/04/30/sph-and-mediacorp-remain-silent-on-criticisms-and-concerns-by-various-statements-published-by-different-groups-on-pofma/.

Liesching, *Gilt das NetzDG für Facebook, YouTube und Twitter?*, abrufbar unter: https://community.beck.de/2020/02/11/gilt-das-netzdg-fuer-facebook-youtube-und-twitter.

Learning Centre: Criminal Law: Cybercrime, *Singapore Fake News Laws: Guide to POFMA (Protection from Online Falsehoods and Manipulation Act)*, Singapore Legal Advice (2022/04/25), https://singaporelegaladvice.com/law-articles/singapore-fake-news-protection-online-falsehoods-manipulation/.

Lakeisha Leo, *Singapore takes a 'whole-of-society' approach to combat misinformation: Tan Kiat How*, CNA (2022/04/29) https://www.channelnewsasia.com/singapore/tan-kiat-how-approach-combat-misinformation-local-news-2656731.

Minister for Communications, *Consultation opens on new laws to tackle online misinformation and disinformation*, (2023/06/25), https://minister.infrastructure.gov.au/rowland/media-release/consultation-opens-new-laws-tackle-online-misinformation-and-disinformation.

Ministry of Communications and Information, *Our Organisation*, Who We Are, https://www.mci.gov.sg/about-us.

Ministry of Communications and Information, *Infocomm Media 2025*, https://www.mci.gov.sg/portfolios/infocomm-media/infocomm-media-2025/introduction-to-infocomm-media-2025.

Ministry of Finance, *Use of POFMA on an online posting by Mr Brad Bowyer*, Press Releases (2019/11/25), https://www.mof.gov.sg/news-publications/press-releases/use-of-pofma-on-an-online-posting-by-mr-brad-bowyer.

Marian Ho, *New Codes of Practice for Online Safety in Singapore*, Dentons (2022/07/18), https://dentons.rodyk.com/en/insights/alerts/2022/july/18/new-codes-of-practice-for-online-safety-in-singapore.

Ministry of Communications and Information, *Public Consultation on Enhancing Online Safety for Users in Singapore*, https://www.reach.gov.sg/Participate/Public-Consultation/Ministry-of-Communications-and-Information/public-consultation-on-enhancing-online-safety-for-users-in-singapore.

New Zealand Government-Parliamentary Council Office, *Harmful Digital Communications Act 2015*, https://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html#DLM5711814.

Netsafe, *WHAT IS THE HDCA?*, (2021/09/01), https://netsafe.org.nz/what-is-the-hdca/.

Netsafe, Aotearoa New Zealand Code of Practice for Online Safety and Harms Draft, https://netsafe.org.nz/aotearoa-new-zealand-code-of-practice-for-online-safety-and-harms-draft/.

Netsafe& NZTech, *The Code - Aotearoa New Zealand Code of Practice for Online Safety and Harms*, July 2022, https://thecode.org.nz/wp-content/uploads/sites/38/2023/06/THE-CODE-DOCUMENT-FINAL.pdf.

NZTech, *About the Code*, https://thecode.org.nz/about-the-code/.

NZTech, *About NZTech*, July 21, 2022,

https://nztech.org.nz/reports/creating-collective-impact/.

NZTech, *Governance of the Code*, https://thecode.org.nz/governance/.

NZTech, *The Code - TERMS OF REFERENCE*, https://thecode.org.nz/wp-content/uploads/sites/38/2023/06/THE-CODE-Terms-of-Reference.pdf.

Ofcom, *Call for evidence: categorisation - research and advice*, Consultations (2023/07/11), https://www.ofcom.org.uk/consultations-and-statements/category-1/call-for-evidence-categorisation-research-and-advice.

Ofcom, *Looking ahead to online regulation: It's time to rethink transparency reporting*, News Centre (2023/01/31), https://www.ofcom.org.uk/news-centre/2023/looking-ahead-to-online-regulation-transparency-reporting

Ofcom, *Rule and Guidance: Statutory Rules and Non-Binding Guidance for Providers of On-Demand Programme Services* (2021/12/10), *available at* https://www.ofcom.org.uk/__data/assets/pdf_file/0029/229358/ODPS-Rules-and-Guidance.pdf.

Paul Karp, *Australia's media regulator to get new powers to crack down on online misinformation*, The Gardian (2023/01/19), https://www.theguardian.com/media/2023/jan/20/australias-media-regulator-to-be-get-new-powers-to-crack-down-online-misinformation.

Project Arachnid, *What is Project Arachnid?*, https://www.projectarachnid.ca/en/#what-is-project-arachnid.

Parliamentary Counsel Office, *Films, Videos, and Publications Classification Act 1993*, Version as at 12 April 2022, https://www.legislation.govt.nz/act/public/1993/0094/latest/DLM31

2895.html.

Parliamentary Counsel Office, *Unsolicited Electronic Messages Act 2007*, Version as at 28 October 2021, https://www.legislation.govt.nz/act/public/2007/0007/latest/DLM405134.html.

Parliamentary Counsel Office, *Communications (New Media) Bill*, https://www.lawcom.govt.nz/sites/default/files/publicationAttachments/communications_new_media_bill.pdf.

POFMA Office, *About Us*, https://www.pofmaoffice.gov.sg/about-us/.

Prisca Ang, *PSP member in first Pofma case considering appeal*, STRAITSTIMES (2019/11/29), https://www.straitstimes.com/singapore/psp-member-in-first-pofma-case-considering-appeal.

Public Consultation on Proposed Measures to Enhance Online Safety for Users in Singapore, https://www.reach.gov.sg/Participate/Public-Consultation/Ministry-of-Communications-and-Information/public-consultation-on-enhancing-online-safety-for-users-in-singapore (last visited Aug. 1, 2023).

Ryan Browne, Meta and Microsoft can't self-regulate their metaverses, UK regulator warns, CNBC (2022/10/26), https://www.cnbc.com/2022/10/26/meta-and-microsoft-cant-self-regulate-their-metaverses-ofcom-warns.html (last visited Aug. 15, 2023).

Smart Nation and Digital Government Office, Infocomm Media Industry Transformation Map (ITM), Press Room (2017/11/03), https://www.smartnation.gov.sg/media-hub/press-releases/infocomm-media-industry-transformation-map-itm/ (last visited June 21, 2023).

Singapore Fake News Laws: Guide to POFMA (Protection from Online Falsehoods and Manipulation Act), Singapore Legal Advice (2022/04/25), https://singaporelegaladvice.com/law-articles/singapore-fake-news-protection-online-falsehoods-manipulation/ (last visited June 21, 2023).

Singapore, Lee Hsien Yang issued POFMA order over Facebook post on Ridout Road rentals, SPH circulation data, CNA (2023/07/25), https://www.channelnewsasia.com/singapore/pofma-order-lee-hsien-yang-facebook-post-ridout-road-rentals-sph-circulation-data-3652176 (last visited Aug. 1, 2023).

Schleif/Kettmann, *Komplementär oder konkurrierende: NetzDG und DSA*, abrufbar unter: https://www.hans-bredow-institut.de/de/blog/komplementaer-oder-konkurrierend-netzdg-und-dsa.

Tom Bristow, *POLITICO Pro Morning Tech UK: Budget hopes - Ofcom's next move - DSIT portfolios*, POLITICO (2023/03/15), https://www.politico.eu/newsletter/morning-tech-uk/politico-pro-morning-tech-uk-budget-hopes-ofcoms-next-move-dsit-portfolios/.

Te Tari Taiwhenua-Department of Internal Affairs, *About the Digital Safety Group*, https://www.dia.govt.nz/About-the-Digital-Safety-Group.

Te Tari Taiwhenua-Department of Internal Affairs, *Report harmful online content*, https://www.dia.govt.nz/Digital-Safety-Report-harmful-online-content.

Te Tari Taiwhenua-Department of Internal Affairs, *Classification in New Zealand*, https://www.dia.govt.nz/Commercial-video-on-demand-classification.

Te Tari Taiwhenua-Department of Internal Affairs, *Spam Prevention & Messaging Compliance*, https://www.dia.govt.nz/Spam.

Te Tari Taiwhenua-Department of Internal Affairs, *Internet and website filter*, https://www.dia.govt.nz/digital-child-exploitation-DCEFS.

The Business Times, *Singapore joins other places with laws regulating online content*, International (2022/06/20), https://www.businesstimes.com.sg/international/singapore-joins-other-places-laws-regulating-online-content.

UK Parliament, *Public Bill Committees*, https://www.parliament.uk/mps-lords-and-offices/offices/commons/scrutinyunit/public-bill-committees/.

Zalando, *Zalando files legal action against the European Commission to contest its designation as a "Very Large Online Platform" as defined by the Digital Services Act* (2023/6/27), https://corporate.zalando.com/en/company/zalando-files-legal-action-against-european-commission-contest-its-designation-very-large.

附錄一 一般民眾電話訪問調查問卷

國家通訊傳播委員會

「網際網路傳播社會調查委託研究」
一般民眾電話訪問調查問卷

◆ **您好，我們接受國家通訊傳播委員會（NCC）的委託，正在進行一項有關網路行為風險的電話訪問。打擾您幾分鐘的時間，請您接受我們的訪問，謝謝！**

*民眾有疑問時：
若您有疑問，可至 GRB 政府研究資訊系統網頁（https://www.grb.gov.tw/）查詢「網際網路傳播社會調查委託研究案」，或撥打「165 反詐騙諮詢專線」查詢。

◆ **因為這支電話是由電腦隨機抽出的，請問您目前住在哪一個縣市？**

◆ **請問您是否年滿 18 歲？**

（手機樣本若未滿 18 歲即停止訪問）

*若否：
因為我們需要訪問 18 歲以上的民眾，能不能請您家中 18 歲以上的家人來聽電話？謝謝！

(1) 回答：家中沒有 18 歲以上民眾
對不起，我們是要訪問 18 歲以上的民眾，下次有機會再訪問您，謝謝！

(2) 回答：家人都不在
請問他們大概什麼時候會回來？（約訪）

(3) 回答：可以
（待合格受訪者接聽電話後，重複開場白）

(4) 回答：是
（直接訪問）

第一部分 網路行為與使用平臺（2*n 題）

1.1 請問您近一個月內有使用以下哪些類型的平臺或媒體？
（複選，請逐一提示選項（1）～（6））

- ☐（1）社群媒體平臺（例如：Facebook、Instagram、YouTube、PTT 等）（跳題 1.2）
- ☐（2）通訊軟體（例如：LINE、Messenger、Discord）（跳題 1.2）
- ☐（3）網路新聞平臺（例如：Yahoo 新聞、LINE TODAY）（跳題 1.2）
- ☐（4）拍賣、購物平臺（例如：Yahoo 拍賣、蝦皮購物、露天、淘寶）（跳題 1.2）
- ☐（5）串流影音服務（例如：Netflix、愛奇藝、MyVideo）（跳題 1.2）
- ☐（6）傳統電視（例如：第四台有線電視、中華電信 MOD、無線電視）（跳題 1.2）
- ☐（7）以上都沒有使用（跳答第二部分）

跳題說明：
受訪者選擇平臺選項後，請跳至 1.2，詢問受訪者在該平臺的使用頻率和行為。完成該部分後，再回到第一題進行後續回答。

1.2 請問您一天使用該類型平臺（可帶入受訪者 1.1 回答的選項）**的時間約幾小時？**

- ☐（1）未滿 1 小時
- ☐（2）1～未滿 3 小時
- ☐（3）3～未滿 5 小時
- ☐（4）5 小時以上
- ☐（5）不一定
- ☐（6）不知道／拒答

跳題說明：
請回到 1.1 繼續詢問下一個有使用的網路平臺。全部平臺的使用頻率與目的調查完後，再進入第二部分。

第二部分 知覺網路個人、社會問題與風險危害認知（6 題）

2.1 請依照您的同意程度回答下列問題（政治不實訊息）：

		非常同意	有點同意	有點不同意	非常不同意	不知道/無法回答
1.	我不曾在網路平臺上看到與政治相關的不實訊息 （若受訪者 1.1「僅」選擇（6）或（7），此題不問）					
2.	網路平臺上與政治相關的訊息很多都難以辨識真假。					
3.	政治上的不實訊息影響了每個人的判斷。					
4.	我曾經看過電視新聞將擷取自網路平臺的訊息作為新聞報導。					
5.	我認為電視新聞在報導擷取自網路平臺的訊息前，有做到多方的事實查核。					

2.2 請依照您的同意程度回答下列問題（兒少網路安全）：

		非常同意	有點同意	有點不同意	非常不同意	不知道/無法回答
1.	家裡的未成年人曾經在網路平臺上接觸到色情或暴力內容。					
2.	網路平臺對於未成年人來說是很危險的環境。					
3.	未成年人在網路平臺上接觸到色情或暴力內容的機率很高。					

2.3 請依照您的同意程度回答下列問題（網路交易安全）：

		非常同意	有點同意	有點不同意	非常不同意	不知道/無法回答
1.	我曾經在網路平臺上購物被賣家/店家欺騙。 （若受訪者 1.1「僅」選擇（6）或（7），此題不問）					
2.	我認為使用網路平臺進行消費買賣非常危險。					
3.	使用網路平臺交易被騙的機會很高。					

2.4 請依照您的同意程度回答下列問題（網路霸凌）：

		非常同意	有點同意	有點不同意	非常不同意	不知道/無法回答
1.	我曾經有被網路霸凌的經驗。（例如：人身攻擊、人肉搜索） （若受訪者 1.1「僅」選擇（6）或（7），此題不問）					
2	網路平臺讓霸凌行為變得更嚴重。					
3.	因為有網路平臺，現代人遭受霸凌的機會變高了。					

2.5 請依照您的同意程度回答下列問題（個人權益）：

		非常同意	有點同意	有點不同意	非常不同意	不知道/無法回答
1.	我曾經有在網路平臺上的言論被管理員刪除的經驗。 （若受訪者 1.1「僅」選擇（6）或（7），此題不問）					
2.	為了維護網路安全，我認為政府或網路平臺有權力刪除不適當的言論是合理的。					
3.	政府或網路平臺對不安全言論的管制會讓個人權益被侵害的可能性變高。					

2.6 請問是否有哪些問題是上述我們沒提到、但是您感受深刻的？（開放題）

第三部分 處理的方式與偏好（跳題，實答 9 題）

3.1.1 您覺得在網路平臺上的「政治不實訊息」問題，誰應當負「最大的責任」，並出面處理？

（選兩個，一個一個跳題）

例如：網傳利用溫鹽水漱口可以殺死新冠肺炎。您覺得像這樣的不實訊息問題，應由誰來處理？

☐（1）網路使用者自己（跳題 3.1.2）
☐（2）網路平臺（例如：FB、LINE 等）（跳題 3.1.3、3.1.4）
☐（3）政府機關（跳題 3.1.5）
☐（4）民間專業組織（例如：台灣事實查核中心）（跳題 3.1.6）
☐（5）其他（請說明）

3.1.2 您覺得網路使用者面對「政治不實訊息」的問題該如何處理？

（單選，請逐一唸出選項）

☐（1）自行提升對不實訊息的判斷能力
☐（2）交由事實查核網站或 LINE 官方帳號（例如：台灣事實查核中心、美玉姨等）查核訊息真偽
☐（3）不必在意不實訊息的問題
☐（4）其他（請說明）

3.1.3 您覺得網路平臺粉專管理員面對「政治不實訊息」的問題該如何處理？

（單選，請逐一唸出選項）

☐（1）由各粉專管理員主動巡視、判斷並處置（例如：移除或取消作者/張貼者發言資格）
☐（2）由各粉專管理員依投訴判斷並處置（例如：移除或取消作者/張貼者發言資格）
☐（3）其他（請說明）

3.1.4 您覺得網路平臺面對「政治不實訊息」的問題該如何處理？
（請先問主動或被動處理，再詢問處理方式）

由站方/營運方（例如：FB 總公司）主動處理，方式為：
□（1）主動判斷並加註警語或降低排序
□（2）主動判斷並移除

由站方/營運方（例如：FB 總公司）被動處理，方式為：
□（3）依投訴判斷並加註警語或降低排序
□（4）依投訴判斷並移除

□（5）其他（請說明）

3.1.5 您覺得政府面對「政治不實訊息」的問題「最應該」如何處理？
（單選，請逐一唸出選項）

□（1）由單一主管機關（例如：數位發展部或 NCC，因為是網路環境）判斷是否為不實訊息並決定是否阻斷、移除或裁罰
□（2）由業務主管機關（例如：衛福部或內政部）判斷是否為不實訊息並決定是否阻斷、移除或裁罰
□（3）由法院判斷是否為不實訊息並決定是否阻斷、移除或裁罰
□（4）其他（請說明）

3.1.6 您覺得民間組織面對「政治不實訊息」的問題該如何處理？
（單選，請逐一唸出選項）

□（1）由民間專業組織針對違規者提出警告，並公布名單
□（2）由民間專業組織針對違規者通報平臺或主管機關
□（3）由民間專業組織要求平臺提供第三方認證的透明度報告
□（4）由民間專業組織向提供不實訊息（假新聞）的平臺進行裁罰
□（5）其他（請說明）

3.2.1 您覺得在網路平臺上的「兒少網路安全」問題，誰應當負「最大的責任」，並出面處理？

（選兩個，一個一個跳題）

例如：兒童透過 YouTube 看卡通，看見突然出現含色情暴力的廣告。您覺得像這樣的事件，應該由誰來處理相關兒少網路安全問題？

☐（1）網路使用者自己／父母／長輩（跳題 3.2.2）
☐（2）網路平臺（例如：FB、LINE 等）（跳題 3.2.3、3.2.4）
☐（3）政府機關（跳題 3.2.5）
☐（4）民間專業組織（例如：台灣事實查核中心）（跳題 3.2.6）
☐（5）其他（請說明）

3.2.2 您覺得網路使用者面對「兒少網路安全」的問題該如何處理？

（單選，請逐一唸出選項）

☐（1）監控家中兒少網路平臺使用情形
☐（2）主動學習辨識和協助兒少過濾危險的網路內容
☐（3）其他（請說明）

3.2.3 您覺得粉專管理員面對「兒少網路安全」的問題該如何處理？

（單選，請逐一唸出選項）

☐（1）由各粉專管理員主動巡視、判斷並處置會危害兒少的網路內容（例如：移除或取消作者/張貼者發言資格）
☐（2）由各粉專管理員依投訴判斷並處置會危害兒少的網路內容（例如：移除或取消作者/張貼者發言資格）
☐（3）其他（請說明）

3.2.4 您覺得網路平臺面對「兒少網路安全」的問題該如何處理？
（請先問主動或被動處理，再詢問處理方式）

由站方/營運方（例如：FB 總公司）主動處理，方式為：
☐（1）主動判斷並加註警語或降低排序
☐（2）主動判斷並移除

由站方/營運方（例如：FB 總公司）被動處理，方式為：
☐（3）依投訴判斷並加註警語或降低排序
☐（4）依投訴判斷並移除

☐（5）其他（請說明）

3.2.5 您覺得政府面對「兒少網路安全」的問題「最應該」該如何處理？
（單選，請逐一唸出選項）

☐（1）由單一主管機關（例如：數位發展部或 NCC，因為是網路環境）判斷是否為兒少網路安全問題並決定是否阻斷、移除或裁罰
☐（2）由業務主管機關（例如：衛福部或內政部）判斷是否為兒少網路安全問題並決定是否阻斷、移除或裁罰
☐（3）由法院判斷是否為兒少網路安全問題並決定是否阻斷、移除或裁罰
☐（4）其他（請說明）

3.2.6 您覺得民間組織面對「兒少網路安全」的問題該如何處理？
（單選，請逐一唸出選項）

☐（1）由民間專業組織針對違規者提出警告，並公布名單
☐（2）由民間專業組織針對違規者通報平臺或主管機關
☐（3）由民間專業組織要求平臺提供第三方認證的透明度報告
☐（4）民間專業組織向提供兒少網路安全問題的平臺進行裁罰
☐（5）其他（請說明）

3.3.1 您覺得在網路平臺上的「網路交易安全」問題，誰應當負「最大的責任」，並出面處理？

（選兩個，一個一個跳題）

例如：民眾上購物網站上購物，收到的物品卻與展示圖片落差很大，或是收到假貨。

☐（1）網路使用者自己（跳題 3.3.2）
☐（2）網路平臺（例如：FB、LINE 等）（跳題 3.3.3、3.3.4）
☐（3）政府機關（跳題 3.3.5）
☐（4）民間專業團體（例如：台灣事實查核中心）（跳題 3.3.6）
☐（5）其他（請說明）

3.3.2 您覺得網路使用者面對「網路交易安全」的問題該如何處理？

（單選，請逐一唸出選項）

☐（1）提升自己辨識網路詐騙、釣魚網站等的判斷能力，並提醒自己網路上的交易都具有風險，購物前務必三思
☐（2）不要在網路平臺上購物
☐（3）其他（請說明）

3.3.3 您覺得網路平臺粉專管理員面對「網路交易安全」的問題該如何處理？

（單選，請逐一唸出選項）

☐（1）由各粉專管理員主動巡視、判斷並處置（例如：移除具有詐騙的購物資訊）
☐（2）由各粉專管理員依投訴判斷並處置（例如：移除具有詐騙的購物資訊）
☐（3）其他（請說明）

3.3.4 您覺得網路平臺面對「網路交易安全」的問題該如何處理？
（請先問主動或被動處理，再詢問處理方式）

由站方/營運方（例如：FB 總公司）主動處理，方式為：
□（1）主動判斷並加註警語或降低排序
□（2）主動判斷並移除

由站方/營運方（例如：FB 總公司）被動處理，方式為：
□（3）依投訴判斷並加註警語或降低排序
□（4）依投訴判斷並移除

□（5）其他（請說明）

3.3.5 您覺得政府面對「網路交易安全」的問題該如何處理？
（單選，請逐一唸出選項）

□（1）由單一主管機關（例如：數位發展部或 NCC，因為是網路環境）判斷是否具有網路交易安全的風險，並決定是否阻斷、移除或裁罰
□（2）由業務主管機關（例如：經濟部或農委會）判斷是否具有網路交易安全的風險並決定是否阻斷、移除或裁罰
□（3）由法院判斷是否具有網路交易安全的風險並決定是否阻斷、移除或裁罰
□（4）其他（請說明）

3.3.6 您覺得民間組織面對「網路交易安全」的問題該如何處理？
（單選，請逐一唸出選項）

□（1）由民間專業組織針對違規業者加註警語，並公布名單
□（2）由民間專業組織針對違規者通報平臺或主管機關
□（3）由民間專業組織向未處理好網路交易安全問題的平臺進行裁罰
□（4）其他（請說明）

3.4.1 您覺得在網路平臺上的「網路霸凌」問題，誰應當負「最大的責任」，並出面處理？

（選兩個，一個一個跳題）

例如：有位身材偏豐腴的男性被另名不認識的陌生人偷拍照並上傳到社群平臺，攻擊其身材。您覺得像這樣的事件，應該由誰來處理相關網路霸凌問題？

☐（1）網路使用者自己（跳題 3.4.2）
☐（2）網路平臺（例如：FB、LINE 等）（跳題 3.4.3、3.4.4）
☐（3）政府機關（跳題 3.4.5）
☐（4）民間專業組織（例如：台灣事實查核中心）（跳題 3.4.6）
☐（5）其他（請說明）

3.4.2 您覺得網路使用者面對「網路霸凌」的問題該如何處理？

（單選，請逐一唸出選項）

☐（1）自行提升對網路霸凌的認知與辨別能力，並提醒自己不製造、不跟隨、不傳播、不被影響
☐（2）不必在意網路霸凌的問題
☐（3）其他（請說明）

3.4.3 您覺得網路平臺粉專管理員面對「網路霸凌」的問題該如何處理？

（單選，請逐一唸出選項）

☐（1）由各粉專管理員主動巡視、判斷並處置（例如：移除或取消作者/張貼者發言資格）
☐（2）由各粉專管理員依投訴判斷並處置（例如：移除或取消作者/張貼者發言資格）
☐（3）其他（請說明）

3.4.4 您覺得網路平臺面對「網路霸凌」的問題該如何處理？
（請先問主動或被動處理，再詢問處理方式）

由站方/營運方（例如：FB 總公司）主動處理，方式為：
□（1）主動判斷並加註警語或降低排序
□（2）主動判斷並移除

由站方/營運方（例如：FB 總公司）被動處理，方式為：
□（3）依投訴判斷並加註警語或降低排序
□（4）依投訴判斷並移除

□（5）其他（請說明）

3.4.5 您覺得政府面對「網路霸凌」的問題該如何處理？
（單選，請逐一唸出選項）

□（1）由單一主管機關（例如數位發展部或 NCC，因為是網路環境）判斷是否為網路霸凌問題並決定是否阻斷、移除或裁罰
□（2）由業務主管機關（例如：教育部或內政部）判斷是否為網路霸凌問題並決定是否阻斷、移除或裁罰
□（3）由法院判斷是否為網路霸凌問題並決定是否阻斷、移除或裁罰
□（4）其他（請說明）

3.4.6 您覺得民間組織面對「網路霸凌」的問題該如何處理？
（單選，請逐一唸出選項）

□（1）由民間專業組織針對違規者提出警告，並公布名單
□（2）由民間專業組織針對違規者通報平臺或主管機關
□（3）由民間專業組織要求平臺提供第三方認證的透明度報告
□（4）由民間專業組織向提供網路霸凌問題的平臺進行裁罰
□（5）其他（請說明）

3.5 您覺得當使用者被限制時（例如：平臺處理違規事情有誤），應以何種方式來進行申訴或維護權利？

（單選，請逐一唸出選項）

例如：民眾張貼在社群平臺上之貼文無故被移除、移除理由不合理，或帳號被停權卻未被告知任何理由。

☐（1）透過平臺所建立之內部異議機制進行申訴
☐（2）向業務主管機關（例如：數位發展部或 NCC，因為是網路環境）申訴，由業務主管機關負責處理相關紛爭
☐（3）由民間專業組織，處理相關紛爭
☐（4）透過訴訟，由法院判定使用者權益是否有被限制

第四部分 基本資料（6 題）

1. 請問您目前居住的地方有沒有安裝市內電話？

（本題市話樣本不問）

☐（1）有
☐（2）沒有
☐（3）沒意見／很難說／不知道／拒答

2. 請問您目前有沒有使用手機？

（本題手機樣本不問）

☐（1）有
☐（2）沒有
☐（3）沒意見／很難說／不知道／拒答

3. 生理性別

☐ 男性
☐ 女性
☐ 其他（請說明）_____

4. 年齡

☐ 18-29 歲
☐ 30-39 歲
☐ 40-49 歲
☐ 50-59 歲
☐ 60-69 歲
☐ 70 歲以上
☐ 不知道／拒答

5. 教育程度

☐ 小學及以下
☐ 國中
☐ 高中職及五專
☐ 大學院校（含二技等）
☐ 碩士及以上
☐ 不知道／拒答

6. 職業

☐ 政府聘僱人員（含公務人員及約聘人員）或軍人
☐ 民營企業經理主管
☐ 民營企業辦公室人員（專業人員、助理專業人員或事務工作者）
☐ 民營企業服務及銷售工作人員
☐ 民營企業農、林、漁、牧業生產人員
☐ 民營企業勞動工作者
☐ 家管
☐ 學生
☐ 正在找工作
☐ 退休
☐ 無業
☐ 其他
☐ 不知道／拒答

第五部分 擴充題－串流影音服務（3 題）

*如受訪者於 1.1 勾選（3）「串流影音服務」，則接續詢問以下有關消費者權益保障相關問題。

5.1 在使用串流影音服務時，您是否曾經遭遇過消費爭議？
（複選）

☐（1）退訂（例如：介面上找不到退訂功能，須致電客服處理）
☐（2）續訂（例如：無法更換付費方案，或自動續訂時被重複扣款）
☐（3）服務不穩定或無預警中斷
☐（4）信用卡資料外洩
☐（5）無法聯繫上客服
☐（6）其他（請說明）
☐（7）未曾有過消費爭議

5.2 承上題，在您回答的消費爭議類型中，您認為最需要解決的是？
（單選）

☐（1）退訂（例如：介面上找不到退訂功能，須致電客服處理）
☐（2）續訂（例如：無法更換付費方案，或自動續訂時被重複扣款）
☐（3）服務不穩定或無預警中斷
☐（4）信用卡資料外洩
☐（5）無法聯繫上客服
☐（6）其他（請說明）

5.3 您認為政府面對「串流影音服務的消費爭議」最需要採取的措施為何？
（單選）

☐（1）立法課予服務提供者相關義務（例如：要求業者公告服務使用條款，包含消費者保護措施、服務中斷賠償或隱私政策等）
☐（2）設立單一窗口，作為處理串流影音服務消費爭議的專責機構
☐（3）透過該產業的公協會轉介，以業者自律之方式處理
☐（4）其他（請說明）

～　問卷填答完畢，感謝您的協助　～

附錄二 網路調查問卷

國家通訊傳播委員會

「網際網路傳播社會調查委託研究」
一般民眾網路調查問卷

您好，財團法人電信技術中心接受國家通訊傳播委員會（NCC）的委託，正在進行一項有關網際網路社會問題的研究，需要您的寶貴意見。此份問卷填寫完畢約將花您 10-15 分鐘的時間。您的回覆完全匿名，僅做整體性呈現，請您放心填寫。謝謝！

您的寶貴意見將是本研究成功與否的關鍵。若有任何問題與意見請聯繫：林永翰 副研究員（email：Quinton.Lin@ttc.org.tw)。非常感謝您的支持與協助。

敬祝

身體健康、平安快樂

計畫主持人	財團法人電信技術中心	王牧寰 資深研究員兼副理
共同主持人	國立臺北大學公共行政暨政策學系	林俞君 助理教授
協同主持人	國立政治大學法律系	吳秦雯 副教授
協同主持人	輔仁大學法律學系	林家暘 助理教授
專案經理	財團法人電信技術中心	林永翰 副研究員

敬上

第一部分　網路行為與使用平臺

填答者在 1.1.2（社群網站）、1.2.2（影音分享平臺）、1.3.2（網路論壇）、1.4.2（通訊軟體）及 1.6.2（拍賣、購物平臺）五題之中，至少需有 3 題勾選（1）有使用，才能進入第二部分

1.1.1　請問您是否為任一社群網站（例如：Facebook、Instagram）之註冊會員？

☐（1）是
☐（2）否（跳題至 1.2.1）

1.1.2　承上，請問您近一個月內是否有使用這些您註冊為會員的社群網站（例如：Facebook、Instagram）？

☐（1）有使用
☐（2）沒有使用（跳題至 1.2.1）

1.1.3　請問您平均一天使用這些社群網站的時間約為幾小時？

☐（1）未滿 1 小時
☐（2）1～未滿 3 小時
☐（3）3～未滿 5 小時
☐（4）5 小時以上
☐（5）不一定
☐（6）不知道／拒答

1.1.4　請問您在使用這些社群網站時，是否曾閱讀過這些平臺的服務及使用者條款？

☐（1）有，曾經閱讀過
☐（2）無，不曾閱讀過（跳題至 1.2.1）
☐（3）不知道有服務及使用者條款（跳題至 1.2.1）
☐（4）拒答（跳題至 1.2.1）

1.1.5　請問您在使用這些社群網站時，對這些平臺的服務及使用者條款瞭解程度為何？

□（1）清楚瞭解相關內容
□（2）大致瞭解內容
□（3）有仔細閱讀，但對內容不太瞭解
□（4）有瀏覽過，但沒有仔細閱讀內容
□（5）拒答

1.2.1　請問您是否為任一可自行上傳內容的影音分享平臺（例如：YouTube、TikTok）之註冊會員？

☐（1）是
☐（2）否（跳題至 1.3.1）

1.2.2　請問您近一個月內是否有使用這些您註冊為會員的影音分享平臺（例如：YouTube、TikTok）？

☐（1）有使用
☐（2）沒有使用（跳題至 1.3.1）

1.2.3　請問您平均一天使用這些影音分享平臺的時間約為幾小時？

☐（1）未滿 1 小時
☐（2）1～未滿 3 小時
☐（3）3～未滿 5 小時
☐（4）5 小時以上
☐（5）不一定
☐（6）不知道／拒答

1.2.4　請問您在使用這些影音分享平臺時，是否曾閱讀過這些平臺的服務及使用者條款？

☐（1）有，曾經閱讀過
☐（2）無，不曾閱讀過（跳題至 1.3.1）
☐（3）不知道有服務及使用者條款（跳題至 1.3.1）
☐（4）拒答（跳題至 1.3.1）

1.2.5　請問您在使用這些影音分享平臺時，對這些平臺的服務及使用者條款瞭解程度為何？

☐（1）清楚瞭解相關內容
☐（2）大致瞭解內容
☐（3）有仔細閱讀，但對內容不太瞭解
☐（4）有瀏覽過，但沒有仔細閱讀內容
☐（5）拒答

1.3.1 請問您是否為任一網路論壇（例如：批踢踢實業坊、DCard）之註冊會員？

☐（1）是
☐（2）否（跳題至 1.4.1）

1.3.2 請問您近一個月內是否有使用這些您註冊為會員的網路論壇（例如：批踢踢實業坊、DCard）？

☐（1）有使用
☐（2）沒有使用（跳題至 1.4.1）

1.3.3 請問您平均一天使用這些網路論壇的時間約為幾小時？

☐（1）未滿 1 小時
☐（2）1～未滿 3 小時
☐（3）3～未滿 5 小時
☐（4）5 小時以上
☐（5）不一定
☐（6）不知道／拒答

1.3.4 請問您在使用這些網路論壇時，是否曾閱讀過這些平臺的服務及使用者條款或版規？

☐（1）有，曾經閱讀過
☐（2）無，不曾閱讀過（跳題至 1.4.1）
☐（3）不知道有服務及使用者條款（跳題至 1.4.1）
☐（4）拒答（跳題至 1.4.1）

1.3.5 請問您在使用這些網路論壇時，對這些平臺的服務及使用者條款或版規瞭解程度為何？

☐（1）清楚瞭解相關內容
☐（2）大致瞭解內容
☐（3）有仔細閱讀，但對內容不太瞭解
☐（4）有瀏覽過，但沒有仔細閱讀內容
☐（5）拒答

1.4.1請問您是否為任一通訊軟體（例如：LINE、Messenger、Discord）之註冊會員？

☐（1）是
☐（2）否（跳題至 1.5.1）

1.4.2 請問您近一個月內是否有使用這些您註冊為會員的通訊軟體（例如：LINE、Messenger、Discord）？

☐（1）有使用
☐（2）沒有使用（跳題至 1.5.1）

1.4.3 請問您平均一天使用這些通訊軟體的時間約為幾小時？

☐（1）未滿 1 小時
☐（2）1～未滿 3 小時
☐（3）3～未滿 5 小時
☐（4）5 小時以上
☐（5）不一定
☐（6）不知道／拒答

1.4.4 請問您在使用這些通訊軟體時，是否曾閱讀過這些軟體的服務及使用者條款？

☐（1）有，曾經閱讀過
☐（2）無，不曾閱讀過（跳題至 1.5.1）
☐（3）不知道有服務及使用者條款（跳題至 1.5.1）
☐（4）拒答（跳題至 1.5.1）

1.4.5 請問您在使用這些通訊軟體時，對這些軟體的服務及使用者條款瞭解程度為何？

☐（1）清楚瞭解相關內容
☐（2）大致瞭解內容
☐（3）有仔細閱讀，但對內容不太瞭解
☐（4）有瀏覽過，但沒有仔細閱讀內容
☐（5）拒答

1.5.1 請問您是否為任一網路新聞平臺（例如：Yahoo 新聞、LINE TODAY）之註冊會員？

☐（1）是
☐（2）否（跳題至 1.6.1）

1.5.2 請問您近一個月內是否有使用這些您註冊為會員的網路新聞平臺（例如：Yahoo 新聞、LINE TODAY）？

☐（1）有使用
☐（2）沒有使用（跳題至 1.6.1）

1.5.3 請問您平均一天使用這些網路新聞平臺的時間約為幾小時？

☐（1）未滿 1 小時
☐（2）1～未滿 3 小時
☐（3）3～未滿 5 小時
☐（4）5 小時以上
☐（5）不一定
☐（6）不知道／拒答

1.5.4 請問您在使用這些網路新聞平臺時，是否曾閱讀過這些平臺的服務及使用者條款或版規？

☐（1）有，曾經閱讀過
☐（2）無，不曾閱讀過（跳題至 1.6.1）
☐（3）不知道有服務及使用者條款（跳題至 1.6.1）
☐（4）拒答（跳題至 1.6.1）

1.5.5 請問您在使用這些網路新聞平臺時，對這些平臺的服務及使用者條款或版規瞭解程度為何？

☐（1）清楚瞭解相關內容
☐（2）大致瞭解內容
☐（3）有仔細閱讀，但對內容不太瞭解
☐（4）有瀏覽過，但沒有仔細閱讀內容
☐（5）拒答

1.6.1 請問您是否為任一拍賣、購物平臺（例如：Yahoo 拍賣、蝦皮購物、露天市集、淘寶）之註冊會員？

☐（1）是
☐（2）否（跳題至 1.7.1）

1.6.2 請問您近一個月內是否有使用這些您註冊為會員的拍賣、購物平臺（例如：Yahoo 拍賣、蝦皮購物、露天市集、淘寶）？

☐（1）有使用
☐（2）沒有使用（跳題至 1.7.1）

1.6.3 請問您平均一天使用這些拍賣、購物平臺的時間約為幾小時？

☐（1）未滿 1 小時
☐（2）1～未滿 3 小時
☐（3）3～未滿 5 小時
☐（4）5 小時以上
☐（5）不一定
☐（6）不知道／拒答

1.6.4 請問您在使用這些拍賣、購物平臺時，是否曾閱讀過這些平臺的服務及使用者條款？

☐（1）有，曾經閱讀過
☐（2）無，不曾閱讀過（跳題至 1.7.1）
☐（3）不知道有服務及使用者條款（跳題至 1.7.1）
☐（4）拒答（跳題至 1.7.1）

1.6.5 請問您在使用這些拍賣、購物平臺時，對這些平臺的服務及使用者條款瞭解程度為何？

☐（1）清楚瞭解相關內容
☐（2）大致瞭解內容
☐（3）有仔細閱讀，但對內容不太瞭解
☐（4）有瀏覽過，但沒有仔細閱讀內容
☐（5）拒答

1.7.1 請問您近一個月內是否有使用傳統電視（例如：有線電視〔第四台〕、MOD、無線電視）？

□（1）有使用
□（2）沒有使用（跳題至 1.8）

1.7.2 請問您平均一天使用傳統電視的時間約為幾小時？

□（1）未滿 1 小時
□（2）1～未滿 3 小時
□（3）3～未滿 5 小時
□（4）5 小時以上
□（5）不一定
□（6）不知道／拒答

1.8 目前網路上的危害大致上可分成五大類，包括：政治不實訊息、兒少網路安全、網路霸凌、網路交易安全、個人權益侵害。多數網路平臺都有將他們針對這五大問題的處理方式納入使用者條款之中，我們希望能瞭解您對這些條款的滿意程度。

1.8.1 針對您有使用的網路平臺，請依照您對其使用者條款各項措施的滿意程度進行回答（單選）：

		非常滿意	有點滿意	有點不滿意	非常不滿意	不知道/無法回答
（1）	針對「政治不實訊息」所訂定的使用者條款。（選擇「非常滿意」跳答（3））					
（2）	我感到不滿意的理由是_____。（開放題，非必填）					
（3）	針對「兒少網路安全」所訂定的刪除機制（例如刪除腥羶色內容）。 （選擇「非常滿意」跳答（5））					
（4）	我感到不滿意的理由是_____。（開放題，非必填）					
（5）	針對「網路交易安全」所訂定的防詐機制（例如通報及先行下架商品）。 （選擇「非常滿意」跳答（7））					
（6）	我感到不滿意的理由是_____。（開放題，非必填）					
（7）	針對「網路霸凌」所訂定的防護機制（例如暫時關閉留言功能）。 （選擇「非常滿意」跳答（9））					
（8）	我感到不滿意的理由是_____。（開放題，非必填）					
（9）	針對「個人權益」所訂定的使用者申訴與審查機制。 （選擇「非常滿意」跳答 2.1.1）					

（10）	我感到不滿意的理由是_____。（開放題，非必填）					

第二部分 網際網路社會問題治理結構探詢

2.1 網際網路作為開放的公共討論空間，雖帶來多元的意見交流，卻也讓各種可能形成社會問題的違法資訊或內容因此廣為流通（例如：犯罪集團可能利用拍賣網站販售改造槍枝、或刊登誘騙民眾的訊息）。為了應對網際網路上因此而生的各種社會問題，目前世界各國已發展出各種不同的處理模式。針對不同處理模式的選擇，請依據您的偏好回答以下問題。

2.1.1 面對網路上的違法資訊或內容，如果由您設計一套移除機制，請問您較傾向以怎樣的強度進行處理？請在光譜中選擇您認為最合適的位置，1 為最寬鬆，10 為最嚴格。

	1	2	3	4	5	6	7	8	9	10	
寬鬆 ←→											嚴格
	□	□	□	□	□	□	□	□	□	□	
以網路平臺業者為主，透過自律方式將違法資訊或內容移除											以行政機關或司法機關（法院）為主，依據法令強制將違法資訊或內容移除

2.1.2 承上題，如果要決定這套移除機制所處理的範圍，請問您較傾向哪種做法？請在光譜中選擇您認為最合適的位置，1 為範圍最有限，10 為範圍最廣泛。

	1	2	3	4	5	6	7	8	9	10	
有限 ←→											廣泛
	□	□	□	□	□	□	□	□	□	□	
僅將處理重點放在詐騙、兒少保護等社會重視的違法類型，且配合不同事件類型，分別建立對應的移除機制											無論觸犯的是刑法、民法或政府各級機關訂定的行政法規，所有的「違法」資訊或內容都必須處理，且應建立一套一體適用的移除機制

2.1.3 承上題，如果由行政機關與司法機關共同管理網路上的違法資訊或內容，請問在這套管理機制中，您較傾向如何分配兩者的權限大小？請在光譜中選擇您認為最合適的位置，1 為行政機關擁有最大權限（無法官保留），10 為司法機關擁有最大權限（絕對法官保留）。

行政機關擁有最大權限	1	2	3	4	5	6	7	8	9	10	司法機關擁有最大權限
	□	□	□	□	□	□	□	□	□	□	

行政機關可自行決定裁罰或移除，法院只提供事後的司法救濟

裁罰或移除必須**先行**經過法院的裁判決定

2.2 請參考下圖（一）進行回答。本研究希望能替網路平臺的社會問題找到合適的治理結構，下圖（一）描述一種可能的治理結構。請觀察該結構中政府、網路平臺與使用者間的關係，並回答問題。

2.2 說明：

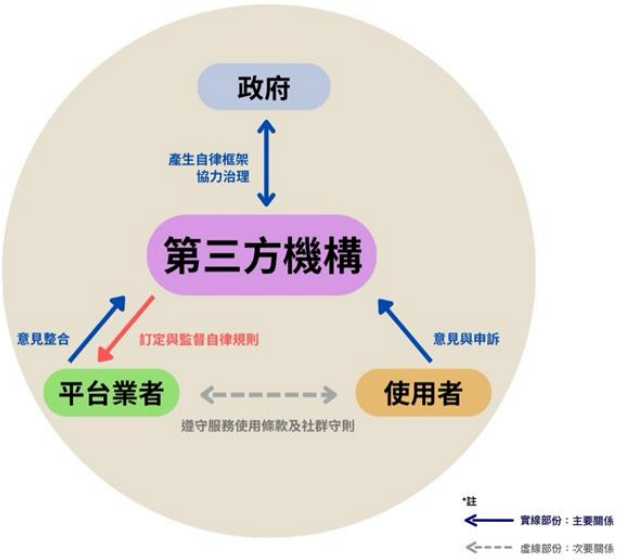
為了建立網際網路社會秩序，本研究基於一般民眾電訪調查及焦點團體座談諮詢學者專家、業者及公民團體所得之前期研究成果，提出以下第三方機構、政府與業者的協力治理模式（圖一）。由政府與第三方機構（**註 1**）協力，整合各方意見，建立各網路平臺共通的自律框架 ，再由各網路平臺依照自律框架，訂定平臺的自律規則，並照章執行，做為平臺與其使用者的自律依據。而倘若使用者發現平臺有違反自律規則，應先向平臺進行申訴；若申訴未果，可向第三方機構投訴，機構受理投訴後若確認平臺違反自律規則，或其自律規則違反共通性自律框架，將通報政府相關業務主管機關進行裁罰。

＊註 1：第三方機構，是指**獨立**的、非政府的第三方的服務機構。一般有三種組成模式：

A.由相關業者組成的商業團體（公會）或協會，如中華民國無店面零售商業同業公會、台北市電腦商業同業公會、台灣網路暨電子商務產業發展協會。

B.由多方團體或個人共同組成，如財團法人中華民國消費者文教基金會（消基會）、台灣事實查核教育基金會（事實查核中心）、台灣展翅協會。

C.由政府捐助成立之財團法人，如財團法人資訊工業策進會（資策會）。



圖（一）

2.2.1.1 請參考圖（一），並請依照您的同意程度回答下列問題（單選）：

		非常同意	有點同意	有點不同意	非常不同意	不知道/無法回答
（1）	在「政治不實訊息」的問題上，我認同應由政府建立各網路平臺共通、整合的自律框架。					
（2）	在「政治不實訊息」的問題上，我認同應由各平臺業者依照自律框架訂定自律規則。					
（3）	在「政治不實訊息」的問題上，我認同平臺業者應該做為維護網路社會秩序的主要執行者。					
（4）	我認同這種治理結構可以處理網路平臺中的「政治不實訊息」問題					
（5）	治理架構中的各個角色都被賦予了最適切的責任（選擇「非常同意」者，跳答 2.2.2.1）					

2.2.1.2 我認為架構中的角色，應該被賦予更多的責任，該角色為（單選）：
（所有選項皆會跳答）

☐（1）政府（跳答 2.2.1.3）
☐（2）網路平臺（跳答 2.2.1.4）
☐（3）第三方機構（跳答 2.2.1.5）

2.2.1.3 我認為政府可做的事情是（單選）：（跳答 2.2.2.1）

☐（1）由單一主管機關判斷是否為政治不實訊息並決定是否阻斷、移除或裁罰。
☐（2）由法院判斷是否為政治不實訊息並決定是否阻斷、移除或裁罰。

2.2.1.4 我認為網路平臺可做的事情是（單選）：（跳答 2.2.2.1）

☐（1）主動判斷並加註警語或降低排序。
☐（2）主動判斷並移除。

2.2.1.5 我認為第三方機構可做的事情是（單選）：（跳答 2.2.2.1）

□（1）要求平臺提供第三方機構認證的透明度報告。
□（2）向傳播政治不實訊息的平臺進行裁罰。

2.2.2.1 請參考圖（一），並請依照您的同意程度回答下列問題（單選）：

		非常同意	有點同意	有點不同意	非常不同意	不知道/無法回答
（1）	在「兒少網路安全」的問題上，我認同應由政府建立各網路平臺共通、整合的自律框架。					
（2）	在「兒少網路安全」的問題上，我認同應由各平臺業者依照自律框架訂定自律規則。					
（3）	在「兒少網路安全」的問題上，我認同平臺業者應該做為維護網路社會秩序的主要執行者。					
（4）	我認同這種治理結構可以處理網路平臺社會的「兒少網路安全問題」。					
（5）	治理架構中的各個角色都被賦予了最適切的責任（選擇「非常同意」者，跳答 2.2.3.1）					

2.2.2.2 我認為架構中的角色，應該被賦予更多的責任，該角色為（單選）：
（所有選項皆會跳答）

☐（1）政府（跳答 2.2.2.3）
☐（2）網路平臺（跳答 2.2.2.4）
☐（3）第三方機構（跳答 2.2.2.5）

2.2.2.3 我認為政府可做的事情是（單選）：（跳答 2.2.3.1）

☐（1）由單一主管機關判斷是否危害兒少網路安全並決定是否阻斷、移除或裁罰。
☐（2）由法院判斷是否危害兒少網路安全並決定是否阻斷、移除或裁罰。

2.2.2.4 我認為網路平臺可做的事情是（單選）：（跳答 2.2.3.1）

☐（1）主動判斷並加註警語或降低排序。
☐（2）主動判斷並移除。

2.2.2.5 我認為第三方機構可做的事情是（單選）：（跳答 2.2.3.1）

□（1）要求平臺提供第三方機構認證的透明度報告。
□（2）向危害兒少網路安全問題的平臺進行裁罰。

2.2.3.1 請參考圖（一），並請依照您的同意程度回答下列問題（單選）：

		非常同意	有點同意	有點不同意	非常不同意	不知道/無法回答
1）	在「網路交易安全」的問題上，我認同應由政府建立各網路平臺共通、整合的自律框架。					
（2）	在「網路交易安全」的問題上，我認同應由各平臺業者依照自律框架訂定自律規則。					
（3）	在「網路交易安全」的問題上，我認同平臺業者應該做為維護網路社會秩序的主要執行者。					
（4）	我認同這種治理結構可以處理網路平臺社會的「網路交易安全」問題。					
（5）	治理架構中的各個角色都被賦予了最適切的責任（選擇「非常同意」者，跳答 2.2.4.1）					

2.2.3.2 我認為架構中的角色，應該被賦予更多的責任，該角色為（單選）：
（所有選項皆會跳答）

☐（1）政府（跳答 2.2.3.3）
☐（2）網路平臺（跳答 2.2.3.4）
☐（3）第三方機構（跳答 2.2.3.5）

2.2.3.3 我認為政府可做的事情是（單選）：（跳答 2.2.4.1）

☐（1）由單一主管機關判斷是否具有網路交易安全的風險，並決定是否阻斷、移除或裁罰
☐（2）由法院判斷是否具有網路交易安全的風險並決定是否阻斷、移除或裁罰。

2.2.3.4 我認為網路平臺可做的事情是（單選）：（跳答 2.2.4.1）

□（1）主動判斷並加註警語或降低排序。
□（2）主動判斷並移除。

2.2.3.5 我認為第三方機構可做的事情是（單選）：（跳答 2.2.4.1）

□（1）針對違規者通報平臺或主管機關。
□（2）向未處理好網路交易安全問題的平臺進行裁罰。

2.2.4.1 請參考圖（一），並請依照您的同意程度回答下列問題（單選）：

		非常同意	有點同意	有點不同意	非常不同意	不知道/無法回答
（1）	在「網路霸凌」的問題上，我認同應由政府建立各網路平臺共通、整合的自律框架。					
（2）	在「網路霸凌」的問題上，我認同應由各平臺業者依照自律框架訂定自律規則。					
（3）	在「網路霸凌」的問題上，我認同平臺業者應該做為維護網路社會秩序的主要執行者。					
（4）	我認同這種治理結構可以處理網路平臺社會的「網路霸凌」問題。					
（5）	治理架構中的各個角色都被賦予了最適切的責任（選擇「非常同意」者，跳答 2.2.5.1）					

2.2.4.2 我認為架構中的角色，應該被賦予更多的責任，該角色為（單選）：
（所有選項皆會跳答）

☐（1）政府（跳答 2.2.4.3）
☐（2）網路平臺（跳答 2.2.4.4）
☐（3）第三方（跳答 2. 2.4.5）

2.2.4.3 我認為政府可做的事情是（單選）：（跳答 2.2.5.1）

☐（1）由單一主管機關判斷是否為網路霸凌問題，並決定是否阻斷、移除或裁罰
☐（2）由法院判斷是否為網路霸凌問題並決定是否阻斷、移除或裁罰。

2.2.4.4 我認為網路平臺可做的事情是（單選）：（跳答 2.2.5.1）

□（1）主動判斷並加註警語或降低排序。
□（2）主動判斷並移除。

2.2.4.5 我認為第三方機構可做的事情是（單選）：（跳答 2.2.5.1）

□（1）向未妥善管理網路霸凌問題的平臺提出警告，並公布名單。
□（2）向未妥善管理網路霸凌問題的平臺進行裁罰。

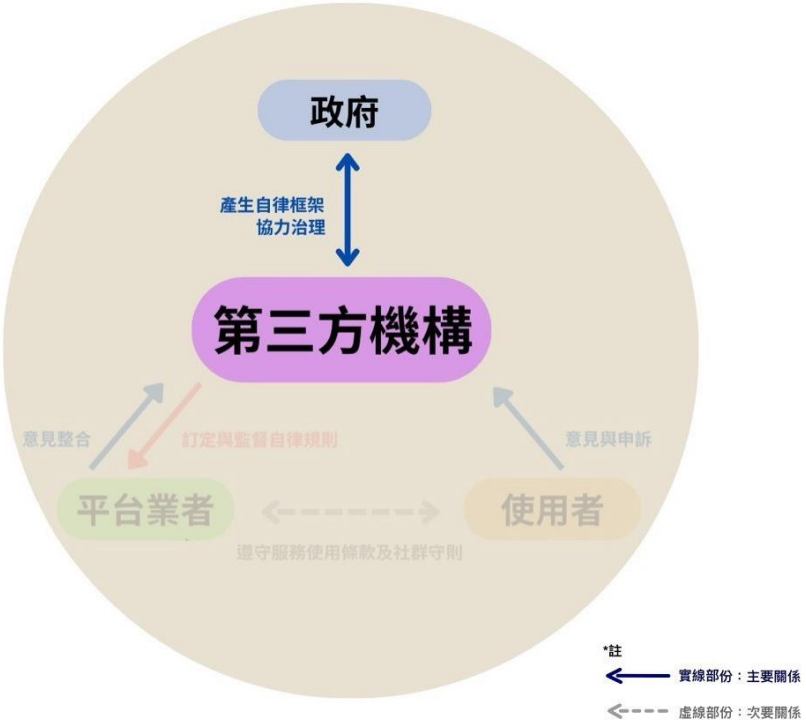
2.2.5.1 請參考圖（一），並請依照您的同意程度回答下列問題（單選）：

		非常同意	有點同意	有點不同意	非常不同意	不知道/無法回答
（1）	在「個人權益保障」的問題上，我認同應由政府建立各網路平臺共通、整合的自律框架。					
（2）	在「個人權益保障」的問題上，我認同應由各平臺業者依照自律框架訂定自律規則。					
（3）	在「個人權益保障」的問題上，我認同平臺業者應該做為維護網路社會秩序的主要執行者。					
（4）	我認同這種治理結構可以處理網路平臺社會的「個人權益保障」問題。					
（5）	治理架構中的各個角色都被賦予了最適切的責任（選擇「非常同意」者，跳答 2.3.1）					

2.2.5.2 您覺得當使用者被限制時（例如：平臺處理違規事情有誤），應以何種方式來進行申訴或維護權利？

□（1）透過平臺所建立之內部異議機制進行申訴。
□（2）向業務主管機關（例如：數位發展部或 NCC，因為是網路環境）申訴，由業務主管機關負責處理相關紛爭。
□（3）由第三方機構，處理相關紛爭。
□（4）透過訴訟，由法院判定使用者權益是否有被限制。

2.3.1 請參考下圖（二）第三方機構與政府之關係，並回答相關問題：



圖（二）

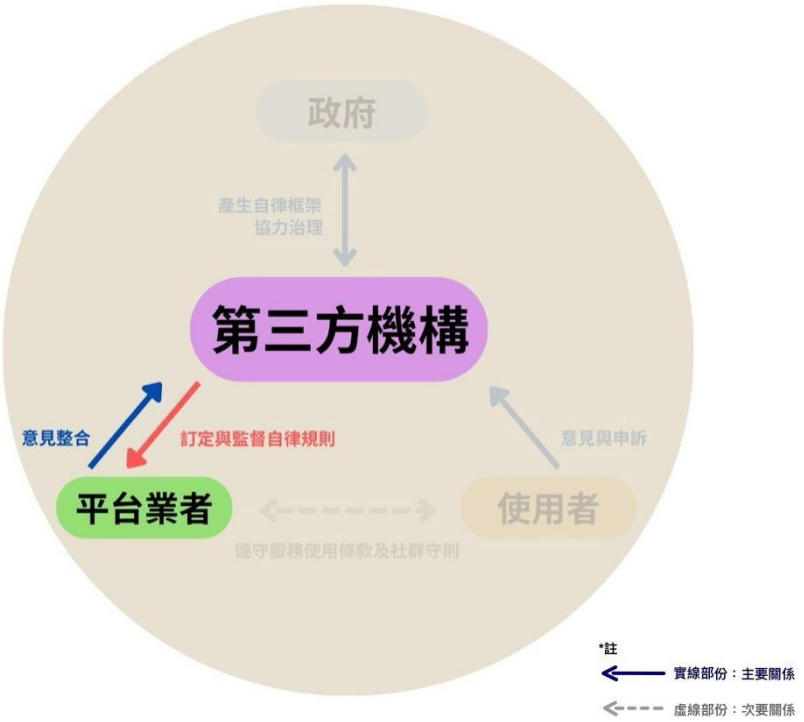
2.3.1.1 承上述，在網路危害的處理中，我較偏好由_____擔任第三方機構。（複選至多選兩項）

□（1）由相關業者組成（註解 A 模式）的第三方機構
□（2）由各方人士組成（註解 B 模式）的第三方機構
□（3）由政府捐助成立的財團法人（註解 C 模式）擔任第三方機構
□（4）其他（請說明）

2.3.1.2 以下問題，請依據您的同意程度回答（單選）

		非常同意	有點同意	有點不同意	非常不同意	不知道/無法回答
1.	我認為第三方機構有能力與政府協力訂定平臺自律框架					
2.	我認為第三方機構有能力判斷平臺是否違反政府訂定的共通性自律框架。					
3.	我認為由第三方機構出面判斷平臺是否違規是公正的。					
4.	我認為第三方機構比政府更適合判斷平臺是否違規。					
5.	承上，理由是：_____（開放題，非必答）					

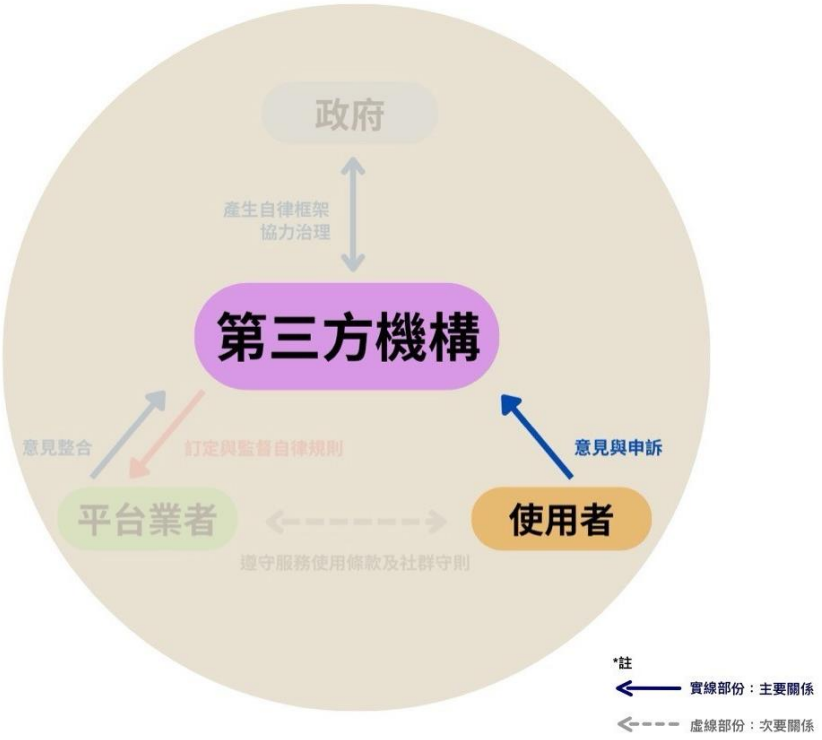
2.3.2 請參考下圖（三）第三方機構與平臺之關係，依據您的同意程度回答下列問題（單選）



圖（三）

		非常同意	有點同意	有點不同意	非常不同意	不知道/無法回答
1.	我認為第三方機構有能力判斷平臺是否違反平臺自訂的自律規則。					
2.	第三方機構能夠協助平臺進行意見整合。					
3.	我認為第三方機構比政府更適合整合網路平臺的意見。					

2.3.3 請參考下圖（四）第三方機構與使用者之關係，依據您的同意程度回答下列問題（單選）：



圖（四）

		非常同意	有點同意	有點不同意	非常不同意	不知道/無法回答
1.	當我向平臺申訴未果時，我願意向第三方機構提出進一步申訴。					
2.	我認為向第三方機構申訴，比向政府機關申訴更能有效解決我在網路平臺遭遇到的問題。					
3.	我認為直接狀告法院，比向第三方機構申訴更能有效解決我在網路平臺遭遇到的問題。					
4.	我認為將我的意見告訴第三方機構，能有效改善整體網路平臺的使用環境。					

第三部分 串流影音服務（3 題）

3.1 請問您近一個月內有使用以下的哪些串流影音服務？
（複選）

- ☐（1）Netflix
- ☐（2）Disney+
- ☐（3）Amazon Prime
- ☐（4）Catchplay+
- ☐（5）HBO GO
- ☐（6）HBO MAX
- ☐（7）Hulu
- ☐（8）Apple TV+
- ☐（9）LINE TV
- ☐（10）愛奇藝
- ☐（11）巴哈姆特動畫瘋
- ☐（12）MyVideo
- ☐（13）Hami Video
- ☐（14）KKTV
- ☐（15）LiTV
- ☐（16）GagaOOLala
- ☐（17）四季線上
- ☐（18）公視+
- ☐（19）楓林網
- ☐（20）小鴨影音
- ☐（21）其他，請說明：_____
- ☐（22）沒有使用（跳題至 4.1）

3.2 請問您一天使用串流影音服務的時間約幾小時？

- ☐（1）未滿 1 小時
- ☐（2）1～未滿 3 小時
- ☐（3）3～未滿 5 小時
- ☐（4）5 小時以上
- ☐（5）不一定
- ☐（6）不知道／拒答

3.3 在使用串流影音服務時，您是否曾經遭遇過消費爭議？
（複選）

☐（1）退訂（例如：介面上找不到退訂功能，須致電客服處理）
☐（2）續訂（例如：無法更換付費方案，或自動續訂時被重複扣款）
☐（3）服務不穩定或無預警中斷
☐（4）信用卡資料外洩
☐（5）無法聯繫上客服
☐（6）其他（請說明）
☐（7）未曾有過消費爭議（跳題至 3.5）

3.4 承上題，在您回答的消費爭議類型中，您認為最需要解決的是？
（單選）

☐（1）退訂（例如：介面上找不到退訂功能，須致電客服處理）
☐（2）續訂（例如：無法更換付費方案，或自動續訂時被重複扣款）
☐（3）服務不穩定或無預警中斷
☐（4）信用卡資料外洩
☐（5）無法聯繫上客服
☐（6）其他（請說明）

3.5 您認為政府面對「串流影音服務的消費爭議」最需要採取的措施為何？
（單選）

☐（1）立法課予服務提供者相關義務（例如：要求業者公告服務使用條款，包含消費者保護措施、服務中斷賠償或隱私政策等）
☐（2）設立單一窗口，作為處理串流影音服務消費爭議的專責機構
☐（3）透過該產業的公協會轉介，以業者自律之方式處理
☐（4）其他（請說明）

第四部分　基本資料

4.1 生理性別

☐ 男性
☐ 女性
☐ 其他（請說明）_____

4.2 年齡

☐ 18-29 歲
☐ 30-39 歲
☐ 40-49 歲
☐ 50-59 歲
☐ 60-69 歲
☐ 70 歲以上
☐ 不知道／拒答

4.3 教育程度

☐ 小學及以下
☐ 國中
☐ 高中職及五專
☐ 大學院校（含二技等）
☐ 碩士及以上
☐ 不知道／拒答

4.4 職業

☐ 政府聘僱人員（含公務人員及約聘人員）或軍人
☐ 民營企業經理主管
☐ 民營企業辦公室人員（專業人員、助理專業人員或事務工作者）
☐ 民營企業服務及銷售工作人員
☐ 民營企業農、林、漁、牧業生產人員
☐ 民營企業勞動工作者
☐ 家管
☐ 學生
☐ 正在找工作

☐ 退休
☐ 無業
☐ 其他
☐ 不知道／拒答

4.5 居住縣市（下拉式選單）

～問卷填答完畢，感謝您的協助～